



Міністерство
фінансів
України

Методологічний бюлетень AML

№41/2026



Зміст

Tether у тіньовій економіці Ірану: нові загрози для міжнародного санкційного режиму та фінансового моніторингу	3
Прозорість бенефіціарної власності у сфері віртуальних активів	6
Єдині стандарти належної перевірки клієнтів: AMLA завершила проєкт PTC за статтею 28(1) AMLR	10
AMLA уніфікує критерії, що визначають момент запуску належної перевірки	14
AMLA визначила мінімальні стандарти для груп, мереж і діяльності в третіх країнах	17
Перегляд регламенту MiCA: практичні пропозиції ESMA щодо реформування крипторинку ЄС	20
SEC пропонує правила зберігання криптоактивів для інвестиційних радників і регульованих фондів	23
Інституційна інфільтрація організованої злочинності: концептуальні основи, міжнародні прецеденти та шляхи реформування правосуддя	26
Екологічна злочинність у ланцюгах постачання: практичні інструменти виявлення та реагування	30
Голова AMLA Бруна Шеґо: від проєктування єдиної антилегалізаційної системи ЄС – до її запуску	34

**Слухайте цей бюлетень
у форматі подкасту**



Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 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.

Tether у тіньовій економіці Ірану: нові загрози для міжнародного санкційного режиму та фінансового моніторингу¹

Звіт Постійного підкомітету з розслідувань Сенату США (PSI) містить результати детального судового блокчейн-аналізу фінансових потоків у мережах криптогаманців, пов'язаних із режимом в Ірані, Корпусом вартових ісламської революції (KBIP) та їхніми регіональними проксі – угрупованнями ХАМАС, «Хезболла» та хуситами (Ансараллах). Емпіричну базу розслідування склала вибірка з 846 унікальних криптовалютних гаманців, включених до санкційних списків або ордерів на арешт активів Управлінням з контролю за іноземними активами Міністерства фінансів США (OFAC) та Національним бюро боротьби з фінансуванням тероризму Ізраїлю (NBCTF) у період із червня 2021 року до серпня 2026 року, доповнена внутрішніми аналітичними інструментами, даними платформ крипторозвідки та витокami конфіденційного листування Центробанку Ірану.



Центральна теза розслідування полягає в тому, що стейблкоїн USDT компанії Tether фактично перетворився на головну нелегальну розрахункову систему для іранського тіньового банкінгу, дозволяючи режиму системно нівелювати ізоляцію від міжнародної системи SWIFT, обслуговувати зовнішньоторговельні операції (передусім контрабанду нафти), фінансувати терористичні організації та здійснювати закупівлі компонентів озброєння. З 846 проаналізованих гаманців 84% проводили операції виключно або майже виключно в USDT (зокрема 87% у списках NBCTF та 57% прямих призначень OFAC, де решта випадків також здебільшого містила транзакції в Tether). Сенат фіксує кардинальний зсув у поведінці незаконних суб'єктів: якщо до 2023 року для збору пожертв і вимагання використовувалися переважно біткоїн та набір різномірних альткоїнів, то починаючи з 2023–2024 років структури на кшталт ХАМАС (зокрема мережа Gaza Now) та фінансові посередники KBIP майже повністю перейшли на публічний фандрейзинг і розрахунки в USDT у мережах Tron та Ethereum через цінову стабільність токена, високу ліквідність і доступність на нерегульованих азійських та близькосхідних біржах.

Історична ретроспектива показує, що з 2018 року іранський уряд цілеспрямовано вибудовував цифровий аналог власної тіньової банківської системи для обходу міжнародних санкцій. Спочатку режим активно заохочував внутрішній майнінг біткоїна за рахунок дешевої субсидованої

¹ <https://www.hsgac.senate.gov/wp-content/uploads/2026-09-28-Crypto-and-Irans-Shadow-Banking-Network.pdf>

електроенергії для подальшого продажу криптовалюти за іноземні фіатні активи, а також розгортав підконтрольні національні біржі (як-от Nobitex). Проте справжній стрибок у масштабах відбувся після масштабної інституціоналізації використання стейблкоїнів поруч із контрабандою золота, готівки та фіктивними підставними компаніями: згідно з аналітичними підрахунками, лише за 2025 рік обсяг операцій з обходу санкцій через криптоактиви зріс на 694%, склавши не менше 2 млрд доларів США в іранському сегменті. У травні 2026 року FinCEN навіть випустив спеціальне офіційне застереження, кваліфікувавши інфраструктуру цифрових активів і великих емітентів стейблкоїнів як ключову опору тіншового банкінгу KBIP.

Окремий блок розслідування розкриває зв'язок криптипотоків із вищим державним керівництвом Ірану. Аналіз витоків внутрішнього листування Центрального банку Ірану (CBI) підтвердив реалізацію спеціальної державної програми «Національний Tether», спрямованої на підтримку курсу національної валюти (ріала) та обробку виручки від підсанкційної нафти. Лише за квітень–травень 2025 року два ідентифіковані гаманці Центробанку прийняли близько 50 млн доларів США в USDT, які одразу перенаправлялися на іранські біржі Nobitex і Ramzinex та автоматизовані міксери, а пов'язана посередницька структура Modex Exchange Company провела через свої адреси майже 600 млн доларів США в еквіваленті USDT, акумулюючи кошти в тому числі від відомих іранських контрабандистів. Масштаби схеми підтверджуються й подальшими арештами: у квітні 2026 року OFAC заблокував ще два гаманці CBI, на балансі яких було заморожено 344,2 млн доларів США у стейблкоїнах Tether.

Аналіз транзакцій виявив розгалужену цифрову мережу «hawala», що зв'язує офіційний Тегеран із регіональними збройними формуваннями. Зокрема, підсанкційні нафтові посередники Аліреза Дерахшан та Араш Естакі Аліванд протягом 2021–2025 років прогнали понад 603 млн доларів США в USDT, спрямовуючи транші фінансовим координаторам «Хезболли», хуситів (мережа Саїда аль-Джамалія) та рахункам KBIP через міжнародні платформи (Bybit, OKX, Gate, Binance, Kyrrex). Лише чотири виявлені транзитні гаманці-хаби за півтора року акумулювали понад 2,7 млрд доларів США за патерном швидкого транзиту. Більше того, розслідування зібрало документальні докази використання цієї інфраструктури для військово-технічного постачання: зокрема, зафіксовано транзакції з гаманців мережі Modex на біржові депозити китайських постачальників мікроелектроніки та навігаційних систем, компоненти яких раніше виявлялися в іранських ударних БПЛА серій «Shahed».

У межах вивчення військових закупівель Сенат виявив прямі листування та пропозиції китайських постачальників компонентів подвійного використання, які відкрито погоджувалися приймати оплату в криптовалюти й надавали для цього конкретні адреси. Зокрема, було відстежено транзакцію на рахунок китайської фірми, що спеціалізується на поставках для безпілотників та пропонує саме той клас напівпровідників вартістю 1–3 долари за одиницю, які регулярно виявляються у збитих безпілотниках Shahed та їхніх російських аналогах Герань. Разом із раніше порушеними справами щодо цивільної конфіскації активів (зокрема заморожуванням майже 600 тис. доларів США в USDT іранського розробника навігаційних систем Мохаммада Абедіні), ці матеріали засвідчують системну роль стейблкоїнів у забезпеченні матеріально-технічної бази для атак на цивільну інфраструктуру в Україні та військові об'єкти США на Близькому Сході.

Ключовий висновок і критична оцінка Підкомітету стосуються відповідальності самої компанії Tether. Попри наявність технічного функціоналу смартконтракту (функція чорного списку, спалювання коштів) та тісний зв'язок з юрисдикцією США (значні обсяги казначейських облігацій, що перебувають на кастодіальному зберіганні у Cantor Fitzgerald), Tether тривалий час дотримувався суто реактивної моделі та вважав виконання вимог OFAC «добровільним». Розслідування виявило системні зволікання: до травня 2023 року компанія взагалі не блокувала гаманці за приписами антитерористичних органів Ізраїлю, а в низці пізніших випадків реагування затримувалося на місяці. У випадку з 39 гаманцями мережі фінансиста «Хезболли» Тауфіка аль-Лава затримка з блокуванням тривала майже рік, що дозволило терористам безперешкодно вивести понад 34,6 млн доларів США через турецькі та глобальні біржі. За адресами, публічно оприлюдненими іранськими контрабандистами в соцмережах або залученими у відкритий краудфандинг бойовиків, Tether нерідко так і не застосував функцію блокування. На цій підставі Підкомітет закликає Конгрес і регулятори ліквідувати юридичний імунітет офшорних емітентів доларових стейблкоїнів та поширити на них суворі норми банківського нагляду й відповідальності за сприяння обходу санкцій.

Висновки

Необхідно поширити юрисдикцію санкційного законодавства та банківського комплаєнсу на офшорних емітентів стейблкоїнів, прив'язаних до фіатного долара, які мають економічний зв'язок зі США через резервні активи в облігаціях казначейства чи американських фінансових посередників.

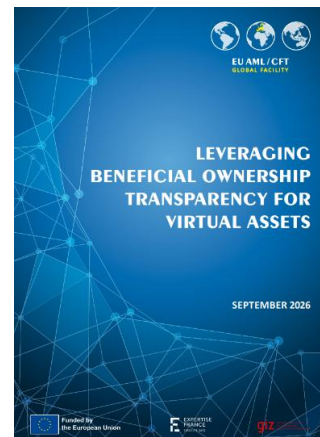
Слід зобов'язати централізованих емітентів стейблкоїнів перейти від несвоєчасного внесення адрес до чорних списків після публікації списків санкцій до проактивного ончейн-моніторингу, адже технічні затримки блокування дають змогу незаконним мережам виводити десятки мільйонів доларів протягом перших годин чи днів.

Доцільно запровадити підвищений нагляд і регуляторні обмеження щодо транзакцій із неліцензованими та офшорними криптовалютними біржами (P2P-майданчиками, пунктами обміну готівки), які функціонують як цифрові аналоги мереж «hawala» і слугують основним каналом обготівкування коштів, пов'язаних з іноземними військовими програмами.

Варто інтегрувати аналіз ланцюгів транзакцій у стейблкоїнах до розслідувань обходу експортного контролю товарів подвійного використання, оскільки цифрові активи дедалі частіше виступають платіжним механізмом для закупівлі мікроелектроніки та компонентів ударних безпілотників.

Прозорість бенефіціарної власності у сфері віртуальних активів ²

Аналітичний звіт Глобального фонду ЄС із протидії відмиванню коштів та фінансуванню тероризму (EU AML/CFT Global Facility) присвячений ролі та практичним механізмам забезпечення прозорості кінцевих бенефіціарних власників (КБВ) у сфері віртуальних активів. Документ систематизує практичні інструменти реалізації Рекомендацій FATF 24 та 25 у взаємозв'язку зі стандартами регулювання постачальників послуг, пов'язаних з обігом віртуальних активів (VASP, Рекомендація 15), належної перевірки клієнтів (CDD, Рекомендації 10 і 22), виконання «правила переказу» (Travel Rule, Рекомендація 16), застосування цільових фінансових санкцій (Рекомендації 6 і 7), виявлення політично значущих осіб (PEPs, Рекомендація 12) та нагляду за кореспондентськими відносинами (Рекомендація 13).



Основна теза звіту полягає в тому, що попри початкову анонімність та децентралізовану технологічну архітектуру віртуальних активів, надійна протидія відмиванню коштів і фінансуванню тероризму залежить від обов'язкової ідентифікації КБВ у точках входу та взаємодії із суб'єктами первинного фінансового моніторингу. Дослідження констатує: якщо транзакції між некастодіальними гаманцями можуть залишатися поза контролем, то конвертація у фіатні валюти чи використання централізованих сервісів неминує потребує залучення VASP. Разом із тим зловмисники масово користуються корпоративними прогалинами: складними багатoshаровими структурами власності, трастами, номінальними керівниками, акціями на пред'явника, регуляторним арбітражем, офшорними незареєстрованими платформами та екзотичними формами на кшталт децентралізованих автономних організацій (DAO). За цих умов класична перевірка формального клієнта є неефективною без встановлення реальних фізичних осіб, які здійснюють контроль або отримують економічну вигоду.

Окремий блок присвячено правовим та організаційним викликам ідентифікації VASP і суб'єктів децентралізованих фінансів (DeFi). Документ наголошує, що ліцензування за Рекомендацією 15 має поширюватися не лише на національні платформи, але й на іноземні VASP, які таргетують внутрішніх користувачів через локалізований інтерфейс, маркетинг чи співпрацю з місцевими банками. Для виявлення неліцензованих операторів органам рекомендовано поєднувати блокчейн-аналітику високоактивних гаманців, вебскрейпінг, аналіз повідомлень про підозрілі операції (STR) та програми для викривачів і «таємних покупців». У сегменті DeFi та DAO, де формальна юридична особа може бути відсутня, контроль і бенефіціарна власність мають встановлюватися не за статутними документами, а через параметри смартконтрактів, розподіл токенів управління, повноваження на зміну коду, розпорядження ключами мультипідпису

² https://www.global-amlcft.eu/wp-content/uploads/2026/09/BO_and_Virtual_Assets-final-digital_compressed.pdf

казначейства (Treasury DAO) чи фактичне отримання прибутку від комісій. У випадках структурування децентралізованих автономних організацій (wrapped DAOs) через товариства з обмеженою відповідальністю (ТОВ) або цільові трасти регуляторам необхідно розмежовувати номінальних учасників і реальних розробників або засновників, які зберігають вирішальний вплив.

Додаткову увагу в дослідженні приділено специфічним індикаторам підозрілості (червоним прапорцям FATF), пов'язаним з анонімізацією користувачів, та системним ризикам використання стейблкоїнів. Автори застерігають, що масова інтеграція стейблкоїнів у розрахунки реального сектору економіки здатна повністю витіснити класичних регульованих посередників, якщо користувачі розраховуватимуться напряму через некастодіальні гаманці без обов'язкової конвертації у фіат. Для мінімізації таких загроз юрисдикціям пропонується розглянути технічні механізми обмеження доступу – інтеграцію «білих списків» або «чорних списків» адрес безпосередньо у смартконтракти емітентів стейблкоїнів, що унеможливило б проведення транзакцій неідентифікованими гаманцями. Водночас аналітики комплаєнсу мають фокусуватися на поведінкових і технічних аномаліях, таких як використання монет підвищеної конфіденційності (Monero), часта зміна IP-адрес через VPN, використання міксерів чи кросчейн-мостів, регулярне досягнення граничних порогів зняття готівки або маніпуляції з відкриттям десятків акаунтів з одного пристрою.

Практичні аспекти проведення належної перевірки клієнтів (CDD) та Travel Rule вимагають від VASP верифікації не лише ініціатора й отримувача платежу, але й проведення повноцінної перевірки контрагентського VASP перед передачею даних, аби виключити контроль з боку підсанкційних осіб чи злочинних угруповань. Особливу загрозу становлять «біржові брокери, які відкривають спільні агреговані рахунки для обслуговування сотень субрахунків без проходження KYC кінцевими користувачами, що вимагає застосування до них жорстких правил кореспондентського банкінгу за Рекомендацією 13. Аналіз підкріплено типовими кейсами: судовими процесами проти біржі Binance, яка свідомо ігнорувала санкційні обмеження, обслуговувала кошти терористичних груп (Hamas, Al-Qaeda, ISIS) та створювала схеми обходу лімітів через «No-KYC» акаунти; легалізацією 120 000 біткоїнів з біржі Bitfinex Іллею Ліхтенштейном через складні транзакційні ланцюги та фіктивні комерційні обґрунтування корпоративних рахунків; а також діяльністю шахрайських крипто-колцентрів, мережу яких було викрито завдяки збігу KYC-фотографій, бейджів та однакових IP-адрес підставних осіб.

Завершальний розділ документа розкриває потенціал міжвідомчої співпраці та використання податкових механізмів як альтернативного джерела розвідданих щодо бенефіціарів віртуальних активів. Впровадження нової системи автоматичного обміну інформацією про криптоактиви OECD CARF (Рамкова система звітності щодо криптоактивів), перші обміни за якою розпочнуться у 2027–2028 роках, передбачає обов'язкову ідентифікацію бенефіціарних власників для «пасивних» корпоративних власників криптоактивів. Документ обґрунтовує можливість законного передання податкової інформації CARF підрозділам фінансової розвідки та правоохоронним органам для цілей фінансового моніторингу на підставі статті 22 Багатосторонньої конвенції про взаємну адміністративну допомогу в податкових справах. Додатково проаналізовано успішний

досвід Бразилії (Інструкція RFB 1888/2019), де обов'язкове декларування операцій резидентами та VASP виявило, що переважна більшість капіталу у віртуальних активах належить юридичним особам, що робить функціонування верифікованих реєстрів бенефіціарів безальтернативною умовою захисту фінансової системи.

На інституційному рівні звіт підсумовує практичні форми технічної підтримки, яку проєкт EU AML/CFT Global Facility готовий надати країнам-партнерам для приведення їхніх систем у відповідність до стандартів FATF. Експертна допомога охоплює комплексний перегляд законодавчої та підзаконної бази щодо прозорості бенефіціарної власності для поширення її на сектор VASP і нетипові структури (як-от цільові трасти чи приватні фонди), налаштування систем верифікації реєстрів КБВ із механізмами повідомлення про розбіжності, оптимізацію процедур ліцензування криптопровайдерів та ризик-орієнтованого нагляду за виконанням обов'язків CDD/KYC. Важливими напрямками також визначено проведення секторальних оцінок ризиків у межах Національних оцінок ризиків та розбудову міжвідомчої взаємодії між підрозділами фінансової розвідки й податковими органами для оперативного обміну даними про власників цифрових активів.

Висновки

Варто адаптувати національні реєстри кінцевих бенефіціарів (FATF P.24/25) до специфіки криптоіндустрії, поширивши обов'язок розкриття структури власності та контролерів на іноземні юридичні особи, що діють як місцеві VASP, а також на трасти та гібридні корпоративні структури.

Необхідно зобов'язати ліцензовані VASP застосовувати правила кореспондентських відносин (FATF P.13) до рахунків обмінних брокерів, які агрегують кошти третіх осіб, вимагаючи повної ідентифікації субліцензіатів і субкористувачів для запобігання використанню агрегованих рахунків як інструментів прихованого відмивання коштів.

Слід запровадити багаторівневий алгоритм оцінки фактичного контролю для DeFi та DAO, визначаючи бенефіціарних власників на основі володіння токенами управління, повноважень щодо зміни смартконтрактів, управління ключами мультипідпису або отримання операційного прибутку.

Доцільно налагодити правовий та оперативний механізм міжвідомчого обміну даними між податковими органами та ПФР на базі стандарту OECD CARF та ст. 22 Багатосторонньої конвенції, що дозволить фінансовій розвідці законно отримувати відомості про бенефіціарів іноземних криптоактивів без ризику попередження підозрюваних клієнтів (tipping-off).

Єдині стандарти належної перевірки клієнтів: AMLA завершила проєкт PTC за статтею 28(1) AMLR

3



30 вересня 2026 року Орган ЄС з протидії відмиванню коштів та фінансуванню тероризму (AMLA) оприлюднив остаточний звіт щодо проєкту регуляторних технічних стандартів (PTC) за статтею 28(1) Регламенту (ЄС) 2024/1624 (AMLR). Документ визначає, яку саме

інформацію підзвітні суб'єкти мають збирати під час стандартної, спрощеної та посиленої належної перевірки клієнтів, які джерела вважаються надійними та незалежними для верифікації, якими атрибутами мають володіти засоби електронної ідентифікації та кваліфіковані довірчі послуги, а також які чинники ризику наглядові органи враховують, вирішуючи, чи може певний електронний грошовий інструмент бути звільнений від заходів належної перевірки (статті 22(6) і 22(7) AMLR). Фактично йдеться про центральний акт другого рівня єдиного антилегалізаційного регламенту ЄС: саме він перетворює загальні обов'язки AMLR на уніфіковану «анкету» клієнта для всіх 27 держав-членів. Проєкт передано Європейській Комісії для ухвалення та подальшого опублікування в Офіційному віснику ЄС.

Документ має тривалу генезу. Його основу підготував Європейський банківський орган (ЕВА) на запит Комісії від 12 березня 2024 року: публічна консультація ЕВА зібрала письмові відгуки 170 респондентів, переважно з фінансового сектору, а у квітні 2025 року до публічних слухань долучилося понад 600 учасників; відповідь ЕВА Комісії датована 30 жовтня 2025 року. AMLA винесла доопрацьований текст на тримісячну консультацію з 9 лютого до 8 травня 2026 року й отримала 325 відповідей, провела 24 березня 2026 року слухання з понад 1 600 учасниками, окремі секторальні зустрічі та консультації з Європейським інспектором із захисту даних. Орган дійшов висновку, що структура й зміст проєкту ЕВА не потребують кардинального перегляду, і обмежився точковими змінами задля правової визначеності, спрощення, застосовності до нефінансового сектору та узгодженості з AMLR. Показово, що AMLA прямо визнала: подальше спрощення заходів спрощеної належної перевірки без фактичного звільнення від обов'язків AMLR неможливе, а таке звільнення виходило б за межі її мандата; тому питання додаткових

³ https://www.amla.europa.eu/document/download/e15ab2e5-4074-4de8-bb9d-613dd8b7fdd1_en?filename=Final%20Report%20-%20draft%20RTS%2028%281%29%20AMLR.pdf

настанов щодо спрощеної перевірки, зокрема для нефінансового сектору, буде предметом подальшого діалогу.

Розділ про ідентифікаційні дані вирізняється високим ступенем деталізації. Для фізичних осіб збираються всі імена та прізвища в тому вигляді, як вони зазначені в документі, що посвідчує особу, або передаються засобами електронної ідентифікації; адреса має містити повну назву країни або її код за ISO 3166, населений пункт із поштовим індексом (і, за потреби, штат), вулицю, номер будинку, квартири та абонентської скриньки. Для керівників юридичних осіб адресу проживання можна замінити адресою зареєстрованого офісу. Місце народження фіксується щонайменше на рівні країни та населеного пункту. Особливої уваги заслуговує норма про громадянство: суб'єкт має вживати розумних заходів, щоб установити, чи не має особа кількох громадянств, фіксувати всі задекларовані громадянства та верифікувати щонайменше одне з них. Для юридичних осіб збираються юридичне та, за наявності відмінностей, комерційне найменування.

Регламентовано й саму верифікацію. Документ, рівнозначний паспорту, має бути виданий уповноваженим органом і містити імена, дату та місце народження, номер і строк дії, фотозображення обличчя, підпис і захисні елементи. Для осіб без громадянства, біженців і осіб під додатковим захистом достатнім вважається виданий уповноваженим органом документ з іменами, датою народження та фотозображенням, а відсутні відомості отримуються з інших надійних і незалежних джерел, якщо немає підстав для підозри. Альтернативна віддалена верифікація допускається лише тоді, коли від особи не можна обґрунтовано очікувати особистої явки й вона не має відповідного засобу електронної ідентифікації, та за низки гарантій: контролю того, що документ пред'являє його власник, цілісності й конфіденційності каналу зв'язку, достатньої якості зображення, відео та звуку, обов'язкового переривання процесу в разі технічних збоїв чи сумнівів, а також збереження копій із позначкою часу для подальшої перевірки. Суб'єкт має обґрунтувати застосування таких заходів і продемонструвати їхню відповідність наглядовому органу. Надійність джерела оцінюється за його репутацією, офіційним статусом і незалежністю, актуальністю, точністю та стійкістю даних до підроблення, причому інформацію слід розуміти незалежно від мови, якою вона викладена.

Низка норм закриває відомі практичні прогалини. Кредитні та фінансові установи мають ідентифікувати й верифікувати особу, яка користується віртуальним IBAN, сам віртуальний IBAN, а також номер, дату відкриття та, за наявності, дату закриття рахунку, до якого він прив'язаний. Для встановлення кінцевих бенефіціарних власників, крім центральних реєстрів, дозволено використовувати інші публічні реєстри (комерційні, реєстри проживання, податкові, паспортні, майнові), надійних постачальників даних, інші кредитні й фінансові установи, суб'єктів групи та засвідчені документи. Щодо проміжних ланок структури власності збираються правова форма, відомості про номінальних директорів чи акціонерів, юрисдикція реєстрації, право, яке регулює траст, частки та права голосу за класами акцій і дані про лістинг, а потреба в додатковій інформації оцінюється з урахуванням кількості рівнів, наявності правових утворень, номіналів і зв'язків із юрисдикціями високого ризику. Для трастів збирається опис класу вигодонабувачів, достатній, щоб визначити, чи стануть конкретні особи встановлюваними на момент виплати або реалізації

набутих прав, а для дискреційних трастів – відомості про об'єкти дискреційних повноважень і осіб, які отримують активи за замовчуванням.

Мету й характер ділових відносин тепер необхідно розуміти через п'ять вимірів: економічне обґрунтування продукту чи послуги, очікувані суми та профіль активності (тип, частота, кількість, розмір і обсяг операцій), джерело коштів, призначення коштів (типи отримувачів, юрисдикція, чи є отримувач вигодонабувачем або посередником) і характер зайнятості або бізнесу клієнта. Обсяг інформації має бути співмірним ризику, з урахуванням даних, які вже наявні, зокрема в межах групи. Щодо політично значущих осіб РТС вимагають визначати статус клієнта, бенефіціарного власника або особи, в інтересах якої здійснюється операція, до встановлення відносин, а щодо наявних клієнтів – з ризик-орієнтованою періодичністю, невідкладно в разі появи нової інформації та після кожного оновлення переліку видатних публічних функцій.

Спрощена й посилена належна перевірка отримали чіткі мінімальні межі. У ситуаціях низького ризику достатньо імен, дати й місця народження, громадянства (або статусу особи без громадянства чи біженця), для юридичних осіб – правової форми, найменування, адреси та, за наявності, реєстраційного номера, податкового номера або LEI; бенефіціарного власника можна ідентифікувати за центральним чи комерційним реєстром, інформацією клієнта або надійним відкритим джерелом, а верифікувати – за іншим джерелом, ніж використане для ідентифікації. Посилена перевірка, навпаки, передбачає відомості про репутацію клієнта й бенефіціарів, їхні близькі зв'язки, ключових контрагентів, а для складних структур без очевидної законної мети – аналіз або експертний висновок щодо їхнього економічного обґрунтування. Наведено й орієнтовний перелік доказів джерела коштів і статків: податкові декларації, довідки про заробітну плату, аудитована звітність, договори кредиту, правовстановлювальні документи на нерухомість, документи про спадщину чи дарування, а також відомості з реєстрів активів і авторитетних медійних чи аналітичних джерел.

Новацією, що безпосередньо стосується санкційного комплаєнсу, є стаття 25 про скринінг на предмет цільових фінансових санкцій. Перевірці підлягають клієнти, бенефіціарні власники та особи, які відповідають критеріям володіння чи контролю, а за підозри в обході санкцій – і представники клієнта. Скринінгу підлягають усі імена фізичних осіб в оригінальному алфавіті та/або латинській транслітерації, юридичні й комерційні найменування, а за наявності в переліках – інші імена, псевдоніми та адреси цифрових гаманців. Перевірка здійснюється під час встановлення відносин, у разі зміни санкційних режимів або нового позначення, у разі зміни даних клієнта (імені, місця проживання, громадянства, бізнесу, бенефіціара), а також регулярно – без невинуватої затримки з моменту оприлюднення санкцій ООН. Окремо визначено дев'ять чинників ризику для звільнення електронних грошових інструментів від заходів належної перевірки (зокрема низькі ліміти, обмежена тривалість і географія використання, геофенсинг, моніторинг продавців і протидія масовим закупівлям), а Додаток I містить вичерпний перелік атрибутів, які мають передавати засоби електронної ідентифікації; у разі їх відсутності бракуючі дані отримуються іншими способами.

Перехідні положення передбачають, що наявні ділові відносини приводяться у відповідність до нових вимог на ризик-орієнтованій основі в строки, встановлені статтею 26(2) AMLR, причому, згідно з преамбулою, одно- та п'ятирічний строки відраховуються від набрання чинності РТС. Сам акт набере чинності на двадцятий день після опублікування та застосовуватиметься через шість місяців, за винятком футбольних агентів і професійних футбольних клубів, для яких датою застосування визначено 10 липня 2029 року. Для підзвітних суб'єктів це означає необхідність уже зараз провести зіставлення чинних анкет KYC, IT-полів і процедур скринінгу з вимогами РТС, адже обсяг змін для більшості суб'єктів визначатиметься не новими принципами, а глибиною деталізації даних.

Висновки

Склад ідентифікаційних даних стає вичерпно стандартизованим: підзвітним суб'єктам і групам, що працюють з ринком ЄС, варто вже зараз зіставити анкети KYC зі статтями 2–5 та Додатком I РТС (повна структура адреси за ISO 3166, усі задекларовані громадянства, місце народження) і закласти відповідні поля в IT-системи до початку застосування акта.

Скринінг на цільові фінансові санкції отримує єдиний мінімальний стандарт: перевірка імен в оригінальному алфавіті та латинській транслітерації, псевдонімів і адрес криптогеманців, а також повторний скринінг при кожній зміні санкційних переліків чи даних клієнта вимагатимуть перегляду налаштувань автоматизованих систем, зокрема для кирилических імен.

Віртуальні IBAN виходять із «сірої зони»: обов'язок ідентифікувати користувача віртуального IBAN, сам vIBAN і рахунок, до якого він прив'язаний, робить фінтех-моделі на основі віртуальних рахунків прозорішими для фінансової розвідки та скорочує можливості для приховування справжнього власника коштів.

Спрощення не означає винятків: AMLA прямо визнала, що не може розширити спрощену належну перевірку без фактичного звільнення від вимог AMLR, тож розраховувати на зменшення обсягу CDD для нефінансового сектору варто лише через майбутні настанови, а не через ці РТС.

AMLA уніфікує критерії, що визначають момент запуску належної перевірки ⁴



Другий проект РТС, оприлюднений AMLA 30 вересня 2026 року, виконує мандат статті 19(9) AMLR і стосується питання, яке сам орган характеризує як «саме серце» антилегалізаційної системи: коли взаємодія з клієнтом є діловими відносинами, коли –

разовою операцією, а коли кілька операцій слід вважати пов'язаними. Від відповіді залежить, чи застосовуються заходи належної перевірки та чи виникає обов'язок постійного моніторингу. Другий елемент мандата – оцінка того, чи потрібні для окремих суб'єктів, секторів або операцій високого ризику нижчі порогові значення, ніж передбачені AMLR. Публічна консультація тривала з 9 лютого до 8 травня 2026 року й зібрала понад двісті відповідей.

Пороговий каркас залишається незмінним. Загальний поріг належної перевірки для разових операцій становить 10 000 євро, а стаття 19 AMLR встановлює нижчі пороги: 1 000 євро для окремих переказів коштів і разових операцій із криптоактивами, 3 000 євро для готівкових операцій і 2 000 євро для ставок і виграшів в азартних іграх. AMLA не знайшла переконливих доказів того, що подальше зниження порогів є необхідним і пропорційним: пропозиції щодо дорогоцінних металів, культурних цінностей і окремих платіжних послуг було відхилено через брак широкої підтримки та доказової бази, а також з огляду на додаткові витрати для суб'єктів і їхніх клієнтів. Оцінка впливу через відсутність кількісних даних від учасників консультації має переважно якісний характер; у всіх трьох питаннях обрано збалансований варіант – горизонтальні критерії з точковими секторальними положеннями – і збережено лише пороги, визначені самим AMLR.

Разова операція визначається від протилежного – як операція або пов'язані з нею послуги, що не здійснюються в межах ділових відносин. Ключовим горизонтальним критерієм тривалості є надання клієнтові постійного доступу до послуг, що підпадають під дію антилегалізаційних вимог; підписка на новини чи суто інформаційний доступ не вважаються таким доступом, а онлайн-реєстрацію за результатами консультації вилучено з переліку ознак. Для суб'єктів, які надають професійні послуги (пункти (a)–(d) і (l) статті 3(3) AMLR), вирішальне значення має те, чи потребує послуга багатьох дій протягом тривалого періоду, а критерій повторюваності оцінюється за наданням послуг через різні проміжки часу або наданням різних послуг; ці критерії не є кумулятивними.

⁴ https://www.aml.europa.eu/document/download/32e5aea0-52dc-4b0c-b93a-b0dd373fcd0f_en?filename=Final%20Report%20-%20draft%20RTS%20under%20Article%2019%289%29%20AMLR.pdf

Найбільш відчутними для ринку є секторальні правила. Для обміну валют, переказу коштів і окремих послуг із криптоактивами ділові відносини виникають, якщо клієнт здійснив три чи більше операції протягом останніх 12 місяців. Для надавачів послуг азартних ігор із фізичними приміщеннями ознакою ділових відносин є участь клієнта в добровільній програмі членства (критерій звужено саме до добровільного членства), а для футбольних агентів і професійних клубів – наявність умовних зобов'язань, пов'язаних із трансфером гравця, тобто відкладених платежів, що залежать від настання певних умов.

Критерії пов'язаних операцій сформульовано як елементи загальної оцінки всіх фактів і обставин. Ідеться про спільне походження або призначення коштів – не лише коли операції здійснює чи отримує та сама особа, а й, за наявною інформацією, коли сторонами є члени сім'ї, ділові партнери, клієнти, що діють узгоджено, дочірні компанії чи бенефіціарні власники того самого материнського утворення, або коли використовується спільна цифрова інфраструктура чи спільні посередники; про спільну мету, зокрема ту саму базову покупку; про інші спільні характеристики, у тому числі операції через різні відділення, агентів чи дистанційні канали, у межах програм лояльності або залежні операції. Часовий критерій визначається як «короткий проміжок», що оцінюється з огляду на характер бізнесу, швидкість і частоту операцій та розмір суб'єкта, тоді як для обміну валют, переказу коштів і окремих криптопослуг встановлено фіксоване вікно в один місяць; для азартних ігор додатковою ознакою є ігри того самого оператора.

Важливим уточненням, унесеним після консультації, є положення про те, що перелік критеріїв не є закритим, а суб'єкти не зобов'язані збирати додаткову інформацію лише для виявлення пов'язаних операцій – вони мають використовувати ту, що вже є в їхньому розпорядженні. Регламент набере чинності на двадцятий день після опублікування та застосовуватиметься через шість місяців, а для футбольних агентів і клубів – з 10 липня 2029 року. Таким чином, контроль за дробленням операцій (структуруванням) з питання національної практики стає уніфікованою вимогою, ефективність виконання якої визначатиметься передусім якістю та зв'язністю внутрішніх даних суб'єкта.

Висновки

Для обміну валют, переказів коштів і низки криптопослуг з'являється чітке кількісне правило: три й більше операції за 12 місяців перетворюють клієнта на учасника ділових відносин із повним обсягом належної перевірки та постійним моніторингом, що на практиці вимагає можливості пов'язувати операції клієнта ще з першої транзакції.

Пов'язані операції оцінюються комплексно, а не за однією формальною ознакою: збіг сторін, спільна мета, спільна цифрова інфраструктура чи посередник, різні канали й агенти мають аналізуватися разом, а для обміну валют, переказів і окремих криптопослуг – у фіксованому місячному вікні.

Нижчих порогів понад передбачені AMLR не буде: AMLA відхилила пропозиції щодо дорогоцінних металів, культурних цінностей і окремих платіжних послуг, тому ризики цих секторів доведеться покривати ризик-орієнтованими заходами, а не порогами.

Якість наявних даних стає ключовим чинником відповідності: суб'єкти не зобов'язані збирати нову інформацію лише для виявлення пов'язаних операцій, але мають використовувати всю наявну, тож розрізненість систем і відсутність єдиного профілю клієнта перетворюються на прямий комплаєнс-ризик.

AMLA визначила мінімальні стандарти для груп, мереж і діяльності в третіх країнах ⁵



Третій документ пакета, оприлюдненого AMLA 30 вересня 2026 року, – проєкт РТС за статтями 16(4) і 17(3) AMLR, які регулюють групові антилегалізаційні вимоги, зокрема в транскордонних групах і в разі діяльності в третіх країнах. Через тісний зв'язок двох

мандатів AMLA підготувала єдиний акт, що охоплює мінімальні групові вимоги та правила обміну інформацією, критерії визначення материнського підприємства в Союзі для суб'єктів зі спільним головним офісом у третій країні без відносин «материнське – дочірнє», умови застосування групових вимог до структур, які не є групами (мережі, партнерства, франшизи), а також мінімальні дії й додаткові заходи на випадок, коли законодавство третьої країни перешкоджає виконанню групових політик. Проєкт розроблено за участю національних наглядових органів, Комісії, ЕВА та приватного сектору й доопрацьовано за результатами консультації з 16 квітня до 15 червня 2026 року; він замінить Делегований регламент (ЄС) 2019/758, який втрачає чинність з 10 липня 2027 року.

Після консультації текст суттєво спрощено: вилючено низку визначень, перелік категорій інформації для обміну перенесено до Додатка I, розділ про перешкоди в третіх країнах скорочено із семи статей до трьох з відмовою від приписових заходів щодо окремих видів правових перешкод, а положення про материнські підприємства та структури – впорядковано. Новим базовим поняттям є «структура» – будь-яка форма організації чи домовленості щонайменше двох зобов'язаних суб'єктів, яка не є групою за AMLR, спрямована на тривалі спільні рамки ділових відносин і характеризується спільним володінням, управлінням, комплаєнс-контролем або їх поєднанням.

Мінімальні групові вимоги покладаються на материнське підприємство в Союзі. Воно має забезпечити задокументовану організаційну модель, у якій груповий менеджер з комплаєнсу наділений повноваженнями ухвалювати рішення; доступ органу управління, внутрішнього контролю та аудиту до необхідної групової інформації; виявлення та мінімізацію конфліктів між антилегалізаційними й комерційними функціями; пропорційну групову оцінку ризиків, що охоплює суб'єктів у третіх країнах, аутсорсинг і покладання на третіх осіб; регулярний задокументований обмін інформацією про ризики, суттєві проблеми та заходи з виправлення; групові політики щодо викривання, повідомлення про інциденти, навчання персоналу, а також

⁵ https://www.aml.europa.eu/document/download/ffcb26fd-0a0e-4f4f-9c3d-9f3ce0a283b5_en?filename=Final%20Report%20-%20draft%20RTS%2016%284%29%20and%2017%283%29%20AMLR.pdf

гарантії того, що суб'єкти групи, які не є зобов'язаними, не перешкоджають виконанню AMLR. Політики затверджує орган управління, процедури й контролі – груповий менеджер з комплаєнсу.

Принципово важливими є норми про обмін інформацією. Материнське підприємство та зобов'язані суб'єкти мають забезпечити передавання відомостей, визначених у Додатку I, будь-якому зобов'язаному суб'єкту групи, коли це доречно, без потреби отримувати погодження материнського підприємства чи іншого суб'єкта; обмін здійснюється за принципом «необхідності знати», захищеними каналами, з дотриманням вимог щодо захисту даних і фундаментальних прав і з веденням записів про обмін, при цьому кожен суб'єкт зберігає власну відповідальність за належну перевірку та рішення щодо ризиків. Обмін із суб'єктами групи поза межами ЄС допускається з урахуванням обмежень права Союзу, держав-членів і відповідної третьої країни; виявлені обмеження мають бути оцінені, а наглядовий орган повідомлений без невиправданої затримки, але не пізніше 28 календарних днів. Ці правила не поширюються на інформацію, визначену статтею 70(2) AMLR.

Для випадків, коли законодавство третьої країни обмежує виконання групових вимог, встановлено послідовний алгоритм: повідомлення наглядового органу протягом 28 календарних днів про країну та характер обмеження; спроба отримати згоду клієнтів і бенефіціарних власників на подолання обмеження, якщо це сумісне з місцевим правом; у разі неможливості – застосування додаткових заходів із переліку з дванадцяти позицій. Серед них – обмеження продуктів і послуг тими, що мають низький ризик, заборона іншим суб'єктам групи покладатися на належну перевірку, проведену філією в третій країні, посилені перевірки, виїзні контролі чи незалежні аудити, погодження відносин підвищеного ризику вищим керівництвом, документування джерела коштів і статків, посилений моніторинг, передавання інформації, що лежить в основі повідомлень про підозрілі операції, материнському підприємству в межах, дозволених місцевим правом, регулярна звітність про метрики ризику, припинення відносин і, як крайній захід, закриття або продаж частини чи всіх операцій. Якщо цього недостатньо, наглядовий орган може вимагати плану мінімізації ризиків, затвердженого органом управління, або коригувальних заходів і застосувати подальші дії відповідно до статті 17(2) AMLR, використовуючи механізми співпраці, зокрема колегії наглядових органів.

Для суб'єктів зі спільним головним офісом у третій країні материнське підприємство в Союзі визначається за двома групами критеріїв. «Достатня значущість» оцінюється за статусом холдингової компанії найвищого рівня консолідації, кількістю транскордонних установ, середньою кількістю клієнтів за два попередні роки (особливо клієнтів високого ризику) та середньою вартістю вхідних і вихідних операцій, а за їх недостатності – за обігом, валютою балансу та чисельністю персоналу. «Достатнє розуміння діяльності» означає здатність визначати стратегію, ухвалювати рішення щодо важливих операцій, координувати управління й контроль або мати суттєві домовленості про аутсорсинг з більшістю суб'єктів у ЄС. Визначене підприємство повідомляє наглядовий орган протягом 28 днів, а той затверджує його протягом 60 днів після отримання повного повідомлення, може обґрунтовано визначити інший суб'єкт, а розбіжності між наглядовими органами можуть бути передані на розгляд AMLA.

Окремий блок стосується мереж, партнерств і франшиз. Групові вимоги застосовуються до структур пропорційно, якщо виконується хоча б одна умова: спільне володіння, спільне управління (зокрема спільний орган управління, однорідна стратегія, розподіл прибутків чи витрат, спільні політики) або спільний комплаєнс-контроль (спільні політики під управлінням внутрішнього контролю, централізовані комплаєнс-операції, спільні аудити, спільний бренд чи франшиза зі спільними аудитами). Голова структури визначається за повноваженнями щодо стратегії, важливих операцій, управління брендом, маркетингом чи франшизою та права виключати учасників, а резервними критеріями є надання ключових технічних послуг, управління комплаєнсом або витратами та, зрештою, показники розміру. У належно обґрунтованих випадках наглядовий орган може дозволити не призначати голову структури за умови спільних систем моніторингу та мінімального набору спільних політик – від оцінки ризиків і належної перевірки до звітування про підозрілі операції, зберігання записів і навчання.

Висновки

Обмін інформацією всередині групи більше не залежить від дозволу материнської компанії: кожен суб'єкт групи має технічно забезпечити передавання даних, визначених Додатком І, за принципом «необхідності знати», зберігаючи власну відповідальність за належну перевірку.

Обмеження законодавства третіх країн отримують чіткий процедурний трек: повідомлення наглядового органу протягом 28 календарних днів, спроба отримати згоду клієнтів, вибір із дванадцяти додаткових заходів і, як крайній захід, вихід з юрисдикції.

Для українських банків у складі банківських груп ЄС це прямий практичний виклик: Україна для них є третьою країною, тож будь-які національні норми про банківську таємницю чи захист даних, що обмежують передавання клієнтської інформації материнській установі, кваліфікуватимуться як перешкода з усіма наслідками за статтями 7–9 РТС.

Мережі та франшизи підпадають під групові вимоги: спільне володіння, управління чи комплаєнс-контроль, зокрема спільний бренд зі спільними аудитами, достатні для того, щоб, наприклад, мережа професійних фірм або франчайзингова мережа мала визначити голову структури та впровадити спільні політики.

Перегляд регламенту MiCA: практичні пропозиції ESMA щодо реформування крипторинку ЄС⁶

Консультаційний документ Європейського органу з цінних паперів та ринків (ESMA) містить узагальнені висновки та законодавчі пропозиції в межах процедури перегляду Регламенту (ЄС) 2023/1114 про ринки криптоактивів (MiCA). Документ ґрунтується на практичному досвіді впровадження регламенту та завершенні 1 липня 2026 року перехідного періоду для постачальників послуг, пов'язаних з обігом криптоактивів (CASP). Звіт адресований Європейській Комісії, національним компетентним органам (NCAs), учасникам фінансового ринку та законодавцям, фокусуючись на усуненні регуляторного арбітражу, посиленні наглядової конвергенції, гармонізації норм MiCA з Директивою MiFID II та майбутнім пакетом інтеграції ринків і нагляду (MISP).



30 September 2023
ESMA/2023/113276571-1721

ESMA Response to the EC
Consultation on the review of
Regulation (EU) 2023/1114 (MiCA)



Головна теза звіту полягає в тому, що стрімка еволюція бізнес-моделей крипторинку потребує точкового розширення сфери застосування MiCA із збереженням принципу технологічної нейтральності та мінімізацією невинного адміністративного навантаження на сумнівних учасників ринку. Хоча чинний регламент заклав фундаментальні стандарти управління та розкриття інформації, між режимами захисту інвесторів у традиційних фінансових інструментах і криптоактивах залишаються системні прогалини. Зокрема, відсутність чітких законодавчих визначень створює небезпеку так званого «децентралізаційного відмивання» у сфері DeFi, викривлених маркетингових практик агресивного залучення роздрібних інвесторів та обігу неліцензованих стейблкоїнів.

Ключовим розділом пропозицій ESMA є уточнення периметра застосування MiCA та надання органу обов'язкових повноважень щодо класифікації цифрових токенів. Наразі розмежування між криптоактивами за MiCA, фінансовими інструментами за MiFID II, утилітарними токенами та NFT викликає розбіжності між національними регуляторами. У зв'язку з цим ESMA пропонує надати регулятору (у співпраці з ЕБА) право видавати обов'язкові до виконання висновки щодо кваліфікації інноваційних і гібридних активів, у тому числі за власною ініціативою регулятора. Окремо підкреслюється потреба законодавчого врегулювання деривативів, розрахунки за якими проводяться у токенах електронних грошей (EMT) чи токенах з прив'язкою до активів (ART), із прямим визнанням таких контрактів фінансовими інструментами під дією MiFID II.

Щодо неавторизованих стейблкоїнів ESMA наполягає на введенні прямої, однозначної заборони: ліцензованим CASP має бути повністю заборонено надавати будь-які передбачені регламентом

⁶

https://www.esma.europa.eu/sites/default/files/2026-09/ESMA75-113276571-1721_Response_to_the_EC_consultation_MiCA_regulation_review.pdf

послуги стосовно ART або EMT, які не відповідають регуляторним вимогам MiCA. Це створить прозорий «бінарний» критерій нагляду та позбавить недобросовісних емітентів можливості отримувати комерційну вигоду через регульовані шлюзи. У сегменті децентралізованих фінансів (DeFi) ESMA пропонує суттєво звузити виняток щодо «повної децентралізації» та запровадити новий регульований вид послуг – діяльність CASP як гейткіпера до DeFi-протоколів. Якщо ліцензований провайдер надає клієнтам технічний інтерфейс, маршрутизує транзакції до смартконтрактів чи виступає посередником, він повинен підлягати чітким обов'язкам щодо розкриття ризиків протоколу, перевірки коду, кібербезпеки та врегулювання конфліктів інтересів.

Окрему увагу в документі зосереджено на регулюванні маркетингових комунікацій, захисті роздрібних споживачів і забезпеченні прозорості витрат. Наглядова практика зафіксувала поширення сумнівних промо-кампаній, де інфлюенсери та треті сторони рекламують ризикові криптоактиви без розкриття конфліктів інтересів, тоді як чинна редакція MiCA не надає наглядовим органам прямих важелів впливу на таких промоутерів. ESMA пропонує встановити чіткі законодавчі зобов'язання для рекламних посередників та обмежити використання агресивних маркетингових прийомів за зразком правил MiFID II, включно з повноваженнями щодо протидії неавторизованим провайдерам із третіх країн, які зловживають правилом зворотної ініціативи. Крім того, вимагається усунути практику оманливих заяв про «нульові комісії», зобов'язавши торговельні платформи розкривати всі приховані елементи витрат, зокрема розмір спредів, що вводять в оману інвесторів.

Документ детально аналізує підходи до регулювання операцій зі стейкінгу, кредитування та позичання. Стейкінг пропонується диференціювати на технічний, пуловий/кастодіальний та ліквідний, поширивши на ліцензованих провайдерів обов'язки розкриття ризиків «слешингу» (втрати активів через помилки валідатора), періодів блокування та правил сегрегації активів на випадок банкрутства CASP. Для криптокредитування й маржинального позичання ESMA вимагає обов'язкової письмової згоди клієнта, ліквідації «чорних скриньок» щодо повторної застави активів та обов'язкового розкриття реальної платоспроможності кінцевих позичальників, що дозволить запобігти каскадним банкрутствам на ринку.

У блоці оптимізації регуляторних процедур ESMA рекомендує централізувати процедуру повідомлення про «білі книги» (Title II white papers) безпосередньо на рівні ESMA, усунувши проміжну ланку національних регуляторів для скорочення бюрократичних витрат. Також пропонується спростити правила надання послуг переказу для інвестиційних фірм, авторизованих за MiFID II, звільнивши їх від необхідності проходження дублюючої процедури окремого ліцензування за статтею 63 MiCA, та гармонізувати пруденційні вимоги до капіталу CASP з режимом IFR/IFD. Додатково обґрунтовуються нові наглядові повноваження: надання національним органам права оперативно блокувати шахрайські вебсайти, закріплення за ESMA повноважень прямого заморожування криптоактивів при підозрах у відмиванні коштів чи маніпулюванні ринком, впровадження постійних заходів втручання в продукти, забезпечення повної прозорості торговельних витрат і прихованих спредів, а також створення концепції опціонального загальноєвропейського правового режиму («28th regime») для безперешкодного функціонування токенизованих ринків капіталу.

У стратегічній перспективі побудови єдиного ринку токенизованих капіталів ESMA наголошує, що масштабування розподілених реєстрів залежить не лише від технологічних рішень, а й від усунення нормативної роздробленості між державами-членами. Без чітких загальноєвропейських норм щодо переходу прав власності, остаточності розрахунків на блокчейні та надійної інтеграції DLT із традиційними біржовими депозитаріями ринок ризикує розпастися на ізольовані національні сегменти. Запропонований додатковий режим («28th regime») покликаний створити єдині правила гри для транскордонного випуску, обігу та клірингу токенизованих цінних паперів, забезпечуючи правову сумісність між новими протоколами та класичною фінансовою інфраструктурою ЄС.

Висновки

Варто наділити ESMA законодавчими повноваженнями видавати обов’язкові до виконання висновки щодо класифікації нових і гібридних криптоактивів (включно з деривативами, розрахунки за якими проводяться у стейблкоїнах), що ліквідує регуляторний арбітраж між нормами MiCA та MiFID II.

Необхідно встановити пряму регуляторну заборону для постачальників послуг криптоактивів (CASP) на здійснення будь-яких операцій чи обслуговування неавторизованих стейблкоїнів (ART та EMT), які не відповідають обов’язковим вимогам регламенту MiCA.

Слід запровадити регулювання діяльності CASP як ліцензованих шлюзів до децентралізованих фінансів (DeFi), встановивши для провайдерів обов’язки належної перевірки смартконтрактів, прозорості відбору протоколів і захисту роздрібних користувачів від технологічних ризиків.

Доцільно надати наглядовим органам повноваження прямого негайного блокування сумнівних криптоактивів у провайдерів послуг у разі підозр щодо відмивання коштів або тероризму, а також право швидкого деактивування шахрайських інтернет-ресурсів для дієвого захисту фінансової системи.

SEC пропонує правила зберігання криптоактивів для інвестиційних радників і регульованих фондів

7



U.S. Securities and Exchange Commission

1 жовтня 2026 року Комісія з цінних паперів і бірж США (SEC) оприлюднила для обговорення пакет правил «Правила зберігання активів радниками та

регульованими фондами; правила зберігання криптоактивів» (Release No. IA-7023; IC-36353; File No. S7-2026-35) обсягом близько 690 сторінок. Пакет передбачає нові правила 17f-8 і 17f-9 за Законом про інвестиційні компанії (зберігання криптоактивів державними трастовими компаніями та самостійне зберігання активів фондів), зміни до правила зберігання за Законом про інвестиційних радників 206(4)-2 з його перенумеруванням на 223-1, а також зміни до вимог щодо ведення записів і форм звітності ADV та N-CEN. Ініціатива продовжує курс, визначений Виконавчим указом 14178 і доповіддю Президентської робочої групи з цифрових активів від 30 липня 2025 року, та напрацювання Робочої групи SEC з криптоактивів, створеної в січні 2025 року; попередня пропозиція щодо захисту активів клієнтів 2023 року була офіційно відкликана 12 червня 2025 року. Строк подання коментарів – 60 днів після опублікування у Федеральному реєстрі.

Обґрунтовуючи пропозицію, SEC констатує, що чинні правила зберігання створювалися для традиційних активів і не враховують специфіки криптоактивів. Кількість традиційних кваліфікованих зберігачів, які підтримують широкий спектр криптоактивів, обмежена, підтримка нових чи нішевих активів запізнюється, що створює ризик концентрації. Регуляторне середовище тривалий час залишалося невизначеним: спільну заяву персоналу 2019 року щодо зберігання брокерами-дилерами відкликано 15 травня 2025 року, роз'яснення Управління контролера грошового обігу щодо банків кілька разів змінювалися, бухгалтерський бюлетень SAB 121 скасовано бюлетенем SAB 122 у січні 2025 року, а питання про те, чи є державні трастові компанії «банками» для цілей правил зберігання, залишалося предметом індивідуального аналізу; лист персоналу SEC від 30 вересня 2025 року про ненаправлення справ до правозастосування не має юридичної сили. Комісія окремо наголошує на специфічних ризиках: незворотності транзакцій, різному рівні безпеки мереж і відмінних від традиційних активів кіберзагрозах. Масштаб питання ілюструють наведені дані: капіталізація криптоактивів у травні 2026 року становила близько 2,7 трлн доларів США проти 800 млрд на початку 2021 року, а за даними Офісу захисника інвесторів SEC криптоактиви мають 9,2 % дорослих американців.

⁷ <https://www.sec.gov/files/rules/proposed/2026/ia-7023.pdf>

Пропозиція вводить низку визначень. Криптоактив – це цифрове представлення вартості, зафіксоване в розподіленому реєстрі, захищеному криптографічними методами, що загалом узгоджується з визначенням «цифрового активу» в Законі GENIUS; криптомережа – блокчейн або подібний розподілений реєстр, у якому криптоактиви генеруються, випускаються та передаються; приватний ключ – криптографічний ключ, що контролює доступ до активу і може бути розділений на частини («шарди»). Ключовим є поняття самостійного зберігання: радник вважається таким, що самостійно зберігає криптоактив клієнта, якщо він володіє будь-якою частиною приватних ключів, необхідних для здійснення транзакції, без залучення дозволеного зберігача.

Самостійне зберігання допускається як крайній захід і за суворих умов. Радник має письмово визначити – первісно й щокварталу, – що дозволеного зберігача для відповідного криптоактиву немає; володіти експертизою щодо кожного активу та документувати її; підтримувати системи захисту від втрати, крадіжки, зловживання та привласнення, які охоплюють управління приватними ключами, спільну авторизацію транзакцій щонайменше двома особами та зберігання активів кожного клієнта на адресах, що містять лише активи цього клієнта, з щорічним переглядом ефективності систем; мінімізувати кіберризики з щорічним переглядом контролів; отримати звіт незалежного аудитора про внутрішній контроль протягом шести місяців від початку зберігання та щороку після цього; щонайменше щокварталу надсилати клієнтам виписки із зазначенням адреси, мережі, залишків і всіх транзакцій із закликом звірити їх із записами в блокчейні. Додатково радник і клієнт мають письмово погодити віднесення кожного криптоактиву до «фінансових активів» за статтею 8 Єдиного торгового кодексу США, що посилює захист клієнта за правом штату.

Для регульованих фондів самостійне зберігання через радника можливе за умови нагляду ради фонду: рада має до початку зберігання та щороку визначати, що активам забезпечуватиметься належна дбайливість, і перевіряти письмове обґрунтування радника щодо відсутності дозволеного зберігача – первісно й щокварталу. Державні трастові компанії можуть виступати зберігачами криптоактивів, якщо радник або фонд, після належного з'ясування, має обґрунтовані підстави вважати, що компанія уповноважена органом банківського нагляду штату надавати такі послуги, має письмові політики захисту криптоактивів і пов'язаних коштів, а також отримує та аналізує її останню аудитовану фінансову звітність і звіт про внутрішній контроль – до залучення та щороку. Активи клієнтів мають бути відокремлені від власних активів трастової компанії.

Пакет також модернізує загальні правила зберігання. Будь-який зареєстрований брокер-дилер зможе виступати зберігачем фонду, якщо зберігання підпадає під правило захисту клієнтів; скасовуються застаріле правило щодо рахунків «вільної готівки» та форма N-17f-1; правила поширюються на компанії з розвитку бізнесу; вимога про реєстрацію аудитора в Раді з нагляду за бухгалтерським обліком публічних компаній (PCAOB) скасовується; уточнюються випадки, коли повноваження на дискреційну торгівлю чи ненавмисне отримання доступу до активів не вважаються зберіганням. Записи дозволено вести безпосередньо в криптомережі, якщо їх можна оперативно надати Комісії в електронному форматі, придатному для читання людиною. Форми ADV і N-CEN доповнюються питаннями про самостійне зберігання, залучення трастових компаній

і токенизовані частки фондів, натомість зміни щодо торгівлі криптоактивами Комісія розглядала, але наразі не пропонує.

З погляду фінансового моніторингу пропозиція, хоча й має передусім пруденційну та захисну природу, формує важливі передумови для прозорості. Вимога зберігати активи кожного клієнта на окремих адресах і щокварталу розкривати клієнтам повний перелік транзакцій створює однозначну атрибуцію адрес конкретним клієнтам, що полегшує блокчейн-аналітику та відстеження коштів. Подвійна авторизація, обов'язкове управління приватними ключами й незалежний аудит внутрішнього контролю знижують ризик внутрішнього привласнення, а визнання записів у криптомережі належною формою регуляторного обліку ставить перед наглядовими органами завдання володіти інструментами їх аналізу.

Висновки

Самостійне зберігання криптоактивів радником допускається лише як крайній захід: щоквартальне письмове підтвердження відсутності дозволеного зберігача, експертиза щодо кожного активу та подвійна авторизація транзакцій формують модель, яку доцільно врахувати при визначенні вимог до кастодіальних постачальників послуг віртуальних активів в Україні.

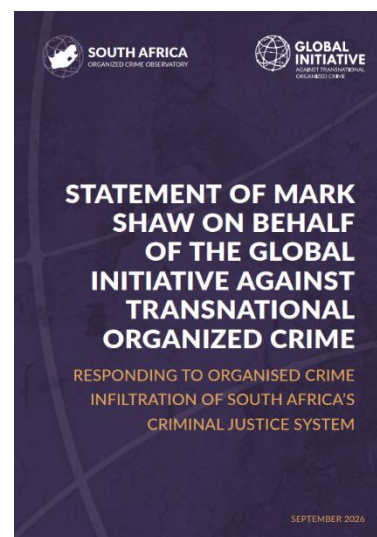
Окрема адреса для активів кожного клієнта та щоквартальна виписка з усіма транзакціями забезпечують однозначну атрибуцію адрес клієнтам, що спрощує блокчейн-аналітику, відстеження коштів і виконання запитів підрозділу фінансової розвідки.

Ключовим об'єктом контролю стає управління приватними ключами: володіння навіть частиною ключа прирівнюється до зберігання, тож політики безпеки ключів, кібербезпеки й внутрішнього контролю мають підтверджуватися незалежним аудитором так само, як фінансова звітність.

Записи дозволено вести безпосередньо в криптомережі за умови їх оперативного надання регулятору в придатному для читання форматі, що створює прецедент визнання блокчейну джерелом регуляторного обліку й вимагатиме від наглядових органів відповідних аналітичних інструментів.

Інституційна інфільтрація організованої злочинності: концептуальні основи, міжнародні прецеденти та шляхи реформування правосуддя⁸

Документ Глобальної ініціативи проти транснаціональної організованої злочинності (GI-TOC) присвячений комплексному аналізу системного проникнення (інфільтрації) організованої злочинності в інститути кримінальної юстиції та обґрунтуванню невідкладних законодавчих та інституційних заходів реагування. Документ спирається на емпіричні дані Глобального індексу організованої злочинності. Згідно з показниками Індексу 2025 року, ПАР посідає 7-ме місце зі 193 країн світу за рівнем криміналізації (а серед конституційних демократій – 5-те місце у світі та 1-ше за межами Латинської Америки), демонструючи критично високий бал укоріненості злочинних акторів у державних інституціях (8,0 з 10) на тлі низької стійкості правоохоронних органів (4,5) та системи захисту свідків (4,0). Звіт розглядає інфільтрацію не просто як кримінологічну проблему, а як пряму екзистенційну загрозу функціонуванню конституційної демократії та верховенству права.



Автор проводить принципову межу між поодинокими актами корупції та інфільтрацією. Якщо класична корупція передбачає отримання разової неправомірної вигоди за конкретне незаконне рішення, то інфільтрація становить тривалі, систематичні та симбіотичні відносини між злочинними групами та посадовими особами, які здійснюють публічну владу. За такого сценарію державні органи починають функціонувати в інтересах синдикатів, надаючи їм довгостроковий захист, службову інформацію, зброю та ресурси. Серед показових прикладів автор наводить справу экс-комісара поліції Джекі Селебі, який за хабарі забезпечував прикриття наркосиндикату, масштабні схеми крадіжки та продажу кримінальним угрупованням понад 9000 одиниць вилученої вогнепальної зброї офіцерами поліції (справа полковника Прінслоо), корупційні зв'язки з вуличними бандами типу «28s», саботаж розслідувань у секторі маршрутних перевезень, де самі високопосадовці поліції володіють нелегальними таксі-парками, а також поширення ринку замовних убивств слідчих, викривачів та свідків (понад 2450 випадків за останні 25 років).

⁸ https://globalinitiative.net/wp-content/uploads/2026/09/Mark_Shaw_GITOC_Madlanga_Statement-final-310826.pdf

Для напрацювання дієвих рішень GI-TOC провела міжнародний діалог експертів із залученням практиків з Італії, Гонконгу, Колумбії, Гватемали, Бразилії, Аргентини, Албанії та Мексики, вивівши сім фундаментальних порівняльних принципів. Перший принцип наголошує, що злочинні синдикати стійкі до норм, які карають лише за індивідуальні діяння; законодавство має криміналізувати саму колективну належність до мафіозних формувань та участь у них (як стаття 416-bis KK Італії чи новий закон Бразилії щодо ультранасильницьких організацій). Другий принцип констатує, що скомпрометована інституція нездатна до внутрішнього самоочищення, навіть маючи формальну незалежність, що зумовлює створення цілком автономних зовнішніх структур – таких як Незалежна комісія проти корупції (ICAC) у Гонконгу або конституційно закріплена Спеціальна антикорупційна структура (SPAK) в Албанії. Третій принцип фіксує переростання окремих посадових зловживань у спільну злочинну практику органу; для ліквідації таких зв'язків необхідні надзвичайні механізми суцільної переатестації всього персоналу (досвід перевірки доброчесності суддів в Албанії, обов'язкове тестування благонадійності в Мексиці) або повна ліквідація та заміна органу (розформування спецслужби DAS у Колумбії).

Четвертий порівняльний принцип розв'язує дилему роботи з оперативними та розвідувальними даними: фрагментація інформації між різними відомствами фрагментує розуміння всієї картини злочинності, але зосередження всіх відомостей в єдиному центрі робить його вразливою ціллю для тотального витoku в разі появи бодай одного підкупленого агента. Успішною моделлю тут виступає італійська архітектура розмежування слідства та обвинувачення (DDA/DNA) зі спільними базами даних SIDDA/SIDNA або колумбійське відокремлення стратегічної цивільної розвідки DNI від кримінального слідства. П'ятий принцип вказує на те, що тиск злочинності робить виконання службового обов'язку та співпрацю зі слідством «приватно ірраціональними» через страх розправи; держава має запровадити дієвий матеріальний та фізичний захист свідків і колабораторів (як в Італії) або забезпечити анонімне колегіальне ухвалення судових рішень судовими колегами без розкриття авторства окремих суддів (досвід Бразилії). Шостий принцип застерігає: антикримінальні структури без прямого конституційного захисту неминуче розпускаються або блокуються політиками, щойно розслідування зачіпають владні інтереси (показовим є примусове не продовження мандата місії CICIG у Гватемалі). Сьомий принцип доводить необхідність незалежного міжвідомчого нагляду над усім сектором кримінальної юстиції загалом за зразком Парламентської антимафіозної комісії Італії.

Спираючись на цей досвід, GI-TOC пропонує поетапну дворівневу програму дій. Перший, короткостроковий етап полягає у терміновому закритті керівних вакансій у правоохоронних органах за прозорими процедурами, затвердженні урядом Національної стратегії боротьби з організованою злочинністю та створенні інклюзивної Ради з питань організованої злочинності за участі експертів і громадськості. Центральним заходом короткострокового блоку має стати невідкладний «кадровий перезапуск» – суцільне позачергове переатестування керівників і співробітників чутливих підрозділів (оперативна робота, речові докази, облік зброї, закупівлі) незалежною комісією, обов'язковий аудит способу життя та декларування активів, включно з майном подружжя й трастів, із можливістю добровільного звільнення. На цьому ж етапі передбачено підписання обов'язкових угод про міжвідомчий обмін інформацією, цільове

фінансування посад цифрових детективів і судових бухгалтерів, регулярну публічну звітність органів та уніфікацію захисту свідків і викривачів.

Другий, довгостроковий етап спрямований на закріплення структурних змін, які не залежатимуть від поточної політичної волі виконавчої влади. Він передбачає створення нової незалежної конституційної інституції – Агентства з протидії організованих злочинності (зі статусом за Главою 9 Конституції ПАР), яке матиме автономні повноваження щодо розслідування інфільтрації публічного сектору та право підтримувати публічне обвинувачення самостійно чи спільно з Генеральною прокуратурою. У кримінальному законодавстві пропонується криміналізувати сам факт інфільтрації та кваліфіковані злочини, вчинені ультранасильницькими бандами, закріпити механізм цивільної конфіскації необґрунтованих активів посадовців без вироку суду із перекладенням тягаря доказування на службовця, а також передбачити за гонконзьким зразком окрему кримінальну відповідальність посадовців за невідповідність рівня життя доходам. На рівні пенітенціарної системи пропонується ввести судову процедуру ізоляції та обмеження комунікацій ув'язнених лідерів синдикатів (аналог режиму 41-bis в Італії), а у сфері врядування – встановити законодавчу заборону на виконання усних політичних наказів керівниками правоохоронних органів шляхом обов'язкового ведення реєстру виключно письмових директив.

Висновки

Неможливість самоочищення скомпрометованих органів: системна інфільтрація є тривалим симбіозом криміналу й посадовців, тому звичайні дисциплінарні заходи не діють – потрібен надзвичайний зовнішній аудит доброчесності персоналу.

Конституційні гарантії для антикримінальних інституцій: спеціалізовані органи боротьби з організованою злочинністю повинні мати пряме закріплення в Конституції (за прикладом албанської SPAK), аби унеможливити їх ліквідацію чи блокування через зміну політичної влади.

Презумпція неправомірності необґрунтованих активів: через складність доведення окремих хабарів держава має запровадити цивільну конфіскацію та кримінальну відповідальність за незаконне збагачення, переклавши тягар доведення походження майна на самого службовця.

Децентралізація слідства при консолідації розвідданих: задля подолання міжвідомчої розрізненості інформація має інтегруватися на рівні спільних аналітичних баз, проте органи досудового розслідування та розвідки повинні зберігати процесуальну автономію, що мінімізує ризик компрометації матеріалів проваджень через інфільтрацію окремого посадовця.

Екологічна злочинність у ланцюгах постачання: практичні інструменти виявлення та реагування⁹

Документ Цільової групи з питань розкриття фінансової інформації, пов'язаної з природою (TNFD) є фундаментальним та деталізованим посібником глобального масштабу, розробленим для практичної інтеграції проблематики екологічних злочинів у загальновизнану аналітичну модель TNFD LEAP (локалізація, оцінювання, аналіз та підготовка). Від самого початку автори встановлюють чіткі регуляторні та процедурні межі застосування документа. Документ не підміняє повноваження правоохоронних, регуляторних чи наглядових органів, не встановлює наявності складу кримінального правопорушення та не є самостійним інструментом встановлення факту незаконності відповідної діяльності. Водночас документ застерігає організації від публічного ототожнення конкретних суб'єктів із вчиненням екологічних злочинів у межах відкритого розкриття інформації, з огляду на вимоги конфіденційності, правові обмеження щодо розкриття чутливої інформації та ризик юридичних наслідків для компанії. Натомість пропонується застосовувати внутрішні процедури оцінювання та управління ризиками, спрямовані на виявлення того, яким чином потенційна або підтверджена незаконна діяльність третіх сторін може впливати на діяльність організації, її ланцюги створення вартості, активи, фінансові результати та інтереси інвесторів. Особливе значення при цьому надається не лише встановленим випадкам екологічних злочинів, а й потенційній експозиції та невизначеності оцінювання, зокрема ситуаціям, коли організація не має достатньої інформації для достовірного встановлення походження продукції, місця її виробництва, законності відповідної діяльності або стану екосистем, від яких залежить її діяльність.



Центральна концептуальна ідея настанови полягає у визнанні екологічної злочинності – протиправних діянь або протиправної бездіяльності, що безпосередньо завдають шкоди природі, – не лише як чинника деградації природних активів, біорізноманіття та екосистем, а й як значного джерела операційних, правових і фінансових ризиків та невизначеності для організацій. Така злочинність може впливати на залежності організацій від природи, характер і масштаби їхнього впливу на природу, а також на здатність достовірно оцінювати пов'язані з природою ризики та можливості. Оскільки злочинна діяльність за своєю природою ретельно маскується через фальсифікацію ліцензій, купівлю підроблених сертифікатів походження сировини, змішування нелегальних партій товару з легальними та корупційні домовленості з місцевою владою, традиційні методи комплаєнсу втрачають свою ефективність. Це призводить до того, що офіційні галузеві бази даних, середньостатистичні показники та стандартні звіти

⁹ https://tnfd.global/wp-content/uploads/2026/09/26-30463-Guidance-on-Environmental-Crime_DIGITAL.pdf?v=1790351964

аудиторів кардинально недооцінюють масштаби негативного впливу на екосистеми та вразливість бізнес-моделей. Ситуація додатково ускладнюється явищем кримінальної конвергенції: екологічні правопорушення більше не є ізольованими випадками браконьєрства чи дрібної вирубки, а виступають прибутковою складовою діяльності транснаціональних злочинних синдикатів, які одночасно залучені до легалізації злочинних доходів (відмивання коштів), податкового та митного шахрайства, ухилення від санкцій, підробки фінансових документів, а в багатьох регіонах – до використання примусової праці, торгівлі людьми та насильницьких захоплень територій. У цьому контексті документ розкриває ключові поняття «сприяння» та «підтримувальної діяльності». Злочинці фізично не здатні реалізувати нелегальну сировину без використання легальної ринкової інфраструктури: морських контейнерних перевізників, лізингових і логістичних операторів, платіжних систем, страхових компаній та банківського сектору, що забезпечує торговельне фінансування та міжнародні розрахунки. Унаслідок цього підприємства транспортного та фінансового секторів займають роль критичних вузлів, маючи стратегічний важіль впливу на перекриття тіньових фінансових потоків, який у разі перевищує їхній безпосередній екологічний відбиток.

Аналітичне поле документа охоплює п'ять пріоритетних категорій екологічних злочинів, визнаних провідними міжнародними інституціями: незаконну вирубку лісів та самовільну зміну цільового призначення земель (зокрема осушення торфовищ і деградацію саван під агрокультури); нелегальний видобуток корисних копалин і мінералів (де окремий акцент зроблено на кустарному видобутку золота із застосуванням ртуті та масштабній діяльності кримінальних «піщаних мафій», що руйнують русла річок); незаконний, непідзвітний та нерегульований рибний промисел, що ведеться із вимкненими системами позиціонування або з перевищенням квот; транскордонну незаконну торгівлю об'єктами дикої природи всупереч вимогам Конвенції CITES; а також злочини у сфері відходів і забруднення, включаючи фіктивну переробку пластику, нелегальний експорт токсичного електронного брухту, незаконні промислові скиди та обіг озоноруйнівних речовин. Водночас документ розглядає глобальні правові тенденції, що змінюють правила гри для бізнесу: закріплення в законодавстві окремих держав «прав природи» та правосуб'єктності річок чи екосистем, кодифікацію злочину «екоциду», а також посилення норм індивідуальної кримінальної відповідальності керівників і топменеджерів компаній за недбалість у контролі за підрядниками.

Практичне застосування цих підходів до оцінювання ризиків забезпечується шляхом їх послідовної інтеграції у чотири фази методології TNFD LEAP. На підготовчому етапі визначення сфери охоплення (Scoping) організації формують робочу гіпотезу та забезпечують міжфункціональну взаємодію між підрозділами, об'єднуючи експертизу фахівців із комплаєнсу, юридичного супроводу, екологічних питань та закупівель. У процесі аналізу вони використовують як результати внутрішніх аудитів, так і відкриті геопросторові дані, типології FATF та аналітичні матеріали міжнародних дослідницьких центрів.

У фазі визначення взаємодії з природою (Locate) організації мають враховувати ризик розриву ланцюгів постачання, зокрема змішування сертифікованої та нелегально отриманої продукції на проміжних етапах – елеваторах, лісопилках, збагачувальних підприємствах або в портах. Такі практики можуть істотно ускладнювати встановлення первинного походження деревини, золота,

сої, пальмової олії чи риби. Документ передбачає необхідність доповнення документальних підтверджень походження продукції незалежною просторовою перевіркою. Зокрема, геолокаційні координати відповідних ділянок доцільно систематично зіставляти з даними супутникового моніторингу знеліснення (GLAD), інформацією про переміщення рибальських суден, межами природоохоронних територій за даними IBAT / WDPA, а також інформацією про кінцевих бенефіціарних власників для виявлення потенційно фіктивних або непрозорих посередників. Виявлені аномалії та розбіжності, зокрема між задекларованими виробничими потужностями підприємств і фактичними обсягами сировини, мають фіксуватися як індикатори підвищеної невизначеності та потенційного екологічного ризику і підлягати подальшій перевірці.

У фазі оцінювання залежностей та впливів (Evaluate) визначається, яким чином злочинні схеми можуть зумовлювати приховані фактори деградації, не відображені в офіційних дозволах, зокрема понаднормовий забір прісної води, браконьєрство з боку найманих працівників у прилеглих лісових територіях або аварійні скиди хімічних речовин, що призводять до виснаження чи знищення природних ресурсів, від яких критично залежить безперервність діяльності самого підприємства. Документ прямо застерігає від використання типових усереднених показників за відсутності безпосередньої верифікації відповідних ділянок та рекомендує здійснювати розрахунки на основі сценарного моделювання із зазначенням допустимого діапазону похибки.

У фазі оцінювання матеріальних ризиків та можливостей (Assess) виявлені чинники класифікуються на фізичні загрози (зсуви ґрунту на нелегальних копальнях, забруднення підземних вод, виснаження рибних запасів) та зростаючі перехідні ризики. Останні посилюються регуляторним тиском, зокрема застосуванням Регламенту ЄС щодо знеліснення (EUDR), Директиви ЄС про захист довкілля через кримінальне право (ECD 2024/1203), американського Lacey Act, а також визнанням екологічних злочинів предикатними до ВК за оновленими стандартами FATF та законодавством ЄС. Для виробничих компаній це створює ризики втрати ринків, арешту вантажів, розірвання контрактів і значних штрафів, а для банків – погіршення фінансового стану клієнтів, знецінення заставного майна та ризик залучення до схем ВК. Водночас інвестиції у цифрову простежуваність і підтвердження законності походження продукції можуть стати конкурентною перевагою, забезпечуючи доступ до регульованих ринків та сталого фінансування.

У заключній фазі підготовки реагування та звітності (Prepare) формується система внутрішнього управління: визначаються відповідальні особи на рівні ради директорів і виконавчого керівництва та встановлюються операційні тригери ескалації для реагування на підозрілі сигнали. Організаціям пропонується структурований алгоритм дій – від первинної верифікації та проведення посиленої перевірки (EDD) до затвердження плану виправних заходів, інформування ПФР, митних органів чи регуляторів та, за потреби, відповідального припинення ділових відносин із дотриманням прав людини. У публічній звітності за стандартами TNFD рекомендовано розкривати інформацію про внутрішні механізми контролю, рівень простежуваності ланцюгів постачання та межі аналітичної невизначеності. При цьому відсутність зафіксованих штрафів не повинна автоматично трактуватися як відсутність екологічної злочинності. Загалом документ

розглядає запобігання екологічним злочинам як складову корпоративної безпеки, фінансової стійкості та правового комплаєнсу.

Висновки

Варто інтегрувати індикатори екологічних злочинів у чинні процедури фінансового моніторингу та поглибленої перевірки клієнтів (EDD), не створюючи паралельних структур комплаєнсу, а також поєднати контроль фінансових потоків із перевіркою законності походження сировини.

Необхідно перейти від формальної перевірки документів до просторової перевірки даних, звіряючи задекларовані постачальниками обсяги та ділянки видобутку із супутниковими знімками і межами заповідних зон (IBAT).

Слід запровадити структурований п'ятирівневий алгоритм ескалації: від додаткової верифікації та складання плану виправних дій до офіційного інформування фінансової розвідки чи правоохоронних органів і відповідального припинення ділових відносин.

У нефінансовій звітності TNFD доцільно розкривати якісні параметри внутрішнього контролю, частку простежуваних ланцюгів та ступінь невизначеності даних, категорично уникаючи публічного звинувачення конкретних суб'єктів у злочинах для недопущення необґрунтованих публічних звинувачень.

Голова AMLA Бруна Шеґо: від проєктування єдиної антилегалізаційної системи ЄС – до її запуску ¹⁰

Видання Money Laundering Bulletin оприлюднило 25 вересня 2026 року ексклюзивне інтерв'ю голови AMLA Бруни Сеґо (Bruna Szego), підготовлене Сарою Льюїс, щодо викликів на шляху до запуску 10 липня 2027 року єдиного антилегалізаційного регламенту ЄС. Описуючи роботу органу формулою «будувати літак у польоті», голова AMLA виокремлює три операційні виклики: масштаб мандатів, що потребує чіткої послідовності (пріоритет погоджено з Комісією для актів, найважливіших для ринку, як-от належна перевірка клієнтів, для наглядової конвергенції та для співпраці підрозділів фінансової розвідки); дані та інфраструктуру, адже аналіз ризиків потребує доступних, гармонізованих і надійних даних із 27 юрисдикцій; і різноманіття антилегалізаційного ландшафту, особливо в нефінансовому секторі. Станом на серпень 2026 року AMLA має працівників з усіх 27 держав-членів; у 2027 році орган переходить від проєктування системи до її експлуатації, а з 2028 року розпочне прямий нагляд.

Голова AMLA відверто визнає, що рівень конвергенції між державами-членами нині низький, найбільше – у нефінансовому секторі, який є більшим, фрагментованішим і новішим для антилегалізаційних обов'язків, з наглядом, розподіленням між значною кількістю органів, а подекуди – з ще не сформованими наглядовими структурами; повна сукупність зобов'язаних суб'єктів стане зрозумілою лише після транспозиції Шостої директиви (6AMLD). Водночас вона не вважає це загрозою ефективності системи: низька стартова точка очікувана, а інструменти її подолання вже створюються – безпосередньо застосовні норми з липня 2027 року, спільні методології та посібник з нагляду, спільна модель оцінки ризиків, гармонізовані формати повідомлень про підозрілі операції та обміну між ПФР, експертні (взаємні) оцінки, а також доступні матеріали й онлайн-інструмент для малого бізнесу. Нагляд за транспозицією залишається компетенцією Комісії, а перебирання AMLA нагляду можливе лише щодо окремих фінансових установ, у виняткових випадках і на запит національного наглядового органу.

Криптосектор названо стратегічним пріоритетом: тут складніше встановити кінцевого бенефіціарного власника й відстежити операції, використання криптоактивів зростає, а європейська рамка є новою. Виклики полягають у неоднаковому застосуванні вимог національними органами під час ліцензування й поточного нагляду, у ринковій трансформації після завершення 1 липня 2026 року перехідного періоду за MiCA (частина компаній залишає ринок ЄС, а перехід їхніх клієнтів до інших провайдерів супроводжується послабленням контролів

¹⁰ <https://www.moneylaunderingbulletin.com/legalandregulatory/governmentandinternationalbodies/aml-towards-european-convergence-on-tackling-financial-crime-162680.htm>

у постачальника, що згортає діяльність, неповнотою історичних даних у нового провайдера та ризиком масової відмови в обслуговуванні) і в аналітичній спроможності, зокрема залежності від невеликої кількості постачальників аналітичних інструментів з-поза меж ЄС. Ці ризики AMLA висвітлила в червневій консультативній записці, а до кінця року планує опублікувати стратегічний звіт щодо криптосектору.

Щодо прямого нагляду, який розпочнеться у 2028 році, голова AMLA повідомила, що методологію оцінювання й відбору установ калібрують на реальних даних і валідують разом із національними наглядовими органами; відбір відбудеться у 2027 році, а результати буде повідомлено на початку 2028 року. Право на участь у відборі мають фінансові установи, що працюють щонайменше в шести державах-членах через установу чи шляхом транскордонного надання послуг, а остаточний перелік визначатиметься за ризиковим профілем на основі звітних даних і єдиної методології, результат якої не може змінити ані AMLA, ані національний наглядовий орган одноосібно. Нагляд здійснюватимуть спільні наглядові групи AMLA та національних органів, а включення до переліку, за словами Бруні Сеґо, не є негативною оцінкою установи, а означає єдиного наглядового органу та єдиний набір очікувань для великої транскордонної групи.

Ваша думка важлива!

Яким чином українським аналітикам фінансової розвідки виявляти замасковані потоки іранського тіньового банкінгу в операціях вітчизняного R2P-сегменту та небанківських платіжних систем, якщо розрахунки розпорошуються через мережі підставних осіб («дропів»)?

Як Україні адаптувати положення профільного законодавства про віртуальні активи та гармонізувати його з європейським регламентом MiCA, щоб запобігти використанню іноземних офшорних VASP для обходу вимог фінансового моніторингу та ідентифікації бенефіціарів?

Яких змін потребуватимуть українські стандарти ідентифікації та верифікації клієнтів, щоб відповідати вимогам РТС AMLA до складу даних і засобів електронної ідентифікації, зокрема під час віддаленої верифікації через «Дію»?

Як українським надавачам платіжних послуг виявляти пов'язані операції через спільну цифрову інфраструктуру – пристрої, IP-адреси, гаманці, – не перетворюючи моніторинг на надмірне збирання персональних даних?

Як Україні адаптувати власну систему фінансового моніторингу до нової Директиви ЄС про захист довкілля через кримінальне право (ECD 2024/1203), зокрема щодо запровадження кримінальної відповідальності юридичних осіб і керівників за неналежний нагляд у ланцюгах постачання?

Контакуйте 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-2026-41

Архів

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.



Міністерство
фінансів
України



AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE