Міністерство
фінансів
України

Методологічний бюлетень AML

№43/2026



Зміст

НОР Швейцарії 2026: вісім секторів високого залишкового ризику й переоцінка системи звітування 3

Фінансування тероризму через Люксембург: дрібні суми й транзитна роль фінансового центру 7

Пріоритети системи протидії економічній злочинності Великої Британії 10

Відмивання коштів у новобудовах: як інвестиції в недобудоване житло обходять фінансовий контроль у Великій Британії 15

Людський вимір антикорупційної політики: як когнітивні упередження та соціальні норми впливають на доброчесність 18

Як фінансується війна: навіщо FATF окрема типологія фінансування конфліктів 21

Трофей війни: як конфлікт у М'янмі перебудував ланцюг постачання золота 24

Тіньові мережі Німеччини: як родинні зв'язки допомагають організованій злочинності 27

Бразильська Амазонія: нові коридори контрабанди та експансія криміналу 30

Агентний штучний інтелект і блокчейн: архітектура безпеки, ризики автономії та стандарти управління 34

Протидія злочинам проти природи: досвід розбудови довіри та підтримки екологічних рухів на місцях 37

Стейблкоїни через рік після GENIUS Act: доларова домінанта та розбіжність регулювання 40

Криптовалюта як паралельна фінансова система України: операція БЕБ і неврегульований ринок 42

Попередження SEC щодо інвестиційного шахрайства в соціальних мережах 45

Конференція ACAMS Assembly Las Vegas 2026 48

Еквадор: чому мілітаризація не рятує 51



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.

НОР Швейцарії 2026: вісім секторів високого залишкового ризику й переоцінка системи звітування [1]

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

14 жовтня 2026 року Міжвідомча координаційна група з питань протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї (CGMF) оприлюднила нову Національну оцінку ризиків відмивання коштів і фінансування тероризму Швейцарії (NRA 26). Документ продовжує цикл, започаткований НОР 2015 року та її оновленням 2021 року, і вперше послідовно застосовує повну модель «загроза – вразливість – притаманний ризик – чинники пом'якшення – залишковий ризик». Оцінка спирається на статистику швейцарського підрозділу фінансової розвідки (MROS), Органу нагляду за фінансовими ринками (FINMA), саморегулівних і наглядових організацій, поліцейську статистику злочинності та статистику вироків, а також на шість експертних панелей за участю кантональних і федеральних органів, фінансового сектору, академічної спільноти й неприбуткових організацій. Ризики фінансування розповсюдження зброї з оцінки свідомо виключено: CGMF посилається на окрему секторальну оцінку 2024 року і констатує відсутність суттєвих змін відтоді.

Методологічно важливим є відхід від моделі НОР 2015 року, яка розмежовувала загрози та вразливості, але не враховувала систематично ефект наявних заходів контролю. Нова модель пов'язує притаманний ризик із чинниками пом'якшення й виводить залишковий ризик окремо для 25 секторів і підсекторів, що дозволяє прозоро показати, наскільки ефективними є нагляд і внутрішній контроль. Показово й визначення вразливості: CGMF прямо зазначає, що вразливістю можуть бути і характеристики, які самі по собі вважаються перевагою, зокрема міжнародна інтегрованість фінансової системи чи цифрові платіжні сервіси.

Структурна загроза відмивання коштів для Швейцарії, за висновком документа, не змінилася за своєю природою і залишається високою. Її визначають чотири категорії предикатних злочинів: організована злочинність, корупція, майнові злочини та податкові злочини, причому межі між ними дедалі більше розмиваються через взаємопроникнення злочинних груп. Окремо підкреслено тенденцію інфільтрації організованої злочинності в легальні економічні структури, яка ускладнює розмежування законних і злочинних доходів, а також ризик використання організованої злочинності державними чи афілійованими з державою акторами для обходу

[1] https://cms.news.admin.ch/fileservice/sdweb-docs-prod-nsbcch-files/files/2026/10/14/309573fb-84f6-4c08-9d58-528935252dda.pdf

санкцій, впливових операцій і закупівлі чутливих товарів. У корупційних справах регулярно виявляються зв'язки з державами, що перебувають у конфлікті, та використання фіктивних компаній, які свідомо переносять до юрисдикцій з обмеженою правовою допомогою.

Статистика MROS фіксує домінування шахрайства як предикатного злочину. У 2020–2025 роках 40 725 повідомлень про підозрілу діяльність, або 61% усіх повідомлень, стосувалися шахрайства; їхня річна кількість зросла більш ніж учетверо (з 3 155 у 2020 році до 13 625 у 2025 році), а до правоохоронних органів передано трохи більше ніж кожне п'яте. Такі повідомлення менш складні: медіанний обсяг операцій становить 2 500 швейцарських франків проти 4 800 франків за всіма категоріями, юридичні особи фігурують у 41% випадків, транскордонні операції – у 57%. Для фінансових установ це означає, що основне навантаження формують масові схеми з транзитом коштів жертв через швейцарські рахунки, зокрема з використанням грошових мулів.

Загальна кількість повідомлень до MROS зросла з 5 334 у 2020 році до 21 087 у 2025 році, що пов'язано із запровадженням системи goAML, законодавчими змінами та наглядовим фокусом FINMA на поведінці суб'єктів у частині звітування. На тлі цього зростання MROS переходить до ризик-орієнтованої селекції: частка переданих матеріалів знижується, а середня кількість повідомлень, консолідованих в одне повідомлення правоохоронцям, зросла з 1,3 у 2021 році до 2,2 у 2025 році. Зміни до Закону про протидію відмиванню коштів від 26 вересня 2025 року запроваджують обов'язковий єдиний стандарт даних для повідомлень і надають fedpol повноваження встановлювати технічні вимоги до якості даних. Водночас CGMF визнає, що ключові елементи швейцарської системи звітування частково походять з 1990-х років і потребують комплексної переоцінки.

Загроза фінансування тероризму оцінена як порівняно обмежена, проте з помітним потенціалом зростання. За 2020–2025 роки MROS отримав 523 повідомлення, пов'язані з фінансуванням тероризму (0,8% усіх), з поступовим зростанням з 66 у 2020 році до 114 у 2025 році; до правоохоронних органів передано майже кожне сьоме. Поліцейська статистика зафіксувала лише сім випадків за статтею про фінансування тероризму, а вироків за нею у 2016–2025 роках не було, що документ пояснює конкуренцією норм і складністю доказування в транснаціональних справах, а не рідкісністю явища. Фінансова підтримка дедалі частіше надається дрібними операціями, які важко відстежити, а поширення віртуальних активів і неформальних систем переказу на кшталт хавали може збільшити цей ризик.

Секторальна частина визначає високий залишковий ризик у восьми сегментах: банки з управління капіталом, «інші банки» (насамперед криптобанки), фінтех-установи за статтею 1b Закону про банки, трасти, оператори грошових переказів, постачальники послуг віртуальних активів, юридичні та фідуціарні професії, а також нерухомість. Криптосектор описано детально: на кінець 2024 року в екосистемі «Крипто-долини» налічувалося 1 749 компаній, на кінець 2025 року під наглядом саморегулівних організацій перебували 228 активних постачальників послуг віртуальних активів, а про діяльність з віртуальними активами прозвітували 40 банків, 5 інвестиційних фірм і 2 фінтех-установи. Прямий обсяг торгівлі віртуальними активами у 2025 році оцінено приблизно в 81 млрд франків, а понад 10% населення мали криптовалюту, хоча для

платежів її використовували лише 0,4% опитаних. Нові заходи щодо радників і реєстр прозорості бенефіціарної власності, що набрали чинності 1 жовтня 2026 року, в оцінці ще не враховані.

Документ завершується вісьмома рекомендаціями CGMF. Вони охоплюють забезпечення федеральних органів розвідки й переслідування достатніми людськими, технічними та фінансовими ресурсами; розширення форматів обміну інформацією, зокрема відкриття публічно-приватного партнерства Swiss FIPPP для ширшого кола суб'єктів; якнайшвидше внесення до парламенту законодавчого пакета проти організованої злочинності (проєкт для консультацій очікується до кінця 2027 року); консолідацію розпорошених даних для оцінок ризиків; моніторинг ефективності нового реєстру прозорості та правил для радників; оцінку дизайну системи звітування; надання FINMA права застосовувати фінансові адміністративні санкції; а також перегляд Закону про контроль дорогоцінних металів, за яким штрафи вже підвищено з 2 000 до 250 000 франків.

Висновки

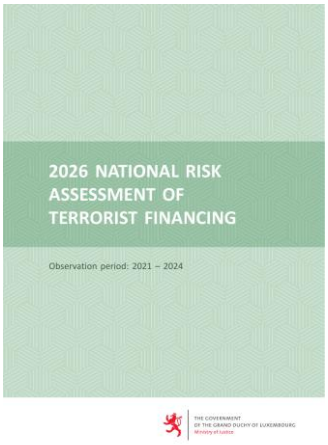
Зростання кількості повідомлень без зміни архітектури звітування стає ризиком саме по собі: учетверо більший потік повідомлень із медіанною сумою 2 500 франків змусив MROS консолідувати матеріали й переглядати систему, створену в 1990-х роках; для українських суб'єктів, які з 2 лютого 2026 року переходять до кейсового звітування, швейцарський досвід підтверджує, що цінність має агрегований кейс, а не кількість окремих повідомлень.

Модель залишкового ризику робить ефективність контролю вимірюваною: розведення притаманного й залишкового ризику для 25 секторів дозволило показати, де нагляд реально знижує ризик (страхування життя, компанії з управління фондами), а де ні (трасти, юридичні професії, нерухомість); такий підхід доцільно закладати в наступні національні та секторальні оцінки, щоб розподіляти наглядові ресурси на основі доказів.

Криптобанки, фінтех-установи та постачальники послуг віртуальних активів визнано зоною високого залишкового ризику: навіть за наявності правила переказу (Travel Rule) й ліцензійного контролю FINMA міжнародна клієнтська база та відсутність надійних даних про обсяги операцій залишають ризик високим, що варто враховувати при проєктуванні українського регулювання ринку віртуальних активів.

Ресурси й дані названо умовою ефективності, а не другорядним питанням: перші дві рекомендації CGMF стосуються кадрів, технологій і консолідації статистики, оскільки, за визнанням самого документа, ключові дані або недоступні, або збираються з надмірними витратами.

Фінансування тероризму через Люксембург: дрібні суми й транзитна роль фінансового центру [2]



Міністерство юстиції Люксембургу 29 вересня 2026 року оприлюднило Національну оцінку ризиків фінансування тероризму (2026 NRA TF), що охоплює період спостереження 2021–2024 років. Документ побудовано за Настановою FATF з оцінки ризиків фінансування тероризму 2019 року і триступеневою схемою «загроза – вразливість – чинники пом'якшення» з виведенням притаманного та залишкового ризику для кожного підсектору. До роботи залучено наглядові органи (CSSF, CAA, AED), саморегулівні організації, міністерства, судові органи, підрозділ фінансової розвідки (CRF) і приватний сектор. Загальний рівень ризику фінансування тероризму оцінено як середній.

Вихідна позиція документа принципова для юрисдикцій із низьким рівнем внутрішньої терористичної загрози. У Люксембурзі не було жодного завершеного теракту, на його території не діє жодна усталена терористична група, а рівень терористичної загрози з 2015 року утримується на другому («середньому») рівні. Проте країна є 19-м фінансовим центром світу і першим у Європі за обсягом інвестиційних фондів, тому, відповідно до настанов FATF для фінансових центрів, ризик фінансування тероризму оцінюється незалежно від внутрішнього терористичного контексту. Сам Люксембург визначено як країну транзиту, а не джерела чи призначення коштів.

Основну загрозу становлять поодинокі виконавці, малі осередки та іноземні бойовики-терористи з невеликими фінансовими потребами, переважно пов'язані з джихадистською ідеологією. Вони користуються базовими продуктами роздрібних банків, платіжних установ, установ електронних грошей і дедалі частіше постачальників послуг віртуальних активів, а кошти здебільшого мають легальне походження: заробітна плата, соціальні виплати, невеликі кредити. Притаманну загрозу від цієї категорії оцінено як середню. Натомість сценарій використання фінансового центру великими міжнародними організаціями на кшталт ІДІЛ чи «Аль-Каїди» визнано теоретичним: аналіз потоків із 56 цільовими юрисдикціями показав, що на них припадає лише 2–3% фінансових потоків країни, а чотири найбільш пов'язані юрисдикції мають економічно обґрунтовані пояснення зв'язків через структурування фондів, управління капіталом, ісламські фінанси та торгівлю.

Структурну вразливість формують два чинники. По-перше, у Люксембурзі розміщено європейські штаб-квартири низки панєвропейських платіжних установ і установ електронних грошей, які працюють за єдиним паспортом ЄС, тож поверхня ризику фактично охоплює весь єдиний ринок. По-друге, висока проникність інтернету та майже повне використання смартфонів молоддю посилюють вплив багатомовних онлайн-кампаній з радикалізації та збору коштів. Не

[2] https://amlcft.public.lu/en/risk-assessments/national/2026nra.html

випадково, за даними CRF, більшість повідомлень про фінансування тероризму надходить від великих установ, що обслуговують клієнтів по всьому ЄС, а у 2024 році лише 7% таких повідомлень стосувалися резидентів Люксембургу.

Кількість повідомлень, пов'язаних із фінансуванням тероризму, залишалася стабільною: 321 у 2021 році, 220 у 2022 році, 223 у 2023 році та 230 у 2024 році; близько 70% повідомлень за 2023–2024 роки стосувалися ісламізму, 10% – ультраправих рухів, 6% – сепаратизму, 2% – лівого тероризму, з піком після нападу ХАМАС 7 жовтня 2023 року. CRF виокремлює п'ять типологій: пожертви іноземним неприбутковим організаціям, підозрюваним у зв'язках з екстремістами, зазвичай до 100 євро, зокрема через онлайн-кампанії; P2P-перекази між непов'язаними особами на нібито гуманітарні потреби (підтримка сиріт, вдів, ув'язнених); купівлю-продаж атрибутики екстремістських ідеологій; операції зі зброєю; зміну споживчої поведінки з переказами та витратами в юрисдикціях підвищеного ризику. Критичним є спостереження, що майже третина повідомлень 2023–2024 років ґрунтувалася на відкритих джерелах і збігах при скринінгу імен, тоді як аналіз зв'язку між діловими відносинами та інформацією про тероризм суб'єкти здійснюють несистемно.

Секторальна оцінка показує, як заходи пом'якшення змінюють профіль ризику. Роздрібні банки, онлайн-установи, платіжні установи, установи електронних грошей і постачальники послуг віртуальних активів мають високий притаманний, але середній залишковий ризик. Ринок віртуальних активів оцінено кількісно: з 15 зареєстрованих постачальників 13 здійснюють перекази криптоактивів (пік – близько 1,3 млн операцій у 2023 році), 10 мають обмінні платформи, через які у 2024 році пройшло близько 30 млн операцій майже на 50 млрд євро, з приростом кількості операцій майже на 90% і вартості майже на 200% за 2022–2024 роки, причому потоки сконцентровано в одній установі, яка водночас є платіжною. Найвищий залишковий ризик зберігається для внутрішніх фідуцій та іноземних трастів, а також для асоціацій без статусу суспільної корисності чи акредитації неурядової організації розвитку, що працюють за кордоном.

Неприбутковий сектор проаналізовано за функціональним визначенням FATF: до релевантної підгрупи входить близько 1 000 асоціацій і фондів, тобто менше 11% зареєстрованих неприбуткових організацій, з яких приблизно 400 працюють переважно за кордоном, зокрема в Камеруні, Сенегалі, ДР Конго та Буркіна-Фасо. Вразливість визначено не на рівні власності, де зв'язки бенефіціарів із цільовими юрисдикціями мінімальні, а на операційному рівні – у точці розподілу коштів у країнах із високою терористичною активністю та слабкою системою протидії фінансуванню тероризму. Основні сценарії зловживання – відволікання законних пожертв, фіктивні благодійні організації, використання благодійного мандату для спрямування коштів пов'язаним із терористами особам і перекази між неприбутковими організаціями.

Окремий розділ присвячено новим ризикам: стейблкоїнам (передусім USDT) і некастодіальним гаманцям; краудфандингу, який до застосування Регламенту ЄС про ПВК/ФТ (AMLR) у липні 2027 року залишається поза наглядом; віртуальним IBAN і миттєвим платежам, що фрагментують фінансовий ланцюг і скорочують час на реагування; документам, підробленим за допомогою штучного інтелекту для дистанційної ідентифікації; ознакам незареєстрованих переказів через

зашифровані месенджери. Документ також звертає увагу, що у 2024 році 30% заарештованих у ЄС за справами про тероризм були віком від 12 до 20 років, і чинні системи протидії фінансуванню тероризму до цього не адаптовані. Пріоритетами наглядової уваги визначено роздрібні банки й онлайн-установи, платіжні установи та установи електронних грошей, постачальників послуг віртуальних активів, неприбуткові організації з міжнародною діяльністю та постачальників послуг трастів і компаній.

Висновки

Ризик фінансування тероризму слід оцінювати незалежно від внутрішнього рівня терористичної загрози: Люксембург без жодного теракту отримав середній загальний рівень ризику через роль хабу панєвропейських платіжних установ і установ електронних грошей; для юрисдикцій із розвиненими платіжними й фінтех-сервісами аналогічний підхід означає оцінку саме транзитного ризику.

Типології дрібних сум потребують поведінкових, а не порогових індикаторів: пожертви до 100 євро, P2P-перекази на «гуманітарні» потреби й купівля атрибутики не виявляються пороговим моніторингом; ефективніші сценарії, що поєднують мережеві зв'язки отримувачів, сигнали із соціальних мереж і зміну транзакційної поведінки.

Повідомлення, засновані лише на збігах скринінгу, мають обмежену аналітичну цінність: майже третина повідомлень спиралася на відкриті джерела без системного аналізу зв'язку з операціями клієнта; методичні рекомендації для суб'єктів моніторингу мають вимагати пояснення, як саме інформація про тероризм пов'язана з конкретними коштами.

Прогалини нагляду до 2027 року потребують проактивних заходів: краудфандингові платформи, віртуальні IBAN, миттєві платежі та стейблкоїни визначено як вектори, що випереджають регуляторні строки AMLR, тому типології й навчання для суб'єктів моніторингу варто оновлювати ще до набрання чинності новими вимогами.

Пріоритети системи протидії економічній злочинності Великої Британії [3]

На тлі зростаючої складності та транснаціонального характеру сучасної злочинності, уряд Великої Британії та ключові правоохоронні й регуляторні органи оприлюднили оновлений перелік системних пріоритетів у сфері боротьби з економічною злочинністю. Цей документ, розроблений Національним агентством з боротьби зі злочинністю (NCA) у тісній співпраці з Управлінням з фінансового регулювання та нагляду (FCA), Податковою та митною службою (HMRC), Міністерством внутрішніх справ та Казначейством, а також за підтримки представників фінансового сектору через UK Finance, являє собою стратегічну дорожню карту для всіх учасників регульованого сектору.

Головна мета — скерувати ресурси приватних компаній туди, де вони можуть мати найбільший вплив на загрозу, зберігаючи при цьому баланс із виконанням їхніх регуляторних обов'язків. Документ наголошує: всі пріоритети є рівнозначними і не мають ієрархічного ранжування, а їхнє впровадження відбувається на засадах державно-приватного партнерства, зокрема через такі структури, як Об'єднаний підрозділ з питань розвідки щодо відмивання грошей (JMLIT).

Першим і, ймовірно, найбільш системним пріоритетом визначено протидію професійним посередникам (Professional Enablers), які своїми послугами сприяють вчиненню економічних злочинів, включаючи шахрайство та ухилення від санкцій. Мова йде про фізичних осіб або організації, чия поведінка є навмисною, необережною, неправомірною, нечесною або недбалою через невиконання своїх професійних та регуляторних зобов'язань. Ці суб'єкти відіграють фундаментальну роль у здатності серйозних організованих злочинців маскувати злочинні активи та відмивати доходи через економіку Великої Британії.

Документ закликає до спільних дій з ідентифікації як злочинних, так і недобросовісних посередників, що діють в країні або впливають на неї, з метою ефективної оперативної та наглядової діяльності. Окремий акцент зроблено на необхідності розуміння того, як найбільш значущі посередники впливають на ситуацію, як їх вербують та які послуги вони надають. Крім того, наголошується на важливості виявлення секторів і послуг, найбільш схильних до ризику, для проведення превентивних заходів та роз'яснювальної роботи. Практичні кроки включають виявлення та картографування професійних посередників, які обслуговують клієнтів з високим ризиком, перевірку клієнтів, які можуть надавати послуги особам, включеним до санкційних списків, та вдосконалення державно-приватних розслідувань мереж фіктивних компаній для поглиблення розуміння схем ухилення від санкцій, зокрема тих, що пов'язані з росією, Іраном та КНДР.

[3] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/832-nca-system-prioritisation-priorities-2026/file

Другий пріоритет стосується політично значущих осіб (PEPs) та транзакційних потоків і корпоративних структур, пов'язаних із зловживанням владою. Визначення цієї категорії охоплює осіб як у Великій Британії, так і за її межами, які обіймають або обіймали важливі державні посади, включаючи глав держав та урядів, високопосадовців, суддів, військових, керівників державних корпорацій та лідерів політичних партій. Важливо, що до категорії ризику віднесено не лише самих PEPs, але й професійних та непрофесійних посередників зловживання владою, зокрема членів родини, подружжя, колишніх партнерів та близьких осіб. У документі наголошується, що представники юридичного, приватного банківського, бухгалтерського секторів, сфери управління активами, постачальників корпоративних послуг займають унікальне місце для посилення колективного розуміння загроз і ризиків, пов'язаних з PEPs та іншими корумпованими елітами.

Серед рекомендованих дій — активне направлення до NCA випадків закордонного хабарництва за участю PEPs, навіть якщо це виходить за межі обов'язкового звітування, а також врахування факторів ризику, пов'язаних з британськими посередниками хабарництва та корупції, у процесах встановлення ділових відносин та належної перевірки.

Третій пріоритет — цифрові активи — зосереджений на захисті громадськості шляхом створення екосистеми цифрових активів, дедалі більш стійкої до злочинного використання. Незаконні суб'єкти прагнуть використовувати цифрові активи та супутні технології для переміщення доходів від шахрайства, програм-вимагачів, ухилення від санкцій та податкових злочинів між юрисдикціями. Цифрові валюти, як зазначається, пропонують можливості для анонімізації та приховування, що дозволяє злочинцям інтегрувати такі кошти у глобальну фінансову систему.

Документ наголошує на необхідності спільної роботи з правоохоронними органами для виявлення та впровадження обізнаності про фактори ризику незаконної цифрової діяльності, обміну наборами даних для створення повнішої розвідувальної картини. Окремо виділяється важливість виявлення доходів від злочинів та потенційних коштів жертв, пов'язаних з незаконною цифровою діяльністю, збору та обміну індикаторами підозрілої діяльності, такої як шахрайські первинні розміщення монет (ICO) або раптове виведення шахраями коштів інвесторів із криптопроєкту (rug pull). Крім того, передбачається розробка комунікаційних кампаній для підвищення обізнаності про ризики шахрайства та відмивання грошей, пов'язані з цифровими активами, а також встановлення критичних процесів для заморожування та арешту підозрілих коштів на платформах постачальників послуг віртуальних активів (VASP).

Четвертий пріоритет — готівкові кошти злочинного походження — охоплює консолідацію, транскордонне переміщення та депонування злочинної готівки в банківську систему Великої Британії, включаючи відділення Пошти. За оцінками, понад 12 мільярдів фунтів стерлінгів щорічно генерується злочинними підприємствами в країні, більша частина яких, як вважається, походить від незаконного обігу наркотиків та акцизного шахрайства. Організовані злочинні групи (OCGs) продовжують використовувати низку бізнесів, включаючи ті, що розташовані на головних вулицях британських міст, а також відділення Пошти для відмивання доходів.

Запропоновані дії включають розвиток наскрізного розуміння того, як злочинці відмивають готівку, хто є задіяними сторонами, як діють банди та де є найбільші можливості для втручання. Окремо згадується використання Публічно-приватної групи з питань податкових злочинів та ухилення від сплати податків для посилення співпраці та обміну розвідданими, зокрема щодо незаконної готівки, отриманої від акцизного шахрайства з алкоголем, тютюном та електронними сигаретами.

П'ятий пріоритет — міжнародне відмивання грошей — стосується відмивання коштів у Великій Британії або через британські корпоративні структури на користь OCG, пов'язаних з пріоритетними юрисдикціями, включаючи діяльність міжнародних контролерських мереж та підпільний банкінг. Економіка, інституції та система корпоративної реєстрації країни підриваються міжнародними організованими злочинними групами, які відмивають свої незаконні фінанси.

Зазначається, що російськомовні OCG несуть відповідальність за багато гучних кібератак проти Великої Британії, відмиваючи свої доходи через різноманітні механізми. Міжнародні злочинні групи використовують міжнародні фінансові центри, такі як ОАЕ, для надання послуг з відмивання грошей через глобальні неформальні системи переказу вартості (IVTS). Китайський підпільний банкінг (CUB) є формою IVTS, поширеною в китайській діаспорі у Великій Британії та інших країнах. Масштаби злочинності, пов'язаної із Західними Балканами, а також супутнє контрабандне переміщення готівки, податкові злочини та відмивання грошей є значними.

Пропоновані дії включають розробку міжнародної рамкової програми даних про потоки коштів, вивчення можливостей для протидії використанню британської фінансової системи закордонними злочинними угрупованнями, розширення обміну розвідданими між приватним сектором щодо виявлених міжнародних загроз відмивання грошей та підтримку ідентифікації міжнародних мереж, що діють у Великій Британії або проти її громадян.

Шостий пріоритет — міжнародне шахрайство — визначається як шахрайство, вчинене міжнародними злочинцями проти жертв у Великій Британії, включаючи OCG, пов'язані зі злочинністю в пріоритетних юрисдикціях, з особливим фокусом на шахрайські "фабрики" (scam compounds). За оцінками, понад 70% шахрайств проти британських громадян або бізнесів походить або опосередковується закордонними юрисдикціями. До юрисдикцій, що становлять найбільш значний рівень загрози, віднесено Гану, Нігерію, Індію та Південно-Східну Азію (з акцентом на Камбоджу, Лаос та М'янму), особливо щодо шахрайств з високим рівнем шкоди, таких як інвестиційне шахрайство, романтичне шахрайство та шахрайство з переадресацією платежів.

Запропоновані дії включають розробку рамкової програми для ідентифікації та обміну тенденціями щодо нових юрисдикцій ризику, вивчення можливостей обміну дієвими даними та сигналами про підозрілу активність зловмисників з метою проєктування захисту від загрози, а також визначення того, які системи, законодавство, шляхи вербування та географічні гарячі точки використовуються мережами, пов'язаними з юрисдикціями ризику.

Сьомий пріоритет — організатори мереж грошових мулів (Money Mule Herders) — стосується експлуатації грошових мулів організаторами, які керують мережами для приховування походження, руху та обготівковування доходів від злочинів, часто шахрайства. Банківські рахунки, що використовуються злочинцями — як без відома власника, так і з його відома з різним ступенем вини — слугують для зберігання та переказу незаконних коштів на інші рахунки, часто дуже швидко. У 2022 році банки виявили понад 39 000 рахунків, що вказують на активність мулів. Мережі грошових мулів відіграють значну і зростаючу роль у сприянні шахрайству, податковим злочинам та фінансуванню тероризму.

Рекомендовані дії включають співпрацю для розуміння методів вербування, покращення комунікаційних та просвітницьких ініціатив для клієнтів і громадськості, розробку узгодженої галузевої методології та моделі обміну даними, зосередженої на мулах та їх організаторах, а також підтримку розвитку готовності системи до реагування на зростаючу кількість звернень щодо підозрілих рахунків мулів.

Восьмий пріоритет — посередники шахрайства (Fraud Enablers) — спрямований на подолання значної кількості шахрайств у Великій Британії, які проводяться телекомунікаційними послугами або онлайн-платформами, включаючи соціальні мережі. Мова йде про інвестиційне шахрайство, романтичне шахрайство та шахрайство з переадресацією платежів, а також про шахрайство, що здійснюється через так званих "інфлюенсерів", які просувають фінансові продукти чи поради. Телекомунікаційні та технологічні компанії надають інфраструктуру та послуги, які дедалі частіше стають мішенню та використовуються злочинцями. Кошти, отримані від шахрайства, використовуються як для особистого збагачення, так і для сприяння подальшій злочинній діяльності, включаючи фінансування тероризму.

Документ закликає ці компанії до співпраці у запобіганні шахрайству, зокрема шляхом виконання зобов'язань за Телекомунікаційною хартією та хартіями щодо онлайн-шахрайства, посилення обміну розвідданими та координації дій з руйнування між правоохоронними органами, банками, телеком-провайдерами, технологічними компаніями та регуляторами.

Дев'ятий, останній у переліку, але не менш важливий пріоритет — фінансування тероризму. У Великій Британії фінансування тероризму зазвичай здійснюється для власних потреб особи, наприклад, для оплати подорожей або проживання, і використовує такі методи, як цифрові активи, послуги грошових переказів, установи електронних грошей, грошові мули та краудфандингові платформи, щоб приховати законні або незаконні фінансові потоки.

Фінансування тероризму відіграє фундаментальну роль у підтримці терористичних організацій, поширенні їхніх ідеологій, вербуванні нових членів та сприянні атакам. Документ наголошує на необхідності продовжувати виявляти поширені та нові загрози й уразливості, покращувати колективне розуміння того, що становить поведінку з фінансування тероризму, через підтримку розширеної звітності про підозрілу активність, пов'язану з тероризмом (TACT SAR). Рекомендується виявляти спільні риси фінансування тероризму в регульованих секторах через надання актуальних тематичних досліджень, розвивати співпрацю з правоохоронними органами

для виявлення індикаторів терористичної діяльності та ділитися ними з фінансовими установами через захищені державно-приватні інформаційні платформи, а також виявляти законодавчі та регуляторні прогалини, які дозволяють фінансування тероризму, та спільно розробляти пропозиції щодо їх усунення.

Підсумовуючи, документ демонструє зрілий та комплексний підхід Великої Британії до протидії економічній злочинності, який базується на тісному державно-приватному партнерстві. Такий підхід дозволяє регульованому сектору, від банків і юридичних фірм до телеком-компаній та постачальників послуг цифрових активів, ефективно розподіляти свої ресурси та зусилля, спрямовуючи їх на найбільш актуальні загрози.

Ключовим лейтмотивом документа є визнання того, що боротьба з економічною злочинністю є спільною відповідальністю, і лише через скоординовані дії, обмін розвідданими та взаємну підтримку між державою та бізнесом можна досягти стійкого прогресу у захисті економіки та суспільства від злочинного впливу.

Висновки

Рівнозначність і партнерство замість ієрархії. Усі дев'ять пріоритетів (від професійних посередників і PEPs до цифрових активів, готівки, міжнародного відмивання та фінансування тероризму) визнаються рівними і не ранжуються, а їх реалізація покладається на державно-приватне партнерство — передусім через структури типу JMLIT та за підтримки UK Finance.

Фокус на "посередниках", а не лише на злочинцях. Ключова новація — зміщення уваги на тих, хто уможливлює злочинність: професійних посередників (юристи, бухгалтери, провайдери корпоративних послуг), посередників шахрайства (телеком та онлайн-платформи) і навіть непрофесійних посередників (родина, оточення).

Транснаціональний вимір як домінанта. Понад 70% шахрайств проти британців походить з-за кордону (Гана, Нігерія, Індія, Південно-Східна Азія), а міжнародне відмивання пов'язується з російськомовними групами, китайським підпільним банкінгом та західнобалканськими мережами — що робить міжнародну співпрацю критичною.

Відмивання коштів у новобудовах: як інвестиції в недобудоване житло обходять фінансовий контроль у Великій Британії [4]



Звіт Transparency International UK (TI-UK) присвячений комплексному дослідженню вразливостей британського ринку первинної нерухомості перед масштабною легалізацією сумнівних капіталів іноземного походження. Дослідження спирається на офіційні оцінки Національного агентства боротьби зі злочинністю (NCA), згідно з якими через сектор нерухомості Великої Британії щорічно може відмиватися до 10 мільярдів фунтів стерлінгів. Власний емпіричний масив даних організації, що наповнюється з 2016 року на основі матеріалів судових процесів, витоків і журналістських розслідувань, налічує понад 2000 об’єктів нерухомості сукупною вартістю понад 12 млрд фунтів, придбаних за підозрілі статки. Систематичний аналіз цієї бази показав, що понад третину всіх сумнівних угод (708 об’єктів на 2,2 млрд фунтів) становлять саме новобудови (630 квартир на 1,6 млрд фунтів) або цілі девелоперські проєкти (78 ділянок на 647 млн фунтів), які розосереджені у понад 150 локаціях Англії та Шотландії (включно з Лондоном, Бірмінгемом, Лідсом і Ліверпулем) та охоплюють діяльність більш як 85 забудовників.

Основна теза доповіді стверджує, що придбання нерухомості на етапі проєктування та зведення є привілейованим інструментом для корупціонерів і транснаціональних злочинних синдикатів завдяки специфічним комерційним механізмам. Насамперед первинний ринок дозволяє здійснювати гуртові придбання цілими поверхами чи пулами квартир, що привертає значно менше підозр фінмоніторингу, ніж купівля однієї розкішної садиби. Крім того, інвестори мають змогу здійснювати «переуступку прав» — перепродавати контракти ще до завершення будівельних робіт і введення об’єкта в експлуатацію. Це дозволяє не лише відмити кошти з отриманням прибутку та уникнути сплати податку під час оформлення документів, а й взагалі не вносити ім'я кінцевого бенефіціара до офіційного земельного кадастру. Водночас забудовники, фінансова стабільність яких прямо залежить від обов’язкових обсягів попередніх продажів для відкриття банківських кредитних ліній, мають потужний економічний стимул закривати очі на походження коштів клієнтів.

Критичним чинником ризику виступає небезпечний правовий вакуум у регулюванні сектору будівництва. Хоча класичні рієлтори, банки та юридичні фірми зобов’язані здійснювати належну перевірку клієнтів (CDD) і з'ясовувати законність джерел багатства, самі забудовники не вважаються суб'єктами первинного фінансового моніторингу за правилами ПВК, якщо вони продають побудоване житло напряму через власні комерційні структури. За даними національної

[4] https://www.transparency.org.uk/sites/default/files/2026-10/Concerning%20Developments.pdf

оцінки ризиків, приблизно 74% забудовників у Великій Британії взагалі не зареєстровані в жодному наглядовому органі у сфері протидії відмиванню коштів. Показовим прикладом став скандал навколо колишнього міністра земельних ресурсів Бангладеш Сайфуззамана Чоудхурі, який за офіційної річної зарплати близько 10 000 фунтів придбав портфель із майже 300 новобудов у забудовника Berkeley Group на 170 млн фунтів через агента-посередника, що зараз перебувають під арештом NCA. Іншим виміром загрози є випадки, коли підсанкційні особи самі виступають забудовниками: так, іранський фінансист Алі Ансарі, пов'язаний із Корпусом вартових ісламської революції (КВІР), зміг через офшор на острові Мен отримати офіційний дозвіл на будівництво 33 елітних апартаментів у Північному Лондоні.

Другою системною вразливістю є конфлікт інтересів серед акредитованих юридичних фірм, яких забудовники рекомендують покупцям і нерідко самі оплачують їхні послуги. Оскільки забудовник є ключовим джерелом доходу для таких юристів, у них формується прямий стимул не ставити незручних запитань і формально штампувати транзакції, аби не втратити вигідне місце в партнерському пулі на майбутні проєкти. Свідченням цього стала справа лондонського житлового комплексу Elephant Park, де єдина акредитована при проєкті юридична фірма Riseam Sharples оформила купівлю 19 квартир компаніям Су Цзянбо, оголошеного владою КНР у розшук за організацію нелегальних азартних ігор (активи згодом заморожені за ордерами на необґрунтовані статки). Ситуація поглиблюється тим, що через високу вартість житла забудовники цілеспрямовано орієнтують маркетинг на покупців із держав із високим рівнем корупції та закритими реєстрами, створюючи сайти китайською мовою та проводячи закриті продажі за кордоном. За такою схемою керівники транснаціонального злочинного угруповання Prince Group, причетні до торгівлі людьми в Камбоджі, відмили понад 280 млн фунтів, придбавши десятки квартир у комплексах Embassy Gardens і Centre Point через юридичну компанію Chan Neill Solicitors, яка спеціалізується на східноазійських інвесторах.

Для захисту ринку первинної нерухомості від кримінального капіталу Transparency International UK пропонує три обов'язкові регуляторні кроки: поширити обов'язки суб'єктів моніторингу у сфері ПВК безпосередньо на забудовників на основі оцінки ризиків; зобов'язати юристів щорічно звітувати перед дисциплінарними наглядовими органами про членство в панелях забудовників для виявлення конфліктів інтересів; а також запровадити регулярне декларування юристами операцій на користь іноземних клієнтів із юрисдикцій високого ризику. Автори підкреслюють, що на тлі урядових планів із нарощування масштабів житлового будівництва ліквідація цих лазівок є критичною умовою, аби нове житло вирішувало соціальну кризу, а не служило «сейфом» для іноземних клептократів.

Висновки

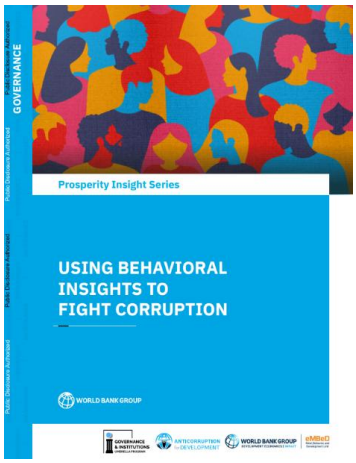
Первинний ринок нерухомості як головний магніт для нелегальних статків: схеми купівлі житла на етапі будівництва стали ключовим каналом відмивання коштів завдяки можливості гуртових покупок, переуступки прав без реєстрації в земельному кадастрі та уникнення податків.

Небезпечний правовий вакуум навколо забудовників: близько 74% британських забудовників офіційно не контролюються антикорупційними та фінансовими наглядовими органами, що дозволяє особам під санкціями та корумпованим чиновникам вільно вкладати сотні мільйонів фунтів у будівельні проєкти.

Комерційний підкуп і формалізм юристів: залучення «кишенькових» юридичних фірм, рекомендованих самими забудовниками, створює системний конфлікт інтересів, за якого юристи зацікавлені схвалювати підозрілі платежі заради збереження вигідних контрактів із забудовником.

Необхідність ліквідації лазівок для іноземних покупців високого ризику: припинення припливу коштів сумнівного походження у сферу будівництва потребує запровадження обов'язкового фінансового моніторингу діяльності компаній-забудовників, забезпечення прозорості переліків акредитованих юристів та посиленого контролю за компаніями, які обслуговують покупців із офшорних юрисдикцій і країн із високим рівнем корупції.

Людський вимір антикорупційної політики: як когнітивні упередження та соціальні норми впливають на доброчесність [5]



Аналітична доповідь Світового банку присвячена системній інтеграції досягнень поведінкових наук у розробку й практичну реалізацію антикорупційних політик. Дослідження опирається на емпіричні висновки рандомізованих контрольованих досліджень, квазіекспериментів та польових інтервенцій у митних, фіскальних, судових, освітніх і правоохоронних органах Мадагаскару, Пуерто-Рико, Філіппін, Румунії, Таджикистану, Бангладеш, Пакистану, Гани, Мексики та Індії. Публікація адресована урядовцям, реформаторам, представникам міжнародних фінансових інституцій та експертам у сфері публічного управління, доводячи, що класичні структурні, нормативні й виключно каральні заходи часто демонструють обмежену ефективність або дають зворотні наслідки, якщо вони не враховують людського фактора, неформальних соціальних норм і когнітивних механізмів прийняття рішень.

Основна теза звіту стверджує, що корупція в державному секторі є не лише продуктом слабкого законодавства чи браку контролю, а й закономірним наслідком людської поведінки в умовах обмеженої раціональності. Традиційне уявлення про правопорушника як про виключно раціонального гравця, якого стримує суворість покарання, розбивається об когнітивні упередження. Зокрема, посадовцям притаманний оптимістичний зсув, через який вони схильні систематично недооцінювати ймовірність власного викриття, а також обмежена етичність, за якої чиновники йдуть на поступові моральні компроміси й виправдовують хабарі традиціями чи низькою оплатою праці. На груповому рівні корупційні практики закріплюються розривом між дескриптивними нормами (переконанням, що «всі беруть») та ін'юнктивними нормами (публічним несхваленням хабарництва), що формує пастку колективної дії, де індивідуальна чесність здається безглуздою. На інституційному рівні поширенню корупції сприяють надмірна складність регуляторних вимог, ускладнені адміністративні процедури, непрозорість процесів ухвалення рішень і широкі дискреційні повноваження посадових осіб. Наскрізним чинником виступає гендерна нерівність: жінки частіше стикаються з вимаганням хабарів чи сексуальних послуг у сферах охорони здоров'я та освіти через вищу залежність від базових послуг і виключеність із закритих патріархальних мереж кумівства.

Для подолання цих викликів Світовий банк пропонує конкретні поведінкові рішення у чотирьох ключових напрямах, починаючи з підзвітності та моніторингу. Експерименти свідчать, що стримуючий ефект забезпечується не суворістю законів, а суб’єктивною помітністю та

[5] https://documents1.worldbank.org/curated/en/099070726123040783/pdf/P179427-27bcb9df-4fb4-4755-95e1-462377a5e4d6.pdf

непередбачуваністю перевірок: незалежна рандомізація розподілу митних декларацій на Мадагаскарі ліквідувала корупційні змови брокерів та інспекторів, а своєчасне оприлюднення результатів муніципальних аудитів у Пуерто-Рико безпосередньо перед виборами знизило зловживання на 66%. Водночас звіт наголошує на ризиках неякісного моніторингу: у Мексиці публічне розголошення корупції місцевої влади без демонстрації покарання винних спровокувало зворотну реакцію, збільшивши схильність школярів до списування на 10% через переконання, що нечесність є загальноприйнятною суспільною нормою.

У сфері цифровізації та спрощення процесів автори закликають до перебудови «архітектури вибору», за якої доброчесна поведінка стає стандартною опцією за замовчуванням. Запровадження електронного податкового декларування в Таджикистані скоротило корупцію за рахунок усунення особистого контакту бізнесу з чиновниками, що значно ускладнило вимагання грошей. Разом із тим звіт застерігає від спрощеного підходу до автоматизації: у Бангладеші запуск публічних інформаційних панелей продуктивності чиновників земельних кадастрів зменшив затримки розгляду справ на 13%, проте у посадовців із найвищою швидкістю обсяг хабарів підскочив на 15% через ефект морального ліцензування, коли власні успіхи у швидкості слугували психологічним виправданням для незаконного заробітку. Відтак системи контролю обов'язково мають бути багатовимірними й містити індикатори доброчесності, кількості скарг і помилок, а не лише швидкість виконання.

У сфері матеріальних стимулів дослідження вказує на небезпеку ізольованих фінансових премій. У пакистанському Пенджабі пряма прив'язка бонусів податківців до суми зібраних податків стимулювала зростання здирництва з пересічних платників на 32%, що доводить необхідність доповнення матеріальних стимулів репутаційними інструментами, об'єктивними формулами розрахунку та захищеними каналами скарг. На рівні зміни соціальних норм доведено ефективність практичних етичних тренінгів: у Гані навчальні сесії з формування професійної ідентичності поліцейських дали стійке зниження хабарництва на дорогах на 20 місяців, а тренінги з комунікації та ввічливості для поліцейських в індійському Раджастхані підвищили задоволеність громадян на 15–19%.

Практична методологія документа базується на чотириетапній діагностиці, яка включає формулювання конкретної спостережуваної поведінки, аналіз драйверів за трирівневою моделлю, картографування маршруту взаємодії користувача з державою для фіксації точок корупційного ризику та польове тестування гіпотез за допомогою спостережень або методів таємного клієнта. На відміну від довготривалих і дорогих інституційних трансформацій, поведінкові інсайти дозволяють досягати відчутних антикорупційних результатів через маловитратні точкові корективи процедур, ліквідацію зайвої паперової бюрократії, рандомізацію перевірок та формування нової організаційної культури.

Висновки

Обмеженість покарань через когнітивні упередження: посадовці схильні недооцінювати ризик власного викриття (оптимістичний зсув), тому суворість покарань без непередбачуваних і публічних перевірок не забезпечує дієвого стримування.

Ризики помилкового проєктування контролю: оприлюднення фактів корупції без вироків сприймається як норма, оцінка чиновників лише за швидкістю стимулює хабарі, а премії за фіскальні показники без перевірки доброчесності призводять до вимагання неправомірної вигоди.

Цифровізація послуг для зменшення корупційних ризиків: електронні сервіси є ефективними, коли вони спрощують адміністративні процедури, мінімізують особисті контакти з посадовцями та обмежують їхні дискреційні повноваження завдяки автоматизації процедур.

Виявлення корупційних ризиків без масштабних реорганізацій: аналіз послідовності дій посадових осіб і користувачів під час отримання послуг дає змогу визначити етапи виникнення корупційних ризиків та зменшити їх завдяки вдосконаленню процедур, спрощенню форм і періодичній зміні відповідальних посадових осіб без значних фінансових витрат.

Як фінансується війна: навіщо FATF окрема типологія фінансування конфліктів [6]



У RUSI Journal вийшла стаття виконавчої директорки організації The Sentry Юстини Гудзовської «FATF має взятися за те, як фінансується війна». Авторка виходить зі спостереження, що перелік юрисдикцій із «сірого» та «чорного» списків FATF значною мірою збігається з переліком країн, які перебувають у стані збройного конфлікту, повстанської діяльності чи гострої нестабільності – від М'янми до ДР Конго та Південного Судану. На її думку, це не випадковість: у конфліктних середовищах слабкі інституції, неефективний нагляд, проникні кордони й відсутність контролю держави над частиною території створюють «регуляторні чорні діри», а незаконні фінансові потоки водночас підтримують насильство.

Центральна теза статті полягає в тому, що FATF жодного разу не розглядала фінансування конфліктів як окреме явище, хоча опублікувала десятки типологічних звітів – від програм громадянства за інвестиції та краудфандингу для фінансування тероризму до програм-вимагачів і екологічних злочинів. Як наслідок, поняття залишається розпорошеним між відмиванням коштів, фінансуванням тероризму, обходом санкцій і фінансуванням розповсюдження. Авторка використовує робоче визначення фінансування конфлікту як діяльності або відносин, що генерують доходи для збройних груп чи сторін конфлікту, і наголошує: мандат FATF технічний, проте його мета включає «безпеку й захищеність», тож фінансова цілісність має прямі наслідки в реальному світі.

Гудзовська перелічує джерела фінансування конфліктів: експлуатацію природних ресурсів (золото, діаманти, нафта, деревина, дика природа), вимагання, контроль торговельних маршрутів, викрадення з метою викупу, контрабанду людей і наркотиків, обхід санкцій та відмивання через торгівлю. Вона підкреслює, що фінансування конфліктів не обмежується недержавними акторами, і як приклад наводить росію, яка, за її оцінкою, переналаштувала всю економіку на воєнні рейки й перетворилася на потужний механізм обходу санкцій і відмивання коштів; корумповані посадовці інших держав при цьому сприяють таким схемам. Стандарти FATF застосовуються, щойно в екосистемі конфлікту з'являються ознаки відмивання, фінансування

[6] https://www.tandfonline.com/doi/full/10.1080/03071847.2026.2712856

тероризму чи предикатних злочинів, проте, на думку авторки, інструменти ПВК/ФТ слід застосовувати ще до документального підтвердження причетності терористичних організацій.

Важливе місце у статті посідає типологічне дослідження MONEYVAL щодо ризиків відмивання коштів, фінансування тероризму та розповсюдження, пов'язаних із доходами від конфліктів. Авторка називає його важливим першим кроком, однак зауважує, що через переважно європейський склад MONEYVAL дослідження спирається на обмежене коло конфліктів і кейсів, значною мірою на контекст російської агресії. Звіт на рівні FATF із залученням регіональних органів з усього світу, за її оцінкою, забезпечив би ширшу доказову базу, глобальний авторитет, спільний понятєвий апарат, вплив на національні оцінки ризиків, виявлення законодавчих прогалин, специфічні для конфліктних зон індикатори та кейси за регіонами й товарами.

Точкою входу до такої типології авторка пропонує зробити «конфліктне золото». За рекордних цін на золото його нелегальна торгівля стала ключовим джерелом доходів для обох сторін війни в Судані та для збройних угруповань на сході ДР Конго, зокрема руху М23, причому більша частина такого золота зрештою відмивається через ОАЕ. Золото також є джерелом фінансування війни росії проти України. Звіт FATF щодо ризиків, пов'язаних із золотом, вийшов понад десять років тому і взагалі не згадує конфлікт. Авторка відкидає побоювання, що типологія стане інструментом тиску на нестабільні держави: навпаки, деталізоване розуміння схем могло б зменшити дерискінг, коли фінансові установи уникають усіх операцій, пов'язаних із конфліктними зонами.

Висновки

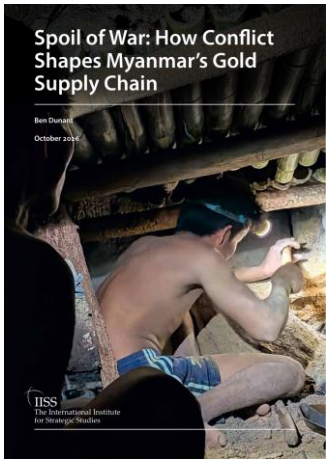
Фінансування конфлікту доцільно розглядати як наскрізну категорію ризику: воно поєднує відмивання коштів, фінансування тероризму, обхід санкцій і злочини, пов'язані з природними ресурсами, тому в оцінках ризиків держави, яка зазнала агресії, такі потоки варто аналізувати як окремий блок, а не розподіляти між різними предикатними злочинами.

Типологія MONEYVAL є базою для глобальної роботи FATF: обмеженість її доказової бази європейськими кейсами є аргументом для просування на рівні FATF окремого проєкту, до якого український досвід виявлення воєнних економічних схем може бути внесений як ключовий внесок.

Золото є перевіреним каналом фінансування війни: кейси Судану, ДР Конго та росії вказують, що суб'єктам моніторингу, які працюють із дорогоцінними металами, необхідні індикатори щодо походження, транзиту через ОАЕ та перероблення, яких не містить звіт FATF 2015 року.

Деталізація ризиків є альтернативою дерискінгу: типологія з конкретними індикаторами дозволяє банкам застосовувати ризик-орієнтований підхід до клієнтів із прифронтових і постраждалих регіонів, а не відмовляти в обслуговуванні за географічною ознакою.

Трофей війни: як конфлікт у М'янмі перебудував ланцюг постачання золота [7]



Міжнародний інститут стратегічних досліджень (IISS) у жовтні 2026 року оприлюднив кейс-дослідження Бена Дюнанта «Трофей війни: як конфлікт формує ланцюг постачання золота М'янми», підготовлене за фінансової підтримки Всесвітньої ради з золота. Дослідження простежує шлях золота від видобутку до продажу на основі інтерв'ю з шахтарями, торговцями та мешканцями шести районів регіону Сагайн і по одному району штатів Качин і Шан, аналізу супутникових знімків, митної статистики та місцевих медіа. Контекст – військовий переворот 2021 року, конфлікт, що забрав понад 100 тисяч життів, падіння ВВП майже на 20% і знецінення місцевої валюти більш ніж утричі, через що золото стало для населення основним засобом збереження вартості.

Ключовий висновок стосується розриву між офіційною та реальною економікою золота. Офіційний видобуток, що враховує лише ліцензовані копальні, скоротився з 846 кг у 2020/21 фінансовому році до 532 кг у 2024/25 році, тоді як, за оцінкою International Crisis Group, неформальний видобуток щонайменше вдесятеро більший, перевищує п'ять тонн на рік і оцінюється майже в 1 млрд доларів. Аналіз супутникових знімків, проведений автором, фіксує різке поширення земснарядів на річках регіону Сагайн після 2021 року, а державна система ліцензування фактично розпалася навіть на територіях, підконтрольних режиму.

Дослідження детально описує, як золото фінансує обидві сторони конфлікту. На територіях опозиції збройні угруповання та органи паралельного Уряду національної єдності запровадили власні режими оподаткування: від 800 тис. к'ятів (186 доларів) раз на пів року до 1,5 млн к'ятів (348 доларів) щомісяця, одноразові збори за земснаряди до 70 млн к'ятів (16 240 доларів), а в окремих районах – податок натурою, зокрема 20 тікалів (326,6 г) золота щомісяця з великих копалень. Водночас оператори копалень на опозиційних територіях сплачують хабарі військовим режиму за безперешкодний рух пального, техніки та золота через блокпости; брокери, які організовують такі перевезення через лінію фронту, беруть 15–30% вартості вантажу. Таким чином, одна й та сама товарна вісь фінансує армії обох сторін, не приносячи державі офіційних надходжень.

Для фахівців з ПВК/ФТ найважливішим є розділ про легалізацію золота на ринку. Мережі золотих крамниць і торговців переміщують метал із сільських районів до Мандалая автошляхами та через внутрішні аеропорти й паралельно функціонують як система переказу готівки: шахтар продає золото в сільській крамниці, а його партнер отримує гроші в партнерській крамниці в Мандалаї без додаткової комісії. Великі афінажні заводи в Янгоні та М'їчіні не вимагають жодних документів про походження, а перероблене золото, яке родини в умовах кризи здають у ломбарди,

[7] https://www.iiss.org/research-paper/2026/10/spoil-of-war-how-conflict-shapes-myanmars-gold-supply-chain/

переплавляється на тих самих підприємствах, що й новодобуте. Додатково зростає кількість неліцензованих афінажних виробництв, які працюють завдяки хабарям місцевій владі й випускають злитки без клейма. Періодичні кампанії режиму спрямовані не на нелегальне золото, а на стримування спекуляцій і стабілізацію курсу.

Окремо проаналізовано зовнішні потоки. Експорт золота легалізували у 2018 році, однак після запровадження у 2020 році жорсткіших платіжних правил, ухвалених у відповідь на включення М'янми до «сірого» списку FATF, він фактично припинився, а після перевороту країна опинилася в «чорному» списку. Значні обсяги контрабанди йдуть до Індії: у 2020/21 фінансовому році М'янма була джерелом 37% вилученого в Індії контрабандного золота, тобто близько 308 кг, що дорівнює 36% офіційного видобутку країни, причому частина злитків мала клейма найбільших ліцензованих афінажних заводів. Митні дані Китаю показують зростання імпорту з М'янми руд і концентратів дорогоцінних металів за товарним кодом 261690 з 234 тонн у 2020 році до 27 788 тонн у 2025 році та 53 005 тонн на 113,98 млн доларів лише в першому півріччі 2026 року, хоча на боці М'янми експорт не зафіксовано. Неформальні мережі «хунді», якими мігранти пересилали кошти додому, після перевороту використовують для виведення заощаджень за кордон, а розрахунки за ними завершуються контрабандою золота до Таїланду.

Автор звертає увагу й на екологічну та соціальну ціну: використання ртуті, концентрації якої біля однієї з копалень у регіоні Мандалай ще до перевороту в 74 рази перевищували безпечний рівень ВООЗ, забруднення річок, втрату сільськогосподарських земель і появу шахтарських поселень із ринками наркотиків. Міжнародні стандарти відповідального постачання щонайменше вимагають посиленої перевірки щодо золота з М'янми, проте практично кожен етап внутрішнього ланцюга, ймовірно, пов'язаний із платежами або військовим режиму, або недержавним збройним угрупованням, тобто з найвищими ризиками за Настановою ОЕСР. Тому, на думку автора, вирішення проблеми неможливе лише через припинення вогню: досвід «капіталізму перемир'я» в Качині після 1994 року показує, що видобуток ресурсів може слугувати й основою тривалого «негативного миру».

Висновки

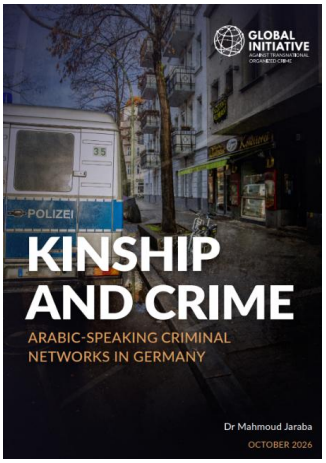
Відсутність вимог щодо походження на етапі афінажу робить золото ідеальним інструментом легалізації: змішування новодобутого й переробленого металу на тих самих заводах і виробництво злитків без клейма унеможливлюють простеження, тому суб'єкти моніторингу, що працюють із дорогоцінними металами, мають вимагати документального підтвердження ланцюга постачання, а не лише перевіряти контрагента.

Мережі торговців золотом одночасно є неформальною системою переказу коштів: передача грошей між партнерськими крамницями та розрахунки «хунді» через контрабанду золота поєднують торговельне відмивання й неформальні перекази, що потребує спільного аналізу товарних і фінансових потоків.

Розбіжності дзеркальної митної статистики є індикатором незаконних потоків: зростання імпорту руд і концентратів до Китаю за відсутності експорту з М'янми та вилучення злитків у сусідніх країнах демонструють, як розриви в торговельних даних дозволяють виявляти незадекларовані потоки дорогоцінних металів.

Фінансування конфлікту через ресурси не обмежується однією стороною: хабарі військовим режиму та податки опозиційних угруповань з одних і тих самих копалень означають, що будь-яке золото з конфліктних регіонів М'янми має розглядатися як високоризикове незалежно від того, хто контролює територію видобутку.

Тіньові мережі Німеччини: як родинні зв'язки допомагають організованій злочинності [8]



Аналітична доповідь міжнародної організації Глобальна ініціатива проти транснаціональної організованої злочинності (GI-TOC) присвячена аналізу функціонування арабомовних кримінальних мереж у Німеччині. Дослідження базується на тривалих етнографічних польових розвідках (2015–2026 роки), конфіденційних інтерв'ю з членами великих родинних груп, співробітниками Федерального відомства кримінальної поліції Німеччини (BKA) та земельних управлінь кримінальної поліції (LKA), онлайн-моніторингу закритих каналів зв’язку та матеріалах судових справ. Документ адресований правоохоронним органам, аналітикам безпеки, законодавцям та фахівцям з інтеграційної політики країн Європи.

Центральна теза дослідження полягає в тому, що родинні зв’язки самі по собі не є синонімом злочинності, проте вони виступають потужною соціальною інфраструктурою довіри, лояльності, взаємодопомоги та неформального регулювання, яку окремі субгрупи цілеспрямовано використовують для ведення протиправної діяльності. Дослідження порівнює дві різні за історією та структурою спільноти: давно вкорінені в Німеччині клани походженням із регіону Мардін (південно-східна Туреччина, які мігрували через Ліван у 1970–1980-х роках) та новіші сирійські угруповання, що сформувалися після міграційної кризи 2015 року. Автор підкреслює неприпустимість стигматизації цілих діаспор через термін «кланова злочинність», вказуючи на необхідність чіткої диференціації між законослухняною більшістю родин та конкретними кримінальними осередками.

Мережі вихідців із Мардіна, зосереджені переважно в Берліні, Бремені, Нижній Саксонії та Північному Рейні-Вестфалії, за десятиліття пройшли шлях від розрізненої дрібної контрабанди через тривалу правову невизначеність (статус «толерованого перебування» Duldung) до складних кримінальних формувань. Їхня діяльність охоплює незаконний обіг наркотиків (кокаїн, канабіс), резонансні майнові крадіжки (як-от викрадення золотої монети «Big Maple Leaf» з музею Боде у 2017 році чи коштовностей із Дрезденського музею у 2019 році), шахрайство та нелегальні фінансові перекази. Сьогодні молоде покоління цих кланів поступово відходить від патріархального контролю старійшин, активно будуючи прагматичні комерційні альянси поза родинними чи етнічними межами, використовуючи цифрові інструменти та прагнучи кооптувати інсайдерів у публічних і комерційних установах.

[8] https://globalinitiative.net/wp-content/uploads/2026/10/Mahmoud-Jaraba-Kinship-and-crime-Arabic-speaking-criminal-networks-in-Germany-GI-TOC-October-2026.pdf

На противагу їм, сирійські угруповання є менш централізованими, значно ширше розселеними по території всієї Німеччини та спираються як на відновлені родові структури, так і на земляцтва на основі спільного регіону походження (міст чи таборів біженців). Основна сфера їхньої кримінальної активності зосереджена навколо організації каналів нелегальної міграції балканським маршрутом (показовим є вирок лідерам мережі «Al-Sarawi» у Баварії у 2025 році), підробки документів (зокрема пересилання оригінальних німецьких посвідок на проживання співвітчизникам до Сирії), роздрібної торгівлі наркотиками та вуличних молодіжних банд у великих містах.

Окрему тривогу в німецьких містах викликає поява вуличних молодіжних банд, які в публічному дискурсі та медіа отримали неформальні назви на кшталт «Talahon» («підійди сюди») чи «хлопці з вокзалу». Ці підліткові та молодіжні угруповання віком від 14 до 25 років збираються довкола вокзалів, торговельних центрів і парків Берліна, Гамбурга, Штутгарта та Ессена, займаючись дрібним наркодилерством, кишеньковими крадіжками, грабежами та демонстративним насильством. Вони значно менше зважають на традиційні табу родини чи авторитет старших, а свій соціальний статус і кримінальну репутацію активно вибудовують через соціальні мережі (зокрема TikTok), поєднуючи агресивну вуличну поведінку з демонстрацією зброї та пачок готівки.

Дослідження детально розкриває транснаціональний вимір цих мереж, який охоплює Німеччину, Швецію, Данію, Нідерланди, Туреччину, Ліван і Сирію. Важливу роль відіграють неформальні механізми врегулювання спорів, зокрема традиційна практика примирення «сульха» (sulha) та посередництво осіб, відомих у Німеччині як «мирові посередники». Їх залучають, зокрема, для врегулювання тривалих конфліктів, пов'язаних із кровною помстою, а також фінансових суперечок між представниками конкуруючих кримінальних угруповань. У певних випадках такі механізми використовуються замість звернення до офіційної судової системи. Фінансові розрахунки в межах відповідної діяльності можуть здійснюватися через неформальні системи переказу коштів, зокрема «hawala», а також із використанням готівки, що ускладнює відстеження руху коштів і створює ризики обходу стандартних механізмів фінансового моніторингу. Окремим транскордонним напрямом стало телефонне шахрайство під виглядом «фальшивих поліцейських», коли підпільні колцентри в турецьких містах (Ізмір, Мерсін) дистанційно ошукують літніх громадян у Німеччині на мільйони євро, використовуючи Туреччину як надійний прихисток від німецького правосуддя.

Крім того, стійкість і закритість кланових структур забезпечується суворим внутрішнім кодексом мовчання та конфіденційності, порушення якого загрожує члену родини соціальним вигнанням, бойкотом або фізичною розправою. У поєднанні з використанням зашифрованих каналів зв'язку (WhatsApp, Telegram, Signal) це робить проникнення поліцейських під прикриттям чи вербування інформаторів у таких середовищах надзвичайно складним завданням. З огляду на це автор наголошує, що поліцейських рейдів і кримінальних покарань замало: подолання феномену вимагає раннього превентивного втручання, розвитку соціальних програм для молоді у проблемних кварталах та адресного відстеження тіньових фінансових потоків.

Висновки

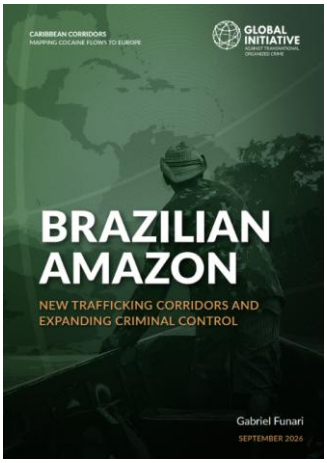
Родинні структури як організаційний ресурс, а не причина злочинності: родинні та земляцькі зв'язки забезпечують кримінальним мережам високий рівень внутрішньої довіри, конспірації та стійкості до проникнення правоохоронців, проте боротьба з цим явищем повинна фокусуватися на конкретних протиправних діяннях та організаторах, а не на стигматизації прізвищ чи цілих громад.

Еволюція поколінь та вихід за етнічні межі: традиційна патріархальна ієрархія поступово втрачає абсолютний вплив; молоде покоління правопорушників формує прагматичні міжетнічні альянси, використовує зашифровані месенджери й штучний інтелект та намагається здобути доступ до інсайдерської інформації в державних і комерційних органах.

Паралельне правосуддя та тіньова фінансова інфраструктура: стійкість угруповань підтримується позасудовими механізмами врегулювання конфліктів та неформальними грошовими переказами «hawala», що виводить фінансові потоки й кримінальні спори з-під контролю офіційної юстиції.

Необхідність раннього втручання та транскордонної взаємодії: оскільки сирійські кримінальні осередки перебувають на стадії активного формування, держава повинна діяти на випередження через адресні фінансові розслідування, перекриття каналів переправлення мігрантів, роботу з молоддю та тісну координацію з європейськими й близькосхідними партнерами, щоб не допустити закріплення нових багатопоколінних мафіозних структур.

Бразильська Амазонія: нові коридори контрабанди та експансія криміналу [9]



Амазонський регіон, який історично сприймався як віддалений та малодоступний простір, стрімко перетворюється на один із ключових вузлів глобальної торгівлі кокаїном. Звіт GI-TOC свідчить про фундаментальну трансформацію наркотрафіку в регіоні. Якщо протягом десятиліть Амазонія слугувала переважно транзитним коридором для переміщення кокаїну з Колумбії, Перу та Болівії до Бразилії та Європи, то нині вона стала ареною жорсткої конкурентної боротьби між транснаціональними злочинними угрупованнями, що супроводжується різким зростанням насильства, диверсифікацією маршрутів та методів контрабанди, а також небезпечною конвергенцією наркоторгівлі з незаконним видобутком золота.

Центральним драйвером цих змін є невпинне зростання попиту на кокаїн у Європі. Саме європейський ринок, де роздрібна ціна кілограма кокаїну сягає 50-70 тисяч євро, забезпечує надприбутки, які дозволяють злочинним синдикатам інвестувати в розширення логістичних мереж. Згідно з даними звіту, придбання кілограма кокаїну в регіонах виробництва в Колумбії чи Перу коштує близько 1000 доларів США. Після перетину кордону Бразильської Амазонії його вартість зростає до 2500-3500 доларів, а на момент відправлення до Європи сягає 4000-5000 доларів за кілограм. Така маржинальність стимулює постійний пошук нових шляхів та методів доставки, що призвело до значного збільшення обсягів вилученого наркотику. Протягом 2019-2024 років державні сили у дев'яти штатах басейну Амазонки вилучили понад 162 тонни кокаїну, що на 574% більше порівняно з попереднім чотирирічним періодом, тоді як федеральна поліція вилучила 118 тонн, що на 84% більше. Водночас правоохоронці визнають, що ці вилучення становлять менше 10% від загального обсягу контрабанди, що свідчить про масштабність проблеми.

Історично склалося так, що головним маршрутом переміщення наркотиків був річковий шлях Солімойнс, який з'єднував потрійний кордон Бразилії, Перу та Колумбії з містом Манаус. Це місто, розташоване на злитті двох найбільших річок регіону, Амазонки та Ріу-Негру, є критичним логістичним вузлом, де наркотики перевантажуються на більші судна для подальшого відправлення до портів Атлантичного узбережжя або до великих споживчих ринків південно-східної Бразилії. Протягом останнього десятиліття боротьба за контроль над цим маршрутом між двома найбільшими бразильськими угрупованнями — Primeiro Comando da Capital (PCC) та Comando Vermelho (CV) — призвела до сплеску насильства. Особливо відзначився своєю жорстокістю конфлікт за участю місцевого угруповання Familia do Norte (FDN), кульмінацією якого

[9] https://globalinitiative.net/wp-content/uploads/2026/09/Gabriel-Funari-Brazilian-Amazon-New-trafficking-corridors-and-expanding-criminal-control-GI-TOC-September-2026-1.pdf

стали масові вбивства в'язнів у 2017 та 2019 роках. Зрештою, завдяки гнучкішій моделі управління та здатності залучати місцеві банди, угруповання CV змогло витіснити PCC з більшості ключових точок регіону, включаючи Манаус, та встановити свою гегемонію.

Однак, найбільш значущою тенденцією останніх років стала зміна географії експорту. Хоча порт Віла-ду-Конде поблизу Белена залишається важливим вузлом, посилення нагляду та домінування CV у цьому регіоні змусили інші угруповання шукати альтернативні шляхи. Новим "гарячим" напрямком став штат Амапа, розташований на північному сході країни, який межує з Французькою Гвіаною. Ізольованість регіону, відсутність сухопутного сполучення з рештою країни та обмежена присутність федеральних правоохоронних органів зробили його привабливим для контрабандистів. Порт Сантана, що знаходиться поруч зі столицею штату Макапа, став стратегічним експортним хабом. На відміну від Белена, де встановлено сканери для перевірки контейнерів, у Сантані така техніка відсутня, а ручні огляди проводяться нерегулярно. Крім того, акваторія навколо Макапи використовується як зона очікування для приблизно 1000 трансатлантичних суден, які прямують до Манауса і назад, що створює ідеальні умови для високотехнологічних методів контрабанди.

Одним із найбільш винахідливих методів, що застосовується в цьому регіоні, є так званий "rip-on/rip-off" (прикріпити-відкріпити). Судна, що прямують з Манауса, змушені кілька днів чекати в дельті Амазонки на прибуття місцевих лоцманів для проходження через складні води. У цей час професійні водолази, часто колишні військові, вночі прикріплюють вантажі кокаїну до двигунів або корпусу суден. Використання підводних човнів, броньованих швидкісних катерів та контейнерів також стає дедалі поширенішим явищем. Іншим тривожним трендом є використання "мулів" — завербованих осіб, зокрема корінних жителів, для перевезення невеликих партій наркотиків на регіональних рейсах, а також використання малих літаків та злітно-посадкових смуг у джунглях.

Ця експансія супроводжується безпрецедентним рівнем насильства. У 2024 році рівень вбивств у Бразильській Амазонії становив 27,3 на 100 тисяч населення, що на 31% вище за середній показник по країні. Штат Амапа, зокрема, перетворився на зону запеклих боїв між місцевими угрупованнями, такими як Familia Terror do Amapá (FTA) та Amigos Para Sempre (APS), які, своєю чергою, діють в інтересах великих синдикатів. Цікаво, що CV, який зараз домінує в регіоні, пропонує місцевим бандам більш "франшизну" модель співпраці з мінімальним втручанням з боку центрального керівництва в Ріо-де-Жанейро, тоді як PCC вимагає суворої дисципліни та ієрархії. Ця гнучкість дозволяє CV швидко нарощувати свою присутність, залучаючи як високопосадовців з конкуруючих угруповань, так і дрібних вуличних торговців. Водночас зростання насильства в Амапі також пов'язане з надзвичайно високим рівнем летальності дій поліції, яка у 2024 році вбила 137 осіб, що становить 35% від усіх вбивств у штаті.

Ще однією критичною загрозою, яку висвітлює звіт, є тісне переплетення наркоторгівлі з незаконним видобутком золота. Зростання світових цін на золото робить цей сектор надзвичайно привабливим для інвестування наркодоларів. Золото використовується не лише для відмивання коштів, а й як валюта для оплати великих партій кокаїну, оскільки його важко відстежити. Крім

того, кримінальні групи використовують логістичну інфраструктуру старателів — малі літаки, злітно-посадкові смуги та корумпованих правоохоронців — для переміщення наркотиків. Це явище спостерігається по всьому басейну, включаючи Французьку Гвіану, де бразильські угруповання, такі як CV, розширюють свою діяльність на місцевих копальнях.

Звіт також наголошує на появі нових, ще не до кінця досліджених маршрутів. Окрім традиційного річкового шляху, спостерігається активізація транскордонних переміщень через Суринам та Французьку Гвіану. Кокаїн з північної Колумбії доставляється до Суринаму, звідки літаками або човнами доправляється до Французької Гвіани та далі до Амапи річкою Ояпок. Хоча цей маршрут поки що перебуває в зародковому стані, він підкреслює зростаючу роль Амапи як ключового вузла транснаціональних потоків.

Підсумовуючи, аналітики GI-TOC закликають до негайних дій. Рекомендації включають посилення транскордонної співпраці правоохоронних органів, покращення наглядового потенціалу в експортних хабах, зокрема встановлення сканерів у порту Сантана, та спрямування слідчих ресурсів на розслідування зв'язків між кокаїном та золотом. Особлива увага приділяється потенційним наслідкам запланованого на жовтень 2025 року початку масштабного видобутку нафти в акваторії Амапи компанією Petrobras, що може ще більше ускладнити криміногенну ситуацію через зростання населення та збільшення кількості суден, які можуть бути використані для контрабанди.

Ситуація в Бразильській Амазонії демонструє, як глобальний попит на наркотики та високі ціни на сировину створюють складні виклики для безпеки, перетворюючи колись ізольований регіон на епіцентр транснаціональної злочинності, що вимагає комплексного та міжнародного підходу до вирішення.

Висновки

Амазонія трансформувалася з транзитного коридору на арену жорсткої конкуренції між організаціями PCC та CV, де останні завдяки "франшизній" моделі управління встановили домінування над ключовими вузлами — Манаусом, Беленом та новим хабом в Амапі.

Зростання європейського попиту та маржинальності (від $1 000 до $5 000 за кг) стимулювало диверсифікацію методів контрабанди — підводні човни, швидкісні катери та малі літаки — і збільшило вилучення кокаїну на 574% за 2019-2024 роки.

Штат Амапа став новим стратегічним експортним вузлом через слабкий нагляд, відсутність сканерів у порту Сантана та близькість до Французької Гвіани, що супроводжується рекордним насильством і надвисокою летальністю.

Наркоторгівля тісно переплелася з нелегальним видобутком золота: золото слугує валютою для оплати кокаїну та засобом відмивання коштів, а логістика старателів використовується для переміщення наркотиків, що створює стійку кримінальну екосистему.

Агентний штучний інтелект і блокчейн: архітектура безпеки, ризики автономії та стандарти управління [10]



Звіт Глобальної ради з питань блокчейн-бізнесу (GBBC) присвячений системному аналізу конвергенції двох ключових технологій сучасності — штучного інтелекту, здатного до автономного планування та багатокрокового виконання цілей (агентний AI), та розподілених реєстрів (блокчейну). У документі наголошується, що AI стрімко еволюціонує від інструменту пасивного генерування контенту до активного учасника цифрової економіки, здатного самостійно ініціювати платежі, укладати угоди, взаємодіяти з іншими агентами та виконувати складні операційні процеси в корпоративних мережах. Такий перехід від взаємодії людини з системою через текстові запити до машинного виконання різко загострює питання довіри, цифрової ідентичності, делегованих повноважень та підзвітності, оскільки скорочення проміжку між ухваленням рішення системою та його практичним виконанням вимагає нових надійних механізмів верифікації. Автори детально розглядають визначення агентного AI, сформульовані провідними глобальними регуляторами, міжнародними організаціями стандартизації (ISO, NIST, IEEE), академічними установами та технологічними гігантами на кшталт Anthropic, Google Cloud і IBM, демонструючи перехід від простих попередньо визначених робочих процесів до динамічного самостійного виконання завдань.

Дослідження глибоко розкриває потенціал синергії цих технологій, підкреслюючи, що блокчейн не робить моделі AI «розумнішими» чи вільними від упереджень, але виконує критично важливу функцію інфраструктури довіри. Застосування розподілених реєстрів, смарт-контрактів та криптографічних ідентифікаторів (DIDs) дозволяє надійно закріплювати повноваження, версії політик, правила транзакцій та створювати незмінні журнали подій, які можна спільно верифікувати без необхідності повністю довіряти лише оператору системи. У звіті проаналізовано низку перспективних сценаріїв і практичних прикладів їх реалізації у сферах комерційної діяльності за участю AI-агентів, цифрових платежів, управління ланцюгами постачання та публічного сектору, а також визначено основні технологічні й операційні перешкоди.

Водночас у звіті детально розглянуто серйозні загрози безпеці, пов’язані з кібератаками, маніпулюванням вхідними запитами до систем штучного інтелекту, витоками даних, зловживанням наданими повноваженнями та несанкціонованою взаємодією між автономними агентами в багатоагентних екосистемах. Зокрема, аналізуються інциденти під час оцінок безпеки

[10] https://assets.ctfassets.net/so75yocayyva/25ovmsGHoq3yzA5E6Sbjeg/1a6e9f06992adf95863558f4f936d1a6/GBBC_GSMI7.0_AgenticAI_2026-Sep-22_FINAL.pdf

(як-от випадок із дослідницькими моделями в середовищі ExploitGym), які доводять необхідність посиленої ізоляції, жорсткого моніторингу та своєчасного реагування на збої на рівні всього процесу виконання.

Для забезпечення ефективного контролю у цій сфері у звіті запропоновано комплексну рамку підзвітності автономних агентів, що охоплює сім послідовних рівнів — від визначення особи або організації, від імені якої діє агент, та встановлення його цифрової ідентичності до визначення меж наданих повноважень, обмежень виконання операцій, інституційної відповідальності, а також дієвих механізмів оскарження рішень і правового захисту. Ця рамка покликана забезпечити збереження повного ланцюжка відповідальності незалежно від ступеня автономії цифрової системи.

Завершується документ практичними рекомендаціями для підприємств і регуляторів щодо впровадження ризик-орієнтованого управління, розвитку відкритих галузевих стандартів (зокрема ініціатив KYA-OS та Proof-of-Control) і вибіркового інтегрування блокчейн-інфраструктури виключно у тих випадках, коли це забезпечує реальну додаткову цінність для спільної перевірки даних. Автори наголошують, що технології повинні впроваджуватися за принципом «довіри за проєктом», поєднуючи технічні запобіжники з ефективним наглядом і прозорими стандартами.

Висновки

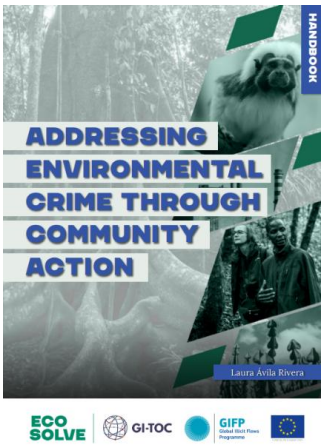
Автономність без втрати підзвітності: перехід AI від генерування відповідей до самостійного виконання послідовності дій не звільняє розробників і організації від відповідальності. Кожна дія автономного агента має бути пов’язана з чітко визначеною особою або організацією, від імені якої він діє, підтвердженою цифровою ідентичністю агента та документально визначеними межами його повноважень.

Блокчейн як доповнення, а не універсальне рішення: блокчейн не забезпечує інтелектуальних можливостей AI, проте може слугувати надійним засобом зберігання цифрових ідентифікаторів, фіксації версій політик, управління повноваженнями та ведення захищених від несанкціонованих змін журналів аудиту, що дають змогу кільком сторонам незалежно перевіряти відповідні записи.

Багаторівнева структура ризиків і потреба в незалежній перевірці: висока швидкість роботи автономних агентів AI створює розрив між виконанням дій і здатністю людини своєчасно їх перевіряти. Це зумовлює потребу в машиночитаних доказах та інфраструктурі для незалежної перевірки дій системи без покладання виключно на її оператора.

Інтеграція стандартів і безпеки на всіх етапах життєвого циклу: управління ризиками агентного AI передбачає застосування стандартів ISO, NIST та IEEE, принципу найменших привілеїв, шифрування, моніторингу й процедур реагування на інциденти вже на етапі проєктування системи, а не лише після виявлення збоїв.

Протидія злочинам проти природи: досвід розбудови довіри та підтримки екологічних рухів на місцях [11]



Практичний посібник, присвячений методології безпечного, етичного та результативного залучення місцевих громад до запобігання та протидії організованій екологічній злочинності. Дослідження систематизує практичний досвід польової роботи у шести країнах із різними безпековими, економічними та політичними контекстами — Бразилії, Колумбії, Індонезії, В'єтнамі, Мадагаскарі та Мозамбіку. Посібник адресований громадським організаціям, міжнародним донорським агентствам, інституціям ООН, природоохоронним службам та правоохоронним органам, пропонуючи перехід від виключно каральних і мілітаризованих методів контролю до системного партнерства з корінними народами й місцевими жителями, які безпосередньо проживають на уразливих природних територіях.

Основна теза доповіді стверджує, що суто силові правоохоронні заходи неспроможні самостійно зупинити виснаження ресурсів і нерідко спричиняють гострі конфлікти з місцевим населенням, підриваючи довіру до державних інституцій та призводячи до соціального відчуження. Корінні народи та локальні спільноти володіють або управляють близько 28% поверхні суходолу планети, де спостерігаються суттєво нижчі темпи знеліснення та деградації екосистем. Завдяки традиційним знанням території вони першими помічають прояви нелегальних рубок, браконьєрства, токсичних викидів та незаконного видобутку корисних копалин. Водночас екологічні захисники стикаються з постійними погрозами, криміналізацією та фізичним насильством із боку кримінальних синдикатів. Досвід програми ECO-SOLVE доводить, що за умови належного визнання прав спільнот та їхньої технічної підтримки добровільні патрулі й моніторинг (як у заповідниках бразильської Амазонії, лісах Камбоджі чи на копальнях М'янми) забезпечують зниження зафіксованих екозлочинів на величину до 80%.

Окрему увагу в посібнику приділено складній соціально-економічній природі взаємодії громад із кримінальними ринками. Авторка наголошує, що місцеві жителі не є однорідною масою: вони можуть одночасно страждати від руйнування природи, чинити опір злочинцям, перебувати в економічній залежності від нелегального промислу або брати участь у промислах, які формальне законодавство вважає правопорушенням, але самі громади сприймають як традиційне звичаєве виживання. Спроби зовнішніх організацій нав'язати штучні легальні альтернативи заробітку (наприклад, екотуризм) нерідко зазнають краху, оскільки їхні економічні вигоди виявляються мізерними, перехоплюються місцевими елітами та не витримують конкуренції з доходами від

[11] https://globalinitiative.net/wp-content/uploads/2026/10/Laura-Avila-Rivera-Addressing-environmental-crime-through-community-action-Handbook-GI-TOC-October-2026.pdf

браконьєрства чи нелегального намиву золота. У зв'язку з цим створення стійких господарських альтернатив має виходити не з кабінетних припущень донорів, а з пріоритетів самих громад щодо прав на землю, доступу до ресурсів і базової фізичної безпеки.

Практичний інструментарій посібника структурує процес залучення громад через поетапний аналіз контексту, оцінку балансу сил між учасниками та безпосередні виїзди на місця. На початковому етапі ключовим є дотримання гуманітарного принципу «Не нашкодь» (Do No Harm), який вимагає враховувати ризики помсти з боку озброєних угруповань і не створювати для активістів надмірної небезпеки через передчасну публічність. Картування стейкхолдерів дозволяє встановити реальний рівень довіри між населенням і владою: якщо в Індонезії виявилося можливим проводити спільні зустрічі активістів із поліцейськими, то в Бразилії через високий рівень насильства та корупції серед силовиків спільні заходи визнано небезпечними, що змусило організаторів перейти до суворо роздільних консультацій. Польові візити допомагають подолати викривлення кабінетної аналітики, виявити незареєстровані низові рухи та чесно окреслити обмежені можливості проєкту без формування завищених очікувань.

Організація багатосторонніх діалогів ґрунтується на принципах інклюзивної та рівноправної участі, що передбачають усунення нерівності, врахування позицій маргіналізованих груп, подолання мовних бар’єрів і створення безпечного психологічного середовища для всіх учасників. Показовим став досвід Мадагаскару, де замість формальних лекцій було створено майданчик для рівного обміну досвідом між низовими активістами та представниками Міністерства довкілля. Це дозволило перетворити взаємні претензії щодо корупції та бездіяльності на конкретні домовленості про створення безпечних каналів передачі оперативної інформації про контрабанду рідкісних видів флори й фауни.

У сфері матеріальної підтримки ECO-SOLVE обґрунтовує необхідність переходу до спрощеного та довірчого мікрофінансування. Стандартні бюрократичні процедури великих донорів зазвичай відсікають невеликі ініціативи через складні форми заявок. На противагу цьому програма успішно надала 22 малі гранти по €20 000 на строк від 6 до 12 місяців, спростивши прийом заявок рідними мовами в текстових редакторах і запровадивши усні консультативні звіти. Водночас авторка вказує на виклик коротких грантів: однорічне фінансування не встигає закріпити довгострокові зміни, що вимагає розробки багаторічних програм підтримки інституційної стійкості.

Завершальним елементом впливу визначено інтеграцію локальних лідерів у глобальні дипломатичні процеси. Завдяки залученню захисників природи з Бразилії, Колумбії та Індонезії до міжурядової експертної групи ООН у Відні в липні 2025 року було забезпечено пряме включення досвіду низового опору у розробку нового міжнародного протоколу проти транснаціональної екологічної злочинності, гарантуючи захист інтересів місцевих громад на наднаціональному рівні.

Висновки

Недостатність суто силових заходів без опори на громади: мілітаризовані природоохоронні заходи без залучення місцевого населення руйнують довіру та провокують конфлікти; натомість визнання прав громад і надання їм інструментів моніторингу суттєво підвищує ефективність запобігання екозлочинам.

Гнучке врахування контексту та ризиків безпеки: рівень взаємодії між громадами та правоохоронцями має визначатися суворо індивідуально; за наявності корупції та загрози розправи спільні заходи є небезпечними, що вимагає окремих захищених каналів комунікації та дотримання принципу «Не нашкодь».

Перехід до доступного та довірчого мікрофінансування: низові екологічні ініціативи потребують відмови від складної донорської бюрократії на користь малих грантів із поданням заявок місцевими мовами, гнучкою звітністю та супроводом, доповнених пошуком моделей довготривалої фінансової підтримки.

Пряме включення місцевих лідерів у міжнародні переговори: пересічні захисники територій повинні залучатися до формування національних політик і глобальних конвенцій ООН проти транснаціональної злочинності, перетворюючи локальний досвід протистояння на юридично зобов'язуючі міжнародні рамки.

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Стейблкоїни через рік після GENIUS Act: доларова домінанта та розбіжність регулювання [12]



20 жовтня 2026 року Дослідницький інститут Deutsche Bank оприлюднив аналітичну добірку Маріон Лабур і Камілли Сіазон «Стейблкоїни: що далі для криптоактивів?», присвячену стану ринку через рік після підписання в США Закону GENIUS. Автори констатують, що ринок вийшов на плато: капіталізація впродовж останніх дванадцяти місяців тримається близько 300 млрд доларів і в жовтні 2026 року становить приблизно 310 млрд доларів, тоді як у 2020 році вона дорівнювала 5 млрд. Ринок надзвичайно концентрований: близько 60% припадає на USDT, близько 23% – на USDC, а приблизно 99% капіталізації прив'язано до долара США та забезпечено переважно казначейськими зобов'язаннями США.

Ключове аналітичне спостереження стосується структури використання: більша частина обігу досі не пов'язана з реальною економічною діяльністю. Нескоригований обсяг транзакцій у 2026 році, за даними Allium, сягнув близько 100 трлн доларів, а скоригований – близько 2,42 трлн; торгівля криптоактивами залишається переважним сценарієм (близько 77%), збереження вартості становить 17–33%, платежі – 5–12%. Водночас платежі стейблкоїнами зросли зі 151 млрд доларів у 2022 році до 375 млрд у 2026 році (з початку року), понад половину становлять платежі бізнесу, а найбільшими категоріями є оплата послуг (56 млрд доларів) і виплата заробітної плати (43 млрд). У транскордонних платежах частка стейблкоїнів у 2025 році становила лише 0,31% вартості, але зростала на 64% проти 9% для фіатних платежів, а за даними МВФ відповідні потоки досягли близько 7,7% ВВП у Латинській Америці та 6,7% – в Африці й на Близькому Сході.

Роздрібне використання залишається периферійним: у гаманцях споживачів утримується близько 14% пропозиції стейблкоїнів, лише 24% споживачів, опитаних Американською асоціацією банкірів, бачать у них суттєві переваги, а самі стейблкоїни функціонують радше як дебетовий інструмент без захисту, властивого кредитним карткам. Натомість інституційне прийняття прискорюється: Mastercard розширив розрахунки до USDC і стейблкоїнів Paxos, понад 140 компаній і фінансових установ запустили у вересні 2026 року консорціумний OpenUSD, пропозиція якого за два тижні досягла 799 млн доларів, а європейські банки запускають і готують стейблкоїни, номіновані в євро та швейцарських франках. Автори прямо зазначають, що для

[12] https://www.dbresearch.com/PROD/IE-PROD/PDFVIEWER.calias?pdfViewerPdfUrl=PROD0000000000655504&rwnode=REPORT

банків і надалі критично важливими залишаються процедури KYC, ПВК/ФТ, санкційний скринінг, моніторинг гаманців і контроль шахрайства.

Окремий блок присвячено Закону GENIUS. Він встановлює для емітентів платіжних стейблкоїнів забезпечення 1:1 готівкою, казначейськими векселями строком до 93 днів, операціями репо чи фондами грошового ринку; поширює на емітентів обов'язки KYC та вимоги Закону про банківську таємницю (BSA) нарівні з банками; забороняє емітентам сплачувати відсотки; надає власникам стейблкоїнів пріоритет перед іншими незабезпеченими кредиторами; вимагає щомісячного розкриття складу резервів і окремого дозволу для емітентів із капіталізацією понад 10 млрд доларів. Закон набирає чинності не пізніше 18 січня 2027 року або через 120 днів після ухвалення остаточних підзаконних актів. Предметом гострої дискусії залишається можливість виплати дохідності через афілійованих осіб і біржі за «трибічною моделлю», а Закон CLARITY щодо структури крипторинку у вересні 2026 року не було ухвалено саме через розбіжності щодо стейблкоїнів.

Геополітичний вимір автори формулюють відверто: стейблкоїни є інструментом збереження доларового домінування та джерелом попиту на державний борг США. Сукупні вкладення емітентів у казначейські зобов'язання оцінено близько 170 млрд доларів, у тому числі близько 141 млрд у Tether, а за даними Банку міжнародних розрахунків приплив 3,5 млрд доларів у доларові стейблкоїни знижує дохідність тримісячних казначейських векселів на 2,5–3,5 базисного пункту. Серед ризиків автори називають відплив депозитів із банків, втрату прив'язки в умовах стресу, загрозу монетарному суверенітету країн, де населення переходить на доларові стейблкоїни (з відповідним застереженням ЄЦБ щодо єврозони), а також ризики протидії фінансовим злочинам через непрозорість переказів поза банківською системою.

Порівняльна таблиця регуляторних режимів показує суттєві розбіжності. У ЄС за Регламентом MiCA токени електронних грошей мають утримувати щонайменше 30% резервів на банківських депозитах, а значущі – щонайменше 60%, з вимогою до власних коштів емітента 2% та 3% відповідно; у жовтні 2026 року Європейський банківський орган класифікував USDC як значущий токен електронних грошей, а консультація щодо перегляду MiCA тривала з травня по вересень 2026 року. У Великій Британії FCA відкрило авторизацію у вересні 2026 року, режим запрацює у жовтні 2027 року, а для системних стейблкоїнів Банк Англії вимагає 30% резервів у вигляді безвідсоткових депозитів у центральному банку та 70% у державних облігаціях і вважає модель мультиемісії непридатною для системного використання, тоді як Єврокомісія розглядає її як допустиму.



Криптовалюта як паралельна фінансова система України: операція БЕБ і неврегульований ринок [13]

14 жовтня 2026 року портал «Антикор» опублікував аналітичне розслідування про тіньовий сегмент ринку віртуальних активів в Україні. Приводом стала операція Бюро економічної безпеки та Офісу Генерального прокурора проти мережі нелегальних обмінних пунктів і конвертаційних центрів, під час якої вилучено рекордну для Бюро суму готівки – 630 млн гривень, а річний обіг мережі оцінено в десятки мільярдів. Фігурантам інкримінують ухилення від сплати податків і легалізацію доходів, одержаних злочинним шляхом. Назву компанії правоохоронці не розкривали; за даними журналістів «Економічної правди», на які посилається видання, ідеться про одного з лідерів ринку обміну валют і транскордонних переказів, який активно використовує віртуальні активи.

Видання співвідносить цю операцію з масштабом ринку. За Global Crypto Adoption Index 2026 компанії Chainalysis Україна посіла 7-ме місце серед 117 країн, а за попереднім дослідженням з Україною пов'язували близько 206,3 млрд доларів криптоактивів за період з липня 2024 року по червень 2025 року, на 52% більше, ніж роком раніше. Національна комісія з цінних паперів та фондового ринку оцінює кількість користувачів віртуальних активів приблизно в 6,5 млн осіб, а потенційний річний обіг ринку – приблизно в 100 млрд доларів. Водночас, як зазначала Державна

[13] https://antikor.info/articles/869191-milliardy_v_teni_i_630_millionov_griven_nalichnymi_ot_beb_kak_kriptovaljuta_stala_paralleljnoj_finansovoj_sistemoj_ukrainy

податкова служба у серпні 2026 року, криптовалюта не має визначеного правового статусу, а спеціального порядку оподаткування операцій із нею немає, тож бюджет фактично не отримує надходжень від цього сегмента.

Аналітично найцінніша частина матеріалу – опис структури ринку та механізмів виведення коштів. Автори виокремлюють три категорії учасників: криптобіржі, онлайн-криптообмінники, які поряд з обміном здійснюють операції з фіатними коштами, картками й готівкою, та пункти «перестановок» і конвертаційні центри. Останні працюють за двома моделями. У першій клієнт переказує криптоактиви на гаманець оператора й отримує готівку за кодом у звичайному пункті обміну валют або кошти на банківську картку. У другій – «перестановці» – клієнт у Києві передає готівку чи криптоактиви, а отримувач в іншій юрисдикції, наприклад у Будапешті, отримує суму за вирахуванням комісії; фізичного переміщення готівки немає, розрахунок здійснюється заліком зустрічних потоків. Такі операції відбуваються поза валютним контролем Національного банку, ліцензуванням та увагою податкових органів і підрозділу фінансової розвідки, а самі схеми, за даними видання, використовуються зокрема у діяльності шахрайських кол-центрів.

Матеріал документує й межі адміністративного реагування. Національний банк 9 жовтня 2025 року заборонив фінансовій компанії та пов'язаним особам надавати фінансові платіжні послуги через інтернет-сервіси, оформлені під іншим брендом, а навесні 2026 року відкликав її ліцензію за безліцензійну діяльність на платіжному ринку; у листопаді 2025 року аналогічну заборону отримали ще два онлайн-обмінники. Проте, за твердженням автора, сервіси продовжували працювати, а операція БЕБ відбулася рівно через рік після першої заборони. Окремо видання наводить оцінки джерел у НБУ та правоохоронних органах щодо середньорічних обсягів операцій найбільших операторів у USDT, сукупно – майже 2 млрд доларів криптоактивів невідомого походження на рік. Ці дані мають оцінний характер і не підтверджені офіційно.

Масштаб ризику ілюструють офіційні дані Державної податкової служби, що надійшли до фінансового комітету Верховної Ради і на які посилається народна депутатка у статті для «Економічної правди»: у першому півріччі 2026 року ДПС підготувала 11 аналітичних висновків з ознаками відмивання коштів через віртуальні активи на загальну суму 9,3 млрд гривень, а також виявила 1,56 млрд гривень несплачених податків і зборів у пов'язаній економічній діяльності. У середньому на один випадок припадає близько 850 млн гривень, що, за її оцінкою, багаторазово перевищує показники інших ризикових сегментів у тому самому звіті. Фінансисти, опитані автором, виокремлюють три системні наслідки неврегульованості: використання віртуальних активів для легалізації злочинних доходів і обходу санкцій через небанківські установи, розширення тіньового сектору зі зменшенням податкових надходжень і штучний дефіцит валюти через виведення ресурсів з економіки.

Законодавчий вимір залишається ключовим. Закон «Про віртуальні активи» від 17 лютого 2022 року ухвалено, але він не набрав чинності, оскільки його дія пов'язана із внесенням змін до Податкового кодексу щодо оподаткування операцій з віртуальними активами. Законопроєкт № 10225-д, ухвалений за основу 3 вересня 2025 року, понад рік перебуває на підготовці до другого читання. Головні розбіжності стосуються розподілу компетенції: НБУ наполягає на чіткому

розмежуванні послуг і піднаглядних установ, тоді як НКЦПФР і профільний комітет пропонують модель, за якої значну частину ринку охоплює Комісія. Принциповою є й суперечка щодо обміну віртуальних активів на готівку: НБУ виступає за заборону з огляду на втрату контрольованості, ризики обходу валютних обмежень і вимог ПВК/ФТ, а позиція комітету передбачає легальні готівкові операції через офіційні каси за умови фінансового моніторингу. Ухвалення закону включено до зобов'язань у межах програми Ukraine Facility зі строком до грудня 2026 року.

Попередження SEC щодо інвестиційного шахрайства в соціальних мережах [14]



Сучасний інвестиційний ландшафт зазнав кардинальних змін: процес купівлі-продажу активів, обговорення ринкових трендів та пошук фінансових порад дедалі частіше переміщується у цифровий простір. Однак разом із зручністю та доступністю інформації з'явилися й нові, витончені загрози.

Офіційне попередження Комісії з цінних паперів і бірж США (SEC) розкриває тривожну картину: групові чати в популярних месенджерах, зокрема WhatsApp, та соціальних мережах перетворилися на головний шлюз для масштабних інвестиційних афер. Шахраї, часто використовуючи штучний інтелект та підроблені документи, будують цілі екосистеми обману, жертвами яких стають сотні роздрібних інвесторів по всьому світу, втрачаючи не лише заощадження, а й віру у фінансові інститути.

Фундаментальна небезпека полягає у самій природі групових чатів, які створюють ілюзію спільноти, експертної думки та колективного успіху. Інвестори часто приєднуються до таких груп за запрошенням знайомих або, що ще небезпечніше, автоматично після кліку на рекламне оголошення в соціальних мережах. Шахраї майстерно експлуатують цю довіру, вдаючись до різноманітних сценаріїв. Один із найпоширеніших методів — видавання себе за відомих фінансових експертів. Зловмисники створюють фейкові чати, нібито керовані відомими гуру ринку, поважними професорами чи успішними CEO. Для переконливості вони використовують технології deepfake, створюючи відео, де реальна відома особа нібито закликає до інвестицій. В інших випадках "лідер" групи може бути повністю вигаданою особою, чий образ ретельно сконструйований для створення авторитету.

Учасникам таких чатів пропонують "ексклюзивні" інвестиційні можливості, найчастіше пов'язані з нібито революційними алгоритмами штучного інтелекту для торгівлі. Шахраї переконують відкрити рахунок на спеціально створеній платформі або завантажити мобільний додаток. Важливо розуміти, що наявність додатку в офіційному магазині, як-от App Store чи Google Play, аж ніяк не гарантує його легітимності. Після реєстрації інвестор бачить на екрані віртуальні "прибутки", які зростають з неймовірною швидкістю, створюючи потужний психологічний ефект. Однак спроба вивести ці кошти стає фатальним моментом. Шахраї вимагають сплатити "податок", "комісію" або "депозит" для розблокування коштів. В іншому, ще більш цинічному сценарії, вони брешуть, що рахунок заморожено SEC або іншим державним органом, і вимагають гроші для його

[14] https://www.sec.gov/newsroom/press-releases/2026-95-sec-charges-multiple-entities-fraud-schemes-totaling-least-15-million-used-whatsapp-other-platforms

"розморожування". Після отримання платежу зловмисники, як правило, припиняють будь-який зв'язок, а інвестор залишається ні з чим, втрачаючи як обіцяні прибутки, так і початкові інвестиції.

Конкретні приклади з матеріалів SEC демонструють промисловий масштаб цієї проблеми. У справі проти Cryptoaiml Ltd. та Cryptoaiml Capital Foundation, а також TSAI Pro Ltd. та TSAI Capital Foundation, Комісія викрила схеми, які завдали збитків на суму понад 15 мільйонів доларів. З серпня 2024 по березень 2025 року ці організації створювали групові чати у WhatsApp, де, видаючи себе за інвестиційних професіоналів, поширювали згенеровані ШІ торгові "сигнали". Інвесторів заманювали на фейкові торгові платформи, де змушували переказувати криптоактиви. Для підвищення довіри шахраї навіть укладали з жертвами фіктивні угоди про управління інвестиціями та розміщували на своїх сайтах скріншоти підроблених форм D, нібито поданих до SEC. Розслідування встановило, що жодної реальної торгівлі не відбувалося, прибутки були вигаданими, а всі кошти привласнювалися.

Схема TSAI Pro Ltd. використовувала дещо іншу, але не менш підступну тактику. З вересня 2024 по березень 2025 року через свій веб-сайт, чати у WhatsApp та публічну сторінку у Facebook вони обіцяли гарантовані прибутки від депонування коштів на їхній платформі для оренди ботів зі штучним інтелектом. Інвесторам також пропонували заробляти, залучаючи інших до цієї "програми", що є класичною ознакою фінансової піраміди. Шахраї переконували, що TSAI повністю регулюється SEC, і навіть розміщували фальшивий сертифікат агентства, посилаючись на підроблену форму D. Насправді ж, як з'ясувалося, жодних ШІ-ботів не існувало, а кошти інвесторів ніколи не використовувалися для отримання прибутку.

Окрім видавання себе за експертів та створення фейкових торгових платформ, групові чати активно використовуються для проведення схем типу "pump and dump" (накачування та скидання). Шахраї поширюють у чатах неправдиві та оманливі твердження про акції публічних компаній, створюючи штучний ажіотаж і спонукаючи інвесторів до масових покупок. Це призводить до різкого зростання ціни, після чого організатори схеми продають свої активи за завищеною вартістю, а решта учасників зазнає значних збитків. Крім того, шахраї можуть видавати себе за зареєстрованих брокерів або інвестиційних радників, роблячи вигляд, що чат пов'язаний з відомою фірмою. Щоб не стати жертвою шахраїв, які видають себе за інших осіб, SEC рекомендує ретельно перевіряти особу співрозмовника, використовуючи офіційні канали зв'язку, на сайті фірми, та перевіряти фахівця через пошукову систему.

Ключовим елементом усіх цих схем є маніпуляція методами оплати. SEC закликає інвесторів бути надзвичайно обережними, якщо їм пропонують сплатити за інвестиції готівкою, особливо якщо хтось приходить додому за грошима. Не можна інвестувати з тими, хто радить брехати банку про причини зняття коштів. Тривожними сигналами є вимоги переказувати гроші на ім'я приватної особи, на рахунок іншої компанії, ніж та, в яку нібито інвестують, або на підозрілі адреси (наприклад, абонентські скриньки). Також слід насторожитися, якщо платіж призначений для покупки товарів, не пов'язаних з інвестиціями (наприклад, предметів розкоші чи меблів), або якщо вимагають переказу криптоактивів на невідомий гаманець.

Фундаментальна проблема, на яку наголошує SEC, полягає в тому, що інвестори ніколи не повинні покладатися виключно на інформацію з групових чатів при прийнятті інвестиційних рішень. Обіцянки високих гарантованих прибутків є класичною ознакою шахрайства, оскільки будь-яка інвестиція пов'язана з ризиком, і потенційно високі прибутки зазвичай супроводжуються високим ризиком.

Шахраї часто використовують складні технології, такі як deepfake та фальшиві сертифікати, щоб створити ілюзію легітимності, але їхня мета залишається незмінною — викрасти гроші. Тому критично важливо ретельно досліджувати будь-яку інвестиційну пропозицію, надіслану в груповому чаті, перевіряти реєстрацію компанії та фахівця на офіційних ресурсах і негайно повідомляти про можливі випадки шахрайства до SEC через онлайн-портал.

Лише пильність та обізнаність можуть захистити від пастки в цифровому середовищі.



Конференція ACAMS Assembly Las Vegas 2026 [15]

Щорічна конференція ACAMS Assembly, що відбулася в Лас-Вегасі з 29 вересня по 1 жовтня 2026 року, стала знаковою подією для світової спільноти з протидії фінансовим злочинам. Головним лейтмотивом заходу, який проходив під егідою провідної галузевої асоціації, стала фундаментальна трансформація індустрії: перехід від кількісного підходу, що полягав у генеруванні якомога більшої кількості звітів та сповіщень, до якісного, ціннісного підходу. Учасники та спікери одностайно наголошували, що лавина повідомлень про підозрілі транзакції не зупиняє злочинців; натомість це роблять кращий інтелект, глибокий аналіз ризиків та реальне партнерство між приватним і державним секторами.

Відкриваючи конференцію, виконавчий директор ACAMS Ніл Штерналь звернувся до історичного контексту, нагадавши, що трагедія 11 вересня 2001 року кардинально змінила світ і професію фахівців з фінансового моніторингу. Вона дала поштовх до створення USA PATRIOT Act, який надав нові інструменти для обміну інформацією та переслідування недобросовісних гравців. Штерналь підкреслив, що хоча за 25 років було розбудовано безпрецедентні спроможності для виявлення незаконних фінансових потоків, місія залишається незмінною: «Зосереджуйтеся на загрозі. Йдіть за грошима». Однак, за його словами, фокус вимагає усвідомлення того, що завтрашні загрози не будуть схожі на вчорашні. Технологічні прориви та зростаюча витонченість кримінальних мереж вимагають від галузі постійного навчання, пильності та готовності кинути виклик звичним методам роботи.

Центральною темою першого дня стала роль Служби боротьби з фінансовими злочинами (FinCEN) Міністерства фінансів США. Виконуюча обов'язки директора FinCEN Дженна Касанова у своєму першому публічному виступі окреслила курс на більш проактивний мандат відомства. Вона зробила безпрецедентну заяву про зворотний зв'язок: якщо фінансова установа витрачає значні ресурси на діяльність, яка не має великої цінності для правоохоронних органів, FinCEN зобов'язана повідомити про це, щоб установа могла перерозподілити ресурси туди, де вони

[15] https://www.acams.org/en/opinion/volume-value-takeaways-acams-assembly-las-vegas-2026

справді потрібні. Її заклик був простим, але глибоким: нагадати всім, що літера «N» у назві FinCEN означає «Network» (Мережа), підкреслюючи важливість колективної взаємодії.

Ця теза знайшла продовження під час круглого столу регуляторів, де представники FinCEN, Управління контролера грошового обігу (OCC), Федеральної корпорації страхування депозитів (FDIC), Федеральної резервної системи та Національної адміністрації кредитних спілок (NCUA) обговорили питання оцінки ризиків, управління ризиками фінтех-компаній та регулювання цифрових активів. Кеннет Корс з OCC наголосив, що розробка програми неможлива без розуміння власних ризиків, а Крісті Корнелл-Пейп з FDIC додала, що саме оцінка ризиків є головним інструментом. Регулятори закликали установи адаптувати свої підходи до конкретного профілю ризику, приділяти належну увагу нагляду за сторонніми фінтех-партнерами та балансувати інновації з управлінням ризиками, особливо в таких нових сферах, як верифікація цифрової ідентичності, стейблкоїни та банківське обслуговування легального бізнесу з марихуаною.

Окрема увага на конференції була приділена питанню національної безпеки та боротьби з тероризмом. Спеціальна презентація, присвячена 25-й річниці терактів 11 вересня, продемонструвала, наскільки децентралізованими та цифровими стали терористичні загрози. Тайлер Хатчер, виконавчий директор з глобальних операцій Служби кримінальних розслідувань IRS (IRS-CI), пояснив, як законодавство дозволяє правоохоронцям застосовувати спеціальні інструменти, зокрема знижені пороги для конфіскації активів, коли йдеться про терористичні організації. На його думку, справжнє руйнування терористичних мереж відбувається саме тоді, коли вдається підірвати їхні фінанси, і USA PATRIOT Act робить цей процес значно ефективнішим, дозволяючи діяти на випередження.

Другий день конференції ознаменувався виступом Коліна М. Макдональда, першого помічника генерального прокурора новоствореного Національного відділу боротьби з шахрайством Міністерства юстиції США. Лише за 180 днів цей підрозділ виріс з одного співробітника до приблизно п'ятисот, зосередившись на шахрайстві у сфері охорони здоров'я, державних пільг, торгівлі та відновленні активів. Макдональд назвав шахрайство в Америці кризою, яку країна не може дозволити собі програти, наголосивши, що мета полягає не лише у поверненні грошей, а й у відновленні надії та довіри. Він прямо заявив, що перемога неможлива без приватного партнерства та співпраці з індустрією. Ця теза перегукується з виступом Ерін Вест, засновниці Operation Shamrock, яка простежила шлях організованої злочинності з Китаю від підпільних ферм з вирощування марихуани в Оклахомі до шахрайських центрів у Південно-Східній Азії. Вона навела приклад колишнього голови Асоціації банкірів Канзасу, який зараз відбуває покарання у федеральній в'язниці, закликавши фахівців «думати на сім кроків вперед».

Не менш важливою була дискусія щодо реформування підходу до Повідомлень про підозрілу діяльність (SAR). Панель, присвячена роз'ясненням FinCEN щодо SAR, висвітлила жовтневе керівництво 2025 року, яке мало на меті не розширити, а уточнити існуючі вимоги. Кейсі Коен, директор з питань правозастосування FinCEN, наголосила, що мета відомства — уникнути надмірного регуляторного тягаря. Вона зазначила, що активність поблизу порогу звіту про

валютні операції (CTR) не вимагає автоматичної подачі SAR про структурування, перегляд поточної діяльності не є обов'язковим, а установи не зобов'язані документувати рішення про неподання SAR. Ден Стіпано з Davis Polk застеріг, що практичний ефект цих змін залежатиме від того, як учасники застосовуватимуть нові правила. Коен підкреслила, що зміни покликані підтримати більш ризик-орієнтований та ефективний підхід до звітування, а не стимулювати подання додаткових звітів.

Питання боротьби з картелями та подальшого розслідування фінансових потоків також було в центрі уваги. Тайлер Хатчер з IRS-CI та Дерек Дженсен з ФБР пояснили, що ліквідація лідерів картелів, як правило, фрагментує організації, а не припиняє їхню діяльність. Хатчер наголосив, що багато індикаторів фінансових злочинів, ефективних десятиліттями тому, залишаються актуальними й сьогодні, включаючи відмивання грошей через торгівлю, фіктивні компанії, сервіси грошових переказів та китайські мережі з відмивання коштів. Він закликав авторів SAR чітко пояснювати, чому діяльність вважається підозрілою, та обирати найбільш відповідну категорію, наголошуючи, що обґрунтована оцінка є важливішою за досягнення ідеального висновку.

Третій день конференції зосередився на людському факторі та технологічній стійкості. Сандіп Абрахам зі Стенфордської лабораторії Starling Lab for Data Integrity поділився результатами річного дослідження, під час якого він взаємодіяв з шахрайськими мережами через вигаданих персонажів. Він описав, як шахраї продають рекламні акаунти, допомагають отримати американські регуляторні реєстрації, а також надають скрипти, які вчать жертв, що говорити банківським працівникам. Однак, за його словами, єдиним місцем, де шахраї стабільно зазнають невдачі, є момент, коли касир банку просить надати документи. «Інвестуйте в своїх касирів, інвестуйте в операції з обслуговування клієнтів, — сказав він, — тому що часто саме вони є тією перепоною».

Питання кібербезпеки та шахрайства також були висвітлені в контексті адаптації до нових реалій. Корі Говард, директор з комплаєнсу та головний комплаєнс-офіцер Coinbase US, зазначив, що криптовалюта перестала бути переважно роздрібним бізнесом для спекулянтів, перетворившись на інституційний ринок та ринок стейблкоїнів, що вимагає зміни методів розслідування та наративних структур SAR. Брайан Сміт, старший віце-президент з розслідувань FINRA, наголосив на необхідності стійкості бізнес-процесів, сформулювавши це через «два П»: «Підготовка» (Prepare) та «Партнерство» (Partner). Він закликав організації заздалегідь розробляти плани реагування на кіберінциденти, проводити навчання та завчасно встановлювати контакти з правоохоронними органами та іншими фінансовими установами для швидкої координації дій у разі атаки.

Підсумовуючи захід, учасники дійшли спільного висновку: установи, які найкраще підготовлені до майбутнього — це ті, що знають свої ризики, розуміють свої дані та тісно співпрацюють з партнерами по обидва боки державно-приватного кордону.



Еквадор: чому мілітаризація не рятує [16]

Останні роки Еквадор, колись відомий як один із найбезпечніших куточків Латинської Америки, перетворився на епіцентр кривавої боротьби з організованою злочинністю. Президент Даніель Нобоа, який прийшов до влади на тлі стрімкого зростання насильства, обрав шлях безпрецедентної мілітаризації та жорсткого силового тиску на кримінальні угруповання. Однак, як свідчить аналіз поточної ситуації, попри гучні арешти та розгортання армії на вулицях і в тюрмах, країна стикається з глибокою кризою, де тимчасові перемоги обертаються новими, ще складнішими викликами. Три роки потому стає очевидним, що стратегія "залізного кулака" не здатна забезпечити стійкого зниження рівня насильства, а лише прискорює фрагментацію злочинного світу, породжуючи нові загрози.

Минулий рік став для Еквадору трагічним рекордом: країна зафіксувала найвищий рівень вбивств у Латинській Америці. Хоча поточного року спостерігається певне зниження кількості вбивств, Еквадор все ще прямує до одного з найкривавіших років у своїй історії. Причини цього стрімкого падіння в безодню насильства криються у комплексі взаємопов'язаних факторів: стрімке зростання незаконного обігу кокаїну, безпрецедентна корупція, втрата державного контролю над в'язницями та, що найважливіше, глибока фрагментація самих злочинних угруповань.

У січні 2024 року, після зухвалого захоплення телевізійного ефіру членами угруповання "Тігеронес" та втечі з в'язниці лідера "Чонерос" Хосе Адольфо Макіаса, відомого як "Фіто", президент Нобоа оголосив в країні "внутрішній збройний конфлікт". Це рішення дозволило йому

[16] https://insightcrime.org/news/why-ecuador-is-losing-its-fight-against-organized-crime/

офіційно визнати 22 кримінальні угруповання терористичними організаціями та розгорнути проти них повномасштабну військову операцію. Варто зазначити, що такий підхід знайшов підтримку і за океаном: Сполучені Штати також визнали "Чонерос", "Тігеронес", "Лобос" та "Чоне Кіллерс" іноземними терористичними організаціями.

Адміністрація Нобоа демонструє відверте бажання тісно координувати свої дії з Вашингтоном, зокрема з адміністрацією президента Дональда Трампа, для подолання кризи. Еквадорський лідер публічно захищав летальні удари США по суднах, підозрюваних у транспортуванні наркотиків у відкритому морі, та координував спільні операції з американськими військовими на території Еквадору. Однак ці дії викликають серйозні питання щодо прозорості та точності розвідки. Зокрема, інцидент із бомбардуванням об'єкта, який офіційні особи назвали табором наркоторговців, викликав скандал: місцеві жителі та правозахисники у коментарях для New York Times заявили, що насправді це була звичайна ферма. Це свідчить про те, що прагнення продемонструвати силу та солідарність із новою мілітаристською парадигмою США може призводити до трагічних помилок та втрати довіри населення.

Попри постійний тиск з боку сил безпеки, який призвів до низки гучних арештів, Еквадору не вдалося конвертувати ці точкові перемоги у системний успіх. Затримання у червні 2025 року лідера "Чонерос" "Фіто", якого згодом екстрадували до США, арешт лідера "Лобос" Вільмера Чаваррії на прізвисько "Піпо" в Іспанії у листопаді 2025 року, а також затримання ватажка "Тігеронес" Вільяма Хоффре Альсівара Баутісти на прізвисько "Віллі" — всі ці події мали б послабити злочинні мережі. Однак доля "Віллі" демонструє всю складність ситуації: незважаючи на арешт в Іспанії у жовтні 2024 року, він був звільнений у грудні наступного року, оскільки еквадорська влада не змогла гарантувати безпеку його утримання у в'язниці вчасно до дедлайну, встановленого іспанською стороною для екстрадиції.

Ці "маленькі перемоги" не лише не зупинили насильство, а й каталізували процес фрагментації, який розпочався ще з розколу "Чонерос". Позбавлені єдиного керівництва, "Чонерос" змушені боротися за збереження єдності та національного впливу, що призводить до внутрішніх чвар. Арешти або загибель лідерів вищої та середньої ланки спровокували запеклу боротьбу за владу всередині таких угруповань, як "Чоне Кіллерс", "Лобос" та "Тігеронес". Замість консолідованого ворога, з яким можна вести переговори або боротися, держава отримала безліч дрібних, жорстоких та непередбачуваних угруповань, які борються за контроль над територіями та ринками. Ця фрагментація робить ситуацію ще більш вибухонебезпечною, оскільки нові лідери часто є більш агресивними та менш схильними до будь-яких домовленостей.

Окремою критичною проблемою залишається пенітенціарна система. Нобоа зробив пріоритетом безпеку в'язниць, наказавши військовим взяти під контроль внутрішню безпеку в січні 2024 року та перевівши сотні ув'язнених до новозбудованої в'язниці максимально суворого режиму "Ель Енкуентро" у листопаді 2025 року. Однак, незважаючи на ці заходи, умови утримання залишаються жахливими, а рівень насильства не знижується. За офіційними даними, у 2025 році в пенітенціарних установах було зафіксовано більше підтверджених випадків насильницької смерті, ніж за два попередні роки разом узяті. Це свідчить про те, що в'язниці продовжують

функціонувати як центри кримінальної активності та розповсюдження насильства, а не як установи виправлення.

Усвідомлюючи обмеженість суто військового підходу, у липні 2026 року уряд Нобоа представив новий план безпеки. Він передбачає певні корективи в поточній мілітаристській стратегії, обіцяючи приділити увагу соціально-економічним умовам, які сприяють зростанню злочинності, зокрема шляхом зниження рівня безробіття та скорочення кількості учнів, які залишають школу. Це можна розцінювати як обережний крок до більш комплексного підходу. Однак, незважаючи на ці заяви, новий план все ще робить значний акцент на міжнародній співпраці. Тісний союз Нобоа з адміністрацією Трампа та його підтримка ініціативи "Щит Америки" свідчать про те, що сила, ймовірно, залишиться домінуючим елементом еквадорської політики.

Таким чином, Еквадор опинився у складній пастці: жорсткі заходи призводять до фрагментації банд і тимчасових арештів, але не вирішують корінних проблем, водночас створюючи ризики надмірного застосування сили та залежності від зовнішніх гравців. Перспективи подолання кризи залишаються туманними, адже країна балансує між необхідністю рішучих дій та потребою у глибоких соціальних реформах, які неможливо провести виключно військовими методами.

Ваша думка важлива!

Які зміни в організації звітування дозволили б суб'єктам первинного фінансового моніторингу й Держфінмоніторингу втримати якість аналізу за швидкого зростання кількості повідомлень?

Які поведінкові індикатори дозволили б банкам і платіжним установам відрізняти P2P-збори, що прикривають фінансування тероризму, від легітимних волонтерських зборів?

Як узгодити інтереси бізнесу, що потребує попереднього фінансування для завершення будівництва, із заходами фінансової безпеки, аби новобудови не ставали спекулятивним прихистком для тіньового капіталу?

Як банкам відрізняти ризики фінансування конфлікту від загального географічного ризику прифронтових регіонів, щоб не обмежувати доступ їхніх мешканців до фінансових послуг?

Як українським банкам поєднати санкційний скринінг криптогаманців клієнтів, які розраховуються в USDT, із вимогами валютного контролю?

Якими контрольними механізмами має супроводжуватися можливий легальний обмін віртуальних активів на готівку, щоб він не відтворював схеми «перестановок» поза валютним контролем?

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-2026-43

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