



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

Елеонора Рузвельт

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій



Звіт FATF щодо професійного відмивання коштів, підпільного банкінгу та хавали ¹

Група з розробки фінансових заходів боротьби з відмиванням коштів (FATF) оприлюднила звіт «Investigating Professional Money Laundering, Underground Banking, and the Use of Hawala and Other Similar Service Providers». Проект вели у співголозуванні Німеччина та Саудівська Аравія; до проектної групи увійшли 22 члени FATF, 7 членів регіональних груп за типом FATF та три спостерігачі — Європол, Інтерпол і Управління ООН з наркотиків і злочинності. Документ оновлює й істотно розширює звіт FATF 2013 року про роль хавали та подібних постачальників послуг у відмиванні коштів і фінансуванні тероризму, зміщуючи фокус із самої хавали на ширшу конструкцію — професійне відмивання коштів (Professional Money Laundering, далі — PML) як самостійну послугу, у якій підпільний банкінг є інфраструктурним елементом. Для України документ має практичну вагу щонайменше з двох причин: він уперше системно описує стик неформальних мереж переказу вартості з регульованим сектором, і саме цей стик є основною точкою виявлення для банків та інших суб'єктів первинного фінансового моніторингу.

Методологія поєднує дослідження, два структуровані опитування та експертні консультації. Перша анкета була розіслана у вересні 2025 року і збрала відповіді 44 юрисдикцій, друга — у

¹ <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/pml-underground-banking-hawala-fatf-report-2026.pdf.coredownload.pdf>

лютому 2026 року, ще від 11 юрисдикцій; сукупно в дослідженні взяли участь 46 юрисдикцій з усіх регіонів Глобальної мережі. Анкети збирали не лише статистику, а й національні оцінки ризиків, кейси та приклади належної практики. Додатково проведено експертні обговорення на засіданнях у жовтні 2025 і лютому 2026 років та спільну зустріч експертів в Аккрі (Гана) 4–6 листопада 2025 року; проєкт двічі проходив рецензування Глобальною мережею — у лютому й квітні 2026 року. Структура звіту складається з трьох частин: поточний стан (ролі, методи, типології), виклики для виявлення, розслідування та переслідування, і належні практики для компетентних органів. Методологічне застереження, яке варто тримати на увазі, автори формулюють самі: більшість юрисдикцій не має надійних кількісних даних про профілі постачальників і користувачів, тому частки в опитуванні відображають рівень обізнаності органів, а не вимірюють поширеність явища.

Емпірична картина поширеності є найсильнішою частиною документа. Майже 90 % юрисдикцій, які відповіли на анкету, повідомили про наявність систем підпільного банкінгу та HOSSP (хавала та інші постачальники аналогічних послуг) на своїй території; понад 60 % визначають їх як підвищений ризик ВК/ФТ у національних оцінках ризиків; понад 80 % відносять ці системи до основних каналів і технік професійного відмивання; майже 70 % фіксують появу нових типологій і тенденцій. Половина юрисдикцій — членів FATF і майже 30 % юрисдикцій Глобальної мережі, оцінених у четвертому раунді взаємних оцінювань (2014–2024 роки), визнали HOSSP високоризиковими. Термінологічна фрагментація вимірюється так само: 67 % юрисдикцій прямо вживають термін «хавала», решта користується локальними назвами — *hundi*, *fei qian*, *hui kuan*, *padala*, *osusu*, *chika ginko*, *box hand*. Географічно PML найчастіше фіксується в Азії, Західній Європі та Західній Африці. Прогноз респондентів однозначний: ризик використання цих систем для професійного відмивання зростатиме, і причини цього — не кон'юнктурні, а структурні: притаманні властивості систем, сприятливий контекст і доведена здатність адаптуватися до технологічних змін.

Анатомію мережі звіт розкладає на п'ять елементів: підпільні банкіри (хаваладари), які контролюють готівкові пули та реєстри й зазвичай працюють із прикриттям у вигляді легального допоміжного бізнесу; самі пули — резерви для забезпечення негайної платіжної спроможності, що формуються з комерційних потоків, легальних переказів мігрантів і злочинних доходів; клієнти; винагорода; механізми клірингу. Комісія становить приблизно від 0,5 % до 5 %, причому вона прямо ризик-орієнтована: за кошти, щодо яких є підозра у злочинному походженні, беруть більше. Із цього випливає спостереження, яке має самостійну аналітичну цінність: професійний відмивач отримує оплату з обох боків операції — від злочинного клієнта і від клієнта підпільного банкінгу за той самий переказ, — що дозволяє йому знижувати комісію за саме відмивання і робить обслуговування злочинних потоків структурно прибутковим. Аутентифікація здійснюється через токен, найчастіше — унікальний серійний номер банкноти, який передається ланцюгом і має бути пред'явлений при отриманні. Над мережею стоять контролери (*money brokers*, суперфасилітатори, міжнародні мережі контролерів), які координують кореспондентів, збирачів і передавачів у різних юрисдикціях, встановлюють ціни, кредитні ліміти, канали розрахунку й ліміти ліквідності. Прикриттям слугують імпортно-експортні та торговельні компанії, юридичні й аудиторські практики, ріелтори, крамниці, АЗС, ресторани, формальні MVTs, торговці дорогоцінними металами й камінням, туристичні агенції, автосалони, автомийки, казино, магазини мобільного зв'язку, обмінники та будівельні компанії.

Розрахункові механізми систематизовано у п'ять модальностей, і ця систематизація є найбільш придатною до практичного перенесення. Перша — просте двостороннє взаємозарахування, за якого симетричні потоки взагалі не потребують фізичного або фінансового розрахунку. Друга — трикутні та мережеві розрахунки, у яких зобов'язання між двома операторами гаситься через третього, що має надлишкові баланси, а також кліринг через непов'язаних третіх осіб. Третя — розрахунок вартістю: готівкові кур'єри; торговельні схеми з завищенням і заниженням інвойсів, фальсифікованими товаросупровідними документами та фантомними відвантаженнями; товарні заліки через споживчі товари, золото, дорогоцінні

метали й предмети розкоші; тристоронній обмін і «дзеркальні» операції, за яких злочинні кошти в одній юрисдикції обмінюються на місцеві кошти осіб, які прагнуть обійти валютні обмеження; механізми паралельного валютного курсу типу чорного ринку песо. Четверта — розрахунок через формальні канали: компанії-оболонки, рахунки грошових мулів, віртуальні IBAN, дотові й пакетні перекази, смурфінг (внесення злочинної готівки на рахунок нічого не підозрюючого добросовісного відправника, чий власний переказ гасить закордонне зобов'язання), а також кампанії на краудфандингових платформах, що створюють легальний платіжний наратив. П'ята — цифровий розрахунок з використанням віртуальних активів, передусім стейблкоїнів (USDT, USDC, DAI), онлайн-провайдерів платіжних послуг і цифрових банківських платформ.

Найзначнішою новацією порівняно зі звітом 2013 року автори називають «цифрову хавалу» — використання цифрових технологій для координації, виконання, розрахунку або приховування неформального переказу вартості. Її описано шістьма конфігураціями: цифрова координація за традиційного розрахунку (шифровані месенджери WhatsApp, Telegram, Signal за збереження готівкових і торговельних розрахунків); цифровий клієнтський інтерфейс за традиційного міжоператорського розрахунку (банківські перекази, мобільні гаманці, фінтех-застосунки, системи миттєвих платежів на вході, традиційний кліринг усередині); розрахунок у віртуальних активах через VASP, позабіржових брокерів і платіжні установи за схемою «збір фіату — конвертація у ВА — переказ між гаманцями — зворотна конвертація»; вбудовування в регульовану цифрову інфраструктуру (провайдери платіжних послуг, фінтех-платформи, віртуальні IBAN, онлайн-банкінг); застосування передових технологій, зокрема штучного інтелекту для автоматичного структурування операцій, динамічної маршрутизації через дропові рахунки та швидкісних конвертацій «фіат — ВА»; і «хавала-застосунки» — зв'язки шифрованих месенджерів, хмарних сховищ, соціальних мереж, VASP, кредитних застосунків та ігрових платформ. Наслідки цифровізації FATF формулює у чотирьох вимірах: зростання швидкості, зростання непрозорості через перенесення записів у шифровані й ефемерні середовища, ускладнення нашарування та розширення географічного охоплення й стійкості мереж.

Другою наскрізною тенденцією є професіоналізація: перехід від общинних домовленостей до структурованих сервісних інфраструктур відмивання зі спеціалізованими ролями, стандартизованими процесами, ієрархічними або комірковим типом конфігураціями, корпоративним обліком (зокрема цифровими реєстрами) і залученням логістичних та технічних фахівців. До схем систематично залучаються професійні посередники — юристи, бухгалтери, аудиторі, нотаріуси, агенти зі створення компаній, фінансові консультанти, ріелтори, а також казино й джанкет-оператори. Третьою тенденцією є глибока інтеграція з формальним фінансовим сектором: замість роботи повністю поза регульованими каналами оператори комбінують неформальні механізми переказу вартості з легальною фінансовою інфраструктурою, експлуатуючи регуляторні асиметрії та наглядові «сліпі зони». Точками входу й виходу слугують формальні рахунки, фінтех-платформи, провайдери платіжних послуг, онлайн-банкінг і цифрові гаманці; окремо виділено віртуальні IBAN, які маскують справжнє призначення коштів і надають транскордонним переказам вигляду внутрішніх, передплачені картки й ваучери, а також мобільні платіжні термінали, розгорнуті через співучасні або фіктивні бізнеси для проведення фіктивних операцій. Близько 80 % юрисдикцій повідомляють, що ці схеми застосовуються в поєднанні з іншими методами відмивання, утворюючи гібридні ланцюги з торговельним відмиванням, компаніями-оболонками, віртуальними активами, нерухомістю, предметами розкоші й дорогоцінними металами.

Спектр предикатних злочинів у звіті принципово розширено. Найчастіше згадуються наркоторгівля, шахрайство, контрабанда товарів, ухилення від сплати податків, кіберзлочинність, корупція, торгівля людьми та незаконне переправлення мігрантів; далі — фінансування тероризму, незадекларована праця, незаконні азартні ігри, ухилення від санкцій, злочини у сфері інтелектуальної власності, екологічні злочини, незаконний видобуток ресурсів, вимагання, викрадення заради викупу. Ключове формулювання звучить так: через

підпільний банкінг і HOSSP можуть відмиватися доходи практично від усіх видів злочинів. Окремий блок присвячено фінансуванню тероризму: звіт підтверджує висновок 2013 року про HOSSP як значну й сталу вразливість і посиляється на Комплексне оновлення FATF щодо ризиків ФТ, за яким ці системи залишаються основним методом ФТ у високоризикових контекстах — для отримання пожертв з-за кордону, переміщення коштів між регіональними хабами, переказу вартості до зон конфлікту та з них і підтримки децентралізованих осередків. Нові типології ФТ поєднують HOSSP із контрабандою готівки, зловживанням неприбутковими організаціями, доходами від злочинної діяльності та торговельним фінансуванням тероризму; географічно це Близький Схід, Азія і Західна Африка, причому потоки змішуються з легальними переказами діаспори, що додатково ускладнює виявлення.

Кейси, наведені у звіті, ілюструють кожну з описаних модальностей. Нідерландська операція «Klaver» стосувалася однієї з найбільших мереж підпільного банкінгу, виявлених у країні та Європі: за вісім місяців мережа опрацювала близько 500 млн євро злочинних доходів, переважно в інтересах наркоторговельних організацій, за схемою «кур'єри — склад для перерахунку й обліку — перерозподіл іншим злочинним акторам». Бельгійські справи показують поєднання злочинних доходів із попитом легального бізнесу на незадекларовані кошти для виплати зарплат «у конвертах» у будівництві, клінінгу й транспорті, а також кур'єрські розрахунки за кокаїновими потоками з ланцюгом Бельгія — Нідерланди — Іспанія — Марокко — Південна Америка — Дубай. Індійський кейс демонструє транснаціональну схему з компаніями-оболонками, заниженням інвойсів, круговою торгівлею та вихідними переказами. Турецький кейс фіксує перехід від готівкової хавали до технологічних моделей на стейблкоїнах: мережа «цифрової хавали» фінансувала членів ІДІЛ, під час обшуків вилучено близько 57 250 доларів США. Італійський кейс описує інтеграцію схем підпільного банкінгу з регульованою платіжною інфраструктурою — віртуальними IBAN, провайдерами платіжних послуг, платіжними агентами й передплаченими картками — у зв'язку з китайськими мережами підпільного банкінгу. Японський кейс стосується автоматизованих функцій переказу, налаштованих на списання коштів із дропових, третіх або скомпрометованих рахунків після досягнення заданої суми, а німецький — використання краудфандингових і донорських кампаній для створення легального платіжного нарративу.

Виклики згруповано у чотири блоки. Термінологічна фрагментація перешкоджає узгодженому регуляторному й правозастосовному реагуванню та порівнянності даних. Прогалини у знаннях зумовлені обмеженою видимістю: відсутність надійних кількісних даних про постачальників і користувачів не дозволяє будувати обґрунтовані національні оцінки ризиків і прив'язувати їх висновки до конкретних наглядових дій. Регуляторні асиметрії створюють арбітражні можливості як між юрисдикціями, так і всередині них; сюди ж віднесено ефект де-рискінгу, за якого виключення цілих секторів і категорій клієнтів з формального обслуговування виштовхує в неформальні канали не лише злочинні, а й цілком легальні потоки переказів мігрантів, а разом із ними — і частину

Висновки:

- **Майже 90 % юрисдикцій фіксують підпільний банкінг і HOSSP на своїй території**, понад 80 % відносять їх до головних каналів професійного відмивання, а половина членів FATF за IV раундом оцінювань визнала їх високоризиковими.
- **Комісія 0,5–5 % є ризик-орієнтованою, а професійний відмивач заробляє з обох боків операції** — обслуговування злочинних потоків структурно прибутковіше за легальні перекази, і це зміщує стимули всієї мережі.
- **«Цифрова хавала» описана шістьма конфігураціями — від шифрованої координації за традиційного розрахунку до розрахунків у стейблкоїнах (USDT, USDC, DAI); близько 80 % юрисдикцій бачать гібридні ланцюги з TBML і компаніями-оболонками.**
- **FATF прямо пов'язує де-рискінг зі зростанням тіньового сегмента і радить поєднувати правозастосування з фінансовою інклюзією**, а нагляд зосереджувати на точках стику з регульованим сектором (vIBAN, PSP, VASP, дропи).

самих легальних постачальників MVTs. Нарешті, операційні труднощі виявлення й розслідування охоплюють фрагментованість і стійкість мереж, брак стандартизованих індикаторів, складність моніторингу цифрових компонентів, обмеженість традиційних слідчих підходів, перешкоди в міжнародному співробітництві та доказові труднощі у встановленні умислу й відстеженні повного ланцюга відмивання.

Належні практики звіт вибудовує навколо шести стратегічних підходів: створення чіткого правового й регуляторного середовища, що стримує неавторизовану діяльність; перехід від транзакційного правозастосування до системного руйнування ланцюгів професійного відмивання; створення спеціальних механізмів внутрішньодержавної координації; концентрація уваги на точках перетину неформальних мереж із формальною фінансовою системою; використання передових наглядових і слідчих технік і технологій; залучення відповідних громад і секторів. Операційно це розгортається в конкретні заходи: формальні мережі зворотного зв'язку між компетентними органами та підзвітними суб'єктами, цільові державно-приватні партнерства, канали публічного інформування та повідомлення, виявлення за межами традиційних інструментів, ведення централізованої статистики й реєстрів справ, включення підпільного банкінгу та HOSSP до національних оцінок ризиків як окремої складової з прив'язкою висновків до політики й нагляду, поширення контролю на визначені нефінансові установи та професії, поглиблення міжнародного співробітництва і — що варто відзначити окремо — поєднання правозастосування із пропорційними заходами фінансової інклюзії, аби зменшити попит на нелегальні канали. Заклик до дій сформульовано як ефективна імплементація Рекомендацій 3, 5 і 14 та підвищення результативності за безпосередніми результатами 3 і 7.

Острів Мен про перший рік дворічної програми наглядового залучення у сфері ПВК/ФТ/ФР²

Управління фінансових послуг острова Мен (Isle of Man Financial Services Authority, далі — Управління) оприлюднило документ «AML/CFT Supervisory Priorities. Year One Update». Це проміжний звіт про виконання дворічної програми наглядового залучення у сфері ПВК/ФТ/ФР, оголошеної Відділом нагляду з ПВК/ФТ в березні 2025 року. Звіт підсумовує роботу, виконану у 2025/26 фінансовому році, і наперед окреслює пріоритети на 2026/27 рік. Голова Відділу Ешлі Вайт (Ashley Whyte) прямо позиціонує публікацію як виконання раніше взятого зобов'язання звітувати на середині програми.

Модель нагляду описана через Supervisory Methodology Framework: Управління оцінює притаманний і залишковий ризик фірми, виводить рейтинг ризику фінансової злочинності, і саме цей рейтинг визначає інтенсивність наглядового залучення. Ресурси Відділу сконцентровані на суб'єктах із високим і середньо-високим рейтингом; фірми з нижчим рейтингом отримують менш інтенсивний підхід із наголосом на тематичній роботі, роз'ясненні та підвищенні обізнаності. Принципово, що модель залучення описана як відокремлена від моделі нагляду, керованої масштабом впливу (impact-led), яку застосовують інші наглядові підрозділи Управління. Інструментарій охоплює виїзні та невиїзні перевірки, тематичні огляди, запити даних, комплаєнс-зустрічі, галузеві заходи, воркшопи та публікацію настанов. Загальні наглядові пріоритети Управління на 2025–2027 роки згруповані у чотири теми: протидія фінансовій злочинності; культура, врядування та управління ризиками; фінансова й операційна стійкість; якість наглядових даних.

Секторальна тематична робота у першому році програми охоплювала два сегменти ВНУП. Висновки другої фази огляду щодо агентів з нерухомості опубліковано в липні 2025 року: до виїзних перевірок відібрано 12 агентів, під час яких переглянуто 276 клієнтських справ; сукупна вартість операцій сектору за 2023 рік становила 532,85 млн фунтів стерлінгів. Чотири

² <https://www.iomfsa.im/media/3646/aml-cft-supervisory-priorities-year-one-update-august-2026.pdf>

напрями перевірки — оцінка ризиків діяльності, оцінка ризиків клієнта, встановлення нових ділових відносин і навчання персоналу. Друга фаза огляду щодо кредиторів охопила 20 фірм і була сфокусована вужче — на належній та посиленій належній перевірці клієнта, включно з установленням джерела коштів і джерела добробуту. Результати подано у вимірних величинах: 94 % відповідності пункту 4 Кодексу ПВК/ФТ 2019 року («Процедури і контроль») серед 20 інспектованих фірм і 90 % відповідності вимозі щодо проведення посиленої належної перевірки; сектор із 37 кредиторів обслуговує 5 383 клієнти. Обидва звіти побудовані за однаковою логікою: приклади належної практики поряд із зонами, де фірмам слід розглянути необхідність дій.

Робота з постачальниками послуг, пов'язаних з обігом віртуальних активів (VASP), у першому році зосереджувалася на законодавчому середовищі. Зміни до рамки ПВК/ФТ щодо сектору VASP набрали чинності з 20 березня 2026 року; вони стали результатом консультацій з галуззю і мали на меті забезпечити пропорційне та ризик-орієнтоване застосування Кодексу про Travel Rule 2024 року при збереженні відповідності міжнародним стандартам. Окремо Кодекс про Travel Rule підведено під дію наявних регламентів про цивільні санкції у сфері ПВК/ФТ — тобто санкційна спроможність щодо порушень Travel Rule з'явилася до, а не після тематичної перевірки сектору. Управління оновлює галузеві настанови з урахуванням змін і опублікованої у 2026 році національної оцінки ризиків щодо віртуальних активів, готує звіт за відповідями VASP щодо застосування Travel Rule, а повноцінний тематичний проєкт із цим сектором відкладено до завершення періоду «вкорінення» нових вимог. Наведені показники дають профіль сектору: 82,82 % клієнтів VASP острова Мен є резидентами Великої Британії, 2,42 % клієнтів оцінено як високоризикових, а частка публічних діячів становить 0,06 %.

Основна тематична робота охоплювала фінансування тероризму, фінансування розповсюдження та санкції. Тематичний огляд щодо ФТ розпочато у 2026 році, перевірки стартували у квітні й триватимуть 12–18 місяців; підхід свідомо змінено порівняно з початковою пропозицією 2025 року — інспекційний план побудовано на наявних даних замість розсилання додаткової анкети, аби зменшити навантаження на галузь. Щодо ФР, на анкету Управління відповіли 586 фірм острова: 92,7 % повідомили про задовільний рівень розуміння ризику фінансування розповсюдження, проте лише 66,21 % підтвердили, що проводять відповідне навчання персоналу; протягом 2025/26 року здійснено 7 перевірок. Роз'яснювальну програму з ФР Управління вело спільно з Комісією з нагляду за гральним бізнесом, підрозділом фінансової розвідки, Кабінетом Міністрів та Відділом митниці та

імміграції Казначейства, публікуючи відеоматеріали й брошури з поясненням суті ФР, оглядом санкційних режимів, індикаторами та типологіями для фінансового й нефінансового секторів; підсумковий тематичний звіт очікувався у серпні 2026 року. Санкційна тематика дала найкритичніші результати: за 98,5 % відповідей на анкету першої фази у другій фазі лише 83 % інспектованих фірм відповідали пункту 4(1)(a)(ii) Кодексу, а 50 % не мали належної оцінки технологічних ризиків; усього в межах проєкту проведено 11 перевірок, з них 5 — у 2025/26 наглядовому році. Зонами покращення названо документування процесу ухвалення рішень, надійнішу належну перевірку клієнта, ефективніше використання скринінгових інструментів і повніше врахування санкційного ризику в оцінці ризиків діяльності.

Висновки:

- **Дворічна програма з наперед опублікованим календарем перетворює нагляд на передбачуваний процес:** фірми знають теми й строки заздалегідь, а регулятор отримує порівнянні дані двох хвиль тієї самої анкети.
- **Двофазна модель «анкета всім — перевірки вибірці» дає вимірні показники:** 98,5 % відповідей у санкційній тематиці, 83 % відповідності пункту 4(1)(a)(ii) Кодексу і 50 % інспектованих фірм без належної оцінки технологічних ризиків.
- **Тематика ФР виявила розрив між декларованим і практикою:** 92,7 % фірм заявили про задовільне розуміння ризику фінансування розповсюдження, але лише 66,21 % підтвердили навчання персоналу з цієї теми.

Результати першої фази тематичного огляду щодо оцінки ризиків діяльності (Business Risk Assessment, вимога пункту 5 Кодексу ПВК/ФТ 2019 року) опубліковано в грудні 2025 року. Після завершення у 2023/2024 роках аналогічного огляду, зосередженого на секторі TCSP, Управління провело міжсекторальний огляд, зібравши інформацію через анкету, надіслану 30 піднаглядним суб'єктам різних секторів; звіт першої фази побудовано як порівняння з результатами огляду 2023 року. Показники такі: 99 % фірм підтвердили наявність документованої оцінки ризиків діяльності, 89 % переглядають її щорічно, 95 % враховують національну оцінку ризиків під час оновлення. Друга фаза — невідвізані перевірки оцінок ризиків окремих фірм — мала бути опублікована восени 2026 року; у 2025/26 році проведено 11 перевірок, ще 15 заплановано на 2026/27. Паралельно з грудня 2025 року розгорнуто проєкт щодо звітності та реєстрів, який Відділ нагляду з ПВК/ФТ координує спільно з Відділом портфельного нагляду: запити документів надсилаються обраним фірмам одночасно з повідомленням про їх участь у проєкті; у 2025/26 році проведено сім перевірок, ще 17 передбачено на 2026/27 рік.

Погляд наперед оформлено як календар, що заздалегідь повідомляє галузь про теми, заходи й орієнтовні строки. Політична робота у сфері ПВК/ФТ/ФР прив'язується до Національного плану дій Острова Мен і охоплює оновлення секторальних настанов за результатами набору національних оцінок ризиків, посилення ризик-орієнтованого нагляду та роз'яснювальної роботи щодо неприбуткових організацій і поліпшення наглядового й секторального розуміння схильності ризиків у сфері віртуальних активів. У листопаді 2026 року Управління планує розіслати всім фірмам острова анкету щодо іноземних публічних діячів, аби оцінити, які дії було вжито після публікації тематичного звіту 2023 року за результатами огляду 2021–2023 років. Невідвізані тематичні перевірки сектору страхування, іншого ніж страхування життя, перенесено з 2025/26 на 2026/27 рік через конкуренцію пріоритетів — випадок, коли регулятор публічно фіксує невиконання власного плану.

FinCEN про шахрайські центри та інвестиційні шахрайства з віртуальними активами³

Мережа боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN) оприлюднила два взаємопов'язані документи щодо шахрайств з віртуальними активами. Перший — аналітичне дослідження, підготовлене на виконання статті 6206 Закону про протидію відмиванню коштів 2020 року, яка зобов'язує FinCEN періодично публікувати інформацію про моделі та тенденції загроз. Другий — попередження FIN-2026-Alert005. Ці документи слід читати разом: аналітичне дослідження кількісно описує явище на основі звітності за Законом про банківську таємницю (BSA), а попередження перетворює цей опис на операційний інструмент — індикатори ризику та інструкції щодо подання повідомлень. Така конструкція «кількісний аналіз плюс попередження» сама по собі є методологічним прийомом, придатним до перенесення: зворотний зв'язок суб'єктам звітування надається не у вигляді загальних застережень, а як вимірювана картина плюс конкретні маркери. Емпірична база дослідження охоплює період з 8 вересня 2023 року по 31 грудня 2025 року. За цей час FinCEN отримала 33 904 повідомлення за Законом про банківську таємницю, які стосувалися інвестиційного шахрайства з віртуальними активами, на загальну суму приблизно 12,7 млрд доларів США; повідомлення надійшли приблизно від 1300 різних фінансових установ. Масив сформовано шляхом ручного й автоматизованого перегляду повідомлень, які містили ключові терміни з попередження FinCEN від 8 вересня 2023 року щодо схеми «pig butchering» (FIN-2023-Alert005). FinCEN супроводжує дані застереженням: звітність про підозрілу діяльність відображає лише ту активність, що була виявлена й повідомлена, і не є повним відображенням масштабу явища; масив містить як завершені операції, так і їх спроби, вхідні та вихідні

³ <https://www.fincen.gov/system/files/2026-08/FinCEN-FTA-Digital-Asset-Investment-Scams.pdf>
<https://www.fincen.gov/system/files/2026-08/FinCEN-Alert-Scam-Centers.pdf>

транзакції, перекази між рахунками, помилки подавачів, дублікати за обома напрямками руху коштів і повідомлення про продовжувану чи виправлену діяльність.

Динаміка є найпоказовішою частиною дослідження. У середньому кожного місяця FinCEN отримувала на 10,9 % більше повідомлень, ніж попереднього, а суми зростали в середньому на 18 % на місяць. У жовтні 2023 року надійшло 590 повідомлень на 485,7 млн доларів США, у грудні 2025 року — 2 482 повідомлення на 833,5 млн доларів США. Розподіл за типом подавача розкриває дві різні оптики спостереження: небанківські фінансові установи, які надають послуги з віртуальними активами, подали 18 568 повідомлень (54,8 %) на 5,5 млрд доларів США; депозитні установи — 13 810 повідомлень (40,7 %) на 6,4 млрд доларів США; фірми ринку цінних паперів і ф'ючерсів — 1 504 повідомлення (4,4 %) на 784,5 млн доларів США; інші установи — 22 повідомлення на 8,4 млн доларів США. Із цього співвідношення випливає практичний висновок: постачальники послуг з криптовалютами бачать більше подій, банк — більші суми, і жоден із них поодиночки не має повної картини одного й того самого потоку.

Дві технічні моделі шахрайства описано окремо, оскільки вони по-різному виявляються. За першою жертву спонукають відкрити рахунок у небанківській установі, яка є постачальником послугам з віртуальних активів, придбати конкретний актив і переказати його на адресу, підконтрольну шахраям. Фінансові установи прямо повідомляють про труднощі з виявленням цієї моделі, оскільки формально жертва зберігає контроль над коштами на рахунку аж до самого переказу. За другою моделлю жертву спрямовують переказати фіатні кошти на рахунки, пов'язані з шахраями; при цьому жертва ніколи не набуває жодних віртуальних активів, а видимість купівлі створюють реалістичні мобільні застосунки, вебсайти та дописи в соціальних мережах. У масиві ідентифіковано щонайменше 22 різні віртуальні активи, найчастіше — Ethereum, Tether (USDT) і USD Coin (USDC); шахраї майже завжди обмінювали отримані кошти на стейблкоїни, майже виключно на USDT. Входом у схему слугували переважно централізовані біржі віртуальних активів, а також кіоски (крипто-банкомати), де жертви вносили готівку.

Профіль жертв і структура збитків заслуговують на окрему увагу. Приблизно 25 % повідомлень одночасно стосувалися інвестиційного шахрайства з віртуальними активами та фінансової експлуатації літніх осіб, тоді як особи похилого віку становлять близько 24,4 % населення за переписом 2020 року. Активність зафіксовано в усіх 50 штатах, окрузі Колумбія, на Гуамі, Північних Маріанських островах і в Пуерто-Рико. Джерелами коштів жертв були поточні й ощадні рахунки, зняття з пенсійних рахунків, кредитні лінії під заставу житла, повторні іпотеки, споживчі кредити, готівкові аванси за кредитними картками, ліквідація інвестиційних портфельів і кошти, зібрані в родичів та друзів. Наведені приклади показують порядок збитків: переказ майже 640 000 доларів США з пенсійного фонду; зняття 150 000 доларів США з пенсійного рахунку з подальшим відкриттям кредитної лінії під житло, споживчим кредитом і рефінансуванням іпотеки; втрата понад 1 млн доларів США за шість місяців із коштів від продажу житла померлого родича, повторної іпотеки, пенсійних заощаджень і бізнес-рахунку. FinCEN окремо зазначає, що частина жертв за даними правоохоронних органів і звітності перебуває під ризиком самоушкодження, і фіксує випадки з летальними наслідками — обставина, яка переводить цю типологію з категорії суто майнових злочинів. Шахраї, за спостереженнями FinCEN, дедалі активніше застосовують технології штучного інтелекту, зокрема дипфейки та великі мовні моделі. Окремо описано, за яких обставин установи різного типу помічали активність: банки — коли клієнт переказував кошти небанківській установі для купівлі активів, надсилав переказ із згадкою віртуальних активів, робив великі перекази між власними рахунками для оформлення кредитів чи іпотек або посилався на довіреного «інвестиційного радника», відмовляючись обговорювати деталі; криптосервіси — коли кілька жертв надсилали кошти на ті самі підозрілі адреси; інвестиційні фірми — коли клієнт ліквідовував портфель заради купівлі віртуальних активів.

Попередження FIN-2026-Alert005 переносить фокус із жертви на інфраструктуру. Заявлений масштаб: повідомлені збитки американських жертв від інвестиційних шахрайств з

віртуальними активами зросли з 907 млн доларів США у 2021 році до 7,2 млрд доларів США у 2025 році, а річний дохід шахрайських центрів Південно-Східної Азії оцінюється десятками мільярдів доларів. Самі центри описано як промислові за масштабом об'єкти, розташовані передусім у Камбоджі, М'янмі та Лаосі, з поширенням методології до Південної Азії, Тихоокеанського регіону, Африки, Близького Сходу й Південної Америки. Операторів центрів здебільшого становлять жертви торгівлі людьми: у них вилучають паспорти, утримують до сплати викупу родиною, б'ють за невиконання норми, примушують до комерційного сексу. Рекрутинг відбувається через фальшиві оголошення про високооплачувану роботу для англомовних осіб у Південно-Східній Азії, на Близькому Сході, у Латинській Америці та Східній Європі — остання географічна вказівка робить цю типологію безпосередньо релевантною для України як країни походження потенційних завербованих. Контакт із жертвою ініціюється через соціальні мережі або текстові повідомлення, іноді під виглядом помилково набраного номера; транснаціональні злочинні організації застосовують інструменти штучного інтелекту для масштабування схем.

Механіку відмивання попередження розкладає на три стадії. Перша — збір платежів жертв: через VASP і крипто-кіоски, а також фіатними переказами й через автоматизовану клірингову палату на банківські рахунки, підконтрольні шахраям і професійним відмивачам через мережі грошових мулів та компанії-оболонки; окремо зазначено використання шахрайських установ, а також золотих монет і злитків та подарункових карток. Друга стадія — розшарування в блокчейні: швидке переміщення коштів через численні адреси, змішування в консолідаційних гаманцях, використання міксерів і тумблерів, обміни між блокчейнами й активами, зокрема переведення токенів USDT зі схем шахрайства з мережі Ethereum до мережі Tron із залученням протоколів децентралізованих фінансів. Третя стадія — інтеграція у формальну систему: мережі грошових мулів переказують стейблкоїни на біржі за межами США, після чого кошти проходять через китайські системи підпільного банкінгу з P2P обмінниками та позабіржовими брокерами, які не мають надійних процедур ідентифікації клієнта й антилегалізаційного контролю, а «гарантійні маркетплейси» пов'язують кіберзлочинців із постачальниками послуг підпільного банкінгу; ліквідність забезпечують великі небанківські фінансові установи.

Інституційна складова попередження вибудована навколо камбоджійської групи Huione та її гарантійного маркетплейсу Haowang Guarantee, через який відмито щонайменше 300 млн доларів США у віртуальних активах, зокрема отриманих від кібероперацій КНДР та шахрайств з інвестиціями у віртуальні валюти. Група запустила власний стейблкоїн USDH, який рекламувався як «незаморожуваний» і «не обмежений традиційними регуляторами», а згодом перенесла операції на структуру H-Pay Service PLC, аби уникнути публічної уваги. Регуляторна відповідь США розгорталася послідовно: остаточне правило FinCEN про застосування спеціального заходу за статтею 311 Закону USA PATRIOT, яким групу Huione відсічено від фінансової системи США (жовтень 2025 року, 90 Fed. Reg. 48295), і запропоноване правило про поширення санкційних обмежень групи на H-Pay та наступників (червень 2026 року, 91 Fed. Reg. 38340). Паралельно 23 квітня 2026 року Міністерство юстиції США в межах Scam Center Strike Force висунуло обвинувачення громадянам Китаю, які керували комплексом у М'янмі, вилучило Telegram-канал, що використовувався для вербування, та 503 фальшиві інвестиційні вебсайти; 29 квітня 2026 року оголошено щонайменше про 276 арештів. Міністерство фінансів США застосувало санкції до мереж Південно-Східної Азії 8 вересня 2025 року та до операторів камбоджійських центрів 23 квітня 2026 року, а Державний департамент оголосив винагороду до 10 млн доларів США за інформацію, що призведе до фінансового руйнування центрів Tai Chang у М'янмі. Рамковим документом є Виконавчий указ 14390 від 6 березня 2026 року про протидію кіберзлочинності, шахрайству та хижацьким схемам проти громадян США.

Попередження містить 16 індикаторів ризику, згрупованих у три блоки, і саме вони становлять найбільшу практичну цінність документа. Блок платежів жертв:

- клієнт заявляє, що отримав вказівку від нібито представника правоохоронного чи державного органу здійснити платіж у віртуальних активах, міжнародний переказ або придбати дорогоцінні метали чи подарункові картки;
- клієнт пояснює платіж наймом юридичної фірми для повернення втрачених коштів, але не має документального підтвердження легітимності послуги;
- клієнт знімає кошти з інвестиційного або пенсійного рахунку для купівлі золота і зазначає, що має передати його кур'єрові;
- за відкритими джерелами установа-одержувач заявляє про «схвалення FinCEN»;
- біржа рекламує послуги «без KYC».

Блок гарантійних маркетплейсів:

- операції з токеном, випущеним таким маркетплейсом, без пояснення джерела коштів;
- зміна назви, бренду чи вебсайту провайдера після правозастосовних дій;
- операції з неатрибутованим кластером адрес, який за блокчейн-аналізом поділяє інфраструктуру з відомим маркетплейсом;
- провайдер, що діє в М'янмі, Камбоджі чи Лаосі та приховує місцезнаходження або корпоративну структуру.

Блок технік відмивання:

- використання DeFi протоколів для переведення надходжень із гаманця-агрегатора шахрайських доходів в інший актив чи блокчейн;
- суттєві операції зі стейблкоїном, видавець якого рекламує неспівпрацю з правоохоронними органами або неможливість заморожування;
- ознаки роботи клієнта як позабіржового брокера чи P2P обмінника через велику кількість зустрічних операцій на ліквідності біржі;
- згадка адреси гаманця в месенджері поряд із китайськомовними термінами, пов'язаними з відмиванням коштів.

FinCEN вимагає посилатися на попередження, зазначаючи ключовий термін «FIN-2026-SCAMCENTERS» у полі 2 повідомлення та в описовій частині. Установи мають включати структуровані кіберіндикатори: журнали чатів, телефонні номери та імена користувачів у соціальних мережах, використані шахраєм, підозрілі адреси електронної пошти, тип віртуального активу, адреси гаманців і хеші транзакцій, назви застосунків, а також URL, домен та IP-адресу сервісу, до якого спрямовували жертву.

Для української практики обидва документи мають кілька прикладних вимірів. Найочевидніший — географічний: Східна Європа прямо названа регіоном вербування операторів шахрайських центрів, а українські громадяни водночас можуть виступати і жертвами інвестиційних шахрайств. Другий вимір — інфраструктурний: описаний ланцюг «стейблкоїн USDT у мережі Tron — позабіржовий брокер — P2P обмінник — дропові рахунки» практично збігається з конфігурацією, яка спостерігається на українському ринку віртуальних активів, а отже, індикатори щодо ознак роботи клієнта як позабіржового брокера та щодо стейблкоїнів можуть застосовуватися з мінімальною адаптацією.

Висновки:

- 33 904 повідомлення на 12,7 млрд дол. США приблизно від 1 300 установ за 27 місяців із середнім місячним приростом 10,9 % за кількістю і 18 % за сумами — інвестиційне шахрайство з ВА перестало бути нішевою типологією.
- Структура подавачів розкриває дві оптики: криптосервіси подали 54,8 % повідомлень на 5,5 млрд дол., банки — 40,7 % на 6,4 млрд; жоден із них поодиночі не бачить повної картини одного й того самого потоку.
- **Близько 25 % повідомлень одночасно позначені як фінансова експлуатація літніх осіб**, а джерелом коштів жертв були пенсійні накопичення, кредитні лінії під житло і повторні іпотеки — це знищення заощаджень, а не епізодичний збиток.

Від прозорості до підзвітності: ключові антикорупційні результати Transparency International у 2025 році ⁴

Річний звіт, підготовлений Transparency International, узагальнює результати діяльності глобального руху Transparency International у 2025 році та показує, як його дослідницька, адвокаційна, юридична й комунікаційна робота трансформується у зміни законодавства, державної політики, інституційної практики та конкретні результати правозастосування. Діяльність організації у звіті вибудована навколо шести стратегічних цілей Стратегії до 2030 року: захист публічних ресурсів, припинення потоків «брудних» коштів, забезпечення доброчесності в політиці, підвищення доброчесності бізнесу, забезпечення правозастосування та правосуддя, а також розширення громадянського простору для підзвітності. У ширшому контексті Transparency International виходить із того, що корупція є не лише сукупністю окремих правопорушень, а системним проявом дисбалансу влади, коли політичні та економічні еліти здатні використовувати ресурси, вплив і доступ до процесів прийняття рішень у приватних інтересах. Тому антикорупційна діяльність у документі охоплює не лише кримінальне переслідування, а й запобігання корупції, прозорість державного управління та фінансів, контроль політичного впливу, бенефіціарну власність, корпоративну доброчесність, захист викривачів, доступ громадськості до інформації та можливість громадянського суспільства здійснювати незалежний контроль.

Масштаб діяльності Transparency International у 2025 році відображено через конкретні показники. Організація повідомляє про свій внесок у понад 60 змін у законодавстві, політиці та інституційній практиці, підготовку 62 юридичних подань у справах, пов'язаних із корупцією, та публікацію 67 досліджень і аналітичних матеріалів. Через центри Advocacy and Legal Advice Centres у 53 країнах безкоштовну конфіденційну допомогу отримали понад 14 тис. осіб, які постраждали від корупції або стали її свідками. До найбільш значущих результатів року Transparency International відносить прийняття нових глобальних стандартів щодо політичного фінансування в межах Конвенції Організації Об'єднаних Націй проти корупції (UNCAC), перший вирок європейському політику у справі, пов'язаній з Azerbaijani Laundromat, остаточне припинення схем «золотих паспортів» у ЄС, просування Integrity Pacts у публічних закупівлях, включення протидії корупції як наскрізного пріоритету до глобального порядку денного фінансування розвитку, посилення окремих положень майбутнього антикорупційного законодавства ЄС та захист громадянського простору від обмежувальних законодавчих ініціатив.

Значна частина звіту присвячена захисту публічних ресурсів. Transparency International наголошує, що корупція у сфері державних фінансів безпосередньо зменшує обсяги ресурсів, доступних для розвитку, соціального забезпечення, інфраструктури та базових державних послуг. Відповідно, захист публічних коштів має охоплювати весь їх життєвий цикл — від мобілізації та розподілу до фактичного витрачання, контролю результатів та аудиту. У цьому контексті важливим міжнародним результатом стала Четверта міжнародна конференція з фінансування розвитку у Севільї. Transparency International протягом підготовки до конференції просувала підхід, за якого протидія корупції повинна розглядатися не як окремий тематичний напрям, а як наскрізний принцип усієї системи фінансування розвитку. Підсумковий документ конференції — *Compromiso de Sevilla* — закріпив вимоги щодо посилення прозорості та підзвітності протягом усього циклу управління публічними фінансами та вперше на рівні глобальної угоди прямо визнав корупційні ризики у сфері управління державним боргом. Документ передбачає, зокрема, подальший розвиток глобального публічного реєстру державного боргу та використання механізмів Конвенції ООН проти корупції для запобігання корупційним практикам під час державного кредитування та запозичень.

⁴ https://files.transparencycdn.org/images/2025_-_TransparencyInternationalAnnualReport_EN.pdf

Звіт також демонструє, як міжнародні антикорупційні підходи можуть трансформуватися у національні реформи. У Пакистані значну частину рекомендацій, сформованих у межах альтернативної діагностичної оцінки системи врядування, підготовленої за участі Transparency International, було враховано МВФ у власній оцінці та рекомендаціях, пов'язаних із програмою кредитування країни. Подальша взаємодія сприяла прийняттю парламентом законопроекту щодо більш повного декларування активів державними службовцями. Transparency International намагається використати цей досвід і для просування системнішого залучення громадянського суспільства до подібних діагностичних оцінок у діяльності міжнародних фінансових установ.

Окремим елементом захисту публічних ресурсів залишаються публічні закупівлі, які через значні обсяги державних витрат і складність контрактних процесів є особливо вразливими до корупції та неефективного використання коштів. Флагманським інструментом Transparency International у цій сфері є Integrity Pact — механізм, який поєднує зобов'язання замовників і учасників закупівель щодо прозорості та доброчесності з незалежним моніторингом з боку громадянського суспільства. Незалежний монітор має можливість відстежувати закупівельний процес та оприлюднювати результати, створюючи додатковий рівень зовнішнього контролю. За даними звіту, цей інструмент застосовувався для захисту публічних проєктів загальною вартістю понад €1 млрд у більш ніж 15 країнах. У 2025 році за підтримки Європейської комісії було запущено Integrity Pact Helpdesk, який надає органам влади держав ЄС політичні рекомендації, технічну допомогу та практичні ресурси для застосування Integrity Pacts до інвестицій, що фінансуються Європейським Союзом. В Іспанії механізм було включено до Національного антикорупційного плану та П'ятого плану відкритого уряду, а також передбачено у проєкті законодавства про відкриту адміністрацію.

Водночас Transparency International розглядає державний аудит не просто як технічну перевірку правильності використання коштів, а як елемент ширшої системи підзвітності. У Замбії та Малаві організація сприяла посиленню взаємодії між вищими органами аудиту, медіа та громадянським суспільством. Основна логіка полягає у тому, що сам факт проведення аудиту не гарантує змін, якщо його результати залишаються малодоступними, не отримують належної суспільної уваги або рекомендації не виконуються. Формалізація співпраці з журналістами та громадськими організаціями має забезпечити ширший доступ до інформації про державні фінанси, краще пояснення результатів аудитів і подальший контроль за реакцією органів влади. У Малаві така взаємодія вже сприяла тому, що парламент викликав представників органу аудиту для пояснення результатів перевірок і стану реалізації ключових рекомендацій.

Поряд із фінансовими ресурсами Transparency International розглядає як об'єкт антикорупційного захисту землю, природні ресурси та кліматичне фінансування. У восьми африканських країнах організація працювала над підвищенням доступності інформації щодо земельних прав, адміністративних процедур і механізмів подання скарг. У Замбії громадські зустрічі сприяли прийняттю органами влади зобов'язань щодо видачі земельної документації, відкриття місцевих сервісних центрів та вдосконалення процедур ліцензування компаній. У Кенії журналістські розслідування щодо ймовірно незаконного розподілу державних земель стали підставою для юридичних дій. У Гані було оголошено про поширення земельних адміністративних послуг на всі 90 районів із використанням цифрових інструментів, в Уганді запроваджено професійні стандарти для оцінювачів нерухомості та покращено взаємодію земельних і антикорупційних органів, а у Зімбабве цифрові правила щодо правовстановлюючих документів спрямовувалися на усунення можливостей для підробок і незаконного розподілу землі.

У сфері кліматичного врядування звіт виокремлює ризики, пов'язані з конфліктом інтересів, впливом лобістських груп та недостатньою прозорістю у використанні коштів, спрямованих на реалізацію кліматичних заходів. Transparency International сприяла посиленню вимог Рамкової конвенції Організації Об'єднаних Націй про зміну клімату (UNFCCC) до прозорості учасників глобальних кліматичних переговорів: представники організацій, акредитованих як

спостерігачі на Конференції Сторін Рамкової конвенції ООН про зміну клімату (COP) почали просити розкривати джерела фінансування та підтверджувати відповідність цілям UNFCCC, хоча відповідна вимога поки залишається добровільною. У межах підготовки до COP30 організація сприяла впровадженню додаткових механізмів доброчесності, зокрема механізму омбудсмена, а також посиленню прозорості інфраструктурних проєктів, пов'язаних із проведенням конференції. У ЄС після звернення Transparency International щодо ситуації, коли консалтингова компанія одночасно працювала із промисловими групами та установою, яка регулює відповідний сектор, було посилено політику щодо конфліктів інтересів та належної перевірки зовнішніх консультантів. Крім того, нові правила прозорості лобіювання у ЄС поширилися приблизно на 2 тис. ключових посадовців, а відкритими для аналізу стали дані про десятки тисяч зустрічей представників Європейської комісії та Європейського парламенту.

Другий великий стратегічний напрям документа — припинення потоків «брудних» коштів. Transparency International описує систему переміщення та приховування корупційних доходів як комплекс взаємопов'язаних вразливостей, що включає анонімні компанії, непрозорі юридичні конструкції, трасти, офшорні рахунки та активи, недостатню прозорість власності й участь професійних посередників. Відповідно, організація зосереджується на трьох ключових елементах: прозорості бенефіціарної власності, відповідальності професіоналів, які можуть сприяти приховуванню незаконних активів, та посиленні інституційної спроможності компетентних органів виявляти й розслідувати транскордонні потоки коштів.

Одним із найбільш значущих результатів 2025 року стало рішення Суду Європейського Союзу щодо мальтійської програми набуття громадянства в обмін на інвестиції. Суд визнав, що схема фактично комерціалізувала громадянство ЄС і була несумісною з природою громадянства Союзу та принципом щирого співробітництва. Рішення припинило останню на той момент діючу в ЄС схему «золотих паспортів» та створило правову основу для протидії спробам відновити подібні програми. Transparency International розглядає такі схеми не лише як міграційне або інвестиційне питання, а як вразливість системи протидії фінансовій злочинності: вони могли використовуватися корумпованими та іншими злочинними суб'єктами для отримання безпечної юрисдикції, легітимізації статусу, переміщення коштів та інвестицій у межах ЄС. Організація протягом багатьох років досліджувала відповідні ризики, співпрацювала з журналістами-розслідувачами, формувала доказову базу та здійснювала адвокацію на рівні інституцій ЄС.

Окрему увагу звіт приділяє професійним посередникам, зокрема юристам, бухгалтерам та агентам з нерухомості. Transparency International виходить із того, що ці професії можуть відігравати ключову роль у транскордонних корупційних схемах, оскільки забезпечують створення компаній та інших юридичних структур, проведення операцій із майном і коштами, а також маскування справжніх власників активів. На конференції FfD4 організація просувала посилення регулювання та нагляду за високоризиковими професійними послугами і розширення доступу до інформації про реальних власників компаній, трастів та інших активів. У результаті Compromiso de Sevilla містить положення щодо ефективного регулювання професійних постачальників послуг і підтримки міжнародного обговорення стандартизації відповідних режимів. Паралельно за координації УНЗ ООН було розпочато роботу з картування прогалів у регулюванні та нагляді за професійними посередниками, що має створити основу для подальшого вдосконалення вимог до цих секторів.

Важливою складовою звіту є аналіз нерухомості як інструменту зберігання та приховування незаконних активів. Спільно з Anti-Corruption Data Collective Transparency International розробила Індекс непрозорості власності на нерухомість, який оцінює рівень захищеності ринків нерухомості 24 великих юрисдикцій, переважно держав G20 та ключових фінансових центрів. Індекс дозволяє виявляти прогалини, через які операції з нерухомістю можуть уникати належної перевірки у сфері протидії відмиванню коштів. За результатами оцінювання, у більшості досліджених юрисдикцій досі існують можливості для анонімного придбання або володіння нерухомістю, що ускладнює встановлення походження активів.

Особливе значення у звіті приділено ефективності систем бенефіціарної власності. Transparency International наголошує, що самого створення реєстрів недостатньо, якщо внесені до них відомості не перевіряються або доступ до них фактично ускладнений. У 2025 році організація перевірила практику доступу до інформації про бенефіціарних власників у 14 державах ЄС та виявила значні адміністративні бар'єри, зокрема тривалі строки розгляду запитів, плату, мовні обмеження та складні процедури. Позитивним прикладом названо Швейцарію, де було ухвалено законодавство про федеральний реєстр бенефіціарних власників та зміни у сфері ПВК. Водночас було відхилено підхід, який фактично допускав би презумпцію достовірності неперевірених самодекларацій, що підкреслює важливість не лише збору, а й належної верифікації даних.

Окремий стратегічний напрям стосується доброчесності політики та політичного фінансування. Transparency International визначає непрозоре фінансування партій і виборчих кампаній одним із ключових ризиків прихованого впливу приватних інтересів та захоплення державних рішень. Центральним результатом 2025 року стало прийняття державами-членами Конвенції ООН проти корупції (UNCAC) Резолюції 11/7 щодо політичного фінансування. Вона передбачає прозорість джерел політичного фінансування, їх законність, запобігання неправомірним перевагам окремих приватних інтересів та ефективний нагляд. Робота над резолюцією тривала кілька років: Transparency International проводила консультації з понад 30 державами, а фінальний документ отримав підтримку понад 60 держав-співспонсорів. На рівні ЄС організація також просувала посилення вимог щодо конфліктів інтересів, декларування активів і політичного фінансування, включаючи ризики використання криптоактивів для приховування джерел пожертв.

Практичним інструментом контролю політичної доброчесності є Integrity Watch — відкриті цифрові платформи, які об'єднують інформацію про політичні пожертви, лобістські контакти, активи та інтереси посадовців, державні контракти й зв'язки між компаніями та особами, що приймають рішення. Це дозволяє виявляти потенційні конфлікти інтересів, незадекларовані зв'язки та непропорційний вплив окремих суб'єктів. У 2025 році кількість платформ Integrity Watch у Європі зросла до 22, а європейська платформа розширила масив даних про лобістську активність майже 13 тис. організацій, зареєстрованих у Брюсселі.

У сфері доброчесності бізнесу Transparency International зосереджувалася на корпоративних антикорупційних стандартах, захисті викривачів та практичній підтримці малого і середнього бізнесу. Разом із Міжнародною торговою палатою (ICC) та Глобальним договором ООН (UN Global Compact) було оновлено документ «Обґрунтування доброчесності для бізнесу» (Business Case for Integrity), а в межах Конференції держав-членів Конвенції ООН проти корупції (UNCAC CoSP) організація брала участь в обговоренні питань корпоративної доброчесності та ризиків, пов'язаних із використанням штучного інтелекту. Продовжувалося також поширення інструментарію для малих та середніх підприємств (МСП), розробленого разом із World Economic Forum та застосованого у низці країн Латинської Америки, Азії й Африки.

Значний блок документа присвячено правозастосуванню та правосуддю. Transparency International наголошує, що якісне антикорупційне законодавство має супроводжуватися реальною відповідальністю за порушення. У 2025 році організація працювала з 11 національними відділеннями та чотирма зовнішніми партнерами над стратегічними юридичними справами і здійснила 62 антикорупційні подання. Одним із найбільш помітних результатів став вирок колишньому депутату Бундестагу Едуарду Лінтнеру у справі, пов'язаній з Azerbaijani Laundromat та так званою «ікорною дипломатією». Transparency International розглядає цей результат як важливий сигнал щодо можливості притягнення до відповідальності навіть політично впливових осіб.

Іншим прикладом стала Мальта, де Transparency International допустили до інвестиційного арбітражу як сторону, що надає суду незалежну експертну позицію. Арбітражний трибунал відхилив позов Steward Health Care на €148 млн після того, як мальтійські суди раніше

анулювали відповідну лікарняну концесію через встановлені порушення. У Шрі-Ланці Верховний суд у справі X-Press Pearl зобов'язав групу компаній сплатити \$1 млрд компенсації за екологічну шкоду та призначив нове розслідування корупційних тверджень. Важливими стали й положення Антикорупційної директиви ЄС, які передбачають можливість участі організацій громадянського суспільства у кримінальних антикорупційних провадженнях для представлення потерпілих або суспільного інтересу, а також щорічне звітування держав про практику застосування антикорупційного законодавства.

Останній стратегічний напрям присвячено захисту громадянського простору, викривачів та незалежних антикорупційних організацій. Через Систему ЄС із забезпечення сприятливого середовища для громадянського суспільства Transparency International та її партнери здійснювали моніторинг ризиків для громадянського суспільства у 86 країнах. Механізм використовувався для раннього виявлення загроз та підтримки активістів, зокрема у Бангладеш, Кенії, Республіці Конго та Гамбії. В Угорщині організація разом із партнерами протидіяла законодавчій ініціативі, яка могла суттєво обмежити діяльність НУО та незалежних медіа з іноземним фінансуванням, і відповідний процес зрештою було зупинено.

Значна увага приділяється захисту викривачів. Рекомендації Transparency International були використані B20 та International Labour Organization як орієнтири належної практики. У Словаччині організація та її партнери протидіяли спробі послабити орган із захисту викривачів. Через мережу Advocacy and Legal Advice Centres у 2025 році підтримку отримали понад 14 тис. осіб, а загалом із 2003 року — майже 400 тис. громадян. Інформація, отримана через такі центри, використовується не лише для допомоги конкретним особам, а й для виявлення системних проблем та просування реформ.

Звіт також підкреслює важливість фізичної та цифрової безпеки антикорупційних організацій. Transparency International надавала юридичну, комунікаційну та ІТ-підтримку відділенням, які стикалися з переслідуваннями, кампаніями дискредитації та кібератаками. Водночас було сформовано спільні базові вимоги

цифрової безпеки для глобальної мережі. Для післякризового відновлення показовим є приклад Лівану, де організація підтримувала громадські ініціативи у сфері прозорості відбудови та гуманітарної допомоги. У 2025 році здійснювався нагляд за 23 грантами ЄС для антикорупційної діяльності та ще сімома грантами, спрямованими на громадську участь, прозорість допомоги й посилення співпраці між державою та громадянським суспільством.

Поряд із зовнішньою діяльністю Transparency International розвивала власну інституційну спроможність. Було проведено проміжну оцінку реалізації Стратегії до 2030 року, запроваджено новий Кодекс етики досліджень, розроблено підхід «не нашкодь», посилено механізми управління конфліктами інтересів та цифрової безпеки. Організація також почала вивчати можливості використання штучного інтелекту та автоматизації для управління знаннями й підвищення продуктивності. Фінансові показники демонструють зростання

Висновки:

- **Необхідно посилити прозорість бенефіціарної власності**, забезпечивши не лише ведення відповідних реєстрів, а й належну верифікацію даних та ефективний доступ до них компетентних органів і інших уповноважених користувачів.
- **Доцільно посилити регулювання та нагляд за професійними посередниками**, зокрема юристами, бухгалтерами та агентами з нерухомості, які можуть використовуватися для створення структур, переміщення та приховування незаконних активів.
- **Слід розширити використання механізмів незалежного контролю за публічними коштами**, включаючи Integrity Pacts, державний аудит, відкриті дані та участь громадянського суспільства у моніторингу публічних закупівель і державних інвестицій.
- **Важливо забезпечити практичне застосування антикорупційних стандартів**, посилюючи правозастосування, захист викривачів, контроль політичного фінансування та можливості громадянського суспільства брати участь у забезпеченні відповідальності за корупційні правопорушення.

масштабу діяльності: операційний дохід у 2025 році становив близько €27,4 млн, а трансфери національним відділенням та партнерам — €14 млн, або 51% усіх витрат.

Загалом звіт демонструє перехід від формальної прозорості до фактичної підзвітності та результативності. Самого існування реєстрів, антикорупційних норм чи відкритих даних недостатньо: інформація про бенефіціарних власників має перевірятися і бути доступною для практичного використання, закупівлі — супроводжуватися незалежним контролем, політичне фінансування — ефективним наглядом, професійні посередники — належним регулюванням, а антикорупційне законодавство — реальним правозастосуванням. Водночас ефективна система потребує участі громадянського суспільства, журналістів і викривачів, які можуть виявляти порушення та сприяти притягненню винних до відповідальності. Таким чином, Transparency International формує комплексну модель протидії корупції, що поєднує превентивні механізми, прозорість власності, контроль публічних фінансів, цифрову аналітику, незалежний нагляд, громадську участь та ефективне правосуддя.

Боротьба з фінансовими злочинами у Великій Британії: виклики ШІ, корупції та професійних посередників⁵

37-й випуск спеціалізованого журналу Британського підрозділу фінансової розвідки (UKFIU), який діє у структурі Національного агентства з питань злочинності (NCA), висвітлює поточні загрози у сфері фінансових злочинів та надає практичні рекомендації для всіх стейкхолдерів системи повідомлень про підозрілу діяльність (SAR).

Це видання виконує роль методичного посібника, орієнтованого на посилення спроможності фінансового сектору, правоохоронних органів та регуляторів протидіяти сучасним викликам.

Вступна промова заступника директора UKFIU Вінса О'Браєна задає тон всьому випуску, наголошуючи на необхідності постійної адаптації до нових методів злочинців. Головний акцент робиться на інтеграції зусиль державного та приватного секторів у боротьбі з економічною злочинністю. Особливу увагу привертає попередження про випадки імітації діяльності UKFIU, коли шахраї, видаючи себе за співробітників підрозділу, розсилають листи та електронні повідомлення з вимогою надати персональні дані для нібито завершення транзакцій або виконання вимог щодо боротьби з відмиванням коштів. Це є класичним прикладом фішингу, який використовує авторитет державної інституції для обману громадян. У відповідь на цю загрозу NCA публікує чіткі критерії ідентифікації справжніх комунікацій, наголошуючи, що співробітники ніколи не запитують банківські реквізити, не вимагають віддаленого доступу до комп'ютерів та не просять переказувати кошти. Важливою практичною порадою є рекомендація вичікувати п'ять хвилин перед повторним дзвінком до поліції після підозрілого дзвінка, оскільки шахраї часто не кладуть слухавку, імітуючи з'єднання з оператором.

Однією з ключових тем випуску є аналіз загрози використання штучного інтелекту (ШІ) для обходу процедур належної перевірки клієнтів (CDD). Ця проблема, висвітлена у "бурштиновому попередженні" Joint Money Laundering Intelligence Taskforce (JMLIT), перестала бути теоретичною і стала реальною загрозою для фінансового сектору Великої Британії. Злочинці активно використовують ШІ для маніпуляції документами, що посвідчують особу, створення переконливих фейків (deepfakes) та синтетичних особистостей. Це дозволяє їм маскувати своє справжнє обличчя під час відкриття рахунків, які згодом використовуються для вчинення різноманітних шахрайств та легалізації доходів від наркотрафіку та інших злочинів.

Технології розвиваються настільки швидко, що традиційні методи перевірки стають дедалі менш ефективними, тому автори закликають фінансові установи звертати особливу увагу на

⁵ <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/824-sars-in-action-issue-37/file>

ці ризики та зазначати у своїх SAR спеціальний код 0801-NECC для полегшення аналітичної обробки таких випадків.

Окремий блок статті присвячено проблемі корупції та хабарництва у Великій Британії. Незважаючи на високі міжнародні рейтинги країни за рівнем прозорості, проблема залишається гострою, про що свідчать нещодавні скандали у сфері державних закупівель та політичного лобізму. У статті детально розглядається дія Закону про хабарництво 2010 року, який вважається одним з найжорсткіших у світі, особливо через норму про відповідальність корпорацій за невжиття заходів щодо запобігання хабарництву, навіть якщо керівництво не знало про порушення. Це стимулює компанії будувати проактивну комплаєнс-культуру. Значну роль у розслідуванні та переслідуванні корупційних злочинів відіграють Serious Fraud Office (SFO), City of London Police з їхнім Domestic Corruption Unit та NCA з International Corruption Unit, який бореться з хабарництвом за участю британських громадян або компаній за кордоном.

У статті також згадуються заходи щодо підвищення прозорості, такі як Реєстр закордонних суб'єктів (Register of Overseas Entities), запроваджений у 2022 році для виявлення реальних власників британської нерухомості, що ускладнює відмивання коштів через ринок житла.

Окремої уваги заслуговує розділ, присвячений професійним посередникам (Professional Enablers), які є критичною ланкою у ланцюгу легалізації злочинних доходів та організованої злочинності. У виданні наводиться офіційне визначення, згідно з яким професійний посередник — це особа або організація, яка надає професійні послуги, що сприяють злочинній діяльності, причому їхня поведінка може коливатися від навмисного співучасті до недбалості або свідомого заплуцування очей на порушення. До цієї категорії належать юристи, бухгалтери, банківські службовці, інвестиційні радники, агенти з нерухомості та інші. Аналітики наголошують, що без таких посередників організовані злочинні групи та корумповані еліти не змогли б досягти нинішнього рівня складності у приховуванні походження коштів.

Стратегія NECC передбачає шість ключових напрямків протидії цій загрозі, включаючи посилення обміну інформацією, координацію дій системи та проведення оперативних заходів. Для підзвітних суб'єктів розроблено детальний перелік індикаторів підозрілої поведінки, таких як надання послуг особам з негативними медіа-згадками, спроби приховати кінцевого бенефіціара, використання корпоративних рахунків для сумнівних транзакцій та створення складних корпоративних структур без економічної доцільності. У звітах рекомендується використовувати код XXPRFXX, щоб допомогти правоохоронним органам ідентифікувати такі випадки.

Висвітлюючи практичні аспекти роботи, видання звертається до питання подання SAR у випадках, коли клієнт фінансової установи став жертвою шахрайства. Проведений аналіз показав, що подвійне подання звітів як установою жертви, так і установою отримувача коштів є неефективним та дублює зусилля. Новий підхід, схвалений NCA та FCA, передбачає, що основний SAR має подавати установа, на рахунку якої опинилися вкрадені кошти, оскільки вона володіє більш повною інформацією про підозрілий рахунок. Це дозволяє сконцентрувати ресурси на високоякісній аналітиці та уникнути захаращення системи дублікатними повідомленнями. Такий підхід демонструє прагнення UKFIU до оптимізації процесів в рамках концепції системної пріоритизації.

Іншою важливою темою, порушеною у журналі, є зловживання схемою Enterprise Investment Scheme (EIS), яка створена для стимулювання інвестицій у високоризикові стартапи через податкові пільги. HMRC застерігає, що складна структура та значні податкові вигоди роблять цю схему привабливою для шахраїв, які часто видають себе за "схвалені HMRC" інвестиційні компанії, щоб виманювати кошти у довірливих та фінансово необізнаних громадян. У статті наводяться конкретні індикатори ризику, як-от: відсутність чіткої інвестиційної стратегії у компанії, виплата надмірних комісійних третім особам (понад 20%), рух коштів через численних посередників для заплутування слідів, а також інвестиції від осіб, які не є

досвідченими або високоповажними інвесторами, особливо якщо вони діють не відповідно до своїх фінансових можливостей. Фінансовим установам рекомендується посилювати перевірки у таких випадках та обов'язково зазначати причетність до EIS у своїх SAR, що дозволяє HMRC оперативно реагувати на потенційні порушення.

На завершення, рубрика "Запитайте UKFIU" роз'яснює процедуру розгляду запитів на захист від відмивання коштів (DAML). Автори детально описують, що після подання запиту починається семиденний робочий строк, протягом якого заборонено здійснювати зазначену в запиті дію, однак дозволяється продовжувати іншу роботу, наприклад, аналіз справи, за умови дотримання правил нерозголошення. UKFIU протягом цього періоду оцінює ризики, перевіряє наявність інтересу з боку правоохоронних органів та перспективи повернення активів. У разі потреби вони можуть запросити додаткову інформацію, і якщо відповідь не буде надана вчасно, запит буде закрито. Важливим меседжем є попередження про те, що неякісні SAR можуть бути передані наглядовим органам для вжиття відповідних заходів, що підкреслює важливість підготовки якісних та інформативних повідомлень.

Таким чином, видання демонструє комплексний підхід Великої Британії до боротьби з фінансовими злочинами. Воно не лише попереджає про новітні загрози, як-от використання ШІ та імітація державних органів, але й пропонує чіткі практичні рішення для підвищення ефективності системи фінансового моніторингу, акцентуючи увагу на якості інформації, міжвідомчій взаємодії та відповідальності професійних учасників ринку.

Висновки:

- **Активізація шахрайства з використанням імітації державних органів та ШІ:** злочинці дедалі частіше вдаються до дипфейків та підроблених документів для обходу систем перевірки клієнтів (KYC), а також імітують діяльність офіційних установ для виманювання персональних даних.
- **Ключова роль професійних посередників у легалізації злочинних доходів:** юристи, бухгалтери, банківські менеджери та агенти з нерухомості є критичною ланкою у схемах відмивання коштів, діючи як навмисно, так і через недбалість.
- **Оптимізація системи SAR через уникнення дублювання:** запроваджено новий підхід, за яким основне повідомлення про підозрілу діяльність у випадку шахрайства подає установа-отримувач коштів, а не установа жертви, що дозволяє зосередити ресурси на якісній аналітиці, а не на обробці дублікатів.
- **Вразливість інвестиційних схем до податкових шахрайств:** складні податкові схеми (Enterprise Investment Scheme) активно використовуються шахраями, які маніпулюють інвесторами через обіцянки податкових пільг та створення фіктивних компаній з непрозорою структурою власності та завищеними комісійними.

Звіти окремих інституцій та експертів

Організована злочинність у регіоні Меконгу: трансформація незаконних ринків і нові криміногенні вразливості ⁶

Третій випуск документу, опублікований в межах Мережі протидії транснаціональній злочинності в Меконгу (MNET-СТС), аналізує трансформацію незаконних ринків і криміногенних вразливостей у країнах регіону Меконгу — Камбоджі, Лаосі, М'янмі, Таїланді та В'єтнамі. Документ ґрунтується на відкритих джерелах, офіційних даних та інтерв'ю з представниками державних органів, правоохоронних структур, журналістами й

⁶ <https://globalinitiative.net/wp-content/uploads/2026/08/Mekong-Risk-Monitor-Issue-no.3-August-2026.pdf>

громадянським суспільством. Основна теза випуску полягає в тому, що сучасна організована злочинність у регіоні формується не через одну окрему вразливість, а внаслідок поєднання регуляторних прогалин, корупції, недостатнього державного контролю, транскордонної мобільності, легальної економічної інфраструктури, цифрових платформ і фінансових інструментів. Саме ця сукупність факторів дозволяє злочинним мережам адаптуватися до правоохоронного тиску, переміщувати операції між країнами та секторами, використовувати легальні підприємства як прикриття і залучати законні фінансові та логістичні системи до обслуговування незаконної діяльності. У випуску послідовно розглядаються п'ять напрямів: незаконний міжнародний обіг канабісу з Таїланду, каральна модель реагування на вживання наркотиків у Камбоджі, потенційне перетворення В'єтнаму на територію виробництва кетаміну, криміногенні ризики спеціальної економічної зони Sithandone у Лаосі та монетизація матеріалів сексуальної експлуатації дітей у цифровому середовищі Камбоджі.

Перший тематичний блок присвячено наслідкам лібералізації ринку канабісу в Таїланді. Після легалізації медичного використання канабісу у 2019 році та фактичної декриміналізації більшості частин рослини у 2022 році ринок почав стрімко розширюватися. Водночас реформа не була завершена створенням єдиного комплексного законодавчого режиму. Передбачений спеціальний закон щодо канабісу та конопель не набув чинності, а державне регулювання здійснювалося за допомогою окремих адміністративних і секторальних рішень, що створило тривалий період правової невизначеності. До квітня 2026 року в країні діяло близько 11 тисяч торговельних точок із продажу канабісу, а ще у 2023 році близько 1,38 млн осіб мали дозволи на його вирощування. Така кількість виробників і точок збуту істотно ускладнила контроль за загальними обсягами виробництва, походженням продукції та її кінцевим використанням.

Наслідком стало різке зростання незаконного експорту. Якщо у 2024 році було зареєстровано 786 випадків незаконного обігу із вилученням 4 598 кг канабісу, то у 2025 році — вже 3 135 випадків і 34 719 кг. Лише у січні 2026 року було зафіксовано 464 випадки та вилучено 6 500 кг. Значна частина контрабанди здійснюється через аеропорти: між лютим і груднем 2025 року спеціальна група в основних аеропортах Таїланду виявила 789 спроб незаконного вивезення та вилучила близько 19,2 тонни канабісу. Поряд з авіап перевезеннями використовуються поштові відправлення та морські маршрути, причому саме морські партії, хоча й виявляються рідше, мають значно більший середній обсяг. Документ також звертає увагу на те, що тайський канабіс дедалі частіше вилучається вже у країнах транзиту та призначення, зокрема в Європі.

Особливо важливим є те, що незаконна торгівля дедалі менше нагадує спонтанну діяльність окремих кур'єрів і дедалі більше — професіоналізовану транснаціональну схему. Організовані злочинні групи використовують соціальні мережі для вербування перевізників, оплачують подорожі до Таїланду та пропонують значну винагороду за доставку валіз із канабісом до Європи. У період із лютого по грудень 2025 року в тайських аеропортах було затримано кур'єрів із 47 країн. Паралельно іноземні покупці можуть нап'яму встановлювати зв'язки з тайськими постачальниками, контролюючи якість і тип продукції. Перенасичення внутрішнього ринку також створює економічний стимул для окремих виробників продавати продукцію на більш прибуткових зовнішніх нелегальних ринках. Таким чином, легальне або напівлегальне внутрішнє виробництво фактично стало ресурсною базою для транснаціональної контрабанди.

Проблему поглиблює фрагментація відповідальності між державними органами. Основним регулятором ринку залишається Міністерство охорони здоров'я Таїланду, тоді як роль Управління з контролю за наркотиками Таїланду (ONCB) у протидії контрабанді канабісу після реформи звузилася, а значна частина відповідальності за експортний контроль перейшла до митних органів. При цьому митна служба не має достатньої спроможності для перехоплення всіх незаконних потоків. Крім того, через неоднозначний правовий статус канабісу окремі справи вже не передаються поліції для розширених розслідувань організованих мереж так системно, як раніше. У результаті правоохоронні органи отримують обмежене уявлення про організаторів, постачальників і кінцевих отримувачів прибутку. Автори тому наголошують, що проста повторна криміналізація канабісу не усуне вже

сформовані канали незаконної торгівлі і навіть може витіснити частину ринку в тінь. Натомість необхідна єдина система контролю за всім ланцюгом — вирощуванням, переробкою, дистрибуцією, імпортом та експортом — разом із механізмом простежуваності походження продукції.

Другий блок стосується Камбоджі та надмірно каральної моделі державної політики щодо осіб, які вживають наркотики. У 2025 році камбоджійські органи затримали 26 421 особу у справах, пов'язаних із наркотиками. Станом на березень 2024 року з 45 122 осіб у місцях позбавлення волі 21 644, або близько 48%, утримувалися за наркозлочини, серед них понад дві тисячі неповнолітніх. Хоча законодавство дозволяє прокурорам і судам спрямовувати осіб на реабілітацію замість ув'язнення, на практиці цей механізм використовується недостатньо. Особи, затримані після позитивного тесту на наркотики, фактично опиняються між кількома варіантами — неофіційною оплатою, примусовою реабілітацією або кримінальним провадженням із ризиком ув'язнення.

Документ критично оцінює й саму реабілітаційну систему. У країні функціонують 18 відповідних центрів, однак інтерв'ю з колишніми пацієнтами показують, що частина таких закладів діє радше як місця примусового утримання, ніж лікування. Повідомляється про сувору дисципліну, фізичні покарання, недостатню якість харчування, відсутність належної психологічної допомоги та медикаментозної підтримки при синдромі відміни. Окремою системною проблемою є корупція. Хоча державні центри формально безкоштовні, респонденти повідомляли про вступні платежі у розмірі від 300 до 1 000 доларів США. Неофіційні платежі можуть виникати на різних етапах — від моменту затримання до зміни судової процедури, скорочення покарання, отримання харчування, медичної допомоги або доступу до сімейних відвідувань.

Унаслідок відсутності повноцінного лікування реабілітація часто стає лише тимчасовою перервою у вживанні наркотиків, після якої люди повертаються до залежності. Ситуацію ускладнює перенаселеність пенітенціарної системи та широке застосування попереднього ув'язнення: станом на грудень 2024 року близько 75% осіб у камбоджійських в'язницях перебували під вартою до винесення обвинувального вироку. Значну частину функцій, які не забезпечує держава, перебирають на себе громадські організації. Вони надають допомогу зі зменшення шкоди, медичні направлення, психологічну підтримку, професійне навчання, допомогу з працевлаштуванням, юридичний супровід та сприяють поверненню людей до сімей і громад. Автори наголошують, що з поширенням нових синтетичних наркотиків потреби осіб, які їх вживають, ставатимуть ще складнішими, тоді як наявна система до цього не готова. Тому політика має поступово зміщуватися від покарання до профілактики, лікування та реінтеграції, а правоохоронні ресурси — від низових споживачів і дрібних розповсюджувачів до великих постачальників та організованих мереж.

Третій тематичний блок аналізує можливу зміну ролі В'єтнаму в регіональній економіці синтетичних наркотиків. Центральним прикладом є ліквідація у березні 2025 року в Нячанзі найбільшого, за офіційними повідомленнями, виробничого об'єкта такого типу, виявленого у країні. Було вилучено близько 1,4 тонни кетаміну з чистотою майже 99% та майже 80 тонн прекурсорів. Операція включала окремі виробничі, складські та фінальні обробні майданчики, а передбачуваний організатор діяв під прикриттям бізнесу з розведення декоративних риб і залучив китайських, тайванських та в'єтнамських фахівців.

Цей випадок має принципове значення, оскільки В'єтнам традиційно розглядався передусім як транзитна країна для переміщення метамфетаміну, кетаміну та інших наркотиків між центрами виробництва, ринками споживання та експортними маршрутами. Виробництво означає якісно інший рівень проникнення злочинної діяльності у легальне середовище, адже потребує довгострокового доступу до нерухомості, промислового обладнання, прекурсорів, робочої сили та компаній-прикриттів. Водночас автори обережні у висновках: наразі немає достатніх доказів, що В'єтнам уже став сформованим центром виробництва кетаміну. Нячанг

пропонується розглядати як сигнальну подію, яка може свідчити про ширшу регіональну тенденцію.

Особливе занепокоєння викликає те, що мережа встигла орендувати землю, встановити промислове обладнання, закупити або імпортувати хімічні речовини, найняти персонал і розпочати виробництво до втручання правоохоронних органів. Моніторинг почався лише після передачі відповідної інформації китайськими органами. Це ставить питання щодо ефективності контролю за прекурсорами, перевірки реальної господарської діяльності підприємств, міжвідомчої координації та можливостей раннього виявлення нетипових закупівель. Автори також зазначають, що регіональний ринок синтетичних наркотиків стає географічно більш гнучким, а транснаціональні групи дедалі частіше використовують компанії-прикриття та законну комерційну інфраструктуру.

Документ окремо визначає індикатори, які слід відстежувати надалі: повторне виявлення виробничих майданчиків, незвичний імпорт лабораторного обладнання та скляного посуду, закупівлі хімічних речовин, що не відповідають заявленому профілю підприємства, поява іноземних хіміків або інвесторів, пов'язаних із невеликими промисловими об'єктами, та переміщення прекурсорів через порти й кордони. Значення має й внутрішній попит: локальний аналіз стічних вод у Ханой показав суттєве зростання концентрації кетаміну, що може створювати стимули для виробництва ближче до ринку споживання. Автори тому наголошують на посиленні раннього виявлення, контролю за прекурсорами та міжнародного обміну інформацією.

Четвертий блок присвячено спеціальній економічній зоні Sithandone у Лаосі. На відміну від попередніх прикладів, тут автори аналізують не вже сформований злочинний ринок, а передумови, які потенційно можуть зробити територію привабливою для організованої злочинності. Спеціальна економічна зона Sithandone була схвалена у 2018 році та позиціонується як великий інвестиційний проєкт із заявленим капіталом близько 9 млрд доларів США та реалізацією до 2050 року. Передбачено створення казино, готелів, курортів, вілл, гольф-поля та іншої інфраструктури. Зона розташована поблизу стику кордонів Лаосу, Камбоджі та Таїланду, що робить її важливим транскордонним вузлом, але одночасно підвищує її вразливість до незаконних потоків.

Особливим фактором ризику є можливе переміщення кримінальних мереж у відповідь на правоохоронний тиск в інших частинах регіону. Посилення боротьби з кібер-шахрайськими центрами у Камбоджі та спеціальній економічній зоні «Золотий трикутник» може стимулювати злочинні групи шукати нові території для діяльності. У провінції Чампасак у Лаосі уже фіксувалися торгівля людьми, значні вилучення наркотиків, контрабанда транспортних засобів та незаконний в'їзд іноземців. Також надходили повідомлення про групи іноземців без належних документів, які намагалися орендувати готелі або цілі будівлі, а окремі особи, пов'язані з кібер-шахрайськими операціями в Камбоджі, використовували провінцію як транзитний маршрут.

Вразливість посилюють модель управління спеціальними економічними зонами, корупційні ризики та майбутня діяльність казино. Автори проводять паралель із спеціальною економічною зоною «Золотий трикутник», яка вже давно асоціюється з наркотрафіком, відмиванням коштів, торгівлею людьми та кібер-шахрайством. Готівково-інтенсивний гральний сектор може використовуватися для інтеграції незаконних доходів, а нечітке розмежування між державними та приватними функціями створює ризик недостатнього контролю. Тому основний акцент зроблено на превентивних заходах: підвищенні прозорості управління, забезпеченні доступу правоохоронних органів, належному регулюванні казино, захисті працівників і врегулюванні соціальних питань ще до того, як злочинні структури зможуть укорінитися в зоні.

П'ятий блок присвячено монетизації матеріалів сексуальної експлуатації дітей у Камбоджі та демонструє, як ця проблема дедалі більше набуває ознак організованої цифрової кримінальної економіки. За наведеними у документі дослідженнями, приблизно кожна десята дитина у

Камбоджі віком 12–17 років — близько 160 тисяч осіб — пережила певну форму сексуальної експлуатації або насильства онлайн. Злочинці використовують соціальні мережі для початкового контакту, після чого переводять комунікацію у приватні або зашифровані месенджери та файлообмінні сервіси. Мережі можуть швидко змінювати назви та переходити на інші платформи після блокування, використовують фальшиві профілі, декілька акаунтів та моделі онлайн-грумінгу. Водночас їхня діяльність дедалі частіше виходить за межі однієї держави та охоплює кілька країн Південно-Східної Азії.

Особливо важливою є фінансова складова. У Telegram виявлялися групи, де користувачам демонстрували короткі попередні фрагменти контенту, а повний доступ надавався після оплати членства у закритій VIP-групі. Типова вартість становила від 1 до 5 доларів США, що забезпечувало низький поріг входу, але дозволяло отримувати прибуток за рахунок значної кількості користувачів. За даними APLE, близько 60% із 303 зафіксованих у 2025 році випадків онлайн-сексуальної експлуатації дітей містили певну форму платної підписки. В окремих випадках використовувалися камбоджійські банківські рахунки та локальні цифрові платіжні сервіси. Це демонструє, що фінансова інфраструктура є не другорядним елементом, а одним із механізмів функціонування і монетизації таких мереж.

Паралельно правоохоронна спроможність залишається недостатньою. Документ вказує на обмежені можливості у сфері цифрової криміналістики, трасування контенту та системної ідентифікації правопорушників. Навіть після затримання окремих осіб копії матеріалів можуть залишатися доступними онлайн, продовжуючи циркуляцію та вторинну віктимізацію постраждалих. Низький рівень повідомлення про такі злочини також ускладнює реагування: серед 226 онлайн-випадків, зафіксованих APLE, було ідентифіковано лише близько 20% постраждалих, а лише 14% брали участь у кримінальних процедурах. Серед причин — стигматизація, страх розголошення, недовіра до системи правосуддя та небажання проходити тривалі юридичні процедури.

Автори пропонують розглядати такі мережі саме як прояв організованої злочинності та залучати до реагування правоохоронні органи, технологічні компанії, фінансові установи, соціальні платформи та громадянське суспільство. Особливе значення надається фінансовим розслідуванням та інструментам протидії відмиванню коштів: відстеженню платежів, моніторингу фінансової інфраструктури, пов'язаної з експлуатаційними мережами, та перекриттю каналів отримання доходів. Одночасно необхідно розвивати спроможності у цифровій криміналістиці, платіжному трасуванні та онлайн-розслідуваннях, а також забезпечувати профілактику і підтримку постраждалих.

У підсумку третій випуск документа показує, що сучасна транснаціональна організована злочинність дедалі частіше існує не поза межами легальної економіки, а всередині неї, використовуючи законні

Висновки:

- **Необхідно посилити регуляторний контроль за секторами та економічною інфраструктурою, вразливими до використання організованою злочинністю,** зокрема виробництвом і обігом наркотичних речовин, спеціальними економічними зонами, казино та цифровими платформами.
- **Доцільно розширити використання фінансових розслідувань для виявлення та припинення діяльності організованих злочинних мереж,** зосереджуючись на відстеженні платежів, встановленні фінансових посередників та перекритті каналів монетизації злочинної діяльності.
- **Слід розвивати системи раннього виявлення нових кримінальних ризиків,** використовуючи індикатори нетипових закупівель прекурсорів і обладнання, невідповідності операцій заявленій господарській діяльності, зміни маршрутів незаконного обігу та переміщення злочинних мереж між юрисдикціями.
- **Важливо посилити міжвідомчу та транскордонну співпрацю,** забезпечивши системний обмін інформацією між правоохоронними органами, фінансовим сектором, регуляторами, технологічними компаніями та громадянським суспільством для комплексного реагування на транснаціональну організовану злочинність.

підприємства, фінансові сервіси, цифрові платформи, логістичні маршрути та інвестиційну інфраструктуру. Легальне виробництво канабісу може забезпечувати товар для незаконного експорту, комерційні підприємства — приховувати виробництво синтетичних наркотиків, спеціальні економічні зони та казино — створювати середовище для проникнення кримінального капіталу, а банківські рахунки й цифрові платежі — забезпечувати монетизацію онлайн-злочинів. Саме тому автори фактично обґрунтовують необхідність переходу від вузького правоохоронного реагування до комплексної моделі, що поєднує раннє виявлення ризиків, регуляторний контроль, фінансові розслідування, антикорупційні заходи, міжнародний обмін інформацією та співпрацю з приватним сектором. Центральним об'єктом протидії має бути не лише конкретний злочин або його безпосередній виконавець, а вся інфраструктура, яка забезпечує сталість злочинної діяльності — фінансові потоки, бізнес-прикриття, логістика, цифрові платформи, корупційні зв'язки та регуляторні прогалини.

Цифрові активи як нова основа фінансової інфраструктури ⁷

Документ аналізує поступове перетворення цифрових активів із відносно відокремленого сегмента криптовалютного ринку на один із елементів нової фінансової інфраструктури. Основна ідея звіту полягає в тому, що блокчейн дедалі частіше використовується не лише для торгівлі криптоактивами, а й як технологічна основа для платежів, розрахунків, випуску та обігу традиційних фінансових інструментів, управління активами та автоматизованої економічної взаємодії. Автори розглядають цей процес через п'ять взаємопов'язаних напрямів: розвиток платежів у стейблкоїнах, токенизацію реальних активів, вибір блокчейн-інфраструктури для традиційних фінансових установ, еволюцію стандартів комплаєнсу та формування нового сегмента автономних платежів за участю AI-агентів. Аналітичну основу звіту переважно становлять власні дані Chainalysis, отримані безпосередньо з блокчейн-мереж, зокрема щодо транзакційних потоків, поведінки гаманців, налаштувань систем моніторингу та ключових характеристик основних блокчейн-мереж.

Одним із центральних напрямів документа є стейблкоїни, які Chainalysis розглядає як один із найбільш зрілих прикладів переходу блокчейн-технологій у сферу реальної економічної діяльності. За оцінкою авторів, у 2025 році скоригований обсяг реальної економічної активності зі стейблкоїнами досяг приблизно 28 трлн дол. США. Важливо, що йдеться не про загальний обсяг усіх транзакцій у блокчейні, а про спеціально скоригований показник, який виключає операції з надання ліквідності, автоматизовану активність ботів та транзакції, пов'язані з максимальним вилученням вартості (MEV), оскільки вони можуть штучно збільшувати показники фактичного економічного використання стейблкоїнів. За даними Chainalysis, з 2023 року цей скоригований показник зростає із середньорічним темпом близько 133%, а за збереження базового тренду до 2035 року може досягти приблизно 719 трлн дол. США.

Водночас автори вважають базовий сценарій доволі консервативним і виділяють два фактори, які можуть значно прискорити подальше поширення стейблкоїнів. Першим фактором є масштабний міжпоколінний трансфер багатства — приблизно 80–100 трлн дол. США, які протягом наступних десятиліть можуть перейти від покоління бебі-бумерів до поколінь міленіалів і покоління Z (зумерів). Другим фактором є поступова інтеграція стейблкоїнів у звичайну торговельну інфраструктуру. У такій моделі користувач фактично перестає сприймати оплату стейблкоїном як окрему криптовалютну операцію, оскільки блокчейн стає прихованим технологічним рівнем платіжної системи. З урахуванням цих двох факторів Chainalysis моделює потенційне зростання річного обсягу стейблкоїнових транзакцій до приблизно 1,5 квадрильона дол. США у 2035 році.

Міжпоколінний трансфер капіталу розглядається не лише як економічний, а й як поведінковий фактор. Звіт виходить із того, що міленіали і зумери поступово ставатимуть домінуючими

⁷ <https://www.chainalysis.com/wp-content/uploads/2026/06/the-new-rails-2026-02-release.pdf>

групами фінансових споживачів у Північній Америці та Європі, причому серед них частка осіб, які вже користувалися або володіли криптоактивами, є значно вищою. За модельними оцінками Chainalysis, лише цей фактор потенційно може додати близько 508 трлн дол. США до щорічного обсягу стейблкоїнових операцій до 2035 року. Для традиційних фінансових установ це означає необхідність адаптувати свої продукти та інфраструктуру до потреб клієнтів, для яких використання інструментів на основі блокчейну вже стає звичною складовою фінансової взаємодії. В іншому разі частина клієнтських потоків може поступово переходити до альтернативних цифрових екосистем.

Окремо аналізується потенційне поширення стейблкоїнів у торговельних точках. Автори наголошують, що такі платежі можуть забезпечувати майже миттєве зарахування коштів, доступність 24/7 та зменшення частини витрат, пов'язаних із традиційною багаторівневою платіжною інфраструктурою. За прогнозою моделлю Chainalysis, кількість транзакцій зі стейблкоїнами, що здійснюються через блокчейн-мережі, може зрівнятися з масштабом операцій Visa і Mastercard приблизно у період між 2031 та 2039 роками, а широке впровадження стейблкоїнів у платіжну інфраструктуру торговельних точок потенційно може забезпечити близько 232 трлн дол. США додаткового щорічного транзакційного обсягу до 2035 року. На цій основі автори роблять висновок, що для банків і платіжних компаній конкуренція дедалі більше відбуватиметься не між окремими фінансовими продуктами, а між різними платіжними інфраструктурами за швидкістю, вартістю та зручністю.

У звіті також простежується перехід традиційних фінансових установ від обережного спостереження за розвитком регуляторного середовища до практичного впровадження інфраструктури на основі блокчейн-технологій. Це проявляється через придбання технологічних платформ, партнерства із спеціалізованими постачальниками та створення рішень, здатних одночасно працювати з традиційними й блокчейн-платіжними каналами. Як приклади автори наводять придбання Stripe компанією Bridge та партнерство Mastercard із BVNK. У цьому контексті блокчейн розглядається вже не як периферійна технологія, а як потенційна базова інфраструктура наступного покоління глобальних платежів.

Наступний великий напрям документа стосується токенизованих реальних активів (RWA). Йдеться про цифрове представлення традиційних активів, таких як облігації, акції, нерухомість або товари, що випускаються й управляються безпосередньо в блокчейн-середовищі. Chainalysis підкреслює, що цей ринок уже поступово виходить за межі експериментальних пілотів. Загальний обсяг RWA наближається до 30 млрд дол. США, а інституційний капітал дедалі більше випереджає роздрібну участь. Це відрізняє поточний цикл розвитку від попередніх етапів крипторинку, де саме роздрібні інвестори часто були першими користувачами нових продуктів. У сегменті RWA банки, фонди та великі керуючі активами дедалі частіше стають безпосередніми драйверами розвитку ринку.

Серед найбільш ліквідних категорій RWA найбільшим інституційним сегментом є токенизований державний борг США, зокрема такі продукти, як BlackRock BUIDL і Circle USYC. Водночас автори звертають увагу на методологічні обмеження: частина даних походить із платформи gwa.huz, яка враховує як ліквідні фінансові інструменти, так і токени, що представляють фізичні або малоліквідні активи. Для таких категорій, як нерухомість, відсутність постійного вторинного ринку ускладнює точне визначення поточної ринкової вартості, тому окремі оцінки необхідно розглядати як наближені.

Швидкість розвитку окремих сегментів RWA також свідчить про активну інституційну участь. Наприклад, кредитування, забезпечене активами, досягло ринкової вартості 1 млрд дол. США приблизно за 6,1 місяця після першого випуску відповідних активів у блокчейн-мережі, спеціалізоване фінансування — за 21,5 місяця, тоді як токенизованим товарам для досягнення такого самого показника знадобилося близько 36,2 місяця. На думку авторів, це демонструє, що після появи достатньо зрозумілої технологічної та регуляторної інфраструктури великі фінансові установи здатні швидко спрямовувати значні обсяги капіталу в on-chain продукти.

Аналіз майже 400 тис. адрес, які утримують RWA, дозволив Chainalysis виявити ще одну важливу тенденцію: токенизовані активи дедалі частіше стають безпосередньою точкою входу користувачів у блокчейн-екосистему. На Ethereum кількість нових гаманців, які отримували RWA протягом перших шести місяців після створення, різко зросла у 2026 році. Особливо виразною ця тенденція є для активів інституційного рівня: адреси, на яких зберігаються токенизовані активи у сегментах спеціалізованого фінансування або кредитування, забезпеченого активами, нерідко отримують перший токенизований реальний актив уже протягом першого тижня після створення. Це може свідчити про використання спеціально створених або попередньо авторизованих гаманців для управління інституційними фінансовими продуктами. Натомість у сегментах токенизованих товарів, акцій та інвестиційних фондів частіше беруть участь давно існуючі crypto-native користувачі.

Окремим показником зрілості RWA-ринку автори вважають поступове зближення його поведінки з традиційними фінансовими ринками. На прикладі токенизованого золота Chainalysis показує, що історично обсяги торгів ним майже не корелювали з традиційним ринком золота та переважно залежали від криптовалютних циклів ліквідності. Однак із другого кварталу 2025 року кореляція почала істотно зростати, у певні періоди перевищуючи 0,70, а у першому кварталі 2026 року залишалася на високому рівні. Це може означати, що зі зростанням ліквідності та інституційної участі токенизовані активи дедалі більше реагують на ті самі макроекономічні фактори, що й традиційні активи, зокрема інфляцію та геополітичні ризики.

Окремий розділ документа присвячено вибору блокчейн-інфраструктури для традиційних фінансових установ. Основна теза полягає в тому, що універсально найкращої мережі не існує. Вибір повинен залежати від конкретного активу, характеру операцій та ризик-профілю установи. Chainalysis пропонує оцінювати блокчейн-мережі за низкою взаємопов'язаних параметрів, серед яких стабільність комісій, пропускна здатність, швидкість остаточного розрахунку, рівень системної взаємозалежності, експозиція до незаконної діяльності та модель управління мережею. Bitcoin і Ethereum розглядаються як найбільш перевірені та ліквідні «інституційні якорі», мережі другого рівня, зокрема Arbitrum, Base та Polygon, — як більш збалансовані рішення з погляду продуктивності та вартості операцій, а Solana, BNB, XRP Ledger і TRON — як високопродуктивні мережі з низькими комісіями, але з окремими специфічними ризиками.

Автори наголошують, що при виборі мережі недостатньо орієнтуватися лише на середню вартість транзакції. Для фінансових установ критичною є також передбачуваність комісій. TRON, наприклад, демонструє відносно стабільний профіль витрат, тоді як Bitcoin має значний ризик різких цінових стрибків у періоди перевантаження. Аналогічно, необхідно розрізняти високу пропускну здатність і фактичну остаточність операції. Solana є одним із лідерів за кількістю транзакцій на секунду, проте Layer-2 рішення можуть мати дуже швидку початкову обробку, але потребувати додаткового часу для остаточного підтвердження транзакцій у базовій мережі. Для великих операцій із токенизованими активами така різниця між швидкістю обробки транзакції та моментом її остаточного розрахунку може мати принципове значення.

Окремо Chainalysis аналізує системну взаємозалежність централізованих бірж. Великі CEX регулярно переказують активи між собою для забезпечення ліквідності та виконання заявок на виведення, однак надмірна залежність від інших платформ може створювати ризик поширення проблем одного учасника на інших. У цьому контексті Solana демонструвала значну волатильність інституційної взаємозалежності, тоді як Bitcoin та Ethereum мали більш стабільний профіль. Автори фактично пропонують розглядати міжбіржову залежність як окремий елемент системного ризику поряд із суто технологічними характеристиками мережі.

Для сфери ПВК/ФТ особливе значення має аналіз експозиції до незаконної діяльності в блокчейн-мережах. За даними Chainalysis, Ethereum, Solana та Base поєднують значні обсяги ліквідності із часткою відомої незаконної активності нижче 1%. TRON водночас має значний

масштаб використання, зокрема як інфраструктура для стейблкоїнових переказів, але частка надходжень від джерел, класифікованих як незаконні, наближається до 4%. Автори прямо зазначають, що це не повинно автоматично означати відмову від певної мережі. Важливішим є питання, чи здатна фінансова установа виявляти, оцінювати та мінімізувати відповідну експозицію за допомогою ефективних інструментів моніторингу.

До інфраструктурних критеріїв також належить модель управління мережею. Bitcoin забезпечує високий рівень незмінності та практично не передбачає централізованого втручання, тоді як деякі Proof-of-Stake і Layer-2 екосистеми мають Security Council, DAO чи інші механізми, здатні реагувати на масштабні технічні інциденти. Для регульованої фінансової установи така відмінність має оцінюватися з урахуванням власних правових та операційних вимог. Тому Chainalysis пропонує сприймати характеристики мереж не як рейтинг, а як матрицю прийняття рішення, в якій оптимальна архітектура визначається конкретним активом і сценарієм використання.

Найбільш безпосередньо пов'язаним із ПВК/ФТ є розділ, присвячений новому базовому рівню комплаєнсу під час здійснення операцій у блокчейн-мережах. Chainalysis розрізняє пряму експозицію, коли кошти надходять безпосередньо від відомого джерела незаконної діяльності, та непряму експозицію, коли між таким джерелом і кінцевим отримувачем коштів є одна або кілька проміжних адрес. Прямий моніторинг уже значною мірою стандартизувався, тоді як підходи до непрямой експозиції залишаються значно менш однорідними. Немає єдиного підходу до того, наскільки віддаленим від первинного ризикового джерела може бути ланцюг транзакцій, щоб відповідний зв'язок і надалі враховувався системою моніторингу, а також який рівень експозиції має бути підставою для формування попередження.

За результатами аналізу конфігурацій систем моніторингу автори констатують значне підвищення загального стандарту комплаєнсу. У 2020–2021 роках лише близько 10% нових організацій застосовували налаштування моніторингу, які відповідали рівню 10% найсуворіших конфігурацій, зафіксованих у 2020 році. До 2026 року майже половина новопідключених організацій уже працює на рівні, який п'ять років тому вважався передовою практикою. Отже, рівень контролю, який раніше вважався передовою практикою, поступово стає базовим стандартом моніторингу операцій у блокчейн-мережах.

Традиційні фінансові установи при цьому демонструють суворіші підходи, ніж криптовалютні біржі. Для непрямой експозиції до потоків, які не віднесені до незаконних категорій, середній мінімальний поріг у криптобірж становить близько 950 дол. США, тоді як у традиційних фінансових установ — близько 150 дол. США. Для незаконних потоків відповідні показники становлять приблизно 100 та 55 дол. США. Для найбільш чутливих категорій, серед яких санкційні суб'єкти та фінансування тероризму, фактично застосовується майже нульова толерантність. Водночас для **програм-вимагачів, шахрайських схем, даркнет-ринків та деяких інших категорій ризику** пороги непрямой експозиції можуть у 10–20 разів перевищувати пороги прямої експозиції. Chainalysis наголошує, що такі відмінності можуть використовуватися злочинцями для ускладнення виявлення незаконних потоків, зокрема шляхом проведення коштів через додаткові проміжні адреси.

Важливою особливістю є і регіональна неоднорідність. Для прямої експозиції до незаконної діяльності підходи в регіонах Америки, Європи, Близького Сходу та Африки, а також Азійсько-Тихоокеанського регіону загалом є подібними, тоді як підходи до моніторингу непрямой експозиції суттєво відрізняються. Регіон Близького Сходу та Африки демонструє найбільш суворі та концентровані конфігурації, регіон Америки займає проміжну позицію, а Азійсько-Тихоокеанський регіон має в середньому вищі пороги. Це означає, що використання установами однієї й тієї самої платформи блокчейн-аналітики не гарантує однакового рівня ефективності моніторингу та контролю, оскільки він залежить від конкретних налаштувань системи, встановлених порогів і підходів до оцінки ризику. Для належної оцінки контрагента необхідно аналізувати конкретні параметри моніторингу, ризик-апетит установи та регуляторне середовище, в якому вона працює.

На цій основі Chainalysis рекомендує традиційним фінансовим установам орієнтуватися насамперед на стандарти, що застосовуються іншими установами традиційного фінансового сектору, а не на усереднені показники криптоіндустрії, розглядати непрямую експозицію як повноцінний складник комплаєнс-ризиків та приділяти особливу увагу якості даних, на яких ґрунтується робота систем блокчейн-аналітики. Автори підкреслюють, що навіть правильно встановлені пороги не дадуть належного результату, якщо адреси неправильно атрибутовані до суб'єктів або ризикових категорій. Тому належна перевірка постачальника аналітики має охоплювати не лише формальне покриття мереж, а й якість кластеризації, категоризації та практичну ефективність даних у реальних системах моніторингу.

Завершальна частина документа присвячена автономним платежам, які можуть здійснюватися AI-агентами без безпосередньої участі людини в кожній окремій операції. Як приклад аналізується протокол x402, розроблений Coinbase. Його модель дозволяє інтегрувати стейблкоїнову оплату безпосередньо у веб-запит: AI-агент отримує вимогу щодо оплати, самостійно оцінює її, здійснює платіж у блокчейн-мережі та повторно надсилає запит із підтвердженням оплати. Це дає змогу здійснювати платежі без використання традиційних механізмів виставлення рахунків, створення окремих платіжних облікових записів та ручного підтвердження кожної транзакції.

На Base кількість x402-транзакцій зросла від майже нульового рівня у середині 2025 року до понад 100 млн у першому кварталі 2026 року. Значна частина раннього вибухового зростання була пов'язана зі спекулятивною активністю навколо PING, однак ця активність водночас стала масштабним навантажувальним тестом для протоколу. Структура операцій поступово змінюється: частка транзакцій на суму понад 1 дол. США зросла приблизно з 49% до 95%, а показник переходу користувачів від тестування до реальних платежів за шість місяців збільшився приблизно у чотири рази. Це може свідчити про поступовий перехід від суто експериментального використання до більш регулярних сценаріїв.

При цьому Chainalysis не стверджує, що автономні платежі за участю агентів штучного інтелекту вже набули широкого поширення серед традиційних фінансових установ. Нинішні

Висновки:

- **Доцільно посилити моніторинг непрямой експозиції у блокчейн-мережах**, оскільки значні відмінності між прямими та непрямыми порогами можуть використовуватися для обходу систем ПВК/ФТ.
- **Варто запровадити багатофакторну оцінку блокчейн-інфраструктури** з урахуванням вартості, швидкості, остаточності розрахунків, системної взаємозалежності, незаконної експозиції та моделі управління.
- **Слід інтегрувати стейблкоїни та токеновані реальні активи у стратегічне планування фінансових установ**, зважаючи на їх перехід від експериментального до інституційного використання.
- **Необхідно забезпечити підготовку комплаєнс-систем до автономних платежів за участю штучного інтелекту**, передбачивши моніторинг програмно ініційованих транзакцій, гаманців і контрагентської експозиції.

користувачі протоколу залишаються переважно активними учасниками криптовалютної екосистеми, однак сам протокол уже демонструє реальні обсяги транзакцій, сформовану базу користувачів та ознаки регулярного повторного використання. У перспективі, якщо AI-агенти дедалі активніше виконуватимуть економічні функції, їм буде потрібна платіжна інфраструктура, здатна автоматично обробляти велику кількість дрібних транзакцій у реальному часі. Це водночас формує новий напрям комплаєнс-контролю, оскільки фінансовим установам потенційно доведеться аналізувати не лише особу клієнта та окрему транзакцію, а й автономну поведінку програмних агентів, характеристики пов'язаних із ними гаманців, концентрацію операцій та їхню експозицію до ризикової чи незаконної діяльності в блокчейн-мережах.

У цілому звіт демонструє поступове стирання межі між традиційними фінансами та цифровими активами. Стейблкоїни формують нові платіжні й розрахункові

канали, RWA перетворюють блокчейн на інфраструктуру для випуску та дистрибуції традиційних фінансових активів, а системи блокчейн-аналітики поступово стають базовим інструментом інституційного комплаєнсу. Одночасно нові форми автоматизованих платежів розширюють перелік ризиків, які фінансовим установам доведеться враховувати у своїх системах управління ризиками та ПВК/ФТ. Водночас наведені у документі довгострокові прогнози є саме аналітичними оцінками Chainalysis і не повинні сприйматися як гарантований сценарій розвитку ринку.

Шахрайські центри як елемент місцевої економіки: соціальні, економічні та екологічні ризики для Камбоджі⁸

Документ аналізує індустрію онлайн-шахрайства в Камбоджі не як ізольоване явище кіберзлочинності, а як масштабну транснаціональну незаконну економіку, яка поступово вбудовується у місцеві соціальні, економічні та просторові структури. Автори виходять із того, що за останні два десятиліття Камбоджа перетворилася на один із ключових вузлів глобальної індустрії онлайн-шахрайства. Якщо спочатку відповідні операції були переважно пов'язані з казино у прикордонних районах, то з часом шахрайські центри поширилися на другорядні міста, сільські райони, території корінних народів та великі прибережні земельні концесії. У результаті вони почали впливати не лише на криміногенну ситуацію, а й на характер місцевого розвитку, використання земель, структуру зайнятості, мобільність населення, інвестиційні процеси, соціальні зв'язки та довкілля. Саме тому ключова теза дослідження полягає в тому, що онлайн-шахрайство необхідно розглядати одночасно як проблему організованої злочинності, розвитку, ринку праці, земельного врядування, соціального захисту та екологічної політики.

Автори наголошують, що масштабні правоохоронні операції проти шахрайських центрів, проведені владою Камбоджі у 2025 році, хоча й призвели до скорочення частини операцій та депортації або виїзду десятків тисяч працівників, не ліквідували структурних умов існування цієї індустрії. Польові дані свідчать, що територіальні та інфраструктурні мережі, на яких вона базується, значною мірою збереглися. У низці районів продовжується будівництво об'єктів, пов'язаних із шахрайською діяльністю, зберігається вербування працівників, а самі операції поступово переходять у більш розосереджені та менш помітні форми. Це демонструє високу адаптивність кримінальної економіки: закриття конкретного шахрайського центру або проведення рейду не означає руйнування всієї системи, оскільки залишаються будівлі, логістичні маршрути, інвестиційні зв'язки, місцеві посередники, робоча сила та економічна залежність громад від такої діяльності.

Одним із центральних аспектів документа є аналіз географічного поширення онлайн-шахрайства. Автори виокремлюють три основні форми його територіальної дифузії: прикордонні коридори, в яких казино та шахрайські центри формують єдину економічну систему; великі земельні концесії та великі інвестиційно-будівельні та інфраструктурні проекти; а також нові сільські й віддалені території, включаючи землі корінних народів. Особливе значення у цьому процесі мають другорядні міста. Вони достатньо інтегровані у національні транспортні, енергетичні й телекомунікаційні мережі, щоб підтримувати складні транснаціональні операції, але водночас залишаються менш помітними для державного контролю, медіа та громадськості, ніж столиця чи великі урбанізовані центри. Унаслідок цього інфраструктура, створена для економічного розвитку, транскордонної торгівлі та залучення інвестицій, паралельно створює сприятливі умови для поширення незаконної економічної діяльності.

Найбільш усталена модель поширення онлайн-шахрайства сформувалася у прикордонних містах, насамперед у Баветі, Пойпеті та Прумі. Завдяки своєму географічному розташуванню

⁸ <https://globalinitiative.net/wp-content/uploads/2026/08/Gabriel-Fauveaud-Ronan-Kemp-Divided-lands-How-cyber-scams-reshape-communities-economies-and-ecosystem-in-Cambodia-GI-TOC-August-2026.pdf>

Бавет на кордоні з В'єтнамом і Пойпет на кордоні з Таїландом тривалий час відіграють важливу роль у транскордонній торгівлі та регіональних транспортних потоках. Вони були включені до регіональних економічних коридорів та отримували значні інвестиції у транспорт, телекомунікації й спеціальні економічні зони. У другій половині 2010-х років цей процес був додатково посилений припливом китайського капіталу. Паралельно уряд Камбоджі активно розвивав казино-економіку, орієнтовану передусім на іноземних відвідувачів із сусідніх держав, де азартні ігри були заборонені або істотно обмежені. Проте розвиток казино відбувався не у нейтральному економічному середовищі. Прикордонні райони Камбоджі історично були пов'язані з контрабандою, незаконною торгівлею природними ресурсами, наркотиками, зброєю та іншими товарами, а контроль над такими територіями часто здійснювали місцеві політико-економічні еліти, які накопичували капітал через поєднання легальних і нелегальних видів діяльності.

Таке історичне поєднання казино, готівкових потоків, транскордонної мобільності, корупційних зв'язків та існуючих кримінальних мереж створило сприятливе середовище для переорієнтації економічної моделі, сформованої навколо казино у складнішу систему онлайн-шахрайства. Автори зазначають, що прикордонні шахрайські центри поступово перестали бути окремими закритими об'єктами і перетворилися на центри ширших місцевих економічних систем. Навколо них виникає попит на житло, будівництво, транспорт, харчування, розваги, охоронні послуги та інші види діяльності. Це означає, що значна частина формально легального місцевого бізнесу починає прямо або опосередковано залежати від існування незаконної індустрії. Внаслідок цього економічна база цілих міст поступово переорієнтовується з традиційних аграрних, торговельних чи виробничих функцій на обслуговування транснаціональної кримінальної економіки.

Важливим чинником закріплення такої моделі автори визначають так зване «grey governance» — середовище, у якому формальні механізми державного управління переплітаються з приватними економічними інтересами та діяльністю кримінальних структур. На прикладі Бавета у дослідженні наведено свідчення працівників про тісні контакти власників і керівників шахрайських центрів із представниками провінційної влади. За оцінками респондентів, правоохоронні заходи можуть застосовуватися вибірково, тоді як більші комплекси, пов'язані з впливовими бізнесменами або політичними покровителями, мають більше можливостей уникати втручання та продовжувати діяльність. Така практика послаблює ефективність державного контролю, підриває довіру населення до правоохоронних органів і створює умови для фактичної безкарності економічно та політично впливових суб'єктів. У цьому контексті корупція виступає не лише супутнім ризиком, а одним із системних чинників, що сприяють вкоріненню шахрайської індустрії у місцеву економіку та систему управління.

На прикладі Прума автори показують, як поширення онлайн-шахрайства безпосередньо змінює характер міського розвитку та просторової забудови. Місто спочатку розвивалося навколо казино, однак після 2021 року почало переживати нову хвилю будівельної активності, пов'язаної вже передусім із шахрайськими центрами. На околицях зводилися нові житлові комплекси, вілли та інші об'єкти нерухомості, зростала кількість будівельників, водіїв, охоронців та працівників онлайн-операцій. З кінця 2010-х років змінилася й структура інвесторів — тайський капітал дедалі частіше поступався китайському. У результаті шахрайські центри почали виконувати функцію каталізатора місцевого будівельного й інвестиційного буму.

Водночас дослідження показує, що фізична інфраструктура незаконної економіки може швидко адаптуватися до зміни умов. У Пойпеті після проведення урядових операцій у 2026 році дослідники зафіксували повторне використання спорожнених шахрайських центрів у нічний час невеликими групами осіб, які продовжували діяльність у прихованому режимі. В інших випадках колишні казино використовувалися для пов'язаної незаконної діяльності, включаючи збут наркотиків. Таким чином, навіть після припинення конкретної діяльності самі будівлі, закриті комплекси та транспортна інфраструктура залишаються активом, придатним для повторного використання злочинними мережами.

Важливою рисою досліджуваного явища є його поступова соціальна нормалізація. Для місцевих мешканців онлайн-шахрайство часто перестає сприйматися виключно як зовнішня кримінальна загроза, оскільки воно забезпечує робочі місця та доходи в умовах обмежених альтернатив. Опитані мешканці одночасно визнавали ризики насильства, катувань, експлуатації та невиплати заробітної плати, але позитивно оцінювали можливість заробляти більше, підтримувати сім'ю чи оплачувати навчання. За словами одного з мешканців села, розташованого приблизно за 5 км від Прума, близько 70 % жителів громади їздять туди на роботу, зокрема до казино та пов'язаних з онлайн-шахрайством підприємств. Частина колишніх фермерів переходить у сферу охорони, будівництва, обслуговування казино або безпосередньо онлайн-операцій. Це створює своєрідну пастку залежності: громада може усвідомлювати кримінальний характер індустрії, але водночас бути матеріально зацікавленою в її збереженні через відсутність конкурентоспроможних законних джерел доходу.

Другим важливим просторовим механізмом поширення є великі земельні концесії та мегапроекти. Найбільш виразно ця тенденція простежується у прибережних районах поблизу Сіануквіля та у провінції Кохконг. Починаючи з кінця 2000-х років значні площі земель, у тому числі в межах природоохоронних територій, передавалися інвесторам під масштабні туристичні та великі інвестиційно-будівельні проекти. Після пандемії COVID-19, коли туристичний сектор зазнав різкого спаду, частина таких об'єктів і територій була перепрофільована для розміщення онлайн-шахрайських операцій. У результаті в одному просторовому середовищі почали поєднуватися казино, курорти, інфраструктурні мегапроекти, нові житлові райони та спеціально побудовані шахрайські комплекси. Корпоративна непрозорість і складні ланцюги субпідряду при цьому ускладнюють встановлення фактичних інвесторів, операторів та кінцевих вигодоодержувачів.

У провінції Кохконг наслідком такого розвитку стало масштабне переміщення місцевого населення та втрата доступу до традиційних джерел існування. Сотні домогосподарств були переселені з прибережних територій углиб країни, а наприкінці 2021 року понад 1 100 сімей у районах Ботум-Сакор і Кірі-Сакор, за даними дослідження, були фактично змушені погодитися на запропонований владою механізм оформлення та розподілу земельних ділянок. Втрата доступу до узбережжя, морських і лісових ресурсів позбавляла частину мешканців можливості продовжувати традиційні види господарської діяльності, зокрема рибальство, та змушувала переходити до найманої праці у будівництві й інших сферах, прямо або опосередковано пов'язаних із новими великими проектами та шахрайською індустрією. Майже всі опитані в Кохконзі повідомляли, що або самі працювали у шахрайських центрах чи пов'язаних із ними сферах, або мали такий досвід серед членів сім'ї чи знайомих. Таким чином, зміна порядку використання та розподілу земель безпосередньо впливає на структуру місцевої зайнятості й посилює економічну залежність громад від незаконної індустрії та пов'язаних із нею видів діяльності.

Окремо автори аналізують нову тенденцію до переміщення шахрайських центрів у сільські та віддалені райони. Вона стала більш помітною після посилення державних операцій у 2025 році. Такі території привабливі для організаторів через нижчу видимість, слабший державний нагляд, меншу увагу громадськості та можливість швидкого освоєння значних площ. Водночас саме у сільській місцевості поява великого комплексу може мати особливо сильний трансформаційний ефект, оскільки місцева економіка та соціальна структура є менш диверсифікованими.

Показовим прикладом є місцевість Лаока у провінції Мондулкірі, землі якої традиційно заселені, використовуються та управляються корінним народом Бунонг. Приблизно за один рік на або поблизу земель традиційного користування було споруджено комплекс приблизно з 30 будівель. Супутникові та аерофотознімки, наведені у звіті, демонструють надзвичайно швидко зміну території. Після відкриття комплексу навколо нього майже одразу почали концентруватися мігранти, дрібні торговці й неформальні постачальники послуг. Таким чином сформувалася нова економічна екосистема, орієнтована на обслуговування працівників

шахрайського центру, а традиційні форми землекористування та господарювання почали поступатися місцем залежній неформальній економіці.

Особливу роль у цій системі відіграють транспортні мережі. На прикладі водія таксі в Мондулкірі автори демонструють, як формально легальна або неформальна транспортна діяльність інтегрується у логістичну мережу онлайн-шахрайства. Водії через Telegram-групи отримують замовлення від представників шахрайських центрів, перевозять іноземних працівників між різними провінціями, чекають біля об'єктів протягом тривалого часу та фактично стають частиною циркуляційної системи робочої сили. При цьому вони не обов'язково сприймають себе як учасників незаконної діяльності, розглядаючи свою роль виключно як надання транспортних послуг. Цей приклад демонструє, наскільки складно провести чітку межу між безпосередньо кримінальною діяльністю та ширшим колом легальних або напівформальних послуг, від яких залежить функціонування шахрайських центрів.

Суттєвий вплив індустрія має і на ринок праці. У традиційній моделі другорядні міста Камбоджі виконували функцію зв'язку між сільськогосподарськими районами, регіональними ринками та великими міськими центрами. Розвиток онлайн-шахрайства змінює цю функцію, оскільки все більша частина економічної активності спрямовується на обслуговування транснаціональної незаконної індустрії. Молоді працівники залишають плантації та інші традиційні види зайнятості через вищі зарплати у шахрайських центрах. Це призводить до дефіциту робочої сили у сільському господарстві, збільшення навантаження на інших членів сімей та руйнування усталених моделей сімейної й громадської праці. У найбільш маргіналізованих районах незаконна економіка фактично перетворюється на головне або навіть єдине доступне джерело доходу.

Ще одним системним наслідком є зростання земельної нерівності та спекулятивної активності. Поява шахрайських центрів стимулює місцевих землевласників і зовнішніх інвесторів купувати землю в очікуванні подальшого підвищення цін та попиту на житло. Земельні ділянки перетворюються на активи, орієнтовані на потреби іноземних працівників, казино та шахрайських центрів: будуються орендні будинки, вілли, закриті житлові комплекси та розважальні заклади. Проте така модель робить місцевий ринок нерухомості надзвичайно залежним від зовнішніх політичних, регуляторних і безпекових факторів. Після державних рейдів або загострення прикордонної нестабільності попит може різко знижуватися, залишаючи нові об'єкти порожніми та демонструючи вразливість спекулятивно орієнтованого розвитку.

Паралельно посилюється концентрація земель у руках впливових бізнесменів, які мають зв'язки з представниками влади та інвесторів. У низці сільських районів жителі повідомляли про тиск із метою продажу земель під шахрайські комплекси. Особливо вразливими залишаються публічні, комунальні та землі звичаєвого користування. У документі детально описано випадок, коли громадський ставок і прилегла територія були передані інвесторам без належного інформування та погодження з місцевою громадою. Згодом на цьому місці було споруджено великий комплекс. Автори розглядають такі ситуації як прояв ширшої проблеми слабого земельного врядування, коли формальне обґрунтування проєктів через «розвиток» може приховувати непрозорі механізми передачі ресурсів та фактичне привласнення територій через впливових місцевих посередників.

Важливим виміром проблеми є також екологічна шкода. На узбережжі розвиток пов'язаних із шахрайською економікою об'єктів відбувається в межах або поряд із морськими, прибережними та лісовими природоохоронними територіями. Розбудова комплексів, доріг та супутньої інфраструктури сприяє подальшому освоєнню захищених територій, витісненню місцевих громад і скороченню традиційних видів зайнятості, зокрема дрібного рибальства. У східних сільських районах подібні процеси зачіпають каучукові плантації та інші сільськогосподарські землі. Швидке будівництво великих комплексів і пов'язаних об'єктів змінює ландшафт та створює додатковий тиск на природні ресурси.

Особливо гострою проблемою стає забруднення води та накопичення відходів. Невеликі села часто не мають систем водовідведення, очищення стічних вод і поводження з відходами, розрахованих на раптову появу сотень працівників великих комплексів. У Trapeang Phlong жителі повідомляли про істотне погіршення якості води поблизу шахрайських центрів. В окремих водоймах стало неможливо ловити рибу, а забруднення створило ризики для сільськогосподарських земель, зрошувальної води та харчових продуктів. Таким чином, екологічні наслідки шахрайської економіки не обмежуються територією самих комплексів, а можуть безпосередньо впливати на продовольчу безпеку та традиційні засоби існування цілих громад.

Підсумовуючи результати дослідження, автори наголошують, що незаконна економіка у Камбоджі вже не є маргіальною або тимчасовою складовою місцевого розвитку. У ряді територій вона фактично сама стала одним із його визначальних факторів. Вона впливає на те, де та як відбувається будівництво, які земельні активи зростають у ціні, куди переміщується робоча сила, які види бізнесу отримують доходи та які взаємовідносини формуються між місцевими органами влади, інвесторами і населенням. Тому навіть масштабне закриття шахрайських центрів не гарантує ліквідації самої кримінальної екосистеми. Якщо економічна залежність громад, фізична інфраструктура, непрозорі земельні механізми, місцеві політичні зв'язки та обмежені можливості легальної зайнятості залишаються незмінними, відповідна діяльність може швидко відновлюватися або переміщуватися у нові райони.

Саме тому рекомендації авторів мають комплексний характер. Вони пропонують офіційно розглядати онлайн-шахрайство як проблему розвитку, що потребує спеціальних соціально-економічних програм, цільового фінансування та довгострокових політик для постраждалих територій. Важливим є систематичне оцінювання соціальних, економічних та екологічних наслідків діяльності шахрайських центрів і залучення місцевих громад до обговорення проблем та розроблення заходів реагування. Значна увага приділяється широким інформаційним кампаніям, які мають охоплювати не лише потенційних працівників, а й молодь, сім'ї, школи, університети, професійно-технічні заклади та місцеві громади. Автори також пропонують використовувати транспортні мережі як канал профілактики, створювати механізми громадського моніторингу ранніх ознак будівництва шахрайських комплексів, захоплення земель чи екологічної шкоди та передавати таку інформацію незалежним організаціям і компетентним органам для проведення розслідувань і міжнародної співпраці.

Окреме значення для протидії незаконним фінансовим потокам має рекомендація щодо посилення прозорості іноземних інвестицій і належної перевірки великих девелоперських проєктів. Автори пропонують підвищити вимоги до

Висновки:

- **Необхідно розширити підхід до протидії онлайн-шахрайству**, розглядаючи його не лише як проблему кіберзлочинності та організованої злочинності, а й як фактор соціально-економічної трансформації, що впливає на зайнятість, землекористування, місцеве врядування та стан довкілля.
- **Доцільно посилити прозорість та належну перевірку іноземних інвестицій і великих будівельних та інфраструктурних проєктів**, зокрема у сферах казино, нерухомості та спеціальних економічних зон, забезпечивши розкриття власності та координацію між інвестиційними органами, фінансовими регуляторами і правоохоронними органами.
- **Слід запровадити системний моніторинг територій і громад, найбільш уразливих до поширення шахрайської індустрії**, включаючи раннє виявлення будівництва шахрайських комплексів, незаконного привласнення земель, різких змін місцевих ринків праці та пов'язаного екологічного забруднення.
- **Важливо забезпечити економічну диверсифікацію постраждалих територій та створення законних альтернативних джерел зайнятості**, щоб зменшити залежність місцевих громад від казино та шахрайських центрів і мінімізувати ризик відновлення або переміщення такої діяльності після правоохоронних операцій.

розкриття структури власності, посилити перевірку високоризикових інвестицій у казино, нерухомість та спеціальні економічні зони, а також забезпечити тіснішу координацію між органами, відповідальними за інвестиційну політику, фінансовими регуляторами та правоохоронними структурами. Такий підхід має обмежити можливості транснаціональних кримінальних мереж вкладати незаконні кошти у формально легальні інвестиційні та будівельні проєкти. Водночас у найбільш уражених провінціях автори рекомендують активно розвивати законні галузі, здатні створювати стійкі робочі місця та місцеві доходи. Саме економічна диверсифікація розглядається як одна з ключових передумов довгострокового зменшення залежності громад від казино та шахрайських центрів і, відповідно, підвищення їхньої стійкості до повторного проникнення кримінальної економіки.

Пастка Ла-Маншу: чому посилення кордонів живить організовану злочинність⁹

Останнє десятиліття стало періодом безпрецедентної політизації міграції, яка з технічного питання віз, ринку праці та консульських послуг перетворилася на один з головних каталізаторів політичної нестабільності в демократичних країнах. Британський канал (Ла-Манш) став не просто географічним бар'єром, а символом цієї кризи, місцем, де перетинаються людські долі, злочинні інтереси та державна влада. Аналіз, проведений Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC), показує, що ситуація навколо невеликих човнів, які перетинають протоку, є не аномалією, а яскравим проявом глобальної закономірності, яка виникає щоразу, коли маршрут з високим попитом на міграцію стикається з жорстким кордоном. Це явище отримало назву «пастки політики» (policy trap), і розуміння її механізмів є критично важливим для будь-якого уряду, що прагне знайти ефективне та гуманне рішення.

Ключова помилка, яку допускають політики, полягає у сприйнятті контрабандистів як пасивних постачальників послуг, що лише реагують на попит мігрантів. Насправді, як наголошується у звіті, вони є активними творцями та формувачами ринку. Злочинці досліджують слабкі місця в системах прикордонного контролю, виявляють корумповані інституції та прогалини в законодавстві, а потім агресивно рекламують свої послуги.

Використовуючи платформи соціальних мереж, такі як TikTok, Telegram та Facebook, злочинні мережі рекламують маршрути, ціни та навіть пропонують знижки за зняті на відео вдалі перетини, фактично фабрикуючи попит. Цей активний маркетинг призводить до раптових сплесків міграційних потоків, які переполюють приймальні можливості транзитних країн та країн призначення, створюючи хаос і політичну кризу. Таким чином, контрабандисти не просто обслуговують потік, вони його генерують, використовуючи відчай та надії людей як сировину для свого бізнесу.

У відповідь на хаос держави вдаються до укріплення кордонів. Скорочення квот на переселення, ускладнення доступу до процедур надання притулку та розширення практики тримання під вартою – всі ці заходи логічні на перший погляд, але фатальні в довгостроковій перспективі. Вони зменшують пропозицію безпечних та легальних шляхів міграції, не впливаючи на попит. Розрив між попитом та пропозицією – це і є ринок, який займають контрабандисти. Кожне нове обмеження фактично є субсидією для організованої злочинності, розширюючи ринок і роблячи її послуги ще більш затребуваними.

Найменш інтуїтивним, але найважливішим етапом пастки є консолідація ринку внаслідок правоохоронного тиску. Історично переправлення людей було напівформальним і вкоріненим у місцевих громадах промислом. Часто цим займалися колишні мігранти, члени діаспори або місцеві транспортники, які певною мірою підзвітні своїм громадам. Систематичні поліцейські

⁹ <https://globalinitiative.net/wp-content/uploads/2026/08/Tuesday-Reitano-Breaking-the-human-smuggling-policy-trap-GI-TOC-August-2026.pdf>

операції та посилений контроль знижують саме цей, найнижчий, рівень. Дрібні контрабандисти не мають капіталу, щоб витримати конфіскацію майна, операційної безпеки, щоб уникнути стеження, чи юридичних ресурсів для виживання після судового переслідування. Натомість ті, хто можуть адаптуватися та витримати тиск, – це вже професійні злочинні угруповання, які мають корумповані зв'язки, готовність застосовувати насильство, налагоджені канали відмивання грошей та транскордонну логістику.

Отже, замість того, щоб зникнути, ринок переправлення лише консолидується. Він переходить до рук меншої кількості, але більш жорстоких, заможних та захищених акторів. Ціна на послуги зростає, а мігранти стають ще більш вразливими, потрапляючи в боргову кабалу та піддаючись підвищеному ризику. Цей процес наочно демонструє ситуація на французькому узбережжі, де після десятиліття правозастосовних заходів домінують ієрархічні курдські мережі, які територіально контролюють зони запуску човнів і жорстоко конкурують між собою.

Наслідки цієї пастки є руйнівними і виходять далеко за межі безпосередньо моря. По-перше, держава платить двічі – один раз на прямі витрати на правоохоронні заходи, а другий раз – на політичну ціну видимого провалу. Згадані у звіті приклади британсько-руандійського партнерства, яке коштувало приблизно 700 мільйонів фунтів стерлінгів, або ж австралійської офшорної обробки заявок про надання притулку, вартістю понад мільярд австралійських доларів щорічно, яскраво ілюструють це.

По-друге, міграція стає зброєю як у внутрішній, так і в міжнародній політиці. Всередині країн вона стає стрижнем популізму, а на міжнародній арені – важелем тиску. Інцидент у іспанському анклаві Сеута в липні 2026 року, де за один день кордон перетнули десятки тисяч людей, став шокуючим нагадуванням, що країна, яка делегувала контроль за своїм кордоном третій стороні, стає від неї залежною, а ця залежність може бути використана як зброя.

По-третє, соціальна згуртованість руйнується. Хвиля антиімміграційних протестів і заворушень у Великій Британії влітку 2024 року, коли нападам піддавалися готелі, де проживали шукачі притулку, та мечеті, демонструє, як національна політична проблема перетворюється на локальну образу, роз'їдаючи тканину суспільства. І нарешті, єдиним беззаперечним бенефіціаром цього циклу стає організована злочинність, яка отримує надприбутки від торгівлі людськими життями.

Проте, вихід з цієї пастки існує. Глобальний досвід свідчить, що для подолання гострих прикордонних криз необхідний комплексний підхід, що складається з чотирьох взаємопов'язаних елементів.

Перший елемент – це узгоджене з країною відправлення та спільне фінансування управління кордоном. Домовленості мають бути справді партнерськими, визнавати спільні інтереси (наприклад, боротьба зі злочинними мережами) та враховувати неминуче переміщення маршрутів, як це вже сталося, коли човни почали запускати з бельгійського узбережжя.

Другий елемент – це політика повернення, яка є надійною, реалістичною та широко розрекламованою. Угода між ЄС та Туреччиною 2016 року є показовим прикладом: хоч кількість фактичних повернень була невеликою, сама загроза повернення у поєднанні з легальними шляхами для сирійців призвела до значного зниження потоків. Вона працює як комплекс, а не просто як покарання.

Третій елемент – це розвідувально-орієнтоване проактивне порушення діяльності мереж у країнах походження та транзиту. Ключовим тут є націлювання не на виконавців (як правило, самих мігрантів або колишніх мігрантів, які легко замінюються), а на організаторів, фінансистів, постачальників обладнання та відмивачів грошей.

Четвертий, і найважливіший елемент, який Велика Британія тривалий час ігнорувала, – це створення безпечних і легальних маршрутів. Вони не є «жалісливою» поступкою, а прямим інструментом боротьби з контрабандистами, оскільки підривають саму бізнес-модель

злочинців, пропонуючи мігрантам альтернативу. Як показав досвід прийому українських біженців, швидке надання статусу та доступу до ринку праці є найкращим захистом від експлуатації та торгівлі людьми.

Новий прем'єр-міністр Великої Британії Енді Бернем успадкував ситуацію, в якій попередні уряди вже зробили значні інвестиції у перші три елементи – домовленості з Францією, нарощування потенціалу Національного агентства з питань злочинності (NCA) та створення системи санкцій проти контрабандистів. Результати цих зусиль вже помітні: до серпня 2026 року кількість прибуття малими човнами скоротилася на 43% порівняно з попереднім роком. Однак, цей успіх є частковим і може бути оманливим. Значну частину скорочення можна пояснити загальноєвропейським трендом (падіння на 37% за даними Frontex) та змінами в країнах походження, зокрема поверненням сирійців додому після падіння режиму Асада. Головна загроза полягає в тому, що цей успіх не є стабільним, а сам ринок переправлення через канал – надзвичайно пружним.

Найкращим підтвердженням цього та найважливішим тестом для нового уряду є виникнення феномену «зворотного переправлення» (reverse smuggling) – невеликого, але зростаючого потоку мігрантів, які нелегально залишають Велику Британію, прямуючи до континентальної Європи. Цей потік є повністю політично згенерованим. Він виникає через асиметрію у візовому режимі (для деяких національностей, наприклад, бангладешців, отримати британську навчальну візу легше, ніж шенгенську), обмеження мобільності після Brexit та складні умови в самій британській системі надання притулку.

Висновки:

- **Репресії консолідують, а не знищують ринок контрабанди людей.** Поліцейський тиск знищує дрібних, локальних злочинців та звільняє місце для великих, добре фінансованих і жорстоких злочинних угруповань.
- **Контрабандисти — не пасивні посередники, а активні творці попиту.** Вони не просто реагують на бажання мігрантів, а формують його через агресивний маркетинг у соцмережах, створюючи нові потоки та спрямовуючи їх туди, де кордони слабші.
- **Комплексний підхід — єдиний дієвий.** Жоден окремих захід не працює ізольовано. Ефективність досягається лише поєднанням чотирьох елементів: співпраці з країною виходу мігрантів, дієвої політики повернення, проактивного розслідування та створення легальних маршрутів.
- **Відсутність легальних шляхів — це субсидія для злочинців.** Коли держава не пропонує безпечних альтернатив, вона фактично штовхає людей в обійми контрабандистів. Легальні маршрути (навіть обмежені) є не гуманітарною поступкою, а прямим інструментом підризу бізнес-моделі організованої злочинності.

Структура цього ринку на британському боці досі фрагментована, що є унікальною можливістю для уряду. Він перебуває на тій стадії, яку французьке узбережжя пройшло десятиліття тому, – до консолідації та олігополізації злочинними угрупованнями. Якщо Велика Британія зможе запровадити правозастосовні заходи проти цього зворотного потоку, одночасно інтегруючи їх з легальними шляхами та співпрацею з ЄС, вона зможе уникнути повторення помилок минулого. Якщо ж буде обрано лише посилення репресій, країна ризикує створити на своєму узбережжі нову, не менш жорстоку версію курдських кланів, які сьогодні контролюють французький берег.

Підсумовуючи, можна стверджувати, що проблема Ла-Маншу не зникне, навіть якщо цифри прибуття продовжать падати. Велика Британія залишається частиною глобальної системи нелегальної міграції, і її кордони залишатимуться привабливими. Зараз завдання полягає в

тому, щоб перетворити це розуміння на політику, яка витримає випробування наступною хвилею кризи, адже, як свідчить історія, паузи в тиску на кордони завжди бувають короткими.

Глобалізація злочинності: знайомі обличчя на нових територіях ¹⁰

Останні півтора року стали періодом безпрецедентної експансії транснаціональних злочинних угруповань, які, використовуючи прогалини в міжнародному праві та слабкість окремих національних урядів, стрімко поширили свій вплив далеко за межі традиційних регіонів діяльності. Якщо раніше ми звикли сприймати такі організації, як венесуельську «Трен де Арагуа», мексиканське «Нове покоління Халіско» (CJNG), бразильське «Перше столичне командування» (PCC) чи італійську «Ндрангету», виключно в контексті країн походження, то сьогодні їхня присутність фіксується на всіх континентах – від Латинської Америки до Європи, Африки та Азіатсько-Тихоокеанського регіону.

Цей феномен не лише змінює глобальний ландшафт організованої злочинності, а й кидає виклик усталеним методам протидії, які, як свідчить Глобальний індекс організованої злочинності за 2025 рік, дедалі частіше виявляються неефективними через брак скоординованих міжнародних зусиль.

На перший погляд, найпомітнішим трендом мала б стати активізація так званих «мафіозних груп» – структурованих організацій із чіткою ієрархією, територіальною прив'язкою та впізнаваним лідерством. Саме вони найчастіше з'являються у заголовках новин, саме з ними асоціюються нарковійни, корупційні скандали та резонансні вбивства. Однак дані Індексу демонструють дещо несподівану динаміку: середній показник присутності мафіозних груп у світі залишається відносно стабільним, коливаючись від 3,89 у 2023 році до 4,02 у 2024-му та знижуючись до 3,95 у 2025-му. Натомість найбільш стрімке зростання, яке зафіксував Індекс, стосується категорії «іноземні актори» – показник якої досяг позначки 5,68 у 2025 році, що є найвищим приростом серед усіх типів злочинних суб'єктів.

Ця, на перший погляд, суперечливість має просте пояснення, яке криється в методології оцінювання. Одна й та сама організація класифікується як мафіозна група виключно в межах своєї країни походження. Як тільки вона переносить свою діяльність за кордон – відкриває логістичні хаби, вербує місцевих посередників або інтегрується в чужі кримінальні ринки – вона автоматично переходить до категорії «іноземних акторів» у цих нових юрисдикціях. Таким чином, зростання цього показника є прямим віддзеркаленням процесу глобалізації злочинності: те, що на внутрішньому рівні може виглядати як стагнація або навіть спад (як-от зниження активності «Ндрангети» в окремих регіонах Італії), на міжнародному рівні обертається стрімким поширенням впливу, який охоплює десятки країн одночасно.

Найяскравішим прикладом цієї тенденції є венесуельський картель «Трен де Арагуа», який у себе на батьківщині забезпечує майже максимальний показник мафіозного впливу – 9,5 бали. Однак справжній вибух його активності стався після міграційної кризи, коли тисячі венесуельців, включно з членами угруповання, розосередилися по сусідніх країнах, а масштабний рейд проти лідерів картелю в 2023 році лише прискорив їхню інтеграцію в уже існуючі локальні осередки. Наслідки цього процесу одразу відобразилися на регіональних показниках: у Чилі та Перу бали за присутність іноземних акторів зросли з 5,0 до 6,5, у Болівії – на один пункт до 5,5, тоді як Колумбія та Еквадор і без того мають одні з найвищих у світі оцінок у цій категорії – 7,5 та 8,0 відповідно. Подібна експансія не є стихійною – вона відбувається за чітко визначеними маршрутами, які часто збігаються з потоками легальних мігрантів, що робить її майже непомітною для правоохоронних органів, поки кримінальна інфраструктура вже не пустить коріння в новому середовищі.

Не менш показовою є історія бразильського PCC, який у себе вдома також демонструє високий рівень впливу – 8,0 балів, однак його міжнародна діяльність викликає набагато більше занепокоєння. У сусідньому Парагваї ця організація фактично взяла під контроль частину пенітенціарної системи, що вивело країну на перше місце у світі за рівнем домінування іноземних злочинних угруповань – 9,0 балів. Навіть Уругвай, який традиційно вважався

¹⁰ <https://globalinitiative.net/analysis/foreign-actors-familiar-faces-the-globalization-of-organized-crime-is-being-driven-by-cartels-you-already-know/>

відносно благополучним, відчув на собі зростання присутності РСС, що відобразилося в підвищенні його показника з 2,5 до 4,0 за два роки. Але географія РСС не обмежується Латинською Америкою – через кокаїнові маршрути, що перетинають Атлантику через Західну Африку, група закріпилася на Африканському континенті та в Європі, де вона активно співпрацює з італійськими та балканськими покупцями, одночасно використовуючи китайські мережі для постачання синтетичних прекурсорів і відмивання незаконних доходів. Більше того, РСС укладає логістичні альянси з «Трен де Арагуа», створюючи своєрідне злочинне інтернаціональне об'єднання, яке охоплює весь ланцюжок – від виробництва наркотиків до їхнього розповсюдження на найвіддаленіших ринках.

Італійська «Ндрангета», яку вважають найбагатшою та найвпливовішою мафіозною організацією у світі, забезпечує своїй країні майже максимальний бал у категорії мафіозних груп – 9,0. Проте основна частина її реальної могутності реалізується саме за межами Апеннін. Як провідний гуртовий гравець на європейському ринку кокаїну, «Ндрангета» створила потужні опорні пункти в ключових портах Північного моря – Роттердамі, Антверпені та Гамбурзі. Це миттєво позначилося на показниках іноземних акторів у цих країнах: у Нідерландах бал зріс із 4,5 у 2021 році до 7,0 у 2025-му, у Бельгії – до 6,0, а в Німеччині – до 7,5. Ці цифри ідеально корелюють із логістичними ланцюжками організації, які з'єднують латиноамериканських брокерів, логістичні мережі РСС та албанських посередників із європейськими портами, часто прокладаючи шлях через західноафриканські транзитні пункти. Крім того, «Ндрангета» давно закріпилася в Латинській Америці, Канаді та Сполучених Штатах, що робить її справді глобальним гравцем, чії операції синхронізовані в різних часових поясах і юрисдикціях.

Мексиканські картелі – Сіналоа та CJNG – додають цій картині ще один вимір. У самій Мексиці їхня діяльність забезпечує максимальну оцінку мафіозного впливу – 9,0 балів, однак найбільші темпи зростання спостерігаються далеко за межами країни. За останнє десятиліття ці організації не лише активно включилися в кокаїновий трафік, але й стали ключовими гравцями на ринку синтетичних наркотиків, використовуючи прекурсори, що надходять із Китаю та Індії. Вони розгорнули виробничі потужності з виробництва метамфетаміну в різних частинах Європи, Азії та Африки, діючи через місцевих кримінальних посередників, що дозволяє їм уникати прямого контролю. Особливо показовою є експансія в Австралії та Новій Зеландії, де мексиканські картелі стали основними постачальниками синтетичних наркотиків, що відразу позначилося на показнику Нової Зеландії – він зріс із 3,5 у 2021 році до 5,0 у 2025-му. Водночас їхнє дедалі активніше використання тихоокеанських острівних пунктів перевантаження, зокрема Фіджі та Папуа-Нової Гвінеї, викликає серйозні побоювання, що ці транзитні території можуть самі стати споживчими ринками, що призведе до нової хвилі насильства та зростання рівня організованої злочинності в регіоні, який донедавна вважався відносно безпечним.

Мабуть, найкращою ілюстрацією того, як транснаціональна злочинна діяльність фіксується в категорії «іноземні актори», є історія албанського кокаїнового синдикату Kompania Bello. Ця організація, що складалася з 14 злочинних кланів, на папері вважалася албанською, однак її реальне керівництво здійснювалося з... в'язниці в Еквадорі. Її лідер безпосередньо вів переговори з південноамериканськими постачальниками, тоді як кокаїн переміщувався з Роттердама та Антверпена осередками групи в Нідерландах, Бельгії та Італії. Цікаво, що через таку децентралізовану структуру показник мафіозного впливу самої Албанії впав за три ітерації Індексу з 7,0 до 6,5 – адже група фактично не діяла на території країни свого формального походження. Натомість її сліди чітко проявилися в Еквадорі (8,0), Нідерландах (7,0) та Іспанії (7,5). Kompania Bello ніколи не діяла ізольовано – вона будувала партнерства з еквадорськими брокерами, колумбійськими та мексиканськими картелями, а також використовувала китайську підпільну банківську систему, створюючи багатонаціональну мережу, де представники чотирьох країн взаємодіяли в межах одного нелегального ринку.

Найефективніші правоохоронні операції останніх років, як-от п'ятирічне розслідування Operation Los Blancos під егідою Європолу та Євроюсту, що призвело до демонтажу Kompania

Bello у 2020 році, або проєкт INTERPOL I-CAN, у рамках якого в 2025 році в Боготі було заарештовано «найвищого боса» «Ндрангети» в Латинській Америці, демонструють, що успішна протидія можлива лише за умови дзеркального відображення транснаціональної природи самих злочинних груп. Ці операції об'єднували зусилля десятка країн, використовували спільні розвідувальні дані та координували арешти в різних юрисдикціях одночасно, що дозволяло завдавати нищівних ударів по всіх ланках кримінального ланцюжка.

У той час, коли злочинні мережі стають дедалі більш інтернаціоналізованими, взаємопов'язаними та технологічно оснащеними, зниження рівня міжурядової взаємодії ризикує підірвати один із небагатьох інструментів, який реально довів свою ефективність. Картелі та мафії не визнають національних кордонів, вони використовують будь-яку прогалину в регулюванні, будь-яку суперечність між правовими системами та будь-яку політичну нестабільність для розширення своєї присутності. Їхня глобалізація відбувається набагато швидше, ніж процес адаптації державних інститутів до нових реалій. І поки уряди різних країн зосереджені на внутрішніх проблемах або геополітичному суперництві, злочинні синдикати продовжують будувати власну глобальну інфраструктуру, об'єднуючи зусилля, ресурси та ринки, створюючи паралельний світ, у якому головною валютою є не гроші, а безкарність і здатність діяти швидше, ніж закон.

Саме цей розрив у швидкостях – між злочинною експансією та міждержавною реакцією – стає сьогодні головною загрозою глобальній безпеці, і саме його подолання вимагає не просто більш скоординованих, а принципово нових підходів, заснованих на випереджальній розвідці, спільних юридичних механізмах та політичній волі, яка, на жаль, дедалі частіше стає дефіцитним ресурсом у сучасному світі.

Висновки:

- **Глобалізація злочинності відбувається через експансію.** Найбільше зростання в Індексі організованої злочинності зафіксовано саме в категорії «іноземні актори». Це свідчить про те, що кримінальні організації активно переносять свою діяльність за межі країн походження, створюючи транснаціональні мережі.
- **Найбільші злочинні синдикати світу діють на всіх континентах, інтегруючись у локальні ринки.** Їхня експансія відбувається через логістичні альянси, використання міграційних потоків, контроль над портами та співпрацю з місцевими кримінальними структурами.
- **Транснаціональна природа злочинності вимагає міжнародної координації, однак саме цей інструмент зараз слабшає.** Найуспішніші операції базувалися на спільних розслідуваннях десятка країн. Проте показник міжнародної співпраці показав мінімальне зростання з 2021 року через фрагментацію міжнародних відносин.
- **Кримінальні групи використовують глобальні ланцюги постачання,** що робить боротьбу з ними складною без системного підходу.

Рекомендовані матеріали

Чому футбол поєднує всі фактори ризику одночасно і як готуватися до застосування Регламенту (ЄС) 2024/1624 до клубів і агентів ¹¹

13 червня 2026 року вийшла книга Уні ван ден Берг (Oonagh van den Berg) «The Football Financial Crime Blueprint: Modernising Compliance» — дев'ятий і наразі останній том авторської серії «Modernising Compliance». Підзаголовок визначає жанр точніше за назву: «A Practical Guide to Money Laundering, Fraud, Corruption and Financial Crime Risk in Football» —

¹¹ <https://www.amazon.co.uk/dp/B0H533H5MX>

це не журналістське розслідування і не академічна монографія, а практичний посібник з управління ризиками, орієнтований на комплаєнс-функцію.

Структура книги охоплює десять предметних блоків: відмивання коштів через футбольні клуби, трансфери та інвестиційні структури; корупцію, хабарництво та мережі впливу у світовому футболі; шахрайські ризики у трансферах, спонсорських і комерційних угодах та у діяльності посередників; проникнення організованої злочинності й експозицію до незаконних фінансових потоків; санкції, бенефіціарну власність та офшорні структури; ставки, маніпулювання результатами матчів і загрози доброчесності; проблеми банків і платіжних провайдерів під час обслуговування футбольних клієнтів; крипто-активи, фан-токени та цифрові активи; жіночий і дитячо-юнацький футбол як зони майбутніх ризиків; і, нарешті, практичні рамки врядування, наглядового контролю та управління ризиками фінансової злочинності. Цільова аудиторія заявлена широко — клуби й керівники, керівні органи та ліги, банки й платіжні провайдери, інвестори та спонсори, регулятори й правоохоронні органи, фахівці з комплаєнсу, ПВК/ФТ, протидії шахрайству, ризиків та аудиту, фахівці зі спортивного врядування.

Найцінніший для методологічної роботи елемент книги — не перелік типологій, а модель поєднання факторів ризику, покладена в її основу. Авторка виходить із того, що футбол одночасно містить усі характеристики, кожна з яких окремо є нейтральною: великі фінансові потоки, складні структури власності, активи без об'єктивної ринкової вартості (трансферні права, права на зображення), транскордонні платежі, посередники, множинність юрисдикцій і значний обсяг комерційної активності, побудованої на відносинах, які важко незалежно оцінити. Жодна з цих ознак сама собою не свідчить про неправомірність, але їх сукупність істотно змінює ризикове середовище. Такий підхід — від економіки галузі до контролів, а не навпаки — є прямим запереченням поширеної практики складання переліків індикаторів без розуміння того, чому саме певний сектор є привабливим для злочинних потоків.

Регуляторний горизонт, який робить книгу практично актуальною, задано правом Європейського Союзу. Регламент (ЄС) 2024/1624 (AMLR) включає професійні футбольні клуби та футбольних агентів до кола підзвітних суб'єктів: загальні положення Регламенту застосовуються з 10 липня 2027 року, а щодо клубів і агентів — з 10 липня 2029 року. Держави-члени можуть повністю або частково звільнити від застосування клуби нижчих дивізіонів, а також клуби вищого дивізіону з річним оборотом менше 5 млн євро протягом двох попередніх років; сфера охоплення обмежена операціями з інвесторами, спонсорами, футбольними агентами та трансферами гравців. Для України матеріал релевантний у контексті наближення національного законодавства до пакета ЄС 2024 року: питання про включення професійних футбольних клубів і футбольних агентів до кола суб'єктів первинного фінансового моніторингу постане як частина цього процесу.

ІНШІ НОВИНИ

RUSI про незавершену справу британського антилегалізаційного нагляду: передавання приблизно 60 000 юридичних, бухгалтерських і корпоративних фірм під нагляд FCA і чому консолідація сама собою не гарантує результативності¹²

Королівський об'єднаний інститут оборонних досліджень (RUSI) опублікував коментар Вероніки Стретфорд-Тюк (Veronica Stratford-Tuke), наукової співробітниці Центру фінансів і безпеки RUSI. Предметом аналізу є реформа нагляду у сфері протидії відмиванню коштів щодо юридичного, бухгалтерського секторів і TCSP у Великій Британії: приблизно 60 000 фірм переходять під нагляд FCA замість наявної системи. Авторка визначає цю реформу як

¹² <https://www.rusi.org/explore-our-research/publications/commentary/unfinished-business-effective-uk-anti-money-laundering-supervision>

найзначнішу з незавершених справ, що залишилися після Звіту про взаємну оцінку Великої Британії 2018 року, і підкреслює, що шлях до рішення тривав сім років і охопив два Плани протидії економічній злочинності. Рішення підтверджено відповіддю Казначейства Його Величності на консультації у червні 2026 року; фінансування нової моделі має здійснюватися на основі повного відшкодування витрат, для запровадження режимів обміну інформацією потрібне окреме законодавство, а Управління з питань професійного антилегалізаційного нагляду (OPBAS) продовжує діяти протягом перехідного періоду, який, за оцінкою уряду, «неминуче триватиме кілька років».

Центральна теза коментаря сформульована як умова, а не як заперечення реформи: ризик-орієнтований підхід працює лише тоді, коли наглядовий орган справді розуміє сукупність, яку наглядає. Саме тут авторка бачить головний виклик для FCA, адже піднаглядна сукупність є надзвичайно різномірною — від фірм «великої четвірки» та великих юридичних практик до вуличних конторок із передачі права власності на нерухомість і індивідуальних бухгалтерів. Ключове застереження полягає в тому, що ні FCA, ні професійні наглядові органи не бачать повної картини поодиночі, а отже реформа має бути побудована як передання знань, а не як заміна одного наглядового органу іншим. Це прямо визначає й спосіб оцінювання успіху: авторка формулює тест як питання не про те, наскільки гладко відбудеться передання наглядових функцій, а про те, чи призведе воно до справді ефективного нагляду за великою й різномірною сукупністю фірм.

Другий блок аргументації стосується толерантності до ризику. Фірмам потрібна дискреція, щоб концентруватися на високих ризиках і робити менше там, де ризик низький, без страху негативних наслідків; прозоре формулювання FCA власного апетиту до ризику могло б, за оцінкою авторки, створити спільну мету для регулятора й піднаглядних суб'єктів. У цьому контексті вона критично оцінює рамку вимірювання результативності Казначейства, яка розглядає наглядову активність (моніторинг, забезпечення дотримання, роз'яснювальна робота) та результати виконання «функції гейткіпера»: вимірювання успіху кількістю клієнтів, яким фірми відмовили в обслуговуванні, здатне створити хибні стимули. Це застереження змістовно збігається з висновком звіту FATF щодо де-ризикінгу, розглянутого в цьому ж випуску, — надмірна обережність, стимульована самою системою вимірювання, виштовхує клієнтів у менш прозорі канали, замість того щоб зменшувати ризик.

Третій блок — довіра як інфраструктурна умова нагляду. Авторка фіксує її погіршення: групи експертів з обміну розвідувальною інформацією (Intelligence Sharing Expert Working Groups) було розпущено через розрив довіри, а в окремих секторах, особливо юридичному, взаємна довіра залишається слабкою. Це спостереження має принципове значення для оцінки реформи: консолідація наглядових повноважень сама собою не створює каналів обміну інформацією, а без них ризик-орієнтований нагляд перетворюється на формальну перевірку документів. Практичні рекомендації коментаря спрямовані саме на цю проблему: провести базове опитування рівня розуміння ризиків фірмами з можливістю повторення в часі, використати відрядження фахівців з приватного сектору для передання галузевої експертизи до FCA, реалізувати заявлену амбіцію FCA бути регулятором, керованим даними та цифровими інструментами, зберігши при цьому знання професійних наглядових органів, і залучити правоохоронні органи, щоб фірми розуміли, як саме виглядає ризик відмивання коштів на практиці.

Колапс продовольчого ресурсу: як китайський бізнес знищує екосистеми ¹³

Західноафриканське узбережжя, зокрема акваторія Гвінеї-Бісау, стало ареною екологічної катастрофи, що має далекосяжні наслідки для всього регіону.

¹³ <https://www.occrp.org/en/feature/a-key-food-source-collapsed-off-west-africas-coast-as-chinese-ships-ground-the-species-into-fishmeal>

Розслідування, проведене OCCRP, виявило вражаюче виснаження популяції сардинели – ключового виду риби, який є основним джерелом білка для місцевого населення. Причиною цього колапсу стала діяльність двох великих китайських плавучих фабрик, які переробляли вилов на рибне борошно та риб'ячий жир для експорту, насамперед до Туреччини та В'єтнаму. Незважаючи на те, що уряд Гвінеї-Бісау запровадив заборону на виробництво рибного борошна на початку 2026 року, судна-порушники просто перемістилися південніше, до Сьєрра-Леоне, продовжуючи свою руйнівну діяльність, що ставить під загрозу продовольчу безпеку та засоби для існування ще мільйонів людей.

Згідно з внутрішньою оцінкою, проведеною урядом Гвінеї-Бісау в 2025 році, загальна біомаса шести досліджуваних видів риби скоротилася майже вдвічі порівняно з попереднім дослідженням 2013 року – з приблизно 339 680 до 164 700 тонн. Найбільш критичним є стан сардинели: біомаса виду *Sardinella maderensis* впала майже на 90 відсотків – зі 125 027 тонн у 2013 році до лише 16 433 тонн у 2025 році. Ці цифри, які свідчать про технічний колапс популяції, є результатом систематичного вилову, який здійснювався задля забезпечення сировиною двох плавучих заводів – Tian Yi He 6 та Hua Xin 17, що належать китайським компаніям і прибули до вод Гвінеї-Бісау у 2019 та 2024 роках відповідно.

Прямий зв'язок між діяльністю цих суден та катастрофічним падінням запасів риби визнає і директор департаменту промислового рибальства Міністерства рибальства та морської економіки країни Амаду Джало. Він прямо заявив, що сектор виробництва рибного борошна є очевидною причиною занепаду сардинели. Заборона, введена урядом на початку 2026 року, мала на меті захистити «рибу, призначену для споживання людиною, особливо для незахищених верств населення», оскільки сардинела є критично важливим джерелом дешевого білка. Проте цей крок виявився лише тимчасовим рішенням, яке переклало проблему на плечі сусідньої країни. Згідно з даними моніторингу морського руху, вже у травні-червні 2026 року китайські фабричні судна та флот із шести турецьких риболовецьких суден, які постачали їм сировину, перебазувалися до вод Сьєрра-Леоне, країни, чії рибні запаси також тривалий час перебувають під значним тиском.

Наслідки цієї кризи відчуються не лише на рівні статистичних звітів, а й у повсякденному житті місцевих громад. На віддаленому острові Бубаке в архіпелазі Біжагос, де проживає близько 4000 людей, рибальство є основою виживання. Місцеві рибалки розповідають, що вилов різко скоротився, а сардинела стала надзвичайно рідкісною. Раніше вихід у море тривав день-два, але тепер, щоб спіймати хоч щось, доводиться проводити в морі до п'яти днів, і навіть цього часто недостатньо. Це ставить під загрозу продовольчу безпеку та доходи приблизно 120 000 осіб, зайнятих у риболовному секторі країни.

Екологічні збитки виходять далеко за межі однієї країни, оскільки води навколо архіпелагу Біжагос є ключовими нерестовищами для багатьох мігруючих видів. Це особливо тривожно, враховуючи, що акваторія архіпелагу, який є біосферним заповідником ЮНЕСКО, є домівкою для дельфінів, ламантинів, акул, скатів, морських черепах та численних колоній птахів. Таким чином, діяльність китайських суден підриває не лише продовольчу безпеку, а й біорізноманіття унікальної екосистеми.

Слід зазначити, що для рибного борошна та риб'ячого жиру, вироблених цими плавучими заводами, було налагоджено чіткий експортний канал. Компанія Bissau Wang Sheng Fisheries Development Co SARL, очолювана менеджером Лінь Жигао, яка також є головою і міноритарним акціонером китайської компанії-власника Tian Yi He 6, відповідала за переважну більшість експорту. Згідно з даними зовнішньої торгівлі, за період діяльності фабрик компанія експортувала рибного борошна та жиру на суму щонайменше 141 мільйон доларів США, причому більше ніж на 133 мільйони доларів товару було відправлено до Туреччини та В'єтнаму.

На тлі кризи викликає занепокоєння не лише сама діяльність компаній, а й їхня репутація та дотримання законодавства. Так, материнська компанія Weihai Tianyihe Marine Biotechnology Company Limited ще у 2016 році призупиняла свою діяльність у китайському місті Вейхай

через надмірне забруднення та порушення виробничих норм. У 2020 році активи компанії були заморожені через борги на суму майже 4,6 мільйона доларів, а у 2023 році її було визнано банкрутом, а активи дочірніх структур – заарештовано. Попри це, Tian Yi He 6 продовжує працювати, а представництво компанії в Гвінеї-Бісау очолює керівник, який опинився у центрі судових розглядів у Китаї. Також частина турецьких риболовецьких суден, що обслуговували фабрики, неодноразово притягувалися до відповідальності в Гвінеї-Бісау за незаконні операції в забороненій зоні, відключали системи супутникового стеження, що є типовою ознакою тіньових операцій у риболовстві.

Розслідування показує, що на зміну одного випадку браконьєрства приходить інший, як от переміщення флоту до Сьєрра-Леоне, де місцеві рибалки вже роками скаржаться на виснаження запасів через промисловий вилов.

Таким чином, ситуація біля узбережжя Гвінеї-Бісау є яскравим прикладом глобальної проблеми нерегульованого промислового рибальства, коли економічні інтереси великих корпорацій, часто прихованих за складною структурою власності, ставляться вище за продовольчу безпеку та екологічну стійкість цілих регіонів. Переміщення флоту до Сьєрра-Леоне демонструє, що локальні заборони, без міжнародної координації та моніторингу, є малоефективними. Доки в міжнародному праві не буде створено дієвих механізмів відповідальності за виснаження рибних запасів у виключних економічних зонах прибережних держав, а головне – доки не буде забезпечено прозорість ланцюгів постачання рибного борошна на глобальні ринки, подібні кризи продовжуватимуть повторюватися, залишаючи місцеві громади Західної Африки сам на сам з екологічною катастрофою.

Ефективність ракетних ударів США проти наркотрафіку — міфи та реальність ¹⁴

Повернення Сполучених Штатів до практики завдання ракетних ударів по суднах, підозрюваних у перевезенні наркотиків, яке відбулося наприкінці серпня 2026 року, знаменує собою важливий етап у тривалій та суперечливій війні з наркотрафіком у західній півкулі.

Цей крок, зроблений після двомісячної паузи, демонструє рішучість адміністрації Трампа продовжувати обраний курс, попри зростаючу кількість доказів, які ставлять під серйозний сумнів ефективність такої стратегії. Заяви президента про приголомшливий успіх, зокрема про нібито 98% скорочення морських перевезень наркотиків до США до січня 2026 року, вступають у різке протиріччя з даними прикордонних служб та експертними оцінками, що змушує глибше проаналізувати реальний стан справ.

Ключовим індикатором для оцінки ситуації слугують обсяги вилучень наркотичних речовин, зокрема кокаїну, який є основним вантажем на цільових суднах. Хоча цей показник не є досконалим і не відображає всієї картини, він дає змогу простежити динаміку потоків наркотиків. Аналіз діяльності Прикордонного патруля США (USBP) та Управління польових операцій (OFO) свідчить про те, що за 11 місяців від початку кампанії ракетних ударів у вересні 2025 року, обсяги вилученого кокаїну в портах та на пунктах пропуску скоротилися менш ніж на 3% порівняно з аналогічним періодом попереднього року. Така незначна зміна практично нівелює будь-які заяви про системний успіх.

Додатковим аргументом, що спростовує тезу про значне скорочення пропозиції, є стабільність цін на кокаїн на американському ринку. Економічна теорія стверджує, що значний дефіцит товару неминує призводити до зростання його вартості, однак цього не відбувається, що вказує на те, що ринок залишається насиченим, а канали постачання – живими.

Попри загальну неефективність у глобальному масштабі, ракетні удари справляють локальний вплив, змушуючи злочинні угруповання адаптуватися. Розслідування InSight Crime

¹⁴ <https://insightcrime.org/news/united-states-bets-on-failing-tactic-by-resuming-strikes/>

зафіксували, що на початковому етапі кампанії наркоторговці тимчасово відмовилися від прибережних експортних пунктів у Венесуелі. Майже повністю зупинилися на деякий час перевезення до найближчих островів, таких як Аруба, Кюрасао та Тринідад. Однак ці зміни виявилися тимчасовими, адже вже в червні та липні були зафіксовані нові вилучення наркотиків поблизу Аруби, що засвідчило відновлення роботи цих маршрутів. Крім того, поштовхом для розвитку альтернативних шляхів стало збільшення кількості авіарейсів з наркотиками з Венесуели до Гаяни, а нещодавні конфіскації в сусідньому Суринамі вказують на те, що ці нові напрямки поступово набувають ознак сталих каналів контрабанди.

У відповідь на загрозу з повітря та моря, дилери, за даними аналітиків Управління боротьби з наркотиками (DEA), почали використовувати більші судна та уникати відкритого моря, тримаючись ближче до берегової лінії, щоб зменшити ймовірність бути виявленими та атакованими.

Останні події демонструють, що адміністрація має намір розширювати спектр своїх військових інструментів у регіоні. Летальні удари 23 та 25 серпня були підкріплені спільною операцією з Еквадором 28 серпня, під час якої морська піхота та військово-морські сили США потопили так звану плавучу заправну станцію, що належала еквадорському угрупованню "Чонерос". Примітно, що ця операція відрізнялася від попередніх: перед знищенням судна військові евакуювали особовий склад, що можна розцінювати як спробу коригування тактики на тлі міжнародної критики через численні жертви серед цивільного населення. Ця критика має під собою серйозні підстави. З моменту початку кампанії у вересні 2025 року внаслідок ударів загинуло щонайменше 227 осіб, однак американські посадовці досі не надали переконливих доказів того, що судна чи їхні екіпажі були причетні до наркоторгівлі.

Найбільш тривожним аспектом є непрозорість процесу ухвалення рішень про завдання ударів. Як викрич сенатор Тім Кейн ще в червні, наявність наркотиків на борту судна не входить до трьох критеріїв, які використовуються для визначення цілі. Це ставить під сумнів саму логіку операцій та створює ризик помилкових атак. Додаткові питання до якості розвідки висуває звіт Вашингтонського офісу з питань Латинської Америки (WOLA), який вказує на недостатню ретельність в ідентифікації осіб на борту та їхнього зв'язку зі злочинними організаціями. Нехтування цими процедурами не лише призводить до людських жертв, але й підриває легітимність усієї кампанії.

Ракетні удари є лише вершиною айсберга в рамках ширшої регіональної антинаркотичної стратегії Вашингтона. Ця стратегія включає активну діяльність Берегової охорони США, яка продовжує здійснювати масштабні вилучення, агресивні санкції Міністерства фінансів проти наркобаронів та безпрецедентне рішення Державного департаменту, який з минулого року надав 20 злочинним угрупованням регіону статус іноземних терористичних організацій.

Останні ракетні удари були завдані невдовзі після чергової зустрічі очолюваної США військової ініціативи "Американська антикартельна коаліція", також відомої як альянс "Щит Америки". Ця ініціатива, що активно просувається адміністрацією Трампа, є втіленням курсу на мілітаризацію боротьби з наркотиками, що викликає занепокоєння експертів через потенційну ескалацію насильства та відсутність довгострокової стратегії, спрямованої на боротьбу з причинами проблеми, а не лише її наслідками.

Підсумовуючи, можна констатувати, що попередні дані свідчать про те, що ракетні удари не досягають своєї головної мети, але водночас вони створюють нові ризики та виклики, перетворюючись на елемент політичного тиску, а не на ефективний інструмент боротьби з наркотрафіком.

Ваша думка важлива!

1. Як Україні побудувати антикорупційну систему, в якій відкриті дані, фінансовий моніторинг, державний аудит, захист викривачів і правоохоронне реагування працюватимуть як взаємопов'язаний механізм, а не як окремі інституційні елементи?
2. Яким чином масове поширення стейблкоїнів і токенизованих активів може змінити роль банків та традиційних платіжних систем?
3. Враховуючи величезну кількість зброї, високий рівень корупційних ризиків та складність контролю на довгих ділянках кордону, як уникнути консолідації злочинних мереж на кордонах України в умовах воєнного стану та масового переміщення населення?
4. Наскільки триваюча війна та пов'язана з нею деградація окремих інституцій може створити «сірі зони», якими скористаються транснаціональні злочинні організації для створення своїх осередків в Україні?
5. Як найкраще виміряти рівень розуміння ризику підзвітними суб'єктами в Україні — базове опитування з повторенням у часі чи інший інструмент?

Контакуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-36

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

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