



## “Ми шукаємо ключі там, де горить ліхтар!”

Ходжа Насреддін

### 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**



#### Переосмислення наглядного ландшафту для інтегрованого ринку капіталу в Європі <sup>1</sup>



Аналітичний документ ЄЦБ є одним із найбільш комплексних інституційних досліджень архітектури фінансового нагляду в Євросоюзі за останні роки. Документ вписується у широкий контекст ініціативи Savings and Investment Union (SIU), проголошеної Комісією у березні 2025 року, та безпосередньо реагує на

законодавчий пакет Комісії щодо інтеграції ринків капіталу та реформи нагляду, оприлюднений у грудні 2025 року. Ключовою методологічною рамкою роботи є поєднання двох аналітичних вимірів: горизонтального (картографування наявних моделей нагляду) та вертикального (оцінка відповідності наявної архітектури реальним ринковим структурам та транскордонній активності учасників). Автори свідомо уникають нормативних суджень на користь доказового аналізу (evidence-based assessment), що надає документу особливу вагу у регуляторній дискусії.

<sup>1</sup> <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op383.en.pdf>

Центральний діагностичний висновок документа полягає у фіксації глибокої фрагментації наглядового простору ЄС: станом на дату публікації функціонують 52 національні органи нагляду у сфері ринків капіталу та 16 різних організаційних моделей. При цьому автори систематизують шість базових моделей нагляду — повністю секторальна, частково інтегрована секторальна, twin-peaks, гібридна twin-peaks, повністю інтегрована та функціональна — зазначаючи, що функціональна модель жодного разу не застосовувалася в ЄС. Принципово важливим є те, що підрахунок 52 органів свідомо виключає органи ПВК/ФТ та органи фінансових санкцій — зроблене виключення не є редакційним спрощенням, а відображає методологічне рішення авторів зосередитись на пруденційному та ринковому нагляді, відокремивши від нього вимір комплаєнсу. Для фахівців з ПВК/ФТ ця деталь принципово важлива: реальна кількість органів, з якими взаємодіє суб'єкт первинного моніторингу, є суттєво вищою за зафіксовані 52 одиниці.

Документ розробляє оригінальну таксономію наглядових моделей та детально аналізує, як кожна держава-член ЄС імплементує ту чи іншу модель. Так, 14 з 27 держав обрали повністю інтегровану модель, 4 — twin-peaks або її гібриди, 4 — повну секторальну та 5 — частково інтегровану секторальну. Водночас автори підкреслюють, що навіть в межах однієї категорії суттєві відмінності збережені: наприклад, в Італії Banca d'Italia відповідає за пруденційний нагляд банків та страховиків (через інтегровану IVASS), тоді як окремий орган CONSOB здійснює ринковий нагляд, а COVIP — нагляд за пенсійними фондами. При цьому CSDs, CCPs, управляючі активами, інвестиційні фірми та торгові майданчики перебувають під паралельним наглядом Banca d'Italia і CONSOB. Це унікальний приклад де-факто гібридної twin-peaks моделі всередині формально «повністю інтегрованої» класифікації, що демонструє неадекватність будь-якої чисто формальної таксономії.

Ключовий регуляторний аргумент на користь централізації сформульований через призму чотирьох переваг: по-перше, посилення ефективності ідентифікації та пом'якшення ризиків шляхом вирівнювання мандатів наглядових органів із реальним транскордонним охопленням ключових учасників ринку; по-друге, підвищення ефективності нагляду через удосконалення координації — включаючи обмін даними та кращими практиками; по-третє, спрощення наглядової архітектури шляхом гармонізації практик і зменшення дублювання звітності; по-четверте, забезпечення однорідного застосування Єдиного зводу правил (Single Rulebook) на всій території ЄС, що є передумовою усунення бар'єрів для інтеграції ринку. Цей аргументаційний ланцюжок є критично важливим для розуміння інституційної логіки ЄС щодо нагляду у 2025–2026 роках.

Особливо значущою для сфери ПВК/ФТ є секція, присвячена постачальникам послуг з криптоактивами (CASPs/VASPs). Документ однозначно констатує, що за своєю структурою CASPs є транскордонними суб'єктами, оскільки вони, як правило, здійснюють діяльність у декількох юрисдикціях відповідно до режимів паспортизації. На підставі цього автори ЄЦБ формулюють аргумент на користь прямого нагляду ЄС за всіма CASPs з першого моменту їх появи, а для підгрупи «значних фірм» — запровадження більш суворих правових вимог відповідно до принципу пропорційності (Регламент MiCAR). Це є принциповим відходом від моделі, при якій за CASPs наглядають виключно національні органи. З наглядово-комплаєнсової перспективи така централізація матиме прямий вплив на практики ПВК/ФТ: уніфікований нагляд ESMA означатиме єдині стандарти KYC/AML/CTF, знімаючи можливості для регуляторного арбітражу між юрисдикціями ЄС.

Аналіз чутливості (sensitivity analysis), проведений у Розділі 5, демонструє різні сценарії охоплення нагляду на рівні ЄС залежно від застосованих критеріїв та порогів. Стосовно CSDs та CCPs — близько 40% суб'єктів можуть перейти під прямий нагляд ЄС залежно від обраної методології. Стосовно управляючих активами — підвищена роль ESMA у наглядовій конвергенції може охопити 10–15 найбільших груп, що акумулюють значну частку активів

сектора. Для CASPs — пряме наглядове охоплення на рівні ЄС рекомендується для всього сектора. Детальний аналіз у додатках I, II та III підкріплений картографуванням усіх CSDs та CCPs у ЄС, що надає документу цінну емпіричну базу. Принципово важливо, що автори позиціонують централізацію як таку, що доповнює, а не замінює, роль національних органів для менших, внутрішньо орієнтованих учасників ринку: концептуальна рамка двоярусного (two-tier) нагляду залишається базовою.

З точки зору інституційного процесу, документ вписується у тривалу дискусію навколо Capital Markets Union (CMU), яка розпочалася з першого Плану Дій 2015 року і пройшла три редакції. Авторська позиція полягає у тому, що поточна фрагментація є дедалі менш сумісною з реаліями інтегрованих ринків. Законодавча пропозиція Комісії від грудня 2025 року, на яку документ прямо посилається, включає три потенційно трансформаційних елементи: пряме наглядове охоплення ЄС для великих транскордонних учасників ринку, посилені інструменти наглядової конвергенції для ESMA та реформу управління з метою підвищення ефективності рішень ESMA та її фінансування. Документ ЄЦБ, таким чином, є не суто академічним дослідженням, а аналітичним обґрунтуванням конкретного законодавчого кроку, що визначає позицію Євросистеми у цьому дебаті.

#### Висновки:

- **Централізація нагляду за CASPs на рівні ЄС (ESMA) є прямим наслідком запропонованих реформ** — для суб'єктів ПВК/ФТ це означає перехід від множинних національних вимог до єдиного наглядового стандарту, що суттєво скорочує регуляторний арбітраж у сфері KYC/AML у межах ЄС.
- **Запровадження двоярусного нагляду (рівень ЄС для значних транскордонних гравців, національний рівень для менших внутрішніх суб'єктів)** означатиме диференційований комплаєнс-тягар: великі групи матимуть єдиного наглядача ЄС, малі — збережуть взаємодію з національними органами.
- **Законодавчий пакет Комісії грудня 2025 року, на підтримку якого написаний цей документ ЄЦБ, є дорожньою картою реструктуризації наглядового простору ЄС до 2027–2028 років** — комплаєнс-підрозділи фінансових установ вже зараз мають розпочати оцінку наслідків для своєї операційної моделі нагляду.

## Запобігання незаконній діяльності, пов'язаній з державними коштами та закупівлями<sup>2</sup>

Комунікація ПФР Італії являє собою комплексний нормативно-методологічний документ, що оновлює та систематизує підходи до виявлення підозрілих операцій у сфері державних субсидій та контрактів (appalti pubblici). Документ видано на підставі повноважень ПФР і є обов'язковим

орієнтиром для всіх СПФМ Італії — включаючи банківських та фінансових посередників, а також Pubbliche Amministrazioni (публічні адміністрації), які починаючи з 2022 року були включені до кола підзвітних суб'єктів у рамках імплементації PNRR. Методологічний підхід ПФР базується на синтезі власного аналітичного досвіду: документ є не теоретичним, а операційно-аналітичним,



**Unità di Informazione Finanziaria  
per l'Italia**

<sup>2</sup> [https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione\\_UIF\\_31.03.2026.pdf](https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_UIF_31.03.2026.pdf)

оскільки ґрунтується на повторюваних схемах, виявлених у реальних фінансово-аналітичних розслідуваннях, що надає йому особливу доказову цінність.

Ключовим регуляторним контекстом документа є масштабне зростання обсягів державного фінансування після 2020 року — передусім у зв'язку з реалізацією Національного плану з реалізації відновлення та стійкості (PNRR), що мобілізує кошти ЄС відповідно до Регламенту (ЄС) 2021/241 (Регламент RRF). Зростання публічних асигнувань та ускладнення механізмів їх розподілу закономірно посилює привабливість цих ресурсів для організованої злочинності, і ПФР фіксує тенденцію до зростання кількості та складності схем відмивання та зловживань. У 2023 році ПФР введені два нові набори індикаторів, які замінюють попередні схеми аномальної поведінки, і саме ці нові індикатори стають практичним інструментом для СПФМ.

Документ структурований за чотирма аналітичними осями, кожна з яких відображає практично виявлені вразливості. Перша вісь — аномалії профілю залучених суб'єктів — охоплює перевірку документації anti-mafia та ст. 94 Кодексу публічних контрактів, верифікацію бенефіціарних власників з урахуванням вимог ст. 22 Регламенту RRF. Особливої уваги заслуговують так звані «корпоративні маркери ризику»: нещодавня реєстрація або попередня неактивність компанії; зміни юридичної форми, назви, видів діяльності або переведення юридичної адреси; реструктуризаційні операції — придбання або відчуження підприємств або їх частин; відсутність або недостатня чисельність персоналу порівняно з обсягами бізнесу; невчасне або незаявлене подання звітності; різкий та аномальний ріст обороту. ПФР свідомо поєднує ці індикатори у системну картину, оскільки жоден із них окремо не є достатнім, але їх комбінація формує ризик-профіль, характерний для підставних компаній.

Друга аналітична вісь — аномалії доступу до субсидій та тендерних процедур — містить детальний перелік шахрайських схем, спрямованих на симуляцію відповідності встановленим вимогам. Особливу увагу приділено аналізу фіктивних збільшень статутного капіталу: ПФР описує конкретні механізми — використання банківських чеків, що так і не були пред'явлені до погашення; перекази на суму, меншу від зафіксованої у рішенні про збільшення; внески майном, чия реальна вартість є нижчою за номінальну (наприклад, твори мистецтва); а також відтермінована виплата. У всіх випадках ПФР вимагає перевірки економічної обґрунтованості збільшення відносно розміру підприємства, його операційної діяльності та часового контексту (особливо якщо рішення приймалося незадовго до отримання субсидій або укладення державного контракту). Окремо аналізуються фіктивні гарантії, видані неуповноваженими суб'єктами, у тому числі іноземними, — при цьому ПФР описує складну схему з участю ескроу агентів, які виступають у ролі представників по отриманню винагороди гарантів і слугують для приховання прямих фінансових потоків до фіктивних гарантів.

Третя вісь — моніторинг операційних фінансових потоків після отримання коштів — є практично найбільш деталізованою і безпосередньо операціоналізує зобов'язання з ПВК для банків. ПФР нагадує про обов'язок використання виділених рахунків з обов'язковим зазначенням кодів CIG (Codice Identificativo di Gara) та CUP (Codice Unico di Progetto) у платіжних документах. Перераховані червоні прапорці у сфері руху коштів включають: незаконну монетизацію через готівкові зняття (також дробові); використання коштів на персональні цілі (придбання автомобілів, коштовностей тощо); негайні перекази на пов'язані рахунки або за кордон, особливо до юрисдикцій високого ризику або офшорних зон; перекази на IBAN virtuali (vIBAN) — окремо пояснюється правова природа vIBAN; а також придбання криптоактивів. Особливий акцент зроблений на підпільному банкінгу: мережі підприємств, нерідко пов'язаних із громадянами Азії (переважно Східної Азії), що пропонують транснаціональні неофіційні послуги з переказу коштів і утворюють паралельну банківській фінансову систему.

Четверта вісь — специфіка операційних режимів — підкреслює фрагментованість процесів між різними суб'єктами: банками, публічними адміністраціями, фондowymi операторами та

посередниками. ПФР наголошує на необхідності синергетичного обміну інформацією між усіма ланками ланцюга, що відповідає 4-й Директиві ЄС із ПВК та принципу «whole-chain» моніторингу. Окремо виділено ризики, пов'язані з платформами цифрового кредитування для МСП: автоматизація всіх фаз кредитного процесу не повинна нівелювати вимоги ПВК.

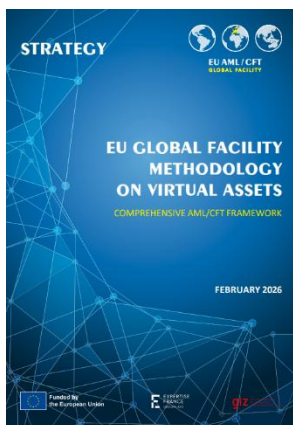
#### Висновки:

- **Публічні адміністрації Італії закріплені як повноправні СПФМ у контексті PNRR** — отже, їх комплаєнс-процеси, включаючи верифікацію бенефіціарних власників підрядників, підлягають пруденційній оцінці нарівні з банківськими.
- **Два нових індикатори для звітування вводяться з квітня 2026 року як обов'язковий формат для підозрілих операцій у сфері державних субсидій і контрактів** — підзвітним суб'єктам необхідно оновити внутрішні процедури ПВК та налаштувати системи транзакційного моніторингу відповідно до нових кодів.
- **Використання криптоактивів та vIBAN як каналів для легалізації коштів від шахрайства з публічними фондами є офіційно закріпленим ризик-сценарієм** — практичний наслідок: банки зобов'язані включити ці типології до матриць оцінки ризиків клієнтів, що отримують або обслуговують державне фінансування.
- **Схеми з фіктивними гарантіями та за участю ескроу агентів описані з рівнем деталізації, що дозволяє безпосередньо використовувати документ як типологічний довідник** — відповідні ознаки мають бути імplementовані у правила транзакційного моніторингу та сценарії виявлення підозрілих операцій.

У ширшому регуляторному контексті, документ ПФР Італії є частиною системного підходу до протидії шахрайству з публічними фондами, що охоплює взаємодію з ANAC (Autorità Nazionale Anticorruzione), CONSOB, IVASS та European Anti-Fraud Office (OLAF). Посилання на спільний документ Banca d'Italia, IVASS, ANAC та AGCM від 28 травня 2020 року та Comunicazione від 18 липня 2025 про верифікацію гарантій вказує на системність підходу та підтверджує, що цей документ є черговим кроком у рамках довгострокової інституційної стратегії ПФР, а не реакцією на

разовий інцидент. Цей методологічний документ є безпосередньо застосовним стандартом для всіх банків та фінансових посередників, що обслуговують отримувачів державних субсидій або підрядників публічних контрактів.

## Методологія Global Facility щодо віртуальних активів<sup>3</sup>



Стратегічний документ Global Facility є оновленою версією першої методології, опублікованої у квітні 2023 року. Цей документ є практичним методологічним стандартом, розробленим за фінансової підтримки Євросоюзу і призначеним для допомоги юрисдикціям — переважно країнам, що розвиваються, та тим, що перебувають у процесі розбудови інституційних спроможностей — у формуванні комплексних AML/CFT-режимів для сектора віртуальних активів. Документ організований за наступною структурою: (1) Стратегічне рішення (Regulation vs Prohibition), (2) Комплексна оцінка ризиків, (3) Нагляд за VASPs, (4) Розслідування та відстеження, (5) Вилучення, конфіскація та управління активами, (6) Протидія фінансуванню розповсюдження зброї

<sup>3</sup> [https://www.global-amlcft.eu/wp-content/uploads/2026/03/VA-Strategy-2026-EN-web\\_compressed.pdf](https://www.global-amlcft.eu/wp-content/uploads/2026/03/VA-Strategy-2026-EN-web_compressed.pdf)

та ухиленню від санкцій. Ця структура відображає цілісний підхід FATF до AML/CFT, адаптований для специфіки сектора ВА.

Найбільш значущим аналітичним внеском документа є актуалізована статистика глобального стану впровадження Рекомендації 15 FATF станом на квітень 2025 року. Із 138 оцінених юрисдикцій лише одна отримала рейтинг «Відповідає»; 29% (40 юрисдикцій) — «здебільшого відповідає» (порівняно з 25%/32 юрисдикціями у 2024); 49% (68 юрисдикцій) — «частково відповідає»; 21% — «не відповідає» (порівняно з 25% у 2024). Таким чином, за рік кількість «не відповідних» юрисдикцій скоротилася, але темп прогресу залишається вкрай повільним. Ці дані є принциповими для розуміння реального масштабу глобальних прогалин у сфері ВА: попри бурхливий розвиток криптосектора протягом останніх 5 років, більше двох третин юрисдикцій не досягли стандарту «здебільшого відповідає». Цей статистичний розрив є структурним ризиком для глобальної фінансової системи.

Документ фіксує критичний зсув у ландшафті ризиків, що відображає принципову зміну порівняно зі станом на 2023 рік: стейблкоїни акумулювали понад 60% загального обсягу незаконних транзакцій у 2024–2025 роках, перевищивши Bitcoin. Автори пояснюють це «дзеркальністю» мотивів: стабільність курсу та зручність переказів приваблюють як легітимних, так і злочинних користувачів рівнозначно. Це означає фундаментальний перегляд матриць ризиків у ТМ-системах: якщо раніше посилення нагляд застосовувався передусім до Bitcoin та Monero, то з 2025 року центр уваги має зміститися на операції зі стейблкоїнами — особливо у точках взаємодії з емітентами стейблкоїнів та банківською системою. Global Facility прямо вказує, що оцінка ризиків має зосередитися на цих точках як системних вузлах вразливості.

Особливу регуляторну значущість має концептуальне вирішення проблеми децентралізованих фінансів (DeFi). Global Facility у повній відповідності із позицією FATF застосовує підхід «substance over form»: якщо DeFi-протокол включає суб'єктів, які мають контроль або достатній вплив на протокол — наприклад, власники адміністративних ключів або токенів управління (governance tokens) — такі суб'єкти можуть підпадати під визначення VASP і відповідно бути об'єктом зобов'язань з ПБК/ФТ. Global Facility прямо підкреслює: «децентралізація» не є щитом від регулювання, і наглядові органи

#### Висновки:

- **Переміщення стейблкоїнів на перше місце у структурі незаконних транзакцій з ВА (понад 60% у 2024–2025 роках) вимагає перегляду ризик-матриць у системах моніторингу операцій** — правила моніторингу підозрілих операцій мають бути скоригованими для підвищення чутливості до транзакцій зі стейблкоїнами, особливо у точках входу/виходу до банківської системи.
- **Статистика відповідності стандартам FATF (лише 1 юрисдикція «Відповідає» із 138 оцінених) є структурним аргументом для підвищення категорії ризику при роботі з VASPs з юрисдикцій з недостатнім режимом ПБК/ФТ** — EDD та транзакційний моніторинг з підвищеним порогом чутливості мають стати стандартом для таких контрагентів.
- **Підхід «substance over form» для DeFi-протоколів означає, що власники токенів управління або адміністративних ключів у DeFi можуть бути об'єктом зобов'язань з ПБК/ФТ** — юридичний та комплаєнс-ризик, що має бути ідентифікований при KYC/CDD клієнтів, залучених до DeFi-екосистем.
- **Навіть юрисдикції з повною заборонаю ВА зобов'язані проводити оцінку ризиків згідно з Рекомендацією 15 FATF:** відсутність регуляторного режиму у країні клієнта не є підставою для зниження категорії ризику, а навпаки — є самостійним фактором підвищення ризику через відсутність наглядового механізму.

мають бути оснащені для ідентифікації централізованих суб'єктів, що ховаються за децентралізованими архітектурами. Це є принципово важливим методологічним роз'ясненням, оскільки багато DeFi-операторів намагаються уникнути статусу VASP саме через формальне посилання на децентралізований характер протоколу.

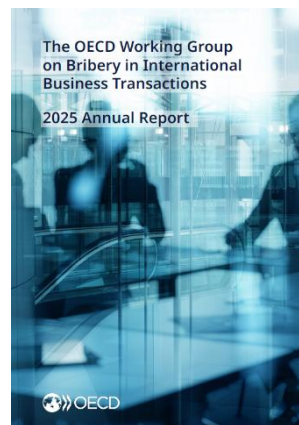
Друга частина документа — є найбільш структурованим аналізом доступних регуляторних опцій. Авторська таксономія виокремлює чотири позиції на спектрі від заборони до регулювання: Повна Заборона, Спостерігати та Очікувати, Обмежене Регулювання та Всеохопне Регулювання. Кожна позиція супроводжується детальним переліком ключових заходів та опису цільового контексту застосування. Принципово важливим є методологічне твердження документа: навіть юрисдикції, що обирають заборону, зберігають зобов'язання з оцінки ризиків (відповідно до Рекомендації 15), оскільки «розуміння ризиків є необхідною умовою ефективного правозастосування». Таким чином, відсутність регуляторного режиму для ВА не звільняє юрисдикцію від вимоги оцінки ризиків — аргумент, що суттєво ускладнює позицію країн, які обрали шлях повної заборони без відповідних механізмів правозастосування.

Розділ щодо Travel Rule визнає, що технічна імплементація вимоги є одним із найскладніших викликів на рівні глобальної фінансової системи. Зобов'язання VASP отримувати, зберігати та передавати інформацію про ініціаторів та бенефіціарів переказів понад встановлений поріг вимагає розробки нових протоколів і стандартів обміну даними між VASPs із різних юрисдикцій і технологічних платформ. Global Facility підтверджує, що станом на 2025 рік реалізація Travel Rule залишається суттєво неоднорідною: різні технічні стандарти (TRISA, OpenVASP, TRUST тощо) співіснують без офіційної гармонізації. Для практиків це означає збереження операційних ризиків при транскордонних переказах — зокрема у ситуаціях, коли VASP-контрагент не підтримує жоден із сумісних протоколів.

Розділи щодо розслідування та відстеження, та вилучення й конфіскації містять деталізовану методологію роботи правоохоронних органів із ВА: крос-чейн розслідування, техніки деанонізації. Окремий розділ щодо фінансування розповсюдження зброї та ухилення від санкцій присвячений конкретним загрозам з боку КНДР та Ірану, включаючи аналіз міксерів та контрзаходів. Загалом документ є унікальним поєднанням стратегічного керівництва та операційних інструментів, що пояснюється його статусом технічної допомоги та орієнтацією на безпосереднє використання інституційними партнерами Global Facility.

## Транснаціональна корупція та виклики правозастосування: аналіз щорічного звіту OECD 2025 <sup>4</sup>

Звіт Організації економічного співробітництва та розвитку щодо діяльності Робочої групи з питань хабарництва у міжнародних ділових операціях за 2025 рік відображає комплексний стан розвитку глобальної системи протидії транснаціональній корупції, зосереджуючись на ефективності імплементації Конвенції OECD про боротьбу з підкупом іноземних посадових осіб як ключового міжнародного інструменту, що встановлює обов'язкові стандарти криміналізації іноземного хабарництва та формує єдину нормативну основу для забезпечення доброчесності у міжнародному бізнесі. У документі наголошується, що корупція у міжнародних транзакціях підриває конкуренцію, підвищує вартість ведення бізнесу та створює



<sup>4</sup> <https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/fighting-foreign-bribery/the-oecd-working-group-on-bribery-2025-annual-report.pdf>

системні ризики для глобальних ринків, а тому Конвенція виконує критичну функцію у боротьбі саме з «пропозиційною стороною» корупції, тобто діяльністю компаній і фізичних осіб, які ініціюють хабарі за кордоном, що відрізняє її від інших міжнародних антикорупційних інструментів.

Центральним елементом звіту є аналіз діяльності Робочої групи з питань хабарництва, яка виступає інституційним механізмом контролю за виконанням Конвенції та відповідних рекомендацій OECD. Група функціонує як платформа міждержавного нагляду, що базується на принципі взаємного оцінювання, і забезпечує постійний моніторинг того, як країни впроваджують антикорупційні зобов'язання у практику. У звіті підкреслюється, що саме завдяки цьому механізму Конвенція стала одним із найбільш суворо контрольованих міжнародних інструментів у сфері боротьби з корупцією, оскільки оцінювання охоплює не лише формальну відповідність законодавства, але й реальну ефективність розслідувань, притягнення до відповідальності та застосування санкцій. Моніторинг здійснюється у чотири фази, причому останні фази орієнтовані саме на оцінку правозастосування, включаючи виїзні місії, взаємодію з приватним сектором і громадянським суспільством, а також аналіз практичних кейсів, що дозволяє отримати повну картину функціонування антикорупційної системи в кожній державі.

Значну увагу у звіті приділено глобальній динаміці участі країн у Конвенції та діяльності Робочої групи. У 2025 році відбулося розширення складу учасників, зокрема Україна стала 47-м членом Робочої групи, що має важливе політичне та інституційне значення, оскільки свідчить про інтеграцію держави у міжнародну систему антикорупційного нагляду та про її готовність дотримуватися високих стандартів прозорості та підзвітності. У документі також зазначається про зростаючий інтерес до приєднання до Конвенції з боку інших держав: Індонезія, Маврикій та Таїланд подали офіційні заявки на вступ, а Саудівська Аравія здійснює реформи з метою приведення свого законодавства у відповідність до вимог Конвенції. Це відображає розширення участі держав у міжнародних антикорупційних механізмах та посилення уваги до впровадження узгоджених підходів у сфері протидії міжнародному хабарництву.

Водночас звіт фіксує фундаментальну проблему сучасної антикорупційної системи — суттєву нерівномірність правозастосування між країнами. Незважаючи на поступове зростання кількості розслідувань та санкцій, особливо щодо юридичних осіб, значна частина держав не демонструє жодних результатів у притягненні до відповідальності за іноземне хабарництво. Це свідчить про наявність системних бар'єрів, серед яких недостатність ресурсів правоохоронних органів, слабка інституційна координація, обмежена політична воля та недосконалість механізмів виявлення правопорушень. Таким чином, ключовим викликом залишається не розробка нових норм, а забезпечення їх ефективного застосування на практиці, що повністю корелює з підходами FATF щодо оцінки ефективності систем протидії відмиванню коштів і фінансуванню тероризму.

Окремий блок звіту присвячений результатам оцінювання окремих країн у межах четвертої фази моніторингу, що дозволяє глибше зрозуміти типові проблеми, які виникають у різних юрисдикціях. Аналіз показує, що навіть країни з розвиненими правовими системами стикаються з труднощами у доведенні справ до судових рішень, забезпеченні відповідальності юридичних осіб, стимулюванні добровільного розкриття правопорушень та впровадженні ефективних комплаєнс-програм у приватному секторі. Значна увага приділяється також питанням захисту викривачів, які визнаються одним із ключових джерел виявлення корупції, однак у багатьох країнах залишаються недостатньо захищеними, що стримує повідомлення про правопорушення та знижує загальний рівень виявлення корупційних схем.

Важливим аспектом звіту є акцент на ролі міжнародного співробітництва у розслідуванні транснаціональних корупційних злочинів. Робоча група активно розвиває мережі взаємодії між правоохоронними органами, зокрема через Global Law Enforcement Network, що дозволяє

координувати розслідування, обмінюватися інформацією та створювати спільні слідчі групи. Наведені у звіті приклади демонструють, що саме завдяки такій кооперації стає можливим розкриття складних схем, які охоплюють кілька юрисдикцій і включають елементи відмивання коштів, використання офшорних структур та залучення посередників. Це підкреслює необхідність інтеграції антикорупційних інструментів із системами фінансового моніторингу, оскільки фінансові потоки є ключовим елементом більшості таких злочинів.

Звіт також демонструє еволюцію підходів до запобігання корупції, зокрема через розвиток корпоративних програм комплаєнсу та колективних ініціатив бізнесу. OECD підкреслює, що ефективні системи внутрішнього контролю, управління ризиками та корпоративної етики стають не лише інструментом запобігання правопорушенням, але й фактором зниження регуляторних ризиків для компаній. Водночас оцінка ефективності таких програм залишається складною, що зумовлює необхідність використання сучасних аналітичних інструментів, включаючи показники ефективності, аналіз даних та оцінку корпоративної культури.

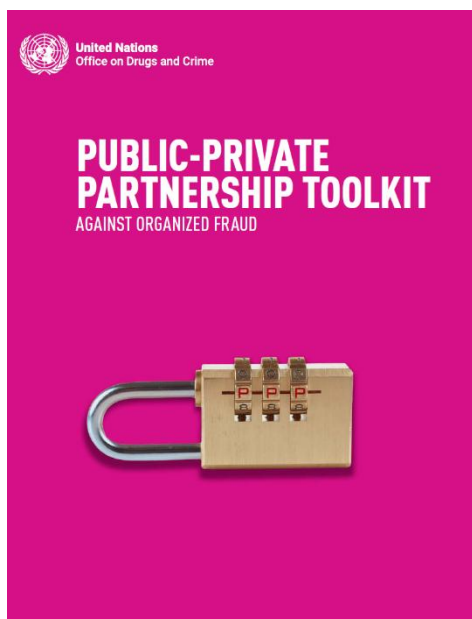
#### Висновки:

- **Критичний розрив між формальним регулюванням і фактичним правозастосуванням.** Наявність законодавства не гарантує ефективності: значна частина країн не має жодних кейсів притягнення до відповідальності. Це означає необхідність переходу від нормативного до операційного підходу.
- **Міжнародна кооперація стає ключовим інструментом боротьби з транснаціональною корупцією.** Ефективні кейси (зокрема за участю України) базуються на спільних розслідуваннях, обміні даними та використанні механізмів спільних слідчих груп (JIT), що має бути інтегровано у практику ПФР та правоохоронних органів.
- **Виявлення корупції залежить від якості інституційних механізмів (викривачі, повідомлення про підозрілі операції, комплаєнс).** Слабкий захист викривачів і низька якість комплаєнс-програм безпосередньо знижують рівень виявлення правопорушень, що є критичним також для систем ПВК/ФТ.
- **Ризик-орієнтований підхід та аналітичні інструменти стають центральними.** Запровадження моніторингової панелі та розвиток аналітично орієнтованого нагляду свідчать про трансформацію у напрямі посилення аналітичного контролю, що має бути інтегровано у національні системи оцінки ризиків.

Додатково у звіті відображено розвиток аналітичних інструментів моніторингу, зокрема створення спеціалізованої інформаційної панелі, яка дозволяє відстежувати прогрес країн у виконанні рекомендацій та виявляти випадки невідповідності. Це свідчить про перехід до більш прозорої та аналітично орієнтованої моделі нагляду, що має значний потенціал для використання у національних системах оцінки ризиків, включаючи сферу ПВК/ФТ.

У цілому звіт формує цілісне уявлення про сучасний стан глобальної боротьби з міжнародним хабарництвом, демонструючи як досягнення у вигляді розширення міжнародного співробітництва, розвитку інституційних механізмів та посилення ролі приватного сектору, так і суттєві виклики, пов'язані з нерівномірністю правозастосування, обмеженою ефективністю виявлення правопорушень та недостатньою інтеграцією антикорупційних заходів у ширші системи фінансового контролю. У контексті ПВК/ФТ цей документ має особливе значення, оскільки підтверджує необхідність комплексного підходу до протидії фінансовим злочинам, де корупція розглядається не ізольовано, а як складова ширших кримінальних екосистем, що включають відмивання коштів, організовану злочинність та незаконні фінансові потоки.

## Публічно-приватні партнерства як ключовий інструмент протидії організованому шахрайству: аналітичний огляд підходу UNODC (2026)<sup>5</sup>



Документ являє собою комплексну концептуальну та практичну рамку, спрямовану на трансформацію підходів до протидії організованому шахрайству шляхом системного залучення публічно-приватних партнерств (PPP) як ключового елементу антикримінальної політики. У центрі цього документа лежить ідея про те, що шахрайство більше не є ізольованим видом злочинної діяльності, а перетворилося на масштабну, транснаціональну та технологічно підтримувану індустрію, яка функціонує за рахунок інтеграції легальних економічних і цифрових систем. Організовані злочинні групи використовують інфраструктуру фінансових установ, телекомунікаційних мереж, цифрових платформ і навіть державних адміністративних механізмів для створення складних, багаторівневих схем, які дозволяють ефективно вводити в оману жертв і легалізувати незаконно отримані доходи.

У цьому контексті документ формує фундаментальну тезу про те, що традиційна модель реагування, заснована виключно на діяльності державних органів, є недостатньою. Це пояснюється тим, що значна частина критичних функцій, які визначають життєвий цикл шахрайства — зокрема комунікація, обробка платежів, управління даними та цифровими сервісами — знаходяться під контролем приватного сектору. Відповідно, ефективна протидія можлива лише за умови інтеграції зусиль держави, бізнесу та громадянського суспільства в рамках єдиної, скоординованої системи, що і визначається як підхід «загальносуспільної взаємодії». У цьому підході кожен із секторів виконує унікальну, але взаємодоповнюючу роль: держава забезпечує правову основу, примусові повноваження та легітимність, приватний сектор — технологічні інструменти, інновації та оперативні дані, а громадянське суспільство — контроль, підзвітність і підтримку.

Ключовим аналітичним інструментом, запропонованим у документі, є концепція «ланцюга шахрайства», яка дозволяє розкласти шахрайство на послідовні етапи — від підготовки до постопераційної фази, включаючи відмивання коштів. Цей підхід має принципове значення, оскільки він дозволяє не лише описати окремі схеми, а й виявити структурні вразливості, які використовуються злочинцями на кожному етапі. Наприклад, на стадії підготовки можуть використовуватися відкриті джерела даних або викрадена інформація для ідентифікації потенційних жертв; на стадії передвиконання — створюються фіктивні компанії або цифрові акаунти; на стадії здійснення — застосовуються методи соціальної інженерії або масові комунікації; на завершальному етапі — відбувається переміщення та легалізація коштів через складні фінансові маршрути. Важливо, що кожна з цих стадій пов'язана з конкретними інституційними середовищами, які можуть виступати як точки втручання для держави або приватного сектору. Таким чином, концепція «ланцюга шахрайства» фактично створює основу для ризик-орієнтованого підходу, аналогічного підходам FATF, і може бути використана для розробки секторних оцінок ризиків та стратегій втручання.

Документ також приділяє значну увагу ролі приватного сектору як ключового джерела даних, технологій і експертизи. Зокрема, підкреслюється, що фінансові установи, фінтех-компанії та технологічні платформи мають доступ до великих масивів даних і розвинені аналітичні

<sup>5</sup> [https://www.unodc.org/res/organized-crime/GFS/publications/UNODC\\_Public-Private\\_Partnership\\_Toolkit\\_Against\\_Organized\\_Fraud\\_EN.pdf](https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_Public-Private_Partnership_Toolkit_Against_Organized_Fraud_EN.pdf)

інструменти, які дозволяють виявляти підозрілі транзакції, аномалії поведінки та нові типології шахрайства. У багатьох випадках саме ці суб'єкти першими фіксують ознаки злочинної діяльності, що робить їх невід'ємною частиною системи раннього попередження. Водночас документ наголошує, що ця роль не повинна призводити до заміщення функцій держави, а навпаки — має бути інтегрована у загальну систему, де кожен учасник виконує визначені функції в межах чітко встановлених правових рамок.

Окремий блок присвячений структурі та типології публічно-приватних партнерств. Вони розглядаються як гнучкі інституційні механізми, які можуть мати різний рівень формалізації — від неформальних обмінів інформацією до інституціоналізованих структур із чітко визначеними повноваженнями та процедурами. Документ описує різні моделі партнерств — добровільні, регульовані та гібридні — і підкреслює, що їхня ефективність залежить від відповідності національному контексту, включаючи правову систему, рівень розвитку фінансового сектору та наявність інституційної спроможності. Особливу увагу приділено міжнародним партнерствам, які є критично важливими з огляду на транснаціональний характер шахрайства та необхідність обміну інформацією між юрисдикціями.

Стратегічна частина документа побудована навколо чотирьох взаємопов'язаних напрямів — сприяння партнерствам, запобігання шахрайству, захист жертв і переслідування злочинців. Ця модель дозволяє сформулювати цілісну політику, яка охоплює як превентивні, так і реактивні заходи. У межах цього підходу публічно-приватні партнерства виконують різноманітні функції, включаючи розробку політик, обмін інформацією, проведення спільних операцій, розробку технологічних рішень та реалізацію програм підвищення обізнаності населення. Важливо, що документ підкреслює необхідність переходу від реактивної моделі до проактивної, де ключову роль відіграють аналітика, прогнозування та раннє виявлення загроз.

Практична частина Toolkit детально описує процес створення та розвитку публічно-приватних партнерств, включаючи етапи планування, реалізації та оцінки ефективності. У цьому процесі особливе

значення надається формуванню довіри між учасниками, яка розглядається як критична умова для ефективного обміну інформацією та координації дій. Довіра забезпечується через прозорість процедур, чітке визначення ролей і відповідальності, а також наявність механізмів підзвітності та контролю. Документ також підкреслює необхідність створення правових і

#### Висновки:

- **PPP є критичною інфраструктурою протидії фінансовим злочинам, а не допоміжним інструментом** Державні органи не здатні самостійно контролювати ключові канали шахрайства (платежі, телекомунікації, цифрові платформи), тому створення PPP має розглядатися як обов'язковий елемент національної системи ПВК/ФТ.
- **Використання концепції «ланцюга шахрайства» є ефективним інструментом для секторної оцінки ризиків** Цей підхід дозволяє ідентифікувати конкретні вразливості на кожному етапі шахрайства та визначити відповідальних суб'єктів (банки, провайдери, платформи), що має пряме практичне застосування для ПФР та СПФМ.
- **Найбільша цінність PPP — у доступі до даних і аналітики приватного сектору.** Фінансові установи та технологічні компанії володіють унікальними даними та інструментами (AI, поведінковий аналіз), які значно підвищують ефективність виявлення підозрілих операцій та схем ВК/ФТ.
- **Ключовим фактором успіху PPP є правове регулювання обміну інформацією та довіра між учасниками.** Без чітких правових механізмів (захист даних, відповідальність, повноваження) та інституційної довіри партнерства стають неефективними або формальними.

технічних механізмів для безпечного обміну інформацією, які враховують вимоги захисту персональних даних і прав людини.

У розділі, присвяченому управлінню публічно-приватними партнерствами, детально розглядаються питання лідерства, стратегічного планування, координації та оцінки ефективності. Управління PPP розглядається як багаторівнева система, що охоплює як стратегічне керівництво, так і операційні механізми, спрямовані на забезпечення сталості та ефективності таких партнерств. Особлива увага приділяється питанням інформаційного обміну, які є одночасно ключовим фактором ефективності та джерелом потенційних ризиків, пов'язаних із конфіденційністю та правами людини. У цьому контексті наголошується на необхідності залучення регуляторів і органів захисту даних для забезпечення відповідності діяльності партнерств правовим стандартам.

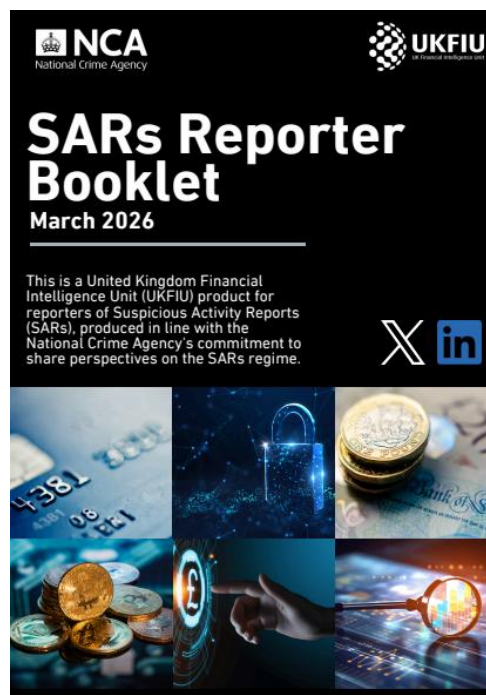
Загалом документ формує комплексне бачення публічно-приватних партнерств як системоутворюючого елементу сучасної архітектури протидії фінансовим злочинам. Він демонструє, що лише через інтеграцію ресурсів, даних і компетенцій різних секторів можна досягти ефективного реагування на складні та динамічні загрози, які становить організоване шахрайство. Таким чином, Toolkit не лише пропонує практичні інструменти, але й формує нову парадигму фінансової безпеки, в якій ключову роль відіграє координація, довіра та спільна відповідальність між державою, бізнесом і суспільством.

## Повідомлення про підозрілу діяльність: фінансова розвідка в дії<sup>6</sup>

Інформаційний бюлетень, випущений Британським підрозділом фінансової розвідки (UKFIU), який діє у структурі Національного агентства з боротьби зі злочинністю (NCA), є важливим елементом системної комунікаційної стратегії, спрямованої на підвищення ефективності національного механізму протидії відмиванню коштів та фінансуванню злочинної діяльності. Це видання виконує одразу кілька ключових функцій: воно забезпечує зворотний зв'язок між державними правоохоронними органами та суб'єктами первинного фінансового моніторингу, демонструє практичну цінність повідомлень про підозрілу діяльність (Suspicious Activity Reports, SARs), а також слугує методологічним орієнтиром для тих, хто щоденно працює на передовій фінансової розвідки.

У передмові Вінса О'Браєна, керівника UKFIU, наголошується, що SARs є критичним ресурсом для правоохоронних органів, адже вони містять не абстрактні підозри, а конкретні, операційно значущі дані: номери телефонів, фізичні та електронні адреси, відомості про компанії, інвестиційну активність, реквізити банківських рахунків, дані про рух коштів та інші активи. Така деталізація дозволяє використовувати SARs у розслідуваннях найрізноманітніших злочинів.

Особливу цінність видання надають практичні кейси, які займають основну його частину. Вони зібрані в результаті систематичних запитів UKFIU до правоохоронних органів і являють собою узагальнення реальних історій використання SARs у ході кримінальних розслідувань. Усі ці



<sup>6</sup> <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/801-sars-reporter-booklet-march-2026/file>

приклади, хоча й подані в знеособленому вигляді, зберігають достатньо деталей, аби читач міг відтворити логіку виявлення підозр, взаємодії звітувача з UKFIU та подальшого розгортання слідчих дій.

Кожен із кейсів демонструє ключову особливість британської системи: тісна взаємодія між приватними інституціями та державними органами, оперативність у прийнятті рішень щодо запитів на захист від легалізації коштів (Defence Against Money Laundering, DAML) та готовність правоохоронних органів негайно використовувати отриману інтелектуальну інформацію для вжиття заходів забезпечення, зокрема для отримання ордерів на арешт рахунків (Account Freezing Orders, AFOs), які дозволяють зберегти активи до завершення розслідування.

Перший із наведених кейсів заслуговує на особливу увагу через свою складність і суспільну резонансність. Підзвітний суб'єкт зафіксував надходження коштів на рахунок підозрюваного з невідомого джерела та їхнє подальше швидке перерахування на інші рахунки. Подальший поглиблений аналіз виявив, що на рахунок надійшло понад 9 000 фунтів стерлінгів від благодійної організації, яка займається наданням допомоги дітям. Це відкриття спонукало звітувача подати численні запити DAML SARs. UKFIU відмовив у задоволенні цих запитів, що дало змогу правоохоронцям розпочати повноцінне розслідування.

У ході слідства було встановлено, що дві окремі групи осіб, до складу яких входили як сам підозрюваний, так і член благодійної організації, використовували фальшиві імена отримувачів та фіктивні платіжні призначення, аби приховати справжню природу трансферів. Формально операції обліковувалися як законні видатки благодійного фонду, однак фактично кошти виводилися на користь учасників групи. Загальна сума викраденого перевищила 300 000 фунтів стерлінгів.

Завдяки оперативному реагуванню правоохоронці змогли отримати ордери на арешт рахунків на суму понад 10 000 фунтів, а подальше розслідування виявило, що один із фігурантів справи витратив на азартні ігри понад 1 мільйон фунтів, що яскраво ілюструє масштаби незаконного збагачення та спосіб життя, який ведуть учасники подібних схем. У підсумку члени обох груп отримали реальні терміни ув'язнення, а розслідування щодо одного з лідерів, чий злочинний дохід оцінюється у понад 1,8 мільйона фунтів, триває досі.

Інший кейс ілюструє ефективність SARs у викритті так званих «підпільних банківських систем», зокрема китайського підпільного банкінгу, який становить значну загрозу для фінансової системи через свою закритість та здатність обслуговувати масштабні потоки нелегального капіталу. Підзвітний суб'єкт звернув увагу на часте внесення великих сум готівки на рахунок клієнта без жодного розумного пояснення. Суми вкладень систематично зростали протягом короткого періоду часу, після чого кошти переказувалися на інші рахунки або знімалися через банкомати. Така поведінка рахунку є класичним індикатором циркуляції коштів від імені третіх осіб та відмивання грошей. Коли підзвітний суб'єкт звернувся до клієнта за поясненнями, отримана відповідь та надані документи не лише не розвіяли підозр, а навпаки, підтвердили наявність незаконної діяльності. Подання SAR дозволило правоохоронцям отримати нові докази до активного розслідування, які раніше не були їм відомі. Було ідентифіковано додаткові банківські рахунки та осіб, причетних до відмивання коштів у складі організованого злочинного угруповання, до якого належав клієнт. Загальний оборот коштів на одному з вторинних рахунків перевищив 190 000 фунтів, а сума переказів — 90 000 фунтів. Розслідування триває, однак уже зрозуміло, що SAR став тим ключовим елементом, який дозволив пов'язати розрізнені фінансові сліди в єдину картину злочинної діяльності.

Окремо варто відзначити випадки, коли SARs дозволяють виявляти складні схеми відмивання коштів через підставні бізнеси, які формально продовжують існувати на папері, але фактично вже не ведуть жодної законної діяльності. У одному з таких прикладів будівельна компанія, яка надавала послуги з технічного обслуговування будівель, продовжувала отримувати понад 200

000 фунтів від третіх осіб, незважаючи на те, що юридично компанія вже була ліквідована в державному реєстрі Companies House. Надані рахунки-фактури не відповідали заявленому виду діяльності, а походження коштів залишалось нез'ясованим. Звітувач подав DAML SAR, і UKFIU відмовив у його задоволенні, що дозволило правоохоронцям отримати ордер на арешт залишку коштів у розмірі понад 200 000 фунтів. У ході розслідування було виявлено ознаки багаторівневого структурування транзакцій (layering), що є характерною ознакою складних схем легалізації злочинних доходів.

Подібна динаміка простежується й у випадку з нещодавно створеним бізнесом, який викликав підозри з самого початку через обмежену торговельну активність, відсутність значущої онлайн-присутності та невідповідність заявленого профілю реальним операціям. Цей бізнес отримав великий платіж від іноземної державної установи, яка не мала жодного відношення до його діяльності. Кошти були негайно перераховані третім особам, включаючи приватні рахунки та не пов'язані з бізнесом компанії, що суперечило інформації, наданій звітувачу під час процедури Know Your Business (KYB). Завдяки оперативному реагуванню UKFIU, який відмовив у задоволенні DAML SAR та направив інформацію в пріоритетному порядку до британського правоохоронного органу, розпочалася міжнародна взаємодія. Спільне розслідування з іноземними колегами дозволило встановити, що кошти були викрадені в рамках онлайн-шахрайської схеми, організованої британським злочинним угрупованням. Для легітимізації своєї діяльності угруповання використовувало фальшиву адресу, створюючи видимість законного бізнесу. У результаті було накладено арешт на понад 400 000 фунтів, які підлягають поверненню іноземній державній установі, що зазнала збитків.

Особливо показовим є приклад трансформації малого підприємства, який демонструє, як зловмисники використовують легітимні бізнес-структури для масштабного відмивання коштів. Готельно-ресторанне підприємство, яке за первісними даними, наданими під час процедури Know Your Customer (KYC), мало обіг у 60 000 фунтів, протягом усього одного року змінило профіль діяльності на кадрові послуги, а його річний обіг зріс до понад 4 мільйонів фунтів. При цьому підзвітний суб'єкт виявив низку критичних невідповідностей: кошти, що надходили на рахунок від кадрових агентств та рекрутингових компаній, негайно перераховувалися сотням третіх осіб, тоді як жодних витрат на заробітну плату, податки чи пенсійні внески, які є обов'язковими для підприємств такого профілю, не здійснювалося. Така поведінка рахунку стала класичним індикатором шахрайства з виплатою заробітної плати (payroll fraud) та відмивання коштів. Підзвітний суб'єкт подав DAML SAR із проханням дозволити перерахувати залишок коштів, однак UKFIU відмовив у задоволенні запиту. Інформацію в пріоритетному порядку було передано відповідному правоохоронному органу, який розпочав розслідування та отримав ордер на арешт коштів у розмірі понад 600 000 фунтів.

Не менш важливими є приклади, що демонструють роль SARs у розслідуванні податкових злочинів, зокрема шахрайств із відшкодуванням податку на додану вартість (ПДВ), які завдають значної шкоди державному бюджету. У одному з таких випадків підзвітний суб'єкт ідентифікував компанію-оболонку, пов'язану з організованим злочинним угрупованням. Попередній аналіз показав, що директор цієї компанії вже був фігурантом інших звітів через підозри в отриманні злочинних доходів та діяльності зі створення підставних підприємств. Рахунок компанії тривалий час був неактивним, однак згодом на нього надійшло відшкодування ПДВ у розмірі понад 320 000 фунтів. Підзвітний суб'єкт подав SAR, інформацію було передано правоохоронцям, які встановили, що податкова декларація була сфальсифікована, а показники в ній штучно завищені для отримання неправомірної виплати. Завдяки отриманій інформації правоохоронний орган зміг оперативно отримати ордер на арешт коштів, а згодом — судові рішення про їхню конфіскацію в повному обсязі.

Ще один масштабний випадок стосувався спроби переказу понад 2 мільйонів фунтів на трейдингову платформу. Переказ було відхилено відповідно до внутрішньої політики

підзвітного суб'єкту, що спонукало до проведення поглибленої перевірки. У результаті він виявив потужні індикатори шахрайства з ПДВ: підроблені документи, використання недійсних номерів платників ПДВ, платежі від офшорних компаній-оболонок, які не мали жодних легітимних бізнес-зв'язків, структуровані зняття готівки, використання сервісів грошових переказів (MSBs) для приховування слідів транзакцій, а також глибокі невідповідності між заявленою діяльністю компанії та реальним рухом коштів на рахунку. Після отримання DAML SAR та відмови UKFIU в його задоволенні, правоохоронці розпочали розслідування і встановили, що компанія була створена виключно для подання фальшивих вимог щодо відшкодування ПДВ. Вона не мала жодного працівника, попри численні зміни директорів, і була ліквідована ще на початку того ж року. У підсумку було накладено арешт на понад 2,4 мільйона фунтів.

Окремий блок кейсів ілюструє використання SARs у боротьбі з наркозлочинністю, зокрема з явищем «county lines» — схемою, за якої дітей та вразливих осіб використовують для розповсюдження наркотиків із великих міст у менші населені пункти, що супроводжується насильством, експлуатацією та контролем. Під час розслідування такої справи правоохоронці звернулися до бази SARs і виявили повідомлення, у якому фіксувалися підозрілі транзакції на рахунку клієнта: часті поповнення мобільного телефону, численні оплати таксі, а також платіжні призначення, що містили пряму чи опосередковану згадку про наркотики. У повідомленні також зазначалося, що рахунок отримував і надсилав великі обсяги коштів третім особам протягом короткого проміжку часу, що є характерною ознакою діяльності, пов'язаної з наркотогівлею. Ця інформація дозволила правоохоронцям ідентифікувати додаткові банківські рахунки, які

#### Висновки:

- **SARs є не формальністю, а операційною основою розслідувань.** Повідомлення про підозрілу діяльність містять конкретні операційні дані (номери телефонів, IP-адреси, реквізити рахунків, платіжні призначення), які дозволяють правоохоронним органам ініціювати розслідування, встановлювати приховані зв'язки між фігурантами та ідентифікувати активи, що підлягають арешту.
- **Ефективність системи залежить від швидкості та якості зворотного зв'язку.** Регулярне надання підзвітним суб'єктам узагальнених кейсів використання SARs у реальних розслідуваннях створює замкнений цикл комунікації, підвищує мотивацію та якість первинних повідомлень, а також формує спільне розуміння актуальних загроз між державою та приватними інституціями.
- **Міжвідомча та міжнародна координація є критичною для розкриття складних схем.** Кейси демонструють ефективність співпраці між національними правоохоронними органами та іноземними партнерами, що дозволяє розслідувати транскордонні схеми відмивання коштів, шахрайства з ПДВ, підпільний банкінг та діяльність організованих злочинних угруповань із використанням підставних компаній.

раніше не були відомі слідству, та встановити нові зв'язки в межах злочинної мережі. Завдяки отриманим даним вдалося розірвати канали постачання наркотиків, захистити дітей від подальшої експлуатації та затримати підозрюваного.

Унікальна аналітична цінність бюлетеня полягає також у тому, що він демонструє, як SARs допомагають встановлювати приховані зв'язки між суб'єктами, які на перший погляд не пов'язані між собою. В одному з кейсів підзвітний суб'єкт подав SAR після того, як закрит рахунок клієнта через підозри у відмиванні коштів. Підозри виникли через змішування незаконних коштів із легальними доходами, підозрілі перекази від третіх осіб, внесення готівки та швидке переміщення коштів з метою приховування їхнього походження. Після подання SAR правоохоронці виявили, що існує ще один суб'єкт, причетний до тієї самої схеми відмивання коштів. Подальше розслідування показало, що обидва суб'єкти входили до своїх систем

онлайн-банкінгу з однієї IP-адреси — факт, який раніше не був відомий слідству. Це дозволило правоохоронцям встановити прямий зв'язок між двома особами та пов'язати їхню діяльність із ширшим розслідуванням наркозлочинності. Було проведено арешти, ініційовано процедуру конфіскації майна, а розслідування триває, очікується винесення вироків.

Підсумовуючи, надзвичайно важливо формувати культуру співпраці між приватними підзвітними суб'єктами та державними правоохоронними органами на основі довіри, прозорості та спільного розуміння загроз. Наведені кейси наочно демонструють, що якісна, деталізована та своєчасна фінансова розвідувальна інформація є фундаментом для розкриття найскладніших злочинних схем. Кожен кейс підтверджує ефективність системи, де ключову роль відіграють не лише силові методи затримання та конфіскації, а й глибока аналітична робота, міжвідомча та міжнародна координація, а також відкритість у комунікації. Такий підхід дозволяє не лише карати злочинців, а й вибудовувати системний, превентивний захист фінансової системи країни від використання її у злочинних цілях.

Для українського контексту, де система фінансового моніторингу також перебуває в стані активного розвитку та адаптації до європейських стандартів, досвід UKFIU є цінним прикладом того, як поєднання законодавчих вимог, технологічного забезпечення та постійного діалогу між державою та бізнесом може перетворити фінансову розвідку на дієвий інструмент протидії злочинності.

## Регулювання

### Операційні правила діяльності VASP в ОАЕ <sup>7</sup>

حكومة دبي  
GOVERNMENT OF DUBAI



Оновлений Exchange Services Rulebook є спеціалізованим нормативним актом, що регулює діяльність постачальників послуг з віртуальними активами (VASPs) з питань обміну віртуальних активів. Документ видано в рамках Регламенту про віртуальні активи та пов'язану діяльність 2023 року і діє кумулятивно з п'ятьма обов'язковими додатковими зводами правил:

Company Rulebook, Compliance and Risk Management Rulebook, Technology and Information Rulebook, Market Conduct Rulebook та Rulebooks, специфічними для інших видів діяльності VASP. Для розуміння регуляторної архітектури VARA (Virtual Assets Regulatory Authority) принципово важливо, що жоден із цих документів не є самодостатнім: Exchange Services Rulebook визначає лише операційні правила для функції обміну, тоді як зобов'язання з ПВК/ФТ, кібербезпеки та ринкової поведінки розподілені між іншими документами. Така модульна архітектура нормативної бази є свідомим регуляторним вибором VARA і відображає принцип пропорційності: VASPs несуть лише ті зобов'язання, що відповідають їхньому ліцензійному профілю.

Частина I документа присвячена розширеним вимогам до складу та функціонування ради директорів. Зокрема, встановлюються суворі критерії незалежності директора: жодна з десяти закріплених підстав виключення не може бути наявною. Ці підстави охоплюють попередню зайнятість у топ-менеджменті VASP або будь-якої компанії Групи протягом 2 попередніх років; пряму або опосередковану участь у контрактах і проектах з Групою сукупною вартістю понад 10% оплаченого статутного капіталу або AED 5 000 000, за умови, що такі контракти виходять за межі звичайної ділової діяльності; більш ніж 7-річне перебування у складі ради; утримання 10%

<sup>7</sup> [https://rulebooks.vara.ae/sites/default/files/en\\_net\\_file\\_store/VARA\\_EN\\_258\\_VER20260331.pdf](https://rulebooks.vara.ae/sites/default/files/en_net_file_store/VARA_EN_258_VER20260331.pdf)

або більше акціонерного капіталу VASP (самостійно або разом із родичами першого ступеня); представлення акціонера, що утримує більше 10% акціонерного капіталу. Ця деталізація означає, що VARA де-факто запозичує стандарти корпоративного управління з традиційних публічних фінансових установ — підхід, що відображає прагнення регулятора інтегрувати сектор ВА у фінансову систему, а не залишати його у правовому вакуумі.

Особливо вагомим є положення про строк зберігання протоколів засідань ради директорів та її комітетів: документ закріплює мінімальний термін зберігання у 8 років — незалежно від вимог будь-яких інших законів або нормативних актів. Ця норма є прямим вираженням принципів FATF щодо записів і відображає усвідомлення VARA важливості документальних свідчень для ретроспективного аналізу ризиків, зокрема у контексті ПВК/ФТ. Формулювання «незважаючи на будь-які вимоги будь-якого закону чи нормативного акту» є нетиповим юридичним прийомом: воно свідомо підпорядковує загальне законодавство ОАЕ нормативному стандарту VARA у питаннях зберігання інформації. Для комплаєнс-спеціалістів це означає, що навіть якщо корпоративне законодавство ОАЕ встановлює нижчі строки зберігання, 8-річний мінімум VARA має пріоритет.

Частина II документа, присвячена публічним розкриттям, запроваджує беспрецедентно детальні вимоги до інформування ринку щодо кожного конкретного віртуального активу, що пропонується для обміну. Перелік інформації, що має обов'язково розкриватися включає: назву та символ активу; дату випуску; ринкову капіталізацію та повністю розбавлену вартість (fully diluted value – загальна ринкова капіталізація криптоактиву, якби всі монети – включно з заблокованими, нереалізованими та ще не випущеними); обсяг в обігу як відсоток від максимальної загальної пропозиції; наявність незалежного аудиту смарт-контракту та дату останнього аудиту; а також максимальну просадку ціни — абсолютну та відносну, із зазначенням дати. Останній індикатор є особливо нетиповим у традиційному регуляторному контексті: він вимагає від VASP надавати потенційним клієнтам структуровану ризикову характеристику активу на основі його ринкової історії. З перспективи ПВК, вимога щодо аудиту смарт контракту є ключовою: вона опосередковано сприяє верифікації технічної природи активу і виявленню потенційних вразливостей, що можуть бути використані для маніпулювання або шахрайства.

Частина III стосується правил функціонування торгового майданчика. Принципово важливою є вимога щодо кодексу поведінки учасників, що надає VASP право застосовувати широкий спектр дисциплінарних заходів: від попередження та планів усунення порушень до анулювання клієнтських ордерів, виключення з майданчика, кримінальних рефералів та повідомлення VARA. Пункт про зобов'язання VASP ділитися інформацією з VARA з метою ринкового нагляду — включаючи дані про великі позиції на корельованих ринках — прямо корелює із зобов'язаннями ПВК/ФТ щодо звітування про підозрілі операції: по суті, це транспонує принцип STR/SAR у специфіку торгового майданчика для криптоактивів. Вимога VARA до прозорості комісійних структур (fee structures) спрямована на попередження стимулів для маніпулювання ринком — поведінки, яка нерідко є елементом більш широких схем відмивання на криптобіржах.

Частина IV регулює маржинальну торгівлю, доступ до якої можливий виключно за наявності спеціального ліцензійного дозволу VARA. Регуляторна логіка тут полягає у тому, що маржинальна торгівля генерує якісно вищий ризиковий профіль — як пруденційний (ризик дефолту клієнта), так і комплаєнсовий (потенційне використання кредитного плеча для маніпулювань). Серед конкретних вимог — зобов'язання VASP мати достатньо активів для задоволення всіх клієнтських зобов'язань у будь-який момент часу; подання до VARA умов маржинальних угод (Margin Trading Agreement) ще до початку надання послуги; а також деталізовані вимоги до Initial Margin та Maintenance Margin, включаючи порядок дій у разі появи від'ємного балансу рахунку клієнта. Ця остання ситуація (negative account balance) регулюється

через Insurance Fund — фонд, що є відповідальністю VASP і слугує буфером у надзвичайних ринкових ситуаціях.

Частина V, присвячена послугам з торгівлі біржовими деривативами (ETD), є найбільш технічно складним розділом і містить вимоги щодо оцінки клієнта, що передбачає структурований аналіз фінансового стану, інвестиційного досвіду, схильності до ризику та цілей клієнта до початку надання ETD-послуг. Вимоги до сегрегації активів у ETD Services захищають клієнтські кошти від взаємозаліку з власними активами VASP. Окремо регулюються «perpetual ETDs» — безстрокові деривативні контракти, характерні для крипторинків і такі, що не мають аналогів у традиційних фінансах. Жорстке обмеження максимального кредитного плеча (leverage limits) є, мабуть, найбільш прямим наглядним обмеженням на ризикованість бізнес-моделі VASP. Загалом, ETD-регулювання VARA демонструє свідоме наближення до стандартів MiFID II та EMIR у контексті криптоактивів, що є частиною ширшої стратегії регулятора — позиціонувати Дубай як юрисдикцію з highest-standards regulatory environment для VA-сектора.

## Звіти окремих інституцій та експертів

**Від глобалізації до конкуренції: як змінюється роль економіки у системі національної безпеки**<sup>8</sup>



Документ є системним аналітичним дослідженням, яке переосмислює місце економіки у структурі національної безпеки в умовах трансформації глобального порядку. Його ключова ідея полягає в тому, що сучасна міжнародна система більше не функціонує як нейтральне середовище економічного обміну, а перетворюється на простір стратегічної конкуренції, де економічні інструменти використовуються державами для досягнення політичних, безпекових і навіть військово-стратегічних цілей. У цьому контексті ринки, фінансові системи, інвестиційні потоки та глобальні ланцюги постачання виступають не лише економічними механізмами, а й інструментами впливу, примусу та стримування.

Автори детально обґрунтовують, що традиційна модель глобалізації, яка базувалася на припущенні про те, що економічна взаємозалежність сприятиме стабільності та зменшенню конфліктності, зазнає суттєвого послаблення. Натомість формується нова реальність, у якій економічні зв'язки можуть використовуватися як важелі тиску, а залежності — як інструменти контролю. Приклади торговельного тиску Китаю на Австралію, енергетичного шантажу росії щодо Європейського Союзу та активного використання санкцій і експортного контролю з боку США демонструють, що економічні інструменти дедалі частіше застосовуються як засоби досягнення стратегічних результатів без прямого військового втручання.

У цьому зв'язку документ вводить концептуально важливу типологію економічного впливу, яка охоплює три рівні — економічний державний вплив, економічний примус і економічне протистояння. Ця градація дозволяє зрозуміти не лише характер інструментів, а й логіку їх ескалації: від точкових, оборотних заходів до довгострокових, системних кампаній, спрямованих на підрив економічної спроможності іншої держави. Важливо, що автори

<sup>8</sup> <https://aspi.s3.ap-southeast-2.amazonaws.com/wp-content/uploads/2026/03/26124030/Markets-as-the-new-frontline.pdf>

підкреслюють багатовимірність цього процесу, де значення мають не лише самі інструменти, а й їх поєднання, тривалість застосування, масштаб впливу та ступінь інтеграції у ширшу стратегію.

Центральне місце у дослідженні займає концепція «інструменталізованої взаємозалежності» (weaponised interdependence), яка пояснює, як держави, що контролюють ключові вузли глобальних економічних мереж — фінансових, логістичних або технологічних — можуть використовувати цю позицію для здійснення стратегічного впливу. Автори показують, що сучасні глобальні системи були оптимізовані під ефективність і мінімізацію витрат, а не під стійкість до шоків або зловживань, що створює передумови для їх використання у геополітичних цілях. Це особливо проявляється у сферах, де існує висока концентрація виробництва або контролю, таких як критичні мінерали, напівпровідники чи фінансова інфраструктура.

На прикладі Австралії детально розкривається, як відкритість економіки, яка традиційно розглядається як стратегічна перевага, одночасно створює системні вразливості. Висока концентрація експорту на обмеженій кількості ринків, значна залежність від імпорту критичних ресурсів, а також суттєва роль іноземного капіталу у фінансуванні економіки формують складну мережу залежностей, які можуть бути використані для тиску. При цьому автори підкреслюють, що сама по собі концентрація не є автоматичною вразливістю — ключове значення має асиметрія залежностей, наявність альтернатив та здатність економіки адаптуватися у часі.

Окремий пласт аналізу присвячений трансформації глобальної фінансової системи, яка дедалі більше фрагментується через створення альтернативних механізмів розрахунків, платіжних систем і валютних інструментів. Держави, що прагнуть зменшити залежність від домінуючих фінансових центрів, розвивають власні інфраструктури, які можуть функціонувати поза межами традиційних систем, таких як SWIFT. Це не призводить до повного розпаду глобального порядку, але створює багаторівневу систему, де різні фінансові архітектури можуть співіснувати та взаємодіяти, що значно ускладнює застосування санкцій, фінансового моніторингу та інших інструментів контролю.

Важливим аспектом є також увага до правової та термінологічної визначеності. Автори наголошують, що нечітке використання понять, зокрема надмірне застосування терміна «економічна війна», може підривати легітимність державних дій і ускладнювати координацію з партнерами. У цьому контексті підкреслюється необхідність чіткого розмежування між законними формами економічного впливу та діями, які можуть наближатися до порушення міжнародного права, що є критично важливим для збереження стабільності міжнародної системи.

Ключовий висновок документа полягає в тому, що сучасні держави не стикаються з дефіцитом інструментів економічної безпеки, а з дефіцитом їх інтеграції. В Австралії існує розгалужена система інституцій, що охоплює питання фінансової стабільності, безпеки, промислової політики та зовнішніх відносин, однак ці елементи функціонують недостатньо узгоджено. Це призводить до ситуацій, коли політичні рішення приймаються у відриві від економічного аналізу або без належного врахування безпекових наслідків, що знижує ефективність державної політики.

У відповідь на це автори пропонують створення національної стратегії економічної безпеки як інтеграційного механізму, який має об'єднати різні інструменти та підходи у єдину систему. Така стратегія повинна забезпечити чітке визначення пріоритетів, встановлення порогів для втручання, координацію між державними органами та ефективну взаємодію з приватним сектором. Особливий акцент робиться на необхідності використання даних і аналітики, що знаходяться у бізнесі, для формування повної картини ризиків, оскільки саме на рівні компаній зосереджена найбільш детальна інформація про реальні економічні залежності.

Значна увага приділяється також інституційній архітектурі, яка має забезпечити реалізацію такої стратегії. Автори підкреслюють важливість центральної координації на рівні уряду, здатної інтегрувати діяльність різних відомств і забезпечувати узгодженість політики. Водночас наголошується на необхідності поєднання цивільних економічних інструментів із можливістю їх посилення у випадку ескалації, включаючи залучення розвідувальних і оборонних компонентів у рамках чітко визначених правових процедур.

Міжнародний вимір також розглядається як критично важливий елемент економічної безпеки. У сучасних умовах ефективність національних заходів значною мірою залежить від рівня координації з союзниками, зокрема у сфері санкцій, експортного контролю та захисту критичних технологій. Автори наводять приклади успішної координації, які демонструють, що саме узгоджені дії дозволяють досягати значного стратегічного ефекту, тоді як фрагментовані підходи створюють можливості для обходу обмежень.

У підсумку документ формує цілісне бачення економічної безпеки як складної, багаторівневої системи управління, що поєднує економічні, політичні та безпекові аспекти. Він підкреслює, що відкритість економіки залишається ключовою перевагою, але лише за умови, що вона підкріплена свідомим управлінням ризиками, здатністю до швидкого реагування та високим рівнем координації між державою, бізнесом і міжнародними партнерами. Такий підхід дозволяє не лише мінімізувати вразливості, а й перетворити економічні інструменти на активний елемент національної стратегії у все більш конкурентному та фрагментованому глобальному середовищі.

#### Висновки:

- **Необхідність переходу від інструментального до системного підходу в економічній безпеці.** Держави повинні інтегрувати економічні, розвідувальні та безпекові інструменти у єдину архітектуру, інакше навіть наявні ефективні механізми (санкції, фінансовий моніторинг, експортний контроль) будуть працювати фрагментарно та із запізненням.
- **Критична роль даних і партнерства з приватним сектором для виявлення ризиків ВК/ФТ та економічного примусу.** Найбільш релевантна інформація про ланцюги постачання, транзакції та залежності знаходиться у бізнесу; без структурованого обміну даними ПФР та регулятори не зможуть своєчасно ідентифікувати ризики, включаючи обходи санкцій та складні схеми фінансування.
- **Вразливість відкритих економік до економічного примусу потребує диференційованого ризик-менеджменту.** Не всі залежності мають критичний характер; необхідним є впровадження методології їх пріоритизації (критичні та некритичні залежності), що безпосередньо відповідає Рекомендації 1 FATF щодо ризик-орієнтованого підходу та практиці проведення секторальних оцінок ризиків.
- **Глобальна фінансова система входить у фазу фрагментації, що знижує ефективність традиційних інструментів у сфері ПВК/ФТ.** Розвиток альтернативних платіжних систем, цифрових валют та паралельних фінансових каналів створює нові можливості для обходу санкцій, що вимагає перегляду підходів ПФР до міжнародного обміну інформацією та аналітики.

## Від відмивання коштів до фінансування розповсюдження ЗМЗ: роль іранських мереж у глобальних схемах обходу санкцій<sup>9</sup>

Документ являє собою глибокий аналітичний огляд трансформації сучасних схем відмивання коштів, обходу санкцій та фінансового забезпечення державної і проксі-активності Ірану в умовах високої геополітичної турбулентності, де фінансові злочини більше не функціонують як ізольовані явища, а виступають складовою цілісної, адаптивної та глобально інтегрованої системи, що поєднує фінансові, торговельні, технологічні та політичні інструменти. Документ фактично демонструє перехід від класичних моделей відмивання коштів до мережевої архітектури, в якій ключову роль відіграють не окремі суб'єкти чи транзакції, а взаємопов'язані ланцюги посередників, корпоративних структур і фінансових потоків, що функціонують у різних юрисдикціях і секторах.

В основі викладеного аналізу лежить розуміння того, що поточна геополітична ситуація — зокрема ескалація військових конфліктів, посилення санкційного тиску та нестабільність глобальних ринків — створює сприятливі умови для розширення нелегальної діяльності, оскільки вона може ефективно маскуватися у легальних економічних процесах. Порушення ланцюгів постачання, збільшення обсягів транскордонних операцій і зростання ролі альтернативних фінансових каналів призводять до того, що незаконні фінансові потоки дедалі частіше інтегруються у звичайні бізнес-процеси, розмиваючи межу між законною та незаконною діяльністю. Це, у свою чергу, формує якісно новий тип ризику — ризик непрямой участі, коли суб'єкти господарювання можуть бути втягнуті у незаконні схеми без прямого контакту з підсанкційними особами або структурами.

Центральним елементом цієї системи виступає так звана «тіньова банківська інфраструктура», яка функціонує як альтернативна глобальна фінансова мережа, побудована на використанні офшорних компаній, номінальних власників, торговельних схем і фінансових посередників. Ця інфраструктура забезпечує переміщення коштів, отриманих від продажу нафти, державних доходів і пов'язаних із державою комерційних операцій, дозволяючи Ірану зберігати доступ до міжнародних фінансових ринків попри масштабні санкційні обмеження. Важливо, що ця система не обмежується традиційними фінансовими каналами, а активно використовує реальний сектор економіки — зокрема торгівлю товарами, інвестиції в нерухомість, інфраструктурні проекти та промисловість — для інтеграції та легалізації коштів.

Особливу роль у функціонуванні цієї системи відіграє корпоративне маскування, яке забезпечує приховування реальних бенефіціарів і дозволяє санкційним суб'єктам діяти через формально незалежні структури. Компанії створюються або набуваються у стратегічно важливих юрисдикціях і секторах, після чого інтегруються у міжнародні ланцюги постачання та фінансові потоки. Такі компанії часто мають ознаки повністю легального бізнесу, включаючи відповідну документацію, історію діяльності та комерційні зв'язки, однак їх реальна функція полягає у забезпеченні доступу до заборонених товарів, переміщенні коштів та обході санкцій. Використання багаторівневих структур власності, номінальних директорів і складних



<sup>9</sup> <https://www.wearethemis.com/uk/resources/publications/conflict-advisory-money-laundering-intelligence-briefing#pub-form-download>

фінансових схем дозволяє значно ускладнити ідентифікацію зв'язків із державними або військовими структурами Ірану.

Окрему увагу в документі приділено практиці використання квазі-легальних бізнесів, яка є одним із найбільш складних для виявлення інструментів. Замість створення нових компаній, що може викликати підозру, мережі використовують уже існуючі підприємства з доброю репутацією, які викупуваються, контролюються або використовуються як платформа для інтеграції нелегальної діяльності. Це дозволяє максимально знизити ризик виявлення, оскільки такі структури вже мають налагоджені відносини з банками, контрагентами та регуляторами. У результаті незаконні фінансові потоки можуть безперешкодно проходити через системи, які формально відповідають вимогам комплаєнсу.

Документ також розкриває важливий аспект взаємозв'язку між відмиванням коштів, фінансуванням тероризму та фінансуванням розповсюдження зброї масового знищення, підкреслюючи, що ці явища більше не існують окремо, а формують єдину фінансову екосистему. Кошти, отримані через складні схеми відмивання, використовуються для підтримки проксі-груп, фінансування військових програм, закупівлі товарів подвійного призначення та розвитку технологій, що мають стратегічне значення для держави. Це означає, що фінансові злочини мають не лише економічний, але й безпековий вимір, що суттєво підвищує їхню значущість у міжнародному контексті.

Важливим компонентом системи є використання нерухомості як інструменту накопичення, збереження та легалізації капіталу. Через складні офшорні структури кошти трансформуються у високовартісні активи у розвинених юрисдикціях, що дозволяє не лише зберігати їх, але й генерувати легальні доходи. Такий підхід забезпечує подвійний ефект: з одного боку, відбувається інтеграція незаконних коштів у легальну економіку, а з іншого — створюється додатковий рівень захисту від конфіскації та санкцій. При цьому характерною ознакою є значна невідповідність між фінансовими результатами основної діяльності та масштабом активів, що виступає одним із ключових індикаторів відмивання коштів.

Географічний вимір дослідження демонструє, що такі мережі функціонують не лише в офшорних або слабко регульованих юрисдикціях, але й активно використовують розвинені економіки, зокрема країни Європейського Союзу. Це пояснюється доступом до високотехнологічних товарів, фінансових інструментів і стабільної правової системи, що дозволяє легітимізувати діяльність. Водночас існуючі розбіжності між санкційними режимами різних країн створюють можливості для регуляторного арбітражу, коли компанії можуть діяти в межах законодавства однієї юрисдикції, одночасно порушуючи обмеження іншої.

Окремо описується роль контрабанди нафти як ключового джерела доходів, що забезпечується через використання так званого «тіньового флоту», який функціонує поза межами стандартних механізмів контролю. Використання прапорів зручності, складних маршрутів, перевантаження вантажів та офшорних структур власності дозволяє приховувати походження ресурсів і інтегрувати їх у глобальні ринки. Отримані доходи потім проходять через багаторівневі фінансові схеми, що унеможлиблює їх просте відстеження.

Суттєвим трендом є також зростаюча роль криптовалют, які використовуються як інструмент обходу санкцій, переміщення коштів та фінансування діяльності проксі-структур. Використання цифрових активів дозволяє уникнути традиційних фінансових каналів, забезпечує високий рівень анонімності та швидкість операцій, а також створює додаткові виклики для регуляторів і фінансових установ. При цьому криптовалюти інтегруються у вже існуючі схеми, а не замінюють їх, що робить загальну систему ще більш складною та стійкою.

Значна увага приділяється операційним викликам для фінансових установ, зокрема проблемі ідентифікації клієнтів і ризику помилкових спрацювань. Використання однакових або подібних імен, складних корпоративних структур і багаторівневих зв'язків ускладнює процес перевірки, що вимагає застосування більш просунутих аналітичних підходів, включаючи нечітке співставлення даних і контекстний аналіз.

#### Висновки:

- Традиційні підходи до ПВК (CDD/санкційний скринінг) є недостатніми для виявлення сучасних іранських схем. Необхідно впроваджувати аналіз мереж, бенефіціарної власності та транзакційних ланцюгів, оскільки ризик переважно є непрямим.
- Найвищий рівень ризику становлять квазі-легальні структури та підставні компанії, інтегровані у легальну економіку. Регуляторам і ПФР слід зміщувати фокус з формальної відповідності на економічну сутність діяльності, особливо у секторах торгівлі, логістики та технологій.
- Відмивання коштів, фінансування тероризму та фінансування розповсюдження ЗМЗ фактично конвергують у єдину систему ризиків. Це потребує інтегрованого підходу до ВК/ФТ/ФР відповідно до рекомендацій FATF (зокрема Р. 1, 7, 30).
- Криптовалюти та альтернативні фінансові канали стають критично важливими інструментами обходу санкцій. Потрібне посилення контролю за VASP, впровадження Travel Rule та аналітики блокчейн-транзакцій на національному рівні.

У підсумку документ формує чітке розуміння того, що сучасні фінансові злочини характеризуються високим рівнем адаптивності, гнучкості та інтеграції у глобальну економіку. Ризики більше не є локальними або статичними, а постійно змінюються, переміщуючись між юрисдикціями, секторами та інструментами. Це вимагає принципово нового підходу до ПВК/ФТ, який базується на глибокому аналізі мережевих зв'язків, поведінкових патернів та динаміки фінансових потоків, а також на використанні сучасних технологій для виявлення прихованих ризиків. Таким чином, документ демонструє, що ефективна протидія таким схемам можлива лише за умови переходу від формального дотримання процедур до стратегічного, аналітично орієнтованого управління ризиками, яке

враховує складність і взаємопов'язаність сучасного фінансового середовища.

## Інновації у платіжних системах: трансформація багаторівневої архітектури грошей<sup>10</sup>



Документ присвячений комплексному аналізу архітектури грошових і платіжних систем через концепцію багаторівневості, яку автор розглядає як фундаментальну властивість сучасної монетарної системи та ключ до розуміння як її історичної еволюції, так і впливу новітніх технологічних інновацій. У центрі дослідження перебуває теза про те, що платіжні системи не є плоскими або однорівневими структурами, а організовані у вигляді ієрархії взаємопов'язаних реєстрів, де кожен рівень виконує окрему функцію, а найвищий рівень — зазвичай центральний банк — забезпечує остаточне врегулювання та стабільність системи. Автор підкреслює, що така багаторівнева організація виникла не випадково, а як результат поєднання факторів

Ulrich Bindell

Innovations and the Layering of Money and Payments

SAFE Working Paper No. 473 | March 2026

Leibniz Institute for Financial Research SAFE  
Sustainable Architecture for Finance in Europe  
info@safe-frankfurt.de | www.safe-frankfurt.de

<sup>10</sup> <https://www.interpol.int/Media/Documents/Publications/Financial-Crime/INTERPOL-Global-Financial-Fraud-Threat-Assessment-March-2026>

ефективності, управління ризиками, інституційного дизайну та необхідності забезпечення інтероперабельності між різними учасниками фінансової системи.

У роботі детально розглядається еволюція різних типів платіжних архітектур, починаючи від найпростішої моделі, де відсутня централізована система обліку і економічні агенти ведуть взаємні зобов'язання у вигляді неструктурованих боргових відносин (IOU-економіка), і закінчуючи сучасною складною дворівневою системою, де комерційні банки обслуговують клієнтів, а міжбанківські розрахунки здійснюються через центральний банк як верхній рівень. Автор показує, що існують також варіанти однорівневих і трирівневих систем, але саме дворівнева модель стала домінуючою, оскільки вона дозволяє ефективно розподілити функції між учасниками: центральний банк забезпечує надійність і довіру, тоді як комерційні банки здійснюють кредитування, інновації та роботу з клієнтами. Важливим елементом цієї архітектури є поняття «старшинства» між реєстрами, де нижчі рівні використовують активи вищих рівнів для здійснення розрахунків, а також поняття інтероперабельності, що забезпечує можливість здійснення платежів між клієнтами різних установ.

Особливу увагу приділено класифікації типів платіжних реєстрів залежно від їхньої балансової структури та ролі у системі. Автор виділяє чотири основні типи: технічні реєстри без власного балансу, які лише відображають розподіл коштів; реєстри, повністю забезпечені активами у старшому реєстрі; вузькі платіжні установи, які тримають резерви не лише у формі центральнобанківських грошей, але й у високоліквідних цінних паперах; та повноцінні банки, які здійснюють кредитування і мають складну структуру активів і зобов'язань. Така типологія дозволяє автору оцінити різні інновації з точки зору їхнього ризик-профілю та ролі у системі, зокрема підкреслюючи, що найменш ризиковими є структури, повністю забезпечені резервами центрального банку, тоді як більш складні моделі створюють додаткові ризики через трансформацію ліквідності та кредиту.

Значна частина дослідження присвячена економічному обґрунтуванню існування багаторівневих систем. Автор пояснює, що фінансова інфраструктура характеризується сильними мережевими ефектами, економією на масштабі та властивостями суспільного блага, що призводить до високої концентрації та обмеженої кількості ключових інфраструктур (наприклад, один RTGS на валюту або обмежена кількість центральних депозитаріїв). У таких умовах багаторівнева структура дозволяє поєднати централізацію базових функцій із децентралізацією взаємодії з клієнтами, що підвищує ефективність і зменшує операційні та кредитні ризики. Водночас автор наголошує, що фінансова система є далекою від ідеального конкурентного ринку, тому її розвиток значною мірою залежить від державної політики, включаючи регулювання, нагляд і операційну діяльність центральних банків.

Ключовим концептуальним елементом є поняття «єдності грошей», яке означає, що всі форми грошей у межах однієї економіки є взаємозамінними за номіналом і приймаються на рівних умовах. Ця властивість забезпечується через механізм конвертованості, коли приватні форми грошей, такі як банківські депозити, можуть бути обміняні на гроші центрального банку. Автор підкреслює, що саме ця конвертованість лежить в основі довіри до фінансової системи та її стабільності, а її порушення може призвести до фрагментації платіжної системи та виникнення паралельних грошових режимів.

У контексті сучасних інновацій автор детально аналізує їхній вплив на багаторівневу архітектуру. У випадку цифрових валют центрального банку (CBDC) розглядаються різні сценарії їхнього впровадження, включаючи як збереження існуючої дворівневої системи, так і потенційний перехід до одношарової моделі, де всі платежі здійснюються безпосередньо через центральний банк. Проте автор зазначає, що центральні банки загалом не підтримують радикальні трансформації, оскільки вони можуть призвести до дестабілізації банківського сектору та зменшення ефективності кредитного процесу. У випадку систем миттєвих платежів

показано, що технологічний прогрес дозволяє скорочувати кількість рівнів у платіжній системі, але не усуває потребу у базовому рівні центрального банку.

Публічні блокчейни та децентралізовані фінансові системи розглядаються як спроба радикального спрощення або навіть ліквідації багаторівневої структури, однак автор критично оцінює ці підходи, вказуючи на численні проблеми, пов'язані з управлінням, правовою визначеністю, відповідальністю та ризиками. Він підкреслює, що навіть у таких системах фактично виникають нові форми ієрархії або залежностей, що свідчить про фундаментальну необхідність багаторівневості у фінансовій системі. Аналогічно, токенизація активів і створення мультиактивних платформ розглядаються не як ліквідація існуючої архітектури, а як її технологічна оптимізація, яка підвищує швидкість, ефективність і гнучкість операцій, але не змінює базових принципів функціонування.

Окремий блок аналізу присвячений стейблкоїнам, які автор розглядає як поєднання вузького банкінгу та цифрових технологій. Хоча на поверхневому рівні операції зі стейблкоїнами можуть виглядати як однорівневі, насправді вони спираються на складну багаторівневу структуру, оскільки їхні резерви зберігаються у банках або центральному банку. Автор підкреслює, що такі інструменти можуть створювати значні ризики для фінансової стабільності, зокрема через перерозподіл депозитної бази банків, підвищення волатильності фінансування та потенційні ефекти під час кризових ситуацій.

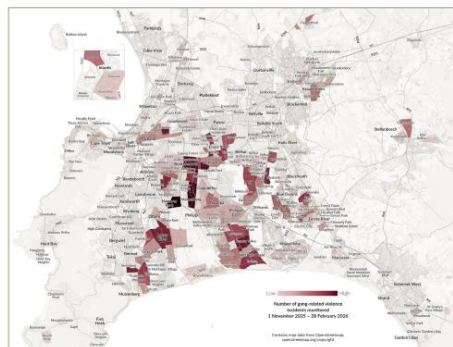
У підсумку документ формує цілісну аналітичну рамку, яка демонструє, що сучасні технологічні зміни не скасовують фундаментальних принципів організації грошових систем, а лише змінюють їхню форму. Основне завдання державної політики полягає у тому, щоб адаптувати регуляторні та інституційні механізми до нових умов, зберігаючи при цьому стабільність, ефективність і єдність грошей як ключові характеристики функціонування фінансової системи.

#### Висновки:

- **Інновації не ліквідують багаторівневу архітектуру, а лише трансформують її — отже, регулювання має бути спрямоване на управління новими формами нашарувань, а не на їх усунення.** Це означає, що при розробці політики щодо CBDC, стейблкоїни чи токенизації необхідно оцінювати їх як елементи існуючої ієрархії, зокрема з точки зору їх підключення до рівня центрального банку та впливу на інтеперабельність.
- **Збереження «єдності грошей» є критичним пріоритетом, і воно прямо залежить від забезпечення конвертованості приватних форм грошей у гроші центрального банку.** Практично це означає необхідність запровадження вимог до стейблкоїнів щодо прямої або ефективної конвертованості в гроші центрального банку, інакше виникає ризик фрагментації платіжної системи.
- **Надання доступу небанківським платіжним провайдерам до рахунків центрального банку є обґрунтованим з точки зору ефективності, але потребує суттєвого посилення механізмів допуску та нагляду.** Регулятори мають перейти від інституційного підходу до ризик-орієнтованих критеріїв доступу, включаючи операційну стійкість, ліквідність та управління ризиками.
- **Стейблкоїни створюють системні ризики через зміну структури фінансування банків і можуть посилювати фінансову нестабільність, особливо у кризових умовах.** Є необхідність встановлення жорстких вимог до резервів, ліквідності, прозорості та, потенційно, доступу до механізмів центрального банку (включаючи рахунки або кредит останньої інстанції).

## Фрагментація замість ієрархії: як розпад банд змінює природу насильства<sup>11</sup>

Черговий випуск щоквартального моніторингу злочинних угруповань Південної Африки, підготовлений GI-TOC, демонструє детальний і тривожний портрет кримінального ландшафту, який перебуває у стані глибокої турбулентності. Цей звіт, що охоплює перший квартал 2026 року, виходить за межі традиційного нарративу про статичний територіальний контроль, натомість розкриваючи набагато більш волатильну реальність, що формується під впливом внутрішньої фрагментації, стратегічної експансії та складної взаємодії між локальними угрупованнями та транснаціональними злочинними мережами.



Центральний висновок полягає в тому, що насильство в регіоні дедалі більше підживлюється не просто суперництвом між усталеними бандами, а структурним процесом розпаду, який проявляється у масових переходах членів між угрупованнями, запеклих лідерських конфліктах та появі нових фракцій. Ці процеси фундаментально змінюють саму природу організованої злочинності, створюючи нові лінії розлому та роблячи кримінальне середовище дедалі більш непередбачуваним.

Одним із головних чинників нестабільності стало явище, відоме як перехід членів одного угруповання до лав іншого. Як зазначається у звіті, це більше не є поодиноким випадком, а перетворилося на "прискорений тренд". Колишній генерал угруповання 28s підкреслює, що "майже кожна банда почала це робити". Ця практика підриває саму основу традиційних кодексів лояльності, які століттями скріплювали бандитські структури. Документ детально описує низку кейсів за участю членів таких найстаріших і найвпливовіших угруповань, як Americans, Hard Livings та Laughing Boys.

Мотивація для таких рішень є складною та багатозоровою. Вона варіюється від економічних стимулів — доступу до наркотиків, зброї та грошей — до агресивних кампаній з вербування, які проводять банди на кшталт Fancy Boys. Однак, мабуть, найсуттєвішим фактором є глибокий розрив між поколіннями. Молодші члени, які виростили в умовах перманентного насильства та економічної скрути, демонструють набагато меншу відданість традиціям і значно охочіше змінюють приналежність заради кращих перспектив.

Такий прагматичний, майже транзакційний підхід до бандитської приналежності має руйнівні наслідки. Коли члени переходять до іншої банди, вони несуть із собою не лише особисту інформацію, а й "зброю та секрети". Це робить їх надзвичайно вразливими: вони стають ціллю для колишніх побратимів, які вважають їх загрозою безпеці, і водночас отримують увесь тягар ворожнечі своєї нової банди. Це запускає нескінченні цикли помсти, які важко передбачити.

Паралельно з цими "переходами", внутрішні лідерські конфлікти стають ще одним потужним генератором насильства, що залишає за собою довгі шлейфи жертв. Найпоказовішим прикладом у звіті є ситуація навколо одного з домінуючих угруповань — Junky Funky Kids (JFKs). Тут розгорнулася запекла боротьба за владу між чинним лідером на прізвище "Ibi" та претендентом Джейсоном "Фебулес" Арендсе. Цей конфлікт уже призвів до майже сотні вбивств на території JFKs лише за перші два місяці 2026 року, причому близько 70 із них, за даними поліції, стали прямим наслідком внутрішньої боротьби.

<sup>11</sup> <https://globalinitiative.net/wp-content/uploads/2026/03/WC-gang-monitor-No-8-GI-TOC-March-2026-1.pdf>



Однак ця суперечка — не просто особиста ворожнеча. Вона є відображенням фундаментального зіткнення двох моделей управління. Ібі керує угрупованням за принципом "франшизи", надаючи лідерам на різних територіях широку автономію, дозволяючи їм самостійно розпоряджатися ресурсами, доки вони залишаються частиною загальної структури. Натомість Арендсе, який є відомим кілером, виступає за централізацію влади, прагнучи консолідувати контроль над усіма потоками доходів та зброї. Його легітимність у власних очах і в очах багатьох рядових бійців підкріплюється членством у могутній в'язничній банді 26s, що дає йому вищий статус, ніж у Ібі, який не має такого "тюремного авторитету".

Крім того, Арендсе вдало використовує соціальні важелі: він почав вносити застави за неповнолітніх членів банди, які опинилися за ґратами за дрібні злочини. Це робить його популярним серед рядових бійців і дозволяє йому купувати їхню лояльність. Цей випадок ілюструє, як тюремна ієрархія та вуличні соціальні стратегії переплітаються, створюючи нові лінії розколу та ескалації насильства.

Хоча Кейп Флетс залишається епіцентром бандитської активності, моніторинг фіксує критично важливу географічну експансію злочинного впливу. Район Салданья, де розташована найглибша природна гавань Південної Африки та великий промисловий порт, переживає сплеск бандитського насильства та торгівлі наркотиками у великих обсягах. Його стратегічна цінність для злочинних мереж різко зросла. Убивство відомого діяча банди 27s Гарта Вільямса у 2023 році створило вакуум влади, який спровокував цикл помст, що втягнув у регіональний конфлікт інші банди. У Салданья-Бей та сусідньому Вреденбурзі виникла гібридна динаміка: місцеві банди, такі як Kutsivales та Dark City, борються за контроль над вуличною торгівлею наркотиками, тоді як інші банди координують більш складні та цілеспрямовані вбивства, часто з в'язниці, щоб контролювати маршрути постачання наркотиків, торгівлю зброєю та незаконний вилов морських ресурсів.

Привабливість регіону для організованої злочинності є багатофакторною. На відміну від ретельно контрольованих портів Кейптауна та Дурбана, Салданья-Бей пропонує слабший нагляд, обмежені можливості правоохоронних органів та розташований поза прямою юрисдикцією столичних органів влади. Це робить його ідеальним альтернативним пунктом ввезення кокаїну, який транспортується з Південної Америки. У звіті згадується вилучення кокаїну на рекордну суму 583 мільйони рандів (понад 30 мільйонів доларів США) з риболовецького судна поблизу Салданья-Бей у 2021 році, що підкреслює масштаби цієї діяльності. За даними дослідження, транснаціональні синдикати, зокрема з Балкан, використовують налагоджені зв'язки з виробниками кокаїну в Бразилії, щоб скидати водонепроникні пакунки з наркотиками у відкритому океані. Звіди їх підбирають місцеві капітани риболовецьких суден, які мають зв'язки з бандами, і тимчасово зберігають у схронах разом зі зброєю та готівкою, перш ніж партіями відправляти на великі міські ринки, де попит значно вищий. Плановане розширення інфраструктури, зокрема створення комерційних терміналів у зоні промислового розвитку Freeport Saldanha, за оцінками експертів, може лише посилити ці вразливості.

Нарешті, моніторинг заглиблюється у підступну роль явища "klipgooiër" — «каменеметання» — як каналу рекрутингу до банд та раннього індикатора ескалації конфлікту. Те, що часто списується на дрібне хуліганство чи безневинні дитячі пустощі, у контексті культури Кейп Флетс є навмисною та стратегічною практикою. Групи дітей, деяким із яких ледь виповнилося вісім років, використовуються старшими членами банд для випробування міцності територіальних кордонів, демонстрації лояльності та провокації суперників. Потім цих дітей індоктринують, і з часом вони отримують ножі, а згодом і вогнепальну зброю. Ця діяльність слугує своєрідним "обрядом посвячення" для молоді в уражених бандитизмом громадах, залучаючи їх до кодексу групової лояльності та помсти.

Набагато важливішим є те, що ці, здавалося б, незначні інциденти діють як "спусковий гачок" для набагато більших конфліктів. Розбите вікно, удар каменем, який спричинив травму, або звинувачення в порушенні території можуть за лічені хвилини перерости в перестрілку з використанням вогнепальної зброї. У відповідь на таку ескалацію поліція провела масштабну операцію в Маненберзі, заарештувавши 17 підозрюваних, включаючи восьмирічного хлопчика. Моніторинг наголошує, що частота та локалізація таких інцидентів, особливо в районах із щільною, спроектованою за часів апартеїду забудовою, де вузькі алеї та дво-триповерхові будинки створюють ідеальне середовище для швидкої провокації та відступу, мають розглядатися як ключовий показник зростання напруженості, що потребує негайної уваги та превентивних заходів.

Таким чином, головні рушії насильства зміщуються від міжбандитського суперництва до внутрішньої фрагментації, тоді як кримінальна економіка виходить за межі традиційних міських центрів, щоб експлуатувати вразливості другорядних портів. Аналіз надзвичайних заходів у звіті,

#### Висновки:

- **Внутрішня фрагментація стала головним драйвером насильства.** Масові переходи членів між угрупованнями та внутрішні конфлікти спричиняють більше жертв і нестабільності, ніж традиційна територіальна боротьба.
- **Транснаціональна злочинність активно освоює "вторинні" порти, створюючи нові гібридні кримінальні екосистеми.** Це призводить до появи нового типу насильства — поєднання вуличних розборок за територію з цілеспрямованими "замовними" вбивствами, що координуються з в'язниць.
- **Тюремна ієрархія залишається ключовим фактором легітимності та влади на вулиці.** Це створює постійний канал впливу між в'язницями та вулицею, ускладнюючи боротьбу з організованою злочинністю.

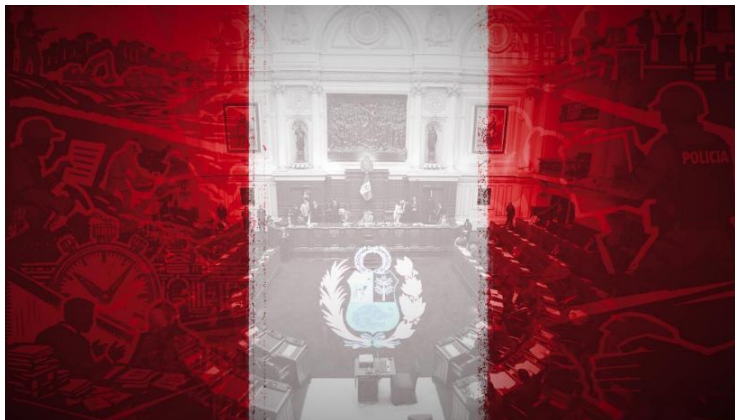
зокрема нещодавнього розгортання Південноафриканських сил національної оборони (SANDF), слугує тверезним нагадуванням про те, що, хоча військові інтервенції можуть забезпечити тимчасову стабілізацію та зменшити кількість вбивств у короткостроковій перспективі, вони неспроможні порушити глибинні кримінальні економіки або вирішити глибоко вкорінені соціальні та економічні умови, які живлять бандитизм.

Оскільки банди стають дедалі більш фрагментованими, але водночас більш інтегрованими в транснаціональні ланцюги постачання, відповідь держави та громадянського суспільства має бути однаково адаптивною. Це вимагає

переходу до розвідувально-орієнтованого підходу в поліцейській роботі, який зосереджуватиметься на моніторингу внутрішньої нестабільності, переходів членів та лідерських суперечок як на ранніх індикаторах насильства. Окрім того, необхідні цілеспрямовані інвестиції в громади: від програм раннього втручання, спрямованих на дітей, до створення економічних альтернатив, які зроблять бандитський "заробіток" менш привабливим.

Зрештою, як слушно підсумовує звіт, лише скоординована, багатосекторальна стратегія, яка поєднує невідкладну стабілізацію з довгостроковою роботою над соціально-економічними причинами злочинності, здатна розірвати це замкнене коло насильства та безкарності, яке десятиліттями тримає в лещатах місцеві громади.

## Як політичний розпад Перу став головним союзником організованої злочинності<sup>12</sup>



Упродовж останнього десятиліття президентський палац Каса-де-Пісарро, що височить над головною площею Ліми, слугував не так осередком державного управління, як символом хронічної нестабільності.

Статистика вражає: станом на лютий цього року Перу пережило восьмого президента за десять років. Останній тимчасовий очільник, Хосе Хері, протримався на посаді лише чотири

місяці, після чого був зміщений через скандальні повідомлення про таємні зустрічі з китайськими бізнесменами, причетними до мереж торгівлі деревиною.

Ця стрімка зміна владних фігур — не просто наслідок політичної кризи, а її найнебезпечніша складова, що створює ідеальне середовище для розквіту організованої злочинності. На відміну від класичної моделі захоплення держави, яку ми спостерігали в інших країнах Латинської Америки, — як-от у Венесуелі за часів Ніколаса Мадуро чи Гондурасі за Хуана Орландо Ернандеса, де злочинність проникала на верхівки влади через корупцію та насильство, — Перу зіткнулося з іншою, не менш руйнівною патологією. Тут не сталося класичного захоплення держави згори. Натомість організована злочинність просто заповнила вакуум, що утворився внаслідок системної слабкості інституцій та відсутності будь-якої послідовної владної вертикалі.

Витоки нинішньої кризи сягають 2018 року, коли президент Педро Пабло Кучинські подав у відставку через корупційний скандал навколо бразильського будівельного гіганта Odebrecht. Цей, здавалося б, окремий епізод запустив ланцюгову реакцію, яка триває досі. Мартіну Віскаррі було оголошено імпічмент у 2020 році за звинуваченнями в отриманні хабарів. Мануель Меріно протримався лише п'ять днів, пішовши у відставку на тлі масових протестів. Франсіско Сагасті виконував обов'язки тимчасового президента до виборів 2021 року, які принесли перемогу Педро Кастільйо. Останній, своєю чергою, спробував розпустити законодавчу владу та керувати країною декретами в грудні 2022 року, що призвело до його арешту. Віцепрезидентка Діна Болуарте, яка отримала владу внаслідок цього перевороту, була глибоко непопулярною й зрештою зазнала імпічменту в 2025 році.

Кожна з цих змін супроводжувалася не лише політичною кризою, а й черговим періодом паралічу державного управління. Найбільш руйнівними ці постійні перестановки виявилися для сфери безпеки. За перші тринадцять місяців правління Кастільйо міністерство внутрішніх справ, яке відповідає за громадську безпеку, змінило сімох очільників. Його наступниця, Болуарте, за майже три роки свого перебування при владі призначила ще сімох міністрів. Кожен новий керівник приносить із собою нову команду, новий стиль роботи й, що найважливіше, новий період дезорієнтації.

Як зазначає один із офіцерів перуанської поліції, кожна зміна супроводжується «мертвим часом», коли не ведеться жодної роботи, не планується жодних стратегій, а рішення просто не приймаються. У країні, де безпекові інституції й без того фрагментовані на десятки поліцейських і прокурорських підрозділів із різними повноваженнями та юрисдикціями, відсутність централізованого керівництва призводить до того, що жоден орган не бере на себе

<sup>12</sup> <https://insightcrime.org/news/peru-political-instability-enables-organized-crime/>

відповідальність за боротьбу з такими загрозами, як наркотрафік або нелегальний видобуток корисних копалин.

Однак якщо виконавча влада страждає від внутрішньої дезорганізації, то Конгрес Перу завдав інституційній спроможності держави значно більш усвідомленої та цілеспрямованої шкоди. У період між 2023 та 2025 роками законодавці ухвалили низку реформ, настільки відверто вигідних для злочинних інтересів, що в експертному середовищі вони отримали назву «злочинних законів». Ці зміни не просто ускладнили роботу антикорупційних органів, а системно демонтували саму архітектуру, створену для переслідування корупції та організованої злочинності.

Однією з найбільш руйнівних стала зміна до закону про ефективне співробітництво — ключового інструменту, завдяки якому вдавалося притягати до відповідальності фігурантів найвищого рівня, зокрема колишнього авторитарного лідера Альберто Фухіморі. Нова редакція закону кардинально скоротила час, який прокурори мають для перевірки показань свідків, запровадила обов'язковий відеозапис усіх свідчень і, що найважливіше, зробила прокурорів потенційними фігурантами кримінальних справ у разі витоку інформації. Наслідком стало фактичне знищення інституту співпраці зі свідками, адже жоден прокурор сьогодні не ризикне братися за складну справу, де його власна свобода може опинитися під загрозою через бюрократичну процедуру.

Паралельно Конгрес узявся за знищення механізмів фінансового контролю над політичною системою. Було внесено зміни до кримінального кодексу, які вилучили політичні партії з-під дії норм про кримінальну відповідальність. Це рішення миттєво зупинило низку триваючих розслідувань щодо відмивання грошей та незаконного фінансування виборчих кампаній, зокрема й ті, що стосувалися президентської кампанії Кікі Фухіморі 2021 року.

Але найбільш структурною зміною стало передання повноважень щодо проведення попередніх кримінальних розслідувань від Генеральної прокуратури до Національної поліції. У супровідному документі Конгресу стверджувалося, що прокурорський нагляд «обмежує дії поліції», однак експерти з безпеки, прокурори та правозахисні організації попередили про катастрофічні наслідки такого кроку. Поліція підпорядковується виконавчій владі, а отже, отримує можливість затримувати або блокувати розслідування, що стосуються державних чиновників. Це не просто технічна зміна, а радикальне порушення балансу між гілками влади, яке відкриває шлях для політично вмотивованого переслідування або, навпаки, захисту корумпованих посадовців.

Окремі законодавчі ініціативи були спрямовані на те, щоб зробити неможливим саме викриття злочинів на ранніх стадіях. Зміни до процедури обшуків зобов'язали поліцію забезпечувати присутність адвокатів захисту під час проведення слідчих дій. Це, по суті, знищило фактор раптовості, який є критично важливим для фіксації доказів. Підозрювані отримують можливість знищити докази або просто втекти до того, як обшук буде завершено.

Не менш руйнівною стала зміна до закону про конфіскацію активів. Відтепер перуанські суди можуть конфіскувати майно лише після винесення обвинувального вироку, що в умовах затяжних розслідувань і корумпованої судової системи робить цей інструмент практично недієздатним. Обвинувачені у корупції можуть вільно розпоряджатися своїми активами протягом усього розслідування, переховувати їх або виводити за кордон.

Крім того, Конгрес ухвалив так званий «Закон проти НПО», який забороняє неурядовим організаціям використовувати міжнародне фінансування для подання позовів проти держави. Це фактично унеможлиблює діяльність правозахисних та антикорупційних організацій, які раніше відігравали ключову роль у моніторингу дій влади та притягненні корупціонерів до відповідальності.

Однак найпоказовішим прикладом того, як Конгрес свідомо використовує законодавство для захисту злочинності, є історія з програмою REINFO — Інтегральним реєстром формалізації гірничодобувної діяльності. Ця програма була створена як тимчасовий механізм, покликаний допомогти дрібним неформальним видобувачам легалізувати свою діяльність. За умовами програми, заявники отримують тимчасовий захист від переслідування за незаконний видобуток, поки вони нібито працюють над дотриманням екологічних, податкових та безпекових вимог.

Однак Конгрес уже вп'яте продовжив дію цієї програми, перетворивши тимчасовий захід на постійний захист для тих, хто не має жодного наміру виходити з тіні. Як зазначають джерела в поліції та гірничодобувній галузі, REINFO стала ідеальним інструментом для розширення нелегального видобутку. Організовані злочинні угруповання використовують реєстр для створення легальних фасадів, під прикриттям яких ведуть абсолютно неконтрольовану діяльність. Це не лише завдає колосальної шкоди довкіллю — особливо в регіонах на кшталт Мадре-де-Діос, де незаконна видобувна діяльність спричинила екологічну катастрофу, — а й створює величезні грошові потоки, які потім спрямовуються на фінансування політичних кампаній.

Симбіоз між нелегальними видобувачами та політичною елітою набув системного характеру. За даними розслідувань, майже в кожній парламентській фракції є представники, так чи інакше пов'язані з нелегальною гірничодобувною промисловістю. Один із колишніх голів Конгресу, Едуардо Сальуана Кавідес, який обіймав цю посаду у 2024–2025 роках, стикнувся з кількома корупційними звинуваченнями, що стосуються його діяльності в регіоні, відомому як осередок незаконного видобутку золота. Попри це, він послідовно голосував за законопроекти, які послаблюють контроль над галуззю.

Як зауважив один із правозахисників, ситуація дедалі більше нагадує історію Пабло Ескобара в Колумбії, але з суттєвим уточненням. Якщо колумбійський наркобарон фінансував політиків, то в сучасному Перу представники злочинних економік уже не просто спонсорують виборчі кампанії, а й самі балотуються до парламенту. Розслідування, проведене перуанським виданням Fauna Electoral, виявило, що щонайменше 55 кандидатів у депутати на майбутніх квітневих виборах мають прямий або опосередкований зв'язок із програмою REINFO.

Масштаби інституційної деградації вражають. Станом на листопад 2025 року зі 130 членів Конгресу лише троє не мали жодних проблем з законом. 54 перебували під слідством, 63 — на стадії попередніх розслідувань, а щодо десяти було відкрито провадження. Це не просто статистика корумпованості окремих посадовців, а свідчення системної кризи, коли законодавчий орган, покликаний стримувати виконавчу владу та забезпечувати верховенство права, сам став найбільшою загрозою для правової системи.

Аналітики наголошують, що ми маємо справу не з класичною корупцією як винятком, а з перетворенням Конгресу на інструмент захисту злочинних інтересів. Це не окремі «нечесні політики», а цілеспрямована законодавча діяльність, спрямована на демонтаж антикорупційних інституцій. Як зазначив один із експертів, політики приходять до Конгресу не для того, щоб служити суспільству, а з єдиною метою — збагатитися за найкоротший можливий час. Така система, позбавлена меритократії та наповнена людьми зі «злочинним мисленням», стає абсолютно відкритою до використання організованою злочинністю. І це не просто теоретична загроза. Законодавчі зміни, ухвалені за останні роки, вже мають конкретні наслідки: провали в боротьбі з наркотрафіком, стрімке зростання нелегального видобутку золота, який за обсягами вже перевершує легальний, і фактичний параліч антикорупційних розслідувань, що стосуються вищих посадовців.

Таким чином, Перу опинилося в пастці, з якої традиційні політичні механізми не здатні вивести. Країна вступає у передвиборчий період, коли виконавча влада паралізована постійними

кадровими перестановками та відсутністю довгострокової стратегії, законодавчий орган відверто діє на користь злочинних угруповань, а судова система, позбавлена інструментів впливу та незалежності, не може забезпечити навіть базової підзвітності.

Організована злочинність, яка ще кілька років тому перебувала на периферії політичного життя, сьогодні стала його невід'ємною частиною, проникаючи в парламент через списки кандидатів, підкуп і пряме лобювання. Історія з REINFO демонструє, що це вже не поодинокі випадки, а системна практика, коли незаконні фінансові потоки не просто обслуговують політику, а формують її порядок денний.

Перуанське суспільство, яке неодноразово виходило на масові протести проти корупції та сваволі влади, сьогодні стикається з викликом значно більшим, ніж просто зміна чергового непопулярного президента. Йдеться про те, чи здатна країна відновити свої інституції настільки, щоб протистояти загрозі, яка вже пустила коріння в найвищих ешелонах влади. Поки двері Каса-де-Пісарро продовжують бути відкритими для злочинців, а Конгрес ухвалює закони, які захищають кримінальні економіки, майбутнє Перу залишається підвішеним у стані глибокої невизначеності, де кожен новий виборчий цикл ризикує не вирішити кризу, а лише поглибити її.

#### Висновки:

- **Політична нестабільність як головний чинник посилення злочинності.** Зміна восьми президентів за десять років та постійна ротація міністрів внутрішньої безпеки створили інституційний вакуум, у якому неможливо розробити чи реалізувати довгострокову стратегію протидії організованій злочинності.
- **Конгрес як активний агент демонтажу інституцій.** Протягом 2023–2025 років перуанський парламент ухвалив низку «злочинних законів», які системно знищили ключові інструменти боротьби з корупцією: скасували кримінальну відповідальність політичних партій, передали слідчі функції від прокуратури до підконтрольної виконавчій владі поліції, унеможливили конфіскацію активів до вироку суду та фактично заборонили діяльність антикорупційних неурядових організацій.
- **Легалізація кримінальних економік через законодавчі механізми.** Програма REINFO, створена для тимчасової легалізації дрібних видобувачів, стала інструментом захисту організованих злочинних угруповань у сфері незаконного видобутку золота.
- **Пряме проникнення злочинних інтересів до законодавчої влади.** Станом на листопад 2025 року лише троє зі 130 депутатів Конгресу не мали проблем з законом.

### ШІ-агенти у протидії фінансовим злочинам <sup>13</sup>

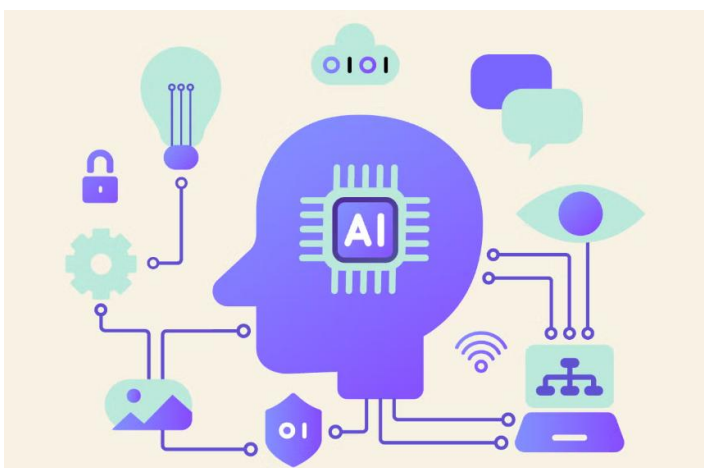
У сучасному ландшафті фінансових послуг, де обсяги транзакційних даних сягають петабайтів, а схеми відмивання грошей і фінансування тероризму стають дедалі витонченішими, перед фахівцями з комплаєнсу постає виклик, який традиційними методами вирішити майже неможливо.

З одного боку, регулятори вимагають дедалі більшої прозорості, швидкості реагування та точності у виявленні підозрілих операцій. З іншого боку, фінансові установи змушені оптимізувати витрати, адже ручний аналіз величезних масивів даних стає непомірно дорогим і

<sup>13</sup> <https://www.acams.org/en/opinion/agentive-workflows-financial-crime>

повільним. Саме в цій точці напруги на сцену виходять великі мовні моделі (LLM) та нова архітектурна парадигма їхнього застосування.

Ключова теза полягає в тому, що успішне впровадження штучного інтелекту у сфері протидії фінансовим злочинам неможливе без чіткого розуміння різниці між «автономними агентами» та «агентними робочими процесами», і саме останні є тією безпечною гаванню, з якої регульованим установам варто розпочинати свою подорож у світ генеративного ШІ.



Автономні агенти уявляються як системи, наділені найвищим ступенем свободи. У такій архітектурі LLM отримує не детальну інструкцію про послідовність кроків, а лише високорівневу мету. Далі агент самостійно вирішує, які інструменти використовувати, у якому порядку їх викликати, як інтерпретувати проміжні результати та коли вважати завдання виконаним. Це відкриває широкі можливості для адаптації до непередбачуваних сценаріїв, але водночас створює значні ризики для регульованого середовища. Поведінка такого агента може бути важкопрогнозованою, його дії — не завжди пояснюваними, а можливість помилки або «галюцинації» моделі може призвести до серйозних комплаєнс-інцидентів.

На противагу цьому, «агентні робочі процеси» пропонують зовсім іншу філософію: тут штучний інтелект виступає не як самостійний виконавець, а як потужний, але контрольований інструмент у руках людини. Послідовність кроків — від визначення джерел даних до формату підсумкового звіту — заздалегідь прописана програмним кодом. LLM виконують окремі, чітко окреслені завдання всередині цього жорсткого каркасу, що робить систему передбачуваною, керованою та значно простішою для аудиту. Саме ця передбачуваність є критично важливою для фінансових інституцій, які працюють під пильним наглядом регуляторів.

Практичний потенціал агентних робочих процесів найкраще розкривається через конкретні приклади, і один із найяскравіших, наведених автором, стосується вилучення транзакцій з нарративу повідомлень про підозрілу діяльність (SARs). Це завдання, яке десятиліттями було каменем спотикання для фахівців з фінансового моніторингу. Традиційно співробітник комплаєнсу мав вручну вичитувати сторінки тексту, виокремлювати звітні номери рахунків, дати, суми та контрагентів, а потім вносити цю інформацію до структурованих баз даних. Процес був не лише виснажливим, але й вразливим до людської помилки. Сьогодні, завдяки агентним робочим процесам, ця рутинна операція може бути повністю автоматизована.

Але справжня цінність тут лежить глибше. Вилучені з SARs структуровані дані про транзакції відкривають три принципово нові можливості. По-перше, вони дозволяють навчати нові, більш точні моделі транзакційного моніторингу, використовуючи реальні приклади раніше поданих звітів як позитивні маркери. По-друге, вони забезпечують безперервність ефективності систем моніторингу під час оновлень: можна перевірити, чи нова версія системи виявляє ті самі підозрілі активності, що й стара, і чи не губить вона активність, яка раніше призводила до подання SARs. По-третє, агрегування цих даних на рівні всієї установи або навіть юрисдикції дозволяє будувати глобальні графи зв'язків, виявляючи складні мережі взаємодій між суб'єктами, які раніше залишалися прихованими в окремих текстових звітах.

Для того щоб такі складні завдання ставали реальністю, автори статті пропонують використовувати арсенал перевірених «архітектурних патернів», кожен з яких вирішує специфічний клас проблем.

Перший і найфундаментальніший патерн — це ланцюжок підказок. У цій моделі LLM викликаються послідовно, немов конвеєр, де результат роботи одного виклику стає вхідними даними для наступного. У контексті обробки SAR це дозволяє розбити складне завдання на логічні, керовані етапи. Спочатку модель виконує виокремлення сутностей, ідентифікуючи в тексті номери рахунків, імена фізичних та назви юридичних осіб, а також найменування фінансових установ. На наступному етапі відбувається мапування — модель встановлює зв'язки між виокремленими сутностями, наприклад, визначаючи, який рахунок належить якій особі. І лише на фінальному етапі, маючи чітке уявлення про структуру даних, модель виокремлює ту частину нарративу, яка безпосередньо описує транзакційну активність для кожного ідентифікованого рахунку. Такий підхід не лише підвищує точність, але й значно спрощує діагностику помилок: якщо на виході отримано некоректний результат, можна точно визначити, на якому саме етапі ланцюжка сталася помилка.

Другий важливий патерн — маршрутизація. Уявіть собі досвідченого диспетчера, який, швидко оцінивши характер вхідного запиту, направляє його до найбільш кваліфікованого виконавця. У ролі такого диспетчера виступає LLM, яка аналізує вхідний нарратив і приймає рішення про подальший маршрут обробки. У наведеному прикладі з транзакціями система використовує два різних модулі. Якщо нарратив містить невелику, але різноманітну кількість конкретних транзакцій, запит спрямовується до LLM, яка безпосередньо синтезує структуровані записи про ці операції. Однак якщо нарратив містить узагальнену інформацію про величезну кількість транзакцій, то в роботу вступає зовсім інший модуль. Це дозволяє обробляти навіть ті SAR, які раніше вважалися «занадто загальними» для автоматизованого аналізу.

Третій патерн — паралелізація — є відповіддю на вимогу швидкості. У світі фінансових злочинів час часто відіграє критичну роль. Замість того, щоб обробляти великий складний нарратив послідовно, система розбиває його на окремі, логічно завершені піднарративи, наприклад, виділяючи опис активності для кожного окремого рахунку або суб'єкта. Кожен із цих піднарративів обробляється незалежно та паралельно, що дозволяє використовувати переваги сучасних хмарних обчислень та значно скорочувати загальний час виконання. Після завершення обробки всіх фрагментів результати агрегуються, а зайві дублікати видаляються, формуючи фінальний, чистий набір даних. Такий підхід не лише пришвидшує роботу, але й підвищує її надійність, оскільки помилка в одному піднарративі не призводить до збою всієї системи.

Нарешті, патерн «оцінювач-оптимізатор» вносить у систему елемент самоконтролю та постійного вдосконалення. У цій архітектурі одна LLM виконує основне завдання, а інша — або навіть та сама модель у різному контексті — виступає в ролі критика, який перевіряє результати та надає зворотний зв'язок. Наприклад, після того, як перша модель виокремила сутності з тексту, друга модель може перевірити, чи не було пропущено жодної важливої організації, чи правильно визначено тип рахунку. Такий процес дозволяє досягти вищої якості результатів.

Втім, автор робить важливе застереження: з появою новітніх моделей міркувань, які внутрішньо виконують подібну саморефлексію та здатні критикувати власні проміжні висновки, необхідність у зовнішньому патерні «оцінювач-оптимізатор» може зменшуватися. Це приклад того, як швидко еволюціонує сама технологія LLM, змінюючи усталені архітектурні практики.

Однак, якими б потужними не були ці архітектурні патерни, автор наголошує на фундаментальному принципі, який відрізняє професійну розробку систем на основі LLM від аматорських експериментів: неможливість побудувати надійну систему без всеосяжної стратегії тестування та оцінювання. Великі мовні моделі, на відміну від детермінованих алгоритмів, є ймовірнісними системами. Два абсолютно однакові запити, надіслані до моделі з інтервалом у кілька секунд, можуть повернути різні, хоча й семантично подібні, відповіді.

Ця властивість, яка є джерелом креативності моделей, у контексті фінансового комплаєнсу перетворюється на ризик. Тому розробка має починатися з найнижчого рівня — модульних

тестів, які перевіряють окремі LLM-виклики на заздалегідь визначених, простих прикладах. Чи зможе модель правильно ідентифікувати ім'я клієнта та назву банку у фразі «Джон, клієнт Банку XYZ, поповнив свій рахунок на 1000 доларів»? Такий підхід дозволяє відловити найгрубіші помилки на ранніх етапах. Далі ці тести ускладнюються та охоплюють цілі робочі процеси. Чи правильно система розіб'є наратив на два піднаративи, якщо в ньому йдеться про два різні рахунки? Чи коректно спрацює маршрутизатор на складному випадку?

Але навіть найкращі модульні тести не дають відповіді на головне питання: наскільки добре система працюватиме в реальних умовах, з усією різноманітністю та непередбачуваністю реальних даних? Для цього потрібні системи оцінювання, які базуються на «золотих» наборах даних. Створення такого набору — це копітка робота, яка вимагає тісної співпраці інженерів з експертами в предметній галузі. Для застосунку з вилучення транзакцій з SAR таким експертом є досвідчений фахівець з фінансового моніторингу, який вручну розмічає набір зразкових наративів, вказуючи, які сутності мають бути вилучені, які транзакції синтезовані. Цей «золотий» набір стає еталоном, бенчмарком, за яким оцінюється будь-яка зміна в системі. Чи покращила нова версія промπτу точність виокремлення номерів рахунків? Чи не призвела зміна базової моделі до зниження повноти (recall) виявлення підозрілих транзакцій? Відповіді на ці питання дають чітко визначені метрики, такі як точність та повнота для завдань виокремлення сутностей, або відсоткова різниця між синтезованими та реальними сумами транзакцій для завдань генерації даних. Лише маючи таку систему вимірювання, можна впевнено рухатися вперед, оптимізувати систему та доводити її надійність перед внутрішніми аудиторами та зовнішніми регуляторами.

Переходячи до практичних аспектів впровадження, автор звертає увагу на важливість вибору правильних інструментів та моделей. Сьогоднішній ландшафт фреймворків для розробки агентних систем є надзвичайно різноманітним і швидкозмінним. Існує спокуса обрати фреймворк із найвищим рівнем абстракції, який дозволяє швидко створити прототип, використовуючи мінімум коду. Однак автор застерігає від прихованих небезпек такого підходу. Високий рівень абстракції часто означає, що фреймворк виконує неявні дії, генерує приховані промпти або має недокументовану поведінку, яка може стати критичною у виробничому середовищі. Наводиться приклад, коли фреймворк автоматично передавав результати роботи інструменту назад до LLM, але коли обсяг цих результатів перевищував контекстне вікно моделі, дані обрізалися, що призводило до втрати критичної інформації. Ця проблема не була очевидною з документації та проявилася лише на певному масштабі. Тому автор рекомендує підходити до вибору фреймворків обережно, віддаючи перевагу прозорості та контрольованості над швидкістю початкової розробки.

Так само виваженим має бути підхід до вибору самої мовної моделі. У сфері фінансових злочинів, де ціна помилки надзвичайно висока, компроміси щодо якості неприпустимі. Тому автор пропонує стратегію «від зворотного»: починати розробку з найкращої, найпотужнішої доступної моделі. Це дозволяє встановити максимально досяжну планку якості для конкретного випадку використання. Коли цей орієнтир досягнуто і створено надійну систему оцінювання, можна розпочинати оптимізацію вартості, експериментуючи з дешевшими, менш ресурсомісткими моделями. Ключовим тут є наявність системи оцінювання, яка з високою точністю покаже, чи не погіршується якість при переході на дешевшу модель. Такий підхід дозволяє знайти оптимальний баланс між вартістю, швидкодією та якістю, що є критичним для масштабування рішення на всю установу.

Впровадження агентних робочих процесів у регульованому середовищі фінансових установ неминуче пов'язане з цілим спектром ризиків, які потребують системного управління. Автор виокремлює чотири ключові категорії.

По-перше, це модельний ризик, властивий будь-якій системі машинного навчання, але загострений ймовірнісною природою LLM. Оновлення базової моделі провайдером може змінити її поведінку, навіть якщо промпти залишаються незмінними. Зміна вхідних даних з часом також може призвести до деградації продуктивності. Стратегія пом'якшення цього ризику полягає у впровадженні вже згаданих систем оцінювання, які постійно моніторять якість роботи, а також у встановленні чітких тригерів для ре-валідації моделі — наприклад, при кожному оновленні версії LLM або при виявленні відхилень у ключових метриках.

По-друге, проблема пояснюваності та можливості аудиту. Традиційні системи моніторингу часто працюють на основі чітких, детермінованих правил, які легко пояснити аудиту. LLM-системи за замовчуванням є «чорними скриньками». Пом'якшення ризику тут вимагає ретельного інженерного підходу: ведення детальних логів усіх вхідних та вихідних даних, усіх викликів інструментів, фіксації промптів та їхніх версій. Для критичних рішень необхідно зберігати не лише результат, але й ланцюжок міркувань моделі, що привів до цього результату. Використання новітніх моделей, які надають явний, читабельний ланцюжок думок, значно спрощує завдання аудиту.

Третя категорія ризику — це питання конфіденційності та безпеки даних. Передача конфіденційної інформації про клієнтів, такої як номери рахунків, суми транзакцій, персональні дані, до сторонніх API LLM-провайдерів викликає серйозне занепокоєння. Де фізично обробляються дані? Чи використовуються вони для навчання моделей провайдера? Чи відповідають ці процеси вимогам щодо локалізації даних, які діють в законодавстві?

Для пом'якшення цих ризиків пропонується багаторівнева стратегія. На першому рівні — використання договірних механізмів, які гарантують, що дані не будуть використані для навчання. На другому, для особливо чутливих випадків — розгортання відкритих моделей у приватних хмарах або локальній інфраструктурі, що дозволяє зберегти дані всередині периметра установи. На третьому — принципи мінімізації даних та контролю доступу: модель має отримувати лише ту інформацію, яка є суворо необхідною для виконання конкретного завдання, а всі операції мають бути залоговані та підлягати аудиту.

Нарешті, четверта категорія ризику — регуляторний комплаєнс. Фінансові установи залишаються підзвітними перед регуляторами за всі свої системи, включаючи ті, що використовують ШІ. У різних юрисдикціях діють різні, іноді суперечливі, вимоги. Автор нагадує про діючі керівництва, такі як SR 11-7 для банків США або нові MAS Guidelines для Сінгапуру. Ключова стратегія тут — проактивна взаємодія з підрозділами комплаєнсу, юридичним відділом та командою валідації моделей на ранніх етапах проекту. Жодна система не має потрапляти у виробниче середовище без повного документального супроводу та, бажано, після періоду паралельного запуску, коли рішення агентної системи порівнюються з рішеннями, прийнятими за існуючою методологією.

У цьому контексті автор ще раз наголошує на принциповій перевазі агентних робочих процесів перед повністю автономними агентами. Оскільки робочі процеси слідує заздалегідь визначеними шляхами, вони за своєю конструкцією є більш передбачуваними та безпечними. Вони залишають контроль над діями системи в руках людини, дозволяють чітко визначити, які джерела даних доступні, які дії дозволені, а які — ні. Вони не приймають рішень без нагляду та моніторингу. Це робить їх ідеальною відповідною точкою для впровадження ШІ в регульованому середовищі. Звісно, рівень управління та нагляду має відповідати ризику конкретного застосунку. Робочий процес, який просто шукає та підсумовує негативні новини про клієнта в інтернеті, вимагатиме менш суворого контролю, ніж процес, який автоматично готує та подає звіт про підозрілу діяльність до державного органу.

**Висновки:**

- **«Агентні робочі процеси», а не «автономні агенти», є безпечною точкою входу.** На відміну від повністю автономних систем, де LLM самостійно визначає послідовність дій, агентні робочі процеси мають заздалегідь визначені кодові шляхи, що забезпечує передбачуваність, керованість та значно нижчий рівень ризику для регульованих фінансових установ.
- **Якість системи визначається не моделлю, а інфраструктурою тестування.** Успішне впровадження неможливе без створення «золотих» наборів даних, розробки метрик оцінювання та постійного моніторингу продуктивності, оскільки ймовірна природа LLM потребує системного підходу до контролю якості.
- **«Архітектурні патерни» дозволяють вирішувати раніше недоступні завдання.** Приклад із вилученням транзакцій з наративів SARs демонструє, як комбінація цих патернів відкриває можливості для навчання моделей моніторингу, забезпечення безперервності систем та побудови глобальних графів зв'язків між суб'єктами.
- **Ризики впровадження потребують системного управління на всіх рівнях.** Модельний ризик, питання пояснюваності, безпека даних та регуляторний комплаєнс мають бути інтегровані в процес розробки з першого дня через раннє залучення юридичних відділів та впровадження практик детального логування й контролю версій.

На завершення документ закликає фінансову спільноту до поєднання сміливості з дисципліною. Темпи розвитку штучного інтелекту є вражаючими: те, що було неможливим для найкращих моделей пів року тому, сьогодні є рутинним завданням. Проект, який два роки тому здавався надто складним через неструктурованість даних або складність логіки, сьогодні може бути реалізований за допомогою одного з описаних патернів. Це створює величезні можливості для підвищення ефективності, зниження операційних ризиків та посилення захисту фінансової системи від зловмисників. Однак реалізація цього потенціалу вимагає не лише технологічної експертизи, а й зрілості в управлінні ризиками.

Ключові уроки для тих, хто розпочинає цей шлях, залишаються незмінними: починати з керованих агентних робочих процесів, а не з непередбачуваних агентів; інвестувати значні зусилля в розробку систем оцінювання якості ще до того, як система буде масштабована; завжди зберігати людський контроль і нагляд за всіма значущими рішеннями; ретельно документувати кожен етап розробки та експлуатації, готуючись до

майбутніх аудитів та перевірок; та будувати міждисциплінарні команди, де фахівці з даних і розробники працюють пліч-о-пліч з експертами з комплаєнсу з першого дня проекту. Саме такий підхід дозволить фінансовим установам не просто йти в ногу з технологічним прогресом, а використовувати його як стратегічну перевагу, діючи безпечно, відповідально та ефективно.

## **Інші новини**

### **Розкрадання коштів на гуманітарному розмінуванні: викриття схеми та системні ризики для України<sup>14</sup>**

Правоохоронні органи викрили масштабну схему привласнення бюджетних коштів, виділених на гуманітарне розмінування територій Херсонської області. Йдеться про регіон, який після деокупації залишається одним із найбільш небезпечних через значне забруднення мінами та

<sup>14</sup> <https://gp.gov.ua/ua/posts/vikrito-sxemu-rozkradannya-byudzetnix-kostiv-na-gumanitarnomu-rozminuvanni>

іншими вибухонебезпечними предметами, а тому реалізація програм розмінування має критичне значення не лише для відновлення інфраструктури, але й для забезпечення базової безпеки населення. За даними слідства, до організації протиправної діяльності були причетні посадові особи та представники комерційних структур, які діяли узгоджено та використовували механізми державного фінансування для привласнення коштів.



Схема функціонувала через укладення договорів на проведення робіт із розмінування із підконтрольними або афілійованими підприємствами. Ці компанії отримували бюджетні кошти в межах відповідних програм, однак фактичне виконання робіт або не здійснювалося у повному обсязі, або ж виконувалося частково та формально. Водночас у звітній документації відображалися повні обсяги виконаних робіт, що створювало видимість належного освоєння коштів. Додатково застосовувався механізм завищення вартості послуг, що дозволяло збільшувати суми фінансування та виводити ще більші обсяги коштів.

Окрему роль у реалізації схеми відіграло документальне прикриття, яке забезпечувало формальну відповідність усіх операцій вимогам законодавства. Через це кошти проходили через офіційні рахунки без негайного виявлення порушень, а контрольні механізми не дозволяли оперативно встановити невідповідність між задекларованими та фактичними результатами робіт. Така модель створювала ілюзію законності та ускладнювала виявлення правопорушень на початкових етапах.

Наслідки функціонування цієї схеми мають не лише фінансовий, але й безпековий характер. Попри витрачені бюджетні ресурси, частина територій фактично залишалася замінованою, що становить пряму загрозу для життя і здоров'я цивільного населення. Це також ускладнює повернення мешканців на деокуповані території, стримує відновлення сільського господарства та економічної діяльності загалом. Таким чином, розкрадання коштів у цій сфері призводить до подвійних втрат: держава втрачає фінансові ресурси, а суспільство — можливість швидкого та безпечного відновлення.

Правоохоронні органи у ході розслідування встановили ключових учасників схеми, механізм її реалізації та задокументували відповідні факти протиправної діяльності. У межах кримінального провадження здійснюється аналіз укладених договорів, фінансових операцій, а також перевіряється відповідність заявлених і фактично виконаних робіт. Проводяться слідчі дії, спрямовані на встановлення повного кола причетних осіб, обсягів завданих збитків і подальше притягнення винних до відповідальності.

Загалом цей випадок демонструє наявність серйозних проблем у системі контролю за використанням бюджетних коштів у критично важливих сферах відновлення, зокрема у гуманітарному розмінуванні. Він також підкреслює, що навіть у секторах, які мають першочергове значення для безпеки держави та населення, існують ризики зловживань, пов'язаних із державними контрактами та недостатньою перевіркою фактичного виконання робіт.

## Ілюзія контролю: чому знищення лідера не руйнує бізнес<sup>15</sup>

Арешт Себастьяна Марсета в Болівії 13 березня 2026 року став тією рідкісною подією, яка змусила навіть звичних до гучних затримань аналітиків говорити про «серйозний удар» по наркотрафіку.

Операція, проведена спільними зусиллями болівійського спецпідрозділу FELCN та американського Управління з боротьби з наркотиками, виглядала бездоганною: Марсета, який довгі роки вважався невловимим, майже одразу після затримання відправили літаком до Сполучених Штатів, де на нього вже чекало звинувачення у змові з метою відмивання грошей.



Для зовнішнього спостерігача це могло б виглядати як класичний триумф правоохоронної системи, черговий доказ того, що довга рука правосуддя здатна дістати злочинця навіть у найвіддаленіших куточках континенту. Однак за цією переможною картинкою ховається набагато складніша, тривожніша і, певною мірою, навіть цинічна реальність сучасного наркобізнесу: усунення ключових фігур, хай навіть таких масштабних, як Марсет, перестало бути фатальною подією для злочинних мереж, перетворившись на тимчасову незручність, яку ринок долає з вражаючою швидкістю та адаптивністю.

Постать Себастьяна Марсета є ідеальною ілюстрацією того, як змінилася архітектура наркотрафіку за останнє десятиліття. Він не був класичним «наркобароном» у стилі Пабло Ескобара, який будував вертикальну імперію, що трималася на страху та територіальній монополії. Натомість Марсет виступив у новій, набагато більш притаманній сучасності ролі — ролі брокера. Його капітал полягав не в гектарах полів коки чи навіть у власному флоті кораблів, а в мережі зв'язків, яку він збирав по крихтах упродовж свого кримінального життя. Ключовим моментом у цій кар'єрі стало перебування в уругвайській в'язниці за торгівлю марихуаною. Саме там, за ґратами, він, імовірно, зав'язав ті контакти, які після звільнення у 2018 році дозволили йому зробити стрімкий стрибок на вершину транснаціональної злочинності. Переїхавши до Болівії, він опинився в точці перетину двох потужних сил: місцевих виробників кокаїну та бразильського Першого столичного командування (PCC), яке вже давно закріпилося в цій країні як ключовий покупець і логістичний партнер.

Мережа, створена Марсетом, вражала своєю витонченістю та географічним охопленням. Це була не імперія, а складна система вузлів, кожен з яких виконував чітко визначену функцію. Сам Марсет виступав як інтегратор: він знаходив покупців у Європі, домовлявся про ціну та гарантував транзит. Фізичний ланцюг поставок виглядав як типовий для сучасного трафіку, але відзначався рідкісною ефективністю. Кокаїн авіацією перекидався з Болівії до Парагваю, де вступали у дію наземні логістичні мережі, які переправляли його до стратегічно важливого водного шляху Парана — Парагвай. Звідти вантажі, вже в контейнерах, вирушали океанськими суднами до портів Африки, а потім — до кінцевих споживачів у Європі.

Фінансова складова цієї системи була вибудована з такою ж інженерною точністю: Федеріко Санторо Васалло, діючи за прямими наказами Марсета, відмивав мільйони доларів через банківську систему Сполучених Штатів, використовуючи складні ланцюжки переказів, підставних компаній та обмінники валют. Те, що Васалло отримав 15 років американської

<sup>15</sup> <https://insightcrime.org/news/marset-capture-cocaine-business/>

в'язниці ще в липні 2025 року, не зруйнувало структуру — вона вже була достатньо диверсифікованою.

Одним із найбільш промовистих свідчень масштабів впливу Марсета стало проникнення його мережі в політичні еліти. Коли парагвайська влада провела масштабну операцію «A Ultranza PY», наслідки виявилися шокуючими навіть для країни, звиклої до корупційних скандалів. Серед засуджених та підслідних опинився діючий сенатор Еріко Галеано, якого визнали винним у відмиванні. Поряд із ним — впливовий бізнесмен Альберто Коубе Аяла та колишній конгресмен Хуан Карлос Озоріо. Цей перелік імен наочно демонструє, що Марсет був не просто наркоторговцем, а центральною фігурою гібридної структури, де кримінальний капітал тісно переплітався з політичним впливом та інституційним захистом. Його здатність залучати на свій бік представників законодавчої влади, бізнесу та правоохоронних органів перетворювала його мережу на подобу паралельного уряду, який контролював ключові транзитні маршрути на півдні континенту.

Однак саме тут, у момент тріумфу правоохоронців, виникає головне запитання, що ставить під сумнів доцільність стратегії, яка десятиліттями домінувала в антинаркотичній політиці: чи справді усунення Марсета означає крах його імперії?

Досвід останніх років, який докладно аналізується в документах цієї справи, дає приголомшливо красномовну відповідь. Сучасний наркотрафік давно перестав бути ієрархічною структурою, яка тримається на хиткій рівновазі довкола одного лідера. Натомість він трансформувався в складну, децентралізовану мережу, де на кожному етапі — від вирощування коки до доставки кінцевому споживачеві — діє кілька незалежних або напівнезалежних операторів. Така архітектура, яка за своєю суттю нагадує принципи роботи сучасного IT-сектору або вільних ринків, робить систему надзвичайно стійкою. Коли один вузол випадає, інші миттєво перерозподіляють його функції, а маршрути, якими він керував, швидко переходять під контроль конкурентів або колишніх партнерів.

Найкраще цю динаміку ілюструють події, що розгорталися ще до того, як Марсет опинився в наручниках. У вересні 2024 року в Болівії був важко поранений під час замаху Ерланд Івар Гарсія Лопес, відомий у кримінальному світі як «Ель Колья». Цей чоловік був ключовою фігурою в структурі Марсета — він відповідав за організацію кокаїнових рейсів та управління аеродромами, які слугували перевалочними базами. За версією болівійської поліції, замах став наслідком конфлікту за контроль над літаками та злітно-посадковими майданчиками. Цей епізод є надзвичайно показовим. Він свідчить про те, що навіть за життя Марсета, коли він ще перебував на вершині влади, його власна мережа вже почала демонструвати ознаки внутрішньої боротьби за ресурси. Маршрути, які він вважав своїми, вже не були його беззаперечною монополією, а аеродроми, які контролював Ель Колья, стали предметом суперечки, що вирішувалася зброєю.

Але ще більш показовим є досвід боротьби з бразильським Першим столичним командуванням, яке десятиліттями залишається одним із найпотужніших злочинних угруповань континенту. РСС, як і багато інших сучасних мереж, будувало свою міжнародну експансію через інституцію брокерів — таких самих, яким був Марсет. Одним із найвідоміших із них був Жілберто Апаресіду дус Сантус, відомий як «Фуміньйо».

Будучи другом дитинства верховного лідера РСС, Фуміньйо витратив роки на те, щоб створити розгалужену систему контактів, необхідну для торгівлі кокаїном та зброєю на міжнародному рівні. Саме він приблизно у 2016 році зустрічався з Домініко Пелле, головою клану Пелле з могутньої калабрійської Ндрангети, закладаючи підґрунтя для стратегічного партнерства між південноамериканським угрупованням та італійською мафією. Коли Фуміньйо був заарештований у Мозамбіку у 2020 році, багато хто очікував, що це стане нищівним ударом по міжнародних амбіціях РСС. Однак цього не сталося. Угруповання не лише не втратило своїх

позицій, але й продовжило зростання, зміцнившись як один із найбільших гравців на світовому ринку кокаїну. Фуміньйо виявився замінним, а його функції — розподіленими між іншими членами мережі.

Та сама модель з вражаючою послідовністю відтворюється і в італійській Ндрангеті, яка сьогодні вважається наймогутнішою мафіозною структурою Європи та ключовим імпортером кокаїну на континент. Ндрангета історично будувала свою експансію в Південній Америці через брокерів, які діяли з великою автономією. Нікола Ассіс та Рокко Морабіто — лише два імені з довгого списку таких посередників, які протягом останніх років були заарештовані (Морабіто у 2017 році, Ассіс у 2019 році) за сприяння трансатлантичним поставкам кокаїну. Однак ці арешти не спричинили колапсу Ндрангети. Навпаки, вона зберегла і навіть зміцнила свою домінуючу позицію на європейському ринку. Секрет криється в самій структурі організації: Ндрангета побудована на принципах горизонтальних зв'язків, де окремі клани мають значну автономію, а функції брокерів розподілені між багатьма виконавцями, що робить систему майже невразливою до втрати однієї, навіть ключової, фігури.

Цей досвід має пряму проекцію на ситуацію з Марсетом. Його арешт, безсумнівно, є важливою подією. Він позбавляє злочинний світ однієї з найбільш досвідчених і добре законспірованих фігур, яка володіла унікальними зв'язками на стику політики, фінансів та логістики. Короткострокові наслідки будуть відчутними: затримки в поставках, плутанина в розрахунках, тимчасовий хаос у мережах, які звикли покладатися на його посередництво. Однак немає жодних підстав вважати, що цей хаос призведе до тривалого колапсу.

Більше того, історія Марсета показує, що процес заміщення може починатися ще до того, як лідер фізично усувається. Конфлікт з Ель Коля, який розгорівся за кілька місяців до арешту, свідчить про те, що всередині структури вже точилася боротьба за активи та маршрути. Імовірно, інші гравці, які залишаються поки що в тіні, вже давно готувалися до моменту, коли Марсет вибуде з гри.

З огляду на це, тактика, яка десятиліттями домінувала в міжнародній антинаркотичній політиці — фокус на полюванні за лідерами та публічні демонстративні арешти, — виглядає дедалі більш архаїчною та стратегічно недалекоглядною. Вона створює ілюзію прогресу, дозволяючи політикам звітувати про успіхи, але не змінює фундаментальних структурних умов, які роблять наркоторгівлю такою прибутковою та живучою. Справжній виклик полягає не в тому, щоб наздогнати чергового втікача, а в тому, щоб демонтувати саму екосистему, яка дозволяє таким мережам існувати.

Це означає необхідність одночасної роботи за кількома напрямками: боротьба з фінансовими потоками, які забезпечують безперерйне функціонування брокерів; системне протистояння проникненню злочинності в державні інституції, яке гарантує безкарність; розвиток альтернативних економічних можливостей у регіонах, де вирощування коки залишається єдиним джерелом існування; та, що найважче, формування механізмів міжнародної координації, здатних відстежувати не окремих осіб, а цілі мережі, які постійно змінюють структуру та адаптуються до нових умов швидше, ніж правоохоронна система встигає на них реагувати.

Поки цього не станеться, арешти таких постатей, як Себастьян Марсет, залишатимуться лише ефектними, але не стратегічними перемогами. Вони дарують коротке відчуття справедливості та створюють публічний наратив про успішну боротьбу з наркозлочинністю, однак не змінюють глибинну структуру. Світова індустрія кокаїну, в якій обертаються десятки мільярдів доларів на рік, довела свою здатність виживати після втрати будь-яких лідерів. І доки не буде знайдено спосіб впливати на саму структуру цього ринку, а не лише на окремі його фігури, ми будемо знову і знову спостерігати один і той самий цикл.

**Ваша думка важлива!**

1. Яким чином можна застосувати моніторинг для аналізу форм дитячої злочинності в Україні, щоб розробити ефективні програми раннього запобігання рекрутингу до кримінальних структур, особливо серед вразливих категорій дітей?
2. Які інституційні запобіжники мають бути створені в Україні, аби унеможливити ситуацію, за якої законодавча влада може системно демонтувати антикорупційні інструменти, особливо в контексті євроінтеграційних вимог щодо незалежності судової системи, спеціалізованих антикорупційних органів та неурядового моніторингу?
3. Яким чином в Україні можна стимулювати приватний сектор до активнішого виявлення та повідомлення про складні схеми легалізації доходів, враховуючи, що на відміну від Великої Британії, в Україні досі відсутня розвинена культура «підзвітного суб'єкта як партнера правоохоронних органів»?
4. Які сектори економіки в Україні (фінансовий сектор, фінтех, криптоіндустрія) повинні бути пріоритетно інтегровані у моделі PPP для протидії організованому шахрайству, виходячи з національної оцінки ризиків?
5. Які фактори можуть визначати вразливість держави до використання її економіки у міжнародних схемах фінансових злочинів?
6. Які конкретні зміни у системі державних закупівель можуть мінімізувати ризик участі афілійованих або фіктивних компаній у проєктах гуманітарного розмінування територій?

**Контакуйте щодо цього документу з Міністерством фінансів України:**

- Email: [aml\\_bulletin@minfin.gov.ua](mailto:aml_bulletin@minfin.gov.ua)
- Поштова адреса: Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- Ідентифікація контакту: стосовно Методологічного Бюлетеня № МінФін-AML-2026-14

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 [\[офіційний веб-сайт Міністерства фінансів\]](#).