



“Або ви керуєте вашим днем, або день управляє вами”

Джим Рон

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



Наглядний звіт Великої Британії 2024-2025 ¹



Anti-Money Laundering and
Counter-Terrorist Financing
Supervision Report 2024-25

Цей документ є 13-м щорічним звітом Казначейства Його Величності (HM Treasury), який виконує законодавче зобов'язання відповідно до Правила 51 Положень про відмивання коштів, фінансування тероризму та переказ коштів (інформація про платника) 2017 року (далі — «MLRs»). Звіт базується на інформації, запитаній у наглядових органів за фінансовий рік **2024-25**, і є фундаментальним джерелом для розуміння ефективності британської системи фінансового моніторингу.

Структура звіту є логічно виваженою та охоплює всі аспекти наглядової діяльності, що дозволяє детально проаналізувати стан справ у сфері AML/CTF. Документ розпочинається з **Передмови**, яка задає тон усьому звіту,

¹ https://assets.publishing.service.gov.uk/media/693308125b5198836f304150/24-25_Annual_Report_.pdf

підкреслюючи важливість боротьби з економічними злочинами. Далі йде **Розділ 1: Вступ**, який окреслює комплексну структуру режиму нагляду у Великій Британії. Тут детально описується критична роль наглядових органів, до яких належать Управління з фінансового нагляду (FCA), Податкова та митна служба Його Величності (HMRC), Комісія з азартних ігор (GC), а також 22 професійні організації-наглядачі (PBSs) у сфері права та бухгалтерського обліку, та OPBAS (Office for Professional Body Anti-Money Laundering Supervision). Цей розділ також анонсує масштабні реформи наглядового режиму, зокрема передачу функцій нагляду за професійними послугами (юридичні, бухгалтерські послуги, послуги трастів та компаній) до FCA, що фактично замінить роль PBSs та OPBAS після повної імплементації.

Розділ 2: «Гейткіпінг» та оцінка ризиків присвячений обов'язкам наглядових органів щодо реєстрації бізнесів для нагляду згідно з MLRs та оцінки ризиків відмивання коштів у їхніх піднаглядних організаціях. «Гейткіпінг» визначається як ключова функція, що гарантує відповідність бізнесів мінімальним необхідним стандартам перед їх входом на ринок. Це включає перевірку «відповідності та належності» (fit and proper checks) ключових осіб, щоб упевнитися, що вони не мають судимостей за релевантні злочини (відмивання коштів, шахрайство тощо). Розділ також деталізує вимогу до наглядових органів застосовувати ризик-орієнтований підхід, спрямовуючи ресурси на сфери з найвищим ризиком експлуатації злочинцями.

Розділ 3: Моніторинг піднаглядних бізнесів є, мабуть, найбільш насиченим статистичними даними. Він деталізує підходи кожного наглядача до моніторингу відповідності MLRs, використовуючи такі методи, як документарні перевірки (desk-based reviews, DBRs) та виїзні перевірки. У цьому розділі наводиться статистика наглядової діяльності, включаючи загальну кількість перевірок, кількість персоналу, задіяного у сфері AML/CTF, та обсяги витрат.

Розділ 4: Забезпечення відповідності описує використання наглядовими органами заходів примусу для просування дотримання стандартів AML/CTF. Це включає спектр заходів від попереджень до штрафів та скасування ліцензій.

Розділ 5: Співпраця, координація та обмін інформацією досліджує освітню роль наглядових органів, їхню співпрацю з іншими наглядачами, правоохоронними органами та приватним сектором.

Особлива увага у документі приділяється майбутнім стратегічним документам. Згадується, що Уряд планує опублікувати нову **Стратегію боротьби з відмиванням коштів та повернення активів** після завершення дії Плану боротьби з економічною злочинністю 2023-26 (ECP2). Також зазначається, що Велика Британія готується до п'ятого раунду оцінювання Групою з розробки фінансових заходів боротьби з відмиванням грошей (FATF), звіт про взаємну оцінку якої буде опубліковано у **2028 році**. Ця оцінка матиме нову методологію, що фокусуватиметься на ефективності системи, а не лише на технічній відповідності законодавства.

Звіт надає глибокий статистичний зріз стану наглядової системи Великої Британії, дозволяючи відстежити динаміку витрат, кадрового забезпечення та інтенсивності перевірок протягом останніх трьох років. Аналіз цих даних вказує на те, що система перебуває під значним тиском необхідності підвищення ефективності на тлі зростання витрат.

Дані, представлені у Таблиці 3.А звіту, демонструють такі ключові показники:

Показник	2022-23	2023-24	2024-25	Аналіз тренду
Загальні витрати на AML/CTF	£35.5 млн	£46 млн	£57 млн	Спостерігається значне зростання витрат (+24% рік до року), що відображає збільшення операційних



				витрат та, ймовірно, інвестиції в технологічні рішення для моніторингу.
Кількість персоналу (FTE), задіяного в AML/CTF	508	708	693	Незначне зменшення (-2%), що може свідчити про оптимізацію штату або перехід до більш автоматизованих методів нагляду.
Кількість перевірок (% від популяції)	6%	10%	8%	Стабілізація рівня перевірок після пікового значення попереднього року. Це вказує на використання більш цільового, ризик-орієнтованого підходу замість випадкових вибірок.
Рівень рецидивізму невідповідності	Дані не збиралися	Дані не збиралися	15%	Новий критичний показник, який вказує на те, що 15% бізнесів, які були визнані невідповідними під час попередньої оцінки, продовжують порушувати правила.
Кількість бізнесів, переведених у категорію вищого ризику	Дані не збиралися	Дані не збиралися	353	Абсолютний показник, що демонструє активну переоцінку ризиків наглядовими органами.

Зростання загальних витрат до **£57 мільйонів** при одночасній стабілізації чисельності персоналу свідчить про те, що наглядові органи, ймовірно, інвестують у складніші інструменти аналізу даних та залучають зовнішніх експертів, замість того щоб просто збільшувати кількість інспекторів. Зменшення відсотка перевірок (з 10% до 8%) корелює з описом у Розділі 3, де наголошується на використанні документарних перевірок (DBR) як більш ефективного інструменту для моніторингу суб'єктів з нижчим рівнем ризику, що дозволяє вивільнити ресурси для глибоких виїзних перевірок високоризикових фірм.

Окремої уваги заслуговує статистика щодо Звітів про підозрілу діяльність (SARs). У звітному періоді наглядові органи проактивно звернулися до **1,412 фірм** із запитом надати їхні SARs для оцінки якості. З **798** звітів, які були оцінені, **62** були визнані неадекватними. Цей процес забезпечення якості є життєво важливим, оскільки звіт підкреслює, що корисність режиму SARs для Національного агентства боротьби зі злочинністю (NCA) залежить саме від якості розвідданих, а не від їх кількості.

Розділ 4 звіту виходить за рамки сухої статистики, надаючи конкретний приклад втручання професійного органу-наглядача (PBS) у діяльність юридичної фірми. Цей кейс є ілюстративним для розуміння глибини проблем у секторі професійних послуг.

У наведеному прикладі юридична практика була визнана такою, що **«потенційно сприяє відмиванню коштів»** через системні провали в процедурах AML. Серед виявлених порушень були:

1. Працівник з питань звітування про відмивання коштів (MLRO) мав обмежене розуміння своїх обов'язків.
2. Відсутність будь-яких записів про проведення навчання персоналу з питань AML.
3. Значні недоліки у процедурах належної перевірки клієнтів (Customer Due Diligence — CDD).

4. Відсутність оцінки ризиків клієнтів або окремих справ.

Втручання наглядача призвело до подання Звіту про підозрілу діяльність (SAR) до Національного агентства боротьби зі злочинністю (NCA), що демонструє зміну ролі наглядових органів: вони все частіше діють як «поліцейські» у своїй сфері, а не лише як адміністратори реєстрів. Цей кейс підкреслює, чому уряд Великої Британії вирішив передати нагляд за професійними послугами до FCA — саморегульвні організації часто не мають достатньої жорсткості або ресурсів для виявлення та покарання таких кричущих порушень на системному рівні.

Висновки:

- **Інтеграція безпекового та фінансового векторів:** Боротьба з незаконними фінансами офіційно класифікована як критичний елемент національної безпеки, що передбачає залучення ресурсів розвідувальних служб (MI5, GCHQ) до розслідування складних схем відмивання грошей та автоматичне підвищення пріоритетності таких справ.
- **Масштаб загрози як драйвер реформ:** Офіційна фіксація обсягу відмивання на рівні 100 млрд фунтів стерлінгів створює політичний мандат для застосування активних заходів, включаючи розширене використання ордерів на багатство нез'ясованого походження (UWO) та агресивну конфіскацію активів без обвинувального вироку.
- **Кібер-фінансова конвергенція:** Регулятор вимагає від установ розглядати кіберзлочинність та відмивання грошей як єдиний екосистемний ризик, що зобов'язує банки впроваджувати інтегровані системи моніторингу, які поєднують аналіз транзакцій з даними про технічні вразливості клієнтів.
- **Геополітичний фільтр комплаєнсу:** Фінансові установи повинні переглянути свої ризик-апетити, включивши до факторів високого ризику будь-які зв'язки з юрисдикціями, що проводять ворожу державну політику, навіть якщо формально ці транзакції не підпадають під прямі санкції.

Глобальний ландшафт ризиків — Індекс Basel AML 2025 ²

Даний документ опублікований Базельським інститутом управління у грудні 2025 року. Цей звіт є провідним незалежним інструментом ранжування та оцінки ризиків відмивання коштів та фінансування тероризму у світі.



Basel AML Index 2025: 14th Public Edition
Global money laundering and financial
crime risk ranking

Звіт супроводжується детальним описом методології, яка є критично важливою для інтерпретації результатів. Basel AML Index — це складений індекс, що базується на **17 індикаторах**, згрупованих у п'ять доменів. Розуміння зважування цих доменів дозволяє зрозуміти, чому певні країни, які традиційно вважаються «безпечними», можуть отримувати погані оцінки.

Структура методології Basel AML Index (17 індикаторів у 5 доменах):

1. Домен 1: Якість структури AML/CFT/CPF (Вага: 50%)

- Це найбільш впливовий домен. Він включає дані зі Звітів про взаємну оцінку FATF (35%), Звіту Державного департаменту США про стратегію контролю за наркотиками (INCSR) (5%), Звіту про торгівлю людьми



² <https://index.baselgovernance.org/api/assets/1cdb5e5f-f4c2-4738-918b-f2c4271c6313.pdf>

(5%) та Глобального індексу організованої злочинності (GI-TOC) щодо флори, фауни та невідновлюваних ресурсів (5%). Велика вага FATF означає, що країни, які не пройшли нещодавню оцінку або мають слабкі результати технічної відповідності, автоматично потрапляють у зону ризику.

2. Домен 2: Ризики корупції та шахрайства (Вага: 17.5%)

- Включає Індекс сприйняття корупції Transparency International (5%), Матрицю ризиків хабарництва TRACE (5%), а також індикатори фінансових злочинів та кіберзалежних злочинів від GI-TOC. Важливо зазначити, що включення індикаторів **шахрайства** є специфічним нововведенням видання 2025 року, що відображає зростаючу стурбованість щодо його масштабів як драйвера відмивання коштів. Це суттєво вплинуло на погіршення оцінок країн з високим рівнем доходу, де кібершахрайство є поширеним явищем.

3. Домен 3: Фінансова прозорість та стандарти (Вага: 17.5%)

- Базується на Індексі фінансової таємниці Tax Justice Network (15%) та Індексі розподілу ресурсів IDA Світового банку (2.5%). Висока вага індексу Tax Justice Network часто «карає» такі юрисдикції, як США та Швейцарія, за їхні закони про фінансову таємницю.

4. Домен 4: Публічна прозорість та підзвітність (Вага: 5%)

- Включає Огляд відкритості бюджету, Базу даних політичного фінансування International IDEA та дані Світового банку.

5. Домен 5: Політичні та правові ризики (Вага: 10%)

- Охоплює індекси незалежності судової системи, верховенства права (World Justice Project) та свободи преси.

Критичним оновленням методології для видання 2025 року є перехід до використання статистичного методу **натуральних розривів Дженкса** (Jenks natural breaks) для категоризації ризиків. Це замінює довільні порогові значення системою, яка краще відображає реальний розподіл даних:

- **Низький ризик:** Оцінка менше 4.70
- **Середній ризик:** Оцінка 4.70 – 6.08
- **Високий ризик:** Оцінка більше 6.08.

Такий підхід зменшує переоповнення категорії «середнього ризику» та покращує порівнянність між юрисдикціями.

Найбільш вражаючим висновком звіту 2025 року є зростання середніх показників ризику в **Північній Америці** та **Західній Європі**.

- **Північна Америка (Оцінка 4.72):** Рівень ризику для США та Канади зріс. Основним драйвером стало різке зростання ризиків **фінансової прозорості** (Домен 3), у поєднанні з помірним зростанням корупційних та політичних ризиків. Оцінка США на рівні 4.72 розміщує їх у категорії «Середнього ризику», що руйнує міф про них як про беззаперечно «безпечну» юрисдикцію. Поганий показник фінансової прозорості, ймовірно, пов'язаний з тривалим опором США повній прозорості бенефіціарної власності та існуванням лазівок для реєстрації компаній-оболонок на рівні окремих штатів.
- **ЄС та Західна Європа:** Приблизно **40%** юрисдикцій у цьому регіоні отримали гірші оцінки, ніж у 2024 році. Хоча більшість залишається в категоріях низького або середнього ризику, лінія тренду свідчить про те, що історично сильні виконавці стагнуть або «скокуються»

Висновки:

- **Системна стагнація ефективності:** Глобальне зниження ризику на мікроскопічні 0.02 бали є індикатором того, що формальне прийняття законів вичерпало свій потенціал; подальший прогрес можливий лише через радикальне підвищення якості правозастосування та реальні вигоди.
- **Ефективність "naming and shaming":** Значний прогрес африканських країн підтверджує дієвість механізмів тиску FATF, демонструючи, що навіть в умовах обмежених ресурсів можливе швидке покращення регуляторного середовища за наявності політичної мотивації.
- **Крипто-ризик як структурна проблема:** Відсутність спеціального регулювання VA у багатьох юрисдикціях компенсується загальними правовими ризиками; для банків це означає, що робота з крипто-клієнтами з країн зі слабким верховенством права автоматично є токсичною, незалежно від наявності місцевої ліцензії VASP.
- **Імператив боротьби з шахрайством:** Визнання шахрайства ключовим генератором незаконних доходів вимагає від фінансових установ перекалібрування систем моніторингу транзакцій для виявлення патернів соціальної інженерії та інвестиційних шахрайств як частини AML-процедур.

назад». Звіт попереджає, що злочинці адаптуються швидше, ніж жорсткі європейські регуляторні рамки.

На противагу цьому, регіони, які часто стигматизуються як високоризикові, продемонстрували вимірювані покращення:

- **Африка на південь від Сахари:** Хоча регіональний середній показник залишається високим (6.14), **70%** юрисдикцій покращили свої оцінки. Це пояснюється покращенням технічної відповідності, викликаним тиском «сірого списку» FATF. Шість юрисдикцій цього регіону успішно вийшли з «сірого списку» FATF у 2025 році. Сім з десяти країн світу, що показали найбільше покращення, — це африканські країни (зокрема, Буркіна-Фасо та Кот-д'Івуар перемістилися з категорії високого до середнього ризику).

- **Південна Азія:** Загальна ефективність залишилася незмінною, оскільки вищі ризики фінансової прозорості були збалансовані покращенням структур AML/CFT.

Звіт підкреслює критичне

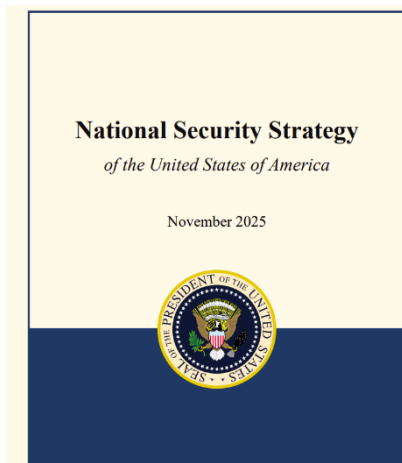
обмеження: **порівнянність результатів**. Оскільки оцінки 4-го раунду FATF не є універсальними, а 5-й раунд тільки розпочинається, покриття даними є нерівномірним. Публічне видання 2025 року включає лише 164 юрисдикції, які відповідали мінімальній вимозі щодо наявності даних (принаймні 65% доступності за всіма індикаторами). Ця прогалина означає, що деякі з найбільш ризикованих юрисдикцій можуть бути повністю виключені з рейтингу через відсутність верифікованих даних, що потенційно викривляє глобальне сприйняття ризику.

Геополітична стратегія — Доктрина «Америка понад усе» (US NSS 2025) ³

«Стратегія національної безпеки Сполучених Штатів Америки», опублікована Білим домом у грудні 2025 року. Цей документ являє собою радикальний відхід від багатосторонності ери Байдена-Гарріс (2021-2024) та антикорупційного фокусу.

NSS 2025 є експліцитно ізоляціоністським документом, орієнтованим на жорстке правозастосування, який переосмислює фінансові злочини не як проблему управління, а як пряму загрозу територіальному суверенітету. Документ структурований навколо захисту «основних національних інтересів», які визначені як захист території, економіки та способу

³ <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>



життя від «ворожого іноземного впливу», включаючи шпигунство, хижацькі торговельні практики, наркоторгівлю та торгівлю людьми.

Найбільш значущим доктринальним зрушенням є формальне проголошення **«Короларію Трампа» до Доктрини Монро** (Trump Corollary to the Monroe Doctrine).

Визначення: США стверджують своє право забезпечити, щоб Західна півкуля залишалася «вільною від ворожого іноземного вторгнення або володіння ключовими активами».

Застосування до фінансових злочинів: Стратегія прямо пов'язує цей короларій з **«наркотерористами, картелями та іншими транснаціональними злочинними організаціями» (TCOs)**. Метою США є змусити уряди півкулі співпрацювати з ними проти цих організацій.

Стратегічні наслідки: Це свідчить про те, що тиск США у сфері AML/CTF на країни Латинської Америки та Карибського басейну посилиться, але зі специфічним фокусом на **торгівлі наркотиками та контрабанді людей**, а не на загальній боротьбі з корупцією чи клептократією. Фокус зміщується на сутності, які фізично загрожують кордонам США або їхнім активам.

Порівняльний аналіз NSS 2025 з попередніми стратегіями виявляє кричуще упущення: текст **не містить** окремого розділу про «корупцію» або «незаконні фінанси» як стратегічні стовпи.

- **NSS Байдена 2022:** Оголошувала протидію корупції «основним інтересом національної безпеки».
- **NSS Трампа 2025:** Згадує «хижацькі торговельні практики» та «дискримінаційні» дії, але уникає мови глобального антикорупційного управління.

Це сигналізує про відхід від використання фінансової системи США для глобальної моралі (наприклад, санкції за Законом Магнітського) до її використання виключно як інструменту економічної війни проти геополітичних суперників (Китай) та фізичних загроз

Висновки:

- **Геополітизація комплаєнсу:** Банки та міжнародні фінансові групи повинні інтегрувати геополітичний аналіз у свої системи оцінки ризиків; транзакції з політично значущими особами (PEP) та державними компаніями з регіонів стратегічного суперництва (Латинська Америка, Індो-Тихоокеанський регіон) підлягають автоматичній посиленій перевірці (EDD) на предмет прихованого державного впливу.
- **ТКО як пріоритет національної безпеки:** Прирівнювання наркокартелів та злочинних синдикатів до загроз національного рівня означає залучення потужностей розвідувального співтовариства США (CIA, NSA) до виявлення та руйнування їхніх фінансових мереж, що призведе до збільшення кількості санкційних списків та блокувань активів.
- **Протидія "стратегічній корупції":** Регуляторний фокус зміщується з виявлення фактів особистого збагачення на ідентифікацію фінансових потоків, що використовуються для підкупу політичних еліт, фінансування дезінформації та створення груп впливу.
- **Захист інвестицій через AML:** Стратегія сигналізує про нову еру "економічного державного ремесла" (economic statecraft), де інструменти боротьби з відмиванням грошей будуть використовуватися як важіль тиску на уряди, що порушують права американських інвесторів або сприяють корупційним схемам конкурентів.

(картелі). Документ пріоритезує «захист економіки США» та «зупинку шкоди, яку іноземні актори завдають», маючи на увазі, що незаконні фінанси є пріоритетом лише тоді, коли вони безпосередньо шкодять економічним інтересам США або сприяють ворожому іноземному впливу.

Стратегія підносить TCOs до рівня загрози національній безпеці 1-го рівня, прирівнюючи їх до ворожих державних суб'єктів. Документ виражає бажання, щоб уряди в півкулі «співпрацювали з США проти наркотерористів». Це узгоджується з іншими виконавчими діями 2025 року, такими як вказівка щодо визнання картелів іноземними терористичними організаціями (FTOs).

Офшорний поворот — Стратегія цифрових фінансів Гернсі ⁴

Поки США замикаються в собі, а Велика Британія консолідує нагляд, Гернсі запустив сміливу контрстратегію. Консультаційний документ «Підтримка зростання за допомогою цифрових фінансів», запущений Комісією з фінансових послуг Гернсі (GFSC) у грудні 2025 року, окреслює регуляторну структуру, розроблену для захоплення ринку цифрових активів.



Цей документ, який охоплює комплексні пропозиції щодо змін законодавства, розроблений на основі широкої взаємодії із зацікавленими сторонами через Цифровий форум Комісії. Консультації триватимуть до **6 березня 2026 року**.

Найбільш сміливою пропозицією є скасування повної заборони на діяльність з роздрібними клієнтами для Постачальників послуг віртуальних активів (VASPs). Раніше Гернсі забороняв VASPs обслуговувати роздрібних клієнтів для захисту споживачів, обмежуючи юрисдикцію лише інституційними криптопотоками. Консультація пропонує оцінювати роздрібних VASPs на основі «індивідуального підходу» (case-by-case basis). Це сигналізує про зміну апетиту до ризику. Гернсі фактично робить ставку на те, що його нагляд є достатньо надійним для управління ризиками роздрібної криптовалюти, яких остерігаються інші юрисдикції.

Пропозиція включає скасування необхідності подвійного ліцензування. Фірма, що має інвестиційну ліцензію та займається кастодіальною діяльністю або токенизацією, більше не потребуватиме окремої ліцензії VASP. Це зменшує регуляторне тертя та витрати, роблячи Гернсі привабливим для гібридних традиційних/крипто фірм.

Гернсі пропонує нову, специфічну структуру для **емітентів стейблкоїнів**.

- **Класифікація:** Стейблкоїни розглядатимуться як окремий клас активів, а не просто як «віртуальні активи».
- **Регулювання:** Емітенти регулюватимуться як «бізнес фінансової фірми» (financial firm business).
- **Забезпечення:** Правила, ймовірно, вимагатимуть 100% забезпечення високоякісними ліквідними активами, що узгоджується зі світовими стандартами, але пропонує більш спрощений «офшорний» тягар дотримання вимог порівняно з режимом MiCA в ЄС.

⁴ <https://www.gfsc.gg/news/supporting-growth-digital-finance>

Консультація вносить ясність у трактування токенизованих цінних паперів.

- **Роз'яснення:** Токенизований цінний папер регулюється *Законом про захист інвесторів*, а не законом про VASP. Це дає впевненість інституційним емітентам: токенизація — це лише зміна формату, а не зміна режиму регулювання.

Висновки:

- **Відкриття роздрібного крипто-ринку:** Скасування заборони на роботу VASP з роздрібними клієнтами створює нові бізнес-можливості, але автоматично підвищує вимоги до захисту споживачів та вимагає впровадження процедур посиленої належної перевірки (EDD) для некваліфікованих інвесторів.
- **СРФ як інтегральна частина KYC:** Оновлення Додатку 2 зобов'язує фінансові установи модифікувати свої анкети KYC та матриці ризиків, додавши специфічні питання щодо товарів подвійного використання та торгових партнерів у юрисдикціях ризику PF, що може призвести до переоцінки значної частини клієнтського портфелю.
- **Технологічний мандат для токенизації:** Дозвіл на використання публічних блокчейнів для фондів (CIS) супроводжується жорсткою вимогою технологічного контролю; адміністратори фондів повинні мати технічну можливість заморожувати токени або примусово вилучати їх у випадку виявлення AML-ризиків, що вимагає використання складних стандартів токенів (наприклад, ERC-1400).
- **Регуляторна підтримка стейблкоїнів:** Створення окремого фреймворку для емітентів стейблкоїнів сигналізує про намір Гернсі конкурувати з MiCA в ЄС, пропонуючи, ймовірно, більш гнучкий, але не менш надійний режим резервування та аудиту активів.

Пропозиція прямо дозволяє токенизацію схем колективного інвестування (фондів) на **публічних блокчейнах**, за умови відповідного контролю. Це значна технічна поступка; багато регуляторів наполягають на приватних/дозволених блокчейнах для регульованих фондів. Гернсі позиціонує себе як доміциль вибору для фондів, орієнтованих на DeFi.

Документи також містять важливі юридичні уточнення щодо кастодіальних послуг для цифрових активів та використання блокчейну в страхових контрактах (ILS - Insurance Linked Securities). Регулятор пропонує керівництво, яке фактично легалізує використання розподіленого реєстру як "єдиного джерела істини" для управління життєвим циклом страхових полісів, за умови, що технологія забезпечує незмінність даних. Водночас, GFSC наголошує на "посиленні комплаєнсу через технології". Це пряма вказівка на те, що ручне управління ризиками у сфері

цифрових фінансів більше не вважається прийнятним. Фірми повинні демонструвати наявність автоматизованих інструментів аналізу блокчейну для відстеження транзакцій у реальному часі та виявлення зв'язків з підсанкційними адресами.

Шахрайство, пов'язане з віртуальним IBAN ⁵

Документ є аналітичним та практично орієнтованим інформаційним бюлетенем від ПФР Швейцарії, присвяченим зростаючим ризикам шахрайства, пов'язаним із використанням Virtual IBAN (vIBAN), та ролі фінансових посередників у їх виявленні й мінімізації. У документі детально пояснюється природа vIBAN як технічного «аліасу» традиційного IBAN, який відповідає стандартам ISO, але не є окремим рахунком, а лише інструментом маршрутизації та

⁵ <https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/fippp-newsletter-2025-12.pdf.download.pdf/fippp-newsletter-2025-12.pdf>



автоматизованої звірки платежів. Саме ця технічна особливість, за якої код країни vIBAN може не відповідати фактичному місцю відкриття базового рахунку,

створює суттєву вразливість з точки зору ПВК/ФТ, оскільки дозволяє маскувати транскордонний характер операцій та вводити в оману як платників, так і фінансові установи, що обробляють платежі. Документ наголошує, що ризик vIBAN не обмежується лише фінансовими установами, які їх емітують, а стосується всіх учасників платіжного ланцюга, оскільки ззовні клієнту або навіть іншому посереднику часто неможливо відрізнити платіж на звичайний IBAN від платежу на vIBAN.

Основний аналітичний фокус бюлетеня зосереджений на типологіях шахрайства, у яких vIBAN використовується як ключовий інструмент підвищення правдоподібності злочинних схем. На прикладі швейцарського контексту систематизовано низку поширених сценаріїв, зокрема «Ні Мум»-шахрайство з використанням deepfake-технологій, спадкове шахрайство, перенаправлення рахунків у межах ВЕС-схем, фіктивні інвестиційні платформи (у тому числі крипто-та фореक्स-проекти), романтичні шахрайства, афери з орендними депозитами та фейкові благодійні збори. В усіх випадках vIBAN відіграє роль інструменту імітації «локального» або «регульованого» рахунку, що знижує критичність сприйняття з боку жертви та відкладає момент виявлення шахрайства до часу, коли кошти вже перераховані до юрисдикцій з низьким рівнем міжнародної співпраці у сфері фінансових злочинів. Окремо підкреслюється, що статистичні дані щодо частки шахрайств із використанням vIBAN відсутні, однак з урахуванням швидкого поширення цього продукту у сфері cash management та платіжних сервісів ризик його зловживання має системний характер і потребує проактивного реагування.

Значна частина документа присвячена практичним рекомендаціям і найкращим практикам для фінансових посередників. Автори наполягають на принциповій важливості збереження цілісності коду IBAN країн, зокрема на тому, що vIBAN з певним кодом країни має бути прив'язаний до рахунку, відкритого в тій самій країні, що прямо корелює з вимогами Рекомендації 16 FATF. Також підкреслюється неприпустимість моделей, метою яких є навмисне маскування транскордонних зв'язків, наприклад складних структур із нечітко визначеним економічним сенсом. У сфері належної перевірки клієнтів акцент робиться на необхідності підтвердження легітимної ділової потреби у використанні vIBAN, застосуванні повноцінних KYC-

Висновки:

- Фінансовим посередникам доцільно негайно переглянути свої продукти та платіжні моделі з використанням vIBAN, щоб виключити сценарії, у яких країновий код IBAN не відповідає фактичній юрисдикції базового рахунку, оскільки це є системною вразливістю з точки зору ПВК/ФТ.
- Системи AML і fraud-моніторингу мають бути технічно доопрацьовані для окремої ідентифікації vIBAN, включно з автоматичним аналізом невідповідностей між IBAN- та BIC-кодами і підвищеним ризиковим скорингом таких операцій.
- Процедури KYC та on-going monitoring слід доповнити спеціальними тригерами щодо обсягів і характеру використання vIBAN, з обов'язковою можливістю швидкого блокування vIBAN у третіх сторінних моделях у разі підозри на шахрайство.
- Регуляторам і фінансовим установам варто заздалегідь орієнтуватися на впровадження стандартів Verification/Confirmation of Payee як ключового інструменту зниження ризиків введення в оману платників при використанні vIBAN.

процедур до третіх сторін, запровадженні механізмів попереднього погодження випуску vIBAN, періодичного перегляду моделей використання та можливості оперативного блокування vIBAN у разі виникнення ризикових подій. На рівні транзакційного контролю документ детально описує очікування щодо прозорості зазначення бенефіціара, інтеграції vIBAN у параметри AML-моніторингу, зіставлення коду країни IBAN і BIC, а також розвитку інструментів моніторингу, включно з попереджувальними сигналами в системах електронного банкінгу і застосуванням контролю для операцій без очевидного торговельного підґрунтя.

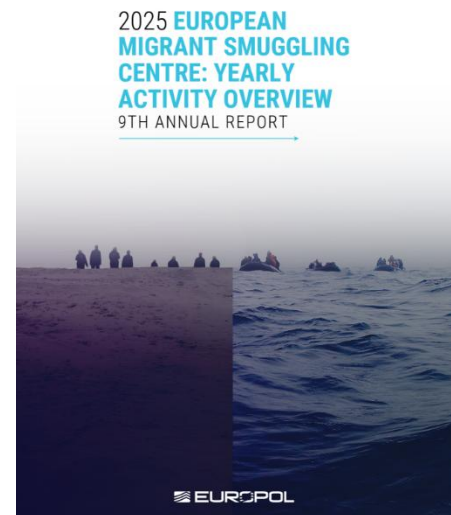
Фінансові сліди експлуатації людей в цифрову епоху ⁶

Документ є дев'ятим щорічним звітом Європейського центру з протидії незаконному переправленню мігрантів (European Migrant Smuggling Centre, EMSC) при Європолі та містить комплексний огляд операційної діяльності, аналітичних спостережень і ключових тенденцій у сфері незаконного переправлення мігрантів і торгівлі людьми за 2024 рік із фокусом на наслідки для безпеки ЄС та міжнародної співпраці.

У звіті послідовно підкреслюється, що незаконне переправлення мігрантів і торгівля людьми розглядаються не лише як міграційна проблема, а як високоорганізований транснаціональний кримінальний бізнес, який системно експлуатує вразливість осіб, зумовлену збройними конфліктами, переслідуваннями, економічною нестабільністю та кліматичними чинниками. Кримінальні мережі, за оцінкою Європолу, демонструють високий рівень адаптивності, масштабованості та глобалізації: різні сегменти злочинного ланцюга (вербування, транзит, логістика, експлуатація, фінансові розрахунки) керуються окремими акторами, тоді як стратегічне управління часто здійснюється з-за меж ЄС, що дозволяє мережам зберігати стійкість навіть після ліквідації окремих осередків.

Значна аналітична увага у звіті приділена цифровізації злочинної діяльності. Зазначається, що соціальні мережі, зашифровані месенджери та інші цифрові платформи стали ключовим середовищем для реклами послуг із незаконного переправлення, вербування виконавців низового рівня, встановлення першого контакту з мігрантами та жертвами торгівлі людьми, а також для координації операцій. Окремо наголошується на зростаючому використанні штучного інтелекту для створення багатомовного рекламного контенту та підроблених документів. У фінансовому вимірі документ фіксує дедалі ширше застосування криптоактивів, гібридних схем hawala з елементами криптовалют, послуг криптоброкерів, готівкових кур'єрів та легальних бізнесів-прикриттів (туристичні агентства, агентства нерухомості) для переміщення і легалізації доходів від злочинної діяльності, що формує децентралізовані та багат шарові фінансові потоки.

У звіті детально описано економіку незаконного переправлення мігрантів, зокрема середні розміри винагород залежно від маршрутів, способів транспортування та супутніх «послуг», що наочно представлено на картографічних матеріалах. Зазначається, що вартість переправлення може коливатися від кількох сотень євро до понад 20 000 євро на особу, а окремі елементи, такі як підроблені документи, фіктивні шлюби або авіаперельоти з використанням фальшивих документів, формують самостійні прибуткові сегменти кримінального ринку. Паралельно



⁶ <https://www.europol.europa.eu/cms/sites/default/files/documents/EMSC-9th-annual-report-2025.PDF>

висвітлюється тенденція до зростання насильства як «інструменту бізнесу»: погрози, викрадення, катування та сексуальне насильство використовуються як для вимагання додаткових коштів у мігрантів і їхніх родин, так і для контролю ринку та протидії конкурентам і правоохоронним органам.

Окремий розділ звіту присвячено торгівлі людьми, яка чітко відмежовується від незаконного переправлення мігрантів за критерієм обов'язкової експлуатації жертв. Документ фіксує еволюцію транснаціональних потоків жертв, диверсифікацію форм експлуатації (сексуальна, трудова, примусове жебрацтво, залучення до злочинної діяльності) та ускладнення організаційних структур злочинних груп, включно з полі-кримінальністю. Особливий акцент

Висновки:

- Боротьба з незаконним переправленням мігрантів і торгівлею людьми має системно фокусуватися на фінансових потоках і бізнес-моделях злочинних мереж, оскільки саме фінансова інфраструктура є найбільш уразливим елементом транснаціональних схем.
- Правоохоронним і наглядовим органам доцільно посилювати аналітику щодо використання криптоактивів, неформальних платіжних систем і легальних бізнесів-прикриттів у цих злочинах, інтегруючи фінансові розслідування як обов'язковий компонент операцій.
- Необхідно інституційно враховувати цифровий вимір злочинності (соцмережі, месенджери, ШІ-інструменти) як повноцінний операційний простір, що потребує спеціалізованих технічних і кадрових спроможностей.
- Моделі оперативних груп та спільних дій, координуваних Європолем, підтвердили свою ефективність і мають розглядатися як базовий стандарт для протидії складним транскордонним кримінальним мережам.

зроблено на ролі цифрового середовища як «нового поля бою», де злочинці не лише вербують жертв, але й здійснюють постійний дистанційний контроль за ними. Фінансові потоки у справах торгівлі людьми, за оцінкою Європолу, є ключовим вразливим місцем злочинних мереж і дедалі частіше використовуються правоохоронними органами як точка входу для їхнього руйнування.

У завершальній частині звіту узагальнено результати операційної діяльності EMSC у 2024 році: сотні підтриманих транскордонних операцій, десятки координаційних «action days», функціонування оперативних робочих груп та інтенсивний обмін інформацією через SIENA. Наводяться конкретні приклади успішних операцій проти великих мереж незаконного переправлення мігрантів і торгівлі людьми, які демонструють ефективність скоординованого підходу, поєднання аналітичних можливостей, оперативної підтримки та судової співпраці на рівні ЄС і з третіми країнами.

Сполучені Штати, Австралія та Велика Британія запровадили санкції проти російської інфраструктури кіберзлочинності⁷

У глобальному просторі протистояння кіберзагрозам, листопад 2025 року ознаменувався значним стратегічним проривом, який виходить за рамки звичайного правоохоронного реагування. Координувана санкційна акція, здійснена Міністерством фінансів Сполучених Штатів у партнерстві з австралійським та британським урядами, не просто додала нові імена до

⁷ <https://home.treasury.gov/news/press-releases/sb0319>



списків спеціально позначених громадян та заблокованих осіб. Вона продемонструвала цілеспрямований перехід до тактики, спрямованої на системне руйнування економічної та операційної екосистеми, що живить найбільш руйнівні форми російської кіберзлочинності.

Об'єктом цільового впливу стали не окремі анонімні хакери, а цілі бізнес-структури, технічна інфраструктура та їх керівники. Прецедент, створений протидією таким організаціям, як Media Land LLC та Aeza Group, вказує на формування нового міжнародного консенсусу щодо того, що нейтралізація загрози неможлива без атаки на її фінансові та логістичні вузли — так звані хостинг-провайдери.

Концепція «непробивного хостингу» (Bulletproof Hosting, BPH) є центральною для розуміння масштабів виклику. На відміну від звичайних хостинг-провайдерів, які дотримуються правил прийнятного використання та співпрацюють з правоохоронцями, BPH-компанії будують свою бізнес-модель на свідомому та активному протистоянні таким вимогам. Вони пропонують послуги, спеціально розроблені для ухилення від виявлення: сервери в юрисдикціях зі слабким регулюванням, швидке видалення лог-файлів, використання підставних компаній для реєстрації доменів, технічна підтримка для подолання блокувань. Це перетворює їх на незамінних постачальників критичної інфраструктури для злочинного світу. Без доступу до надійних і технічно компетентних BPH-провайдерів, кіберзлочинні групи на кшталт Lockbit, BlackSuit або Play не змогли б ефективно розгортати свої сервери управління та контролю, обробляти викупи або координувати масштабні мережеві атаки. Таким чином, Media Land, базована в Санкт-Петербурзі, виступала не пасивним орендодавцем серверів, а активним співучасником, суттєво підвищуючи технологічні можливості та операційну безпеку своїх клієнтів.

Детальний аналіз структури цієї організації, розкритий у прес-релізі OFAC, свідчить про високий ступінь професіоналізму та диверсифікації. Компанія функціонувала не як аморфна група, а як повноцінний бізнес із чіткою ієрархією та розподілом функцій. Генеральний директор Олександр Волосовик (відомий на кіберзлочинних форумах під псевдонімом «Valishanda») безпосередньо займався рекламою послуг і технічним супроводом клієнтів, що свідчить про його глибоке занурення в операційну діяльність, а не лише стратегічне керівництво. Його співробітник Кирило Затолокін відповідав за фінансові потоки та взаємодію з клієнтською базою — функція, ключова для будь-якого комерційного підприємства. Наявність юридичної та фінансової помічниці Юлії Панькової, яка «обробляла фінанси» та допомагала з юридичними питаннями, вказує на спроби формалізувати діяльність та захистити активи, що є ознакою зрілого, а не аматорського, підприємства.

Створення мережі дочірніх компаній, таких як ML Cloud, Media Land Technology та Data Center Kirishi, дозволяло диверсифікувати ризики, розподіляти інфраструктуру та потенційно ускладнювати правоохоронним органам відстеження всіх активів. ML Cloud, зокрема, описується як технічне крило, чия інфраструктура «часто використовувалася спільно з Media Land, що вказує на внутрішню спеціалізацію в рамках однієї кримінальної корпорації.

Окремої уваги заслуговує другий вектор санкційної атаки — продовження тиску на групу Aeza, яка була під санкціями з липня 2025 року. Цей епізод є класичним прикладом гри в «кота та мишу» між санкційними органами та кіберзлочинними організаціями, що прагнуть вижити. Реакція керівництва Aeza на перші санкції — ініціювання стратегії ребрендингу та створення нових юридичних осіб для відокремлення від заблокованої інфраструктури — демонструє їхню адаптивність та розуміння міжнародних фінансових механізмів. Однак відповідь OFAC та їхніх британських партнерів була швидкою. Викриття британської фірми Hypercore Ltd як

«оболонки», призначення нового директора Максима Макарова, який керував спробами ухилення, та ідентифікація помічника Іллі Закірова, що займався створенням нових компаній і платіжних методів, свідчить про глибоке проникнення розвідки в операційні плани групи.

Санкції проти сербської Smart Digital Ideas DOO та узбецької Datavice MCHJ розкривають географію спроб розповсюдити технічну інфраструктуру за межі росії, використовуючи країни з потенційно менш суворим наглядом. Цей крок посилює сигнал про те, що будь-які спроби обійти санкції через треті юрисдикції будуть переслідуватися, а міжнародна співпраця дозволяє OFAC ефективно відстежувати такі маневри.

Правові наслідки цих дій є далекоглядними. Введення осіб до Списку спеціально позначених громадян та заблокованих осіб (SDN List) призводить не лише до заморожування їхніх активів у США, але й накладає де-факто глобальну фінансову ізоляцію. Будь-які операції з такими особами або на їхню користь стають забороненими для американських осіб та компаній, що охоплює величезний спектр діяльності від банківських переказів до надання програмного забезпечення чи хостингу. Оскільки долар США залишається ключовою світовою валютою, а американські фінансові інститути — центральними вузлами глобальної системи, ці санкції створюють непереборний бар'єр для участі в легальній міжнародній економіці. Фінансові установи по всьому світу, побоюючись вторинних санкцій, будуть уникати будь-яких операцій із зазначеними особами, фактично відрізаючи їх від грошових потоків. Крім того, заблокованими автоматично стають будь-які юридичні особи, що на 50% і більше належать відповідним особам, що ускладнює використання складних корпоративних структур для приховування власності.

Широкий геополітичний контекст цієї акції також заслуговує на аналіз. Тристоронній формат (США-Велика Британія-Австралія) не є випадковим і вказує на зростання ролі інтегрованих альянсів у кіберпросторі, подібно до співпраці в рамках AUKUS. Це демонструє здатність ключових західних союзників не лише обмінюватися розвідувальними даними, але й синхронізувати свої найпотужніші невійськові інструменти впливу — фінансові санкції — для досягнення спільної мети. Участь Австралії, яка все частіше стає мішенню для кібератак, підкреслює глобальний характер загрози, що виходить за межі трансатлантичного простору. Координація з Федеральним бюро розслідувань (ФБР) на етапі підготовки санкцій забезпечила їхню доказову основу, пов'язуючи фінансові заходи з кримінальними розслідуваннями. Паралельне оприлюднення Агентством з кібербезпеки та безпеки інфраструктури США (CISA) рекомендацій щодо пом'якшення ризиків від VPN-провайдерів показує комплексний підхід, спрямований як на покарання злочинців, так і на захист потенційних жертв.

Таким чином, цей санкційний крок слід розглядати не як ізольований епізод, а як важливий прецедент у еволюції міжнародної боротьби з кіберзлочинністю. Він означає перехід від переслідування

Висновки:

- **Міжнародна спільнота змінює тактику боротьби з кіберзлочинністю.** Замість переслідування окремих хакерів, удар завдається по технічній та економічній основі їх діяльності.
- **Санкції чітко ідентифікують росію (Санкт-Петербург) як базу для цілих професійних бізнес-структур** (Media Land, Aeza Group), що підтримують глобальну кіберзлочинність.
- **Документ показує, що санкції — це динамічний процес.** Це свідчить про високий рівень координації розвідки та рішучість перекривати будь-які шляхи обходу.
- **Введення до списків OFAC призводить не просто до заморожування активів у США.** Це фактично відрізає цілі компанії та осіб від світової фінансової системи, оскільки будь-які операції з ними стають ризикованими для фінансових установ у всьому світі через загрозу вторинних санкцій.

окремих виконавців до системного натиску на цілі економічні ніші, що роблять їхню діяльність можливою.

Звіти окремих інституцій та експертів

Ескалація контрабанди палива в Лівії: діяльність яка руйнує націю⁸



Неурядова організація The Sentry оприлюднила доповідь, яка вивела на поверхню одну з найнебезпечніших і водночас найменш контрольованих криз сучасної Лівії — системну контрабанду палива. За масштабами збитків, залученими суб'єктами та глибиною проникнення у державні інституції ця схема вже давно перестала бути просто економічним злочином. Вона стала фундаментом повноцінної нелегальної індустрії, що збагачує політичні кланові еліти, фінансує конфлікти, підриває регіональну стабільність і фактично перетворює Лівію на джерело нестабільності в Північній Африці та за її межами.

Доповідь The Sentry демонструє, що корупційні практики у Національній нафтовій корпорації (NOC) та суміжних структурах давно вийшли за межі внутрішньої проблематики. Впливові мережі, що формуються навколо сімей Хафтара у Бенгазі та Дабайби у Тріполі, контролюють

ключові ланки паливного ланцюга, а їхні інтереси підкріплені міжнародними партнерами — насамперед росією та Суданськими силами швидкої підтримки (RSF). Лише за період 2022–2024 років, за оцінками авторів, Лівія втратила приблизно 20 мільярдів доларів. Це колосальна сума, еквівалентна кільком річним бюджетам держави. Вона зникає в тіньових схемах, що паразитують на субсидованому пальному та непрозорих механізмах його імпорту.

У центрі проблеми — субсидії на дизель і бензин, що встановлюють штучно низьку ціну — усього 0,03 долара за літр. Система, задумана для підтримки населення і промисловості, перетворилася на ідеальне середовище для масштабних зловживань. Понад половина державного палива просто не доходить до легального ринку. Значна його частка перехоплюється ще на рівні портів, розподільчих станцій і державних установ, які подають завищені заявки. Ці «надлишки» розчиняються у чорному ринку, де паливо продається у десятки разів дорожче.

Ситуацію ускладнює практика «свопів» — обміну сирової нафти на готове паливо без використання твердої валюти. Цей механізм NOC почав активно застосовувати у 2021 році, коли Центральний банк Лівії припинив фінансування імпорту доларами. Формально свопи мали бути тимчасовим рішенням, але насправді вони перетворилися на інструмент непрозорого імпорту та оптимізації корупційних потоків. Через них Лівія наростила обсяги імпортованого палива з 20,4 млн літрів на день у 2021 році до понад 41 млн літрів у 2024-му, попри відсутність логічної економічної потреби в таких обсягах. Країна фактично імпортує вдвічі більше, ніж спроможна споживати легальними каналами.

Одним із ключових бенефіціарів цієї системи є Садам Хафтар — син Халіфа Хафтара, фактичного правителя східної Лівії. Його структура, Libyan Arab Armed Forces (LAAF), консолідувала під своїм контролем практично весь нелегальний обіг палива у східних регіонах. Використовуючи не лише адміністративні та силові ресурси, а й тісну інтеграцію з NOC і державними установами,

⁸ <https://thesentry.org/wp-content/uploads/2025/11/InsideJob-TheSentry-Nov2025.pdf>

він вибудував фактично паралельну економіку. LAAF контролює дороги, порти, контрольні пропускні пункти та логістичні вузли, через які паливо масово рухається до Середземномор'я або відправляється сухопутними маршрутами в Нігер, Чад і Судан. Штучний дефіцит, створений обмеженнями доступу до офіційного палива, дозволяє LAAF продавати паливо за завищеними цінами — у сорок разів дорожче, ніж офіційна ціна. Люди змушені переплачувати або відмовлятися від транспорту, що лише підсилює соціальну напругу.

Південно-західні райони країни перетворилися на ключову точку перетину інтересів місцевих угруповань, RSF і зовнішніх суб'єктів. Контроль над містами Sabha, Qatrun та Ghat дозволяє силам Хафтара формувати стабільний потік субсидованого палива до Судану. Його використовують у війні в Дарфурі, що надає схемам не лише кримінальний, а й безпосередньо гуманітарний вимір. Лівія фактично, хоча й непрямо, фінансує один із найжорстокіших сучасних конфліктів.

На противагу цьому північно-західна Лівія демонструє інший тип проблеми: симуляцію боротьби з контрабандою. Уряд Абделхаміда Дабайби декларує реформи, але водночас покриває діяльність структур, що активно беруть участь у нелегальних схемах. Мережа Мохамеда Кошлата у Зауїї продовжує організовувати морські перевалки, тоді як Joint Force у Місраті забезпечує логістику для внутрішніх переміщень і взаємодіє з групами Хафтара, попри офіційну політичну ворожнечу між ними. Це руйнує будь-які спроби створити єдиний державний контроль над паливним сектором. Надлишковий імпорт, переплати на мільярди доларів і відсутність реального контролю з боку уряду вказують на те, що проблема давно набула характеру політичної співучасті.

Міжнародний вимір цієї кризи не менш складний. Через лівійські схеми паливо потрапляє не лише до Африки, а й до Європи. Італія, Мальта, Туреччина, Албанія фіксують регулярні потоки контрабандного дизеля, що потрапляє до їхніх портів за допомогою нелегальних морських перевалок між кораблями. Водночас російська Africa Corps та RSF отримують стабільне підживлення для своїх операцій, використовуючи лівійське паливо як дешеве стратегічне забезпечення. Це створює небезпечний прецедент, коли внутрішня корупція однієї держави формує ризики для безпеки цілого регіону.

У своєму фінальному висновку The Sentry наголошує: контрабанда палива у Лівії — це не випадковий результат слабкості держави. Це продумана стратегія клептократії, в якій політичні еліти використовують державні ресурси як власний економічний актив. Без радикальних реформ ситуація лише поглиблюватиметься. Автори закликають до повного перегляду політики субсидіювання, переходу до грошових компенсацій, впровадження хімічного маркування пального, міжнародних санкцій

Висновки:

- **Контрабанда палива в Лівії коштує країні близько 6,7 мільярда доларів на рік**, що підриває економіку, викликає дефіцит твердої валюти, інфляцію та брак палива для населення.
- **Ключові фігури, такі як Саддам Хафтар, промислово організували контрабанду**, контролюючи території, порти та маршрути, з іноземною підтримкою від росії та ОАЕ, що не тільки збагачує корумповані мережі, але й фінансує збройні конфлікти.
- **Контрабанда палива перетворилася на інструмент клептократії**, де нелегітимні правителі використовують її для зміцнення влади, купівлі лояльності озброєних груп та блокування шляху до вільних виборів, водночас підриваючи інституції та легітимну економіку.
- **Без міжнародного втручання, включаючи санкції проти ключових осіб та реформи**, такі як скасування субсидій з заміною на готівкові виплати, прозорість угод та хімічне маркування палива, криза продовжить дестабілізувати Лівію та регіон.

проти ключових фігур, прозорого бюджетування та глобального аудиту. На їхню думку, лише поєднання внутрішнього тиску, зовнішнього контролю та політичної волі може зупинити розростання нелегальної паралельної економіки, що вже сьогодні визначає життя мільйонів лівійців.

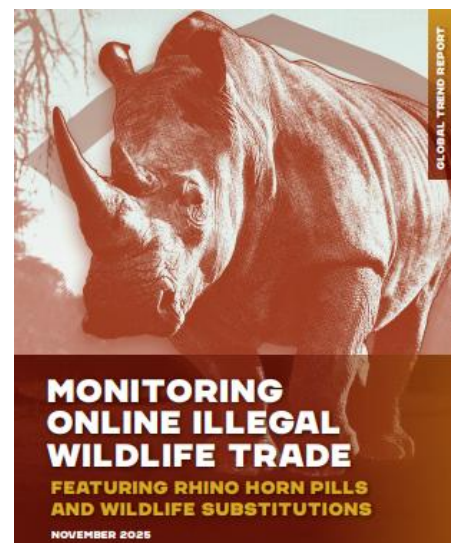
Стан Лівії у цьому контексті — це не просто приклад внутрішньої дисфункції. Це нагадування про те, як корупція, залишена без контролю, здатна перетворитися на повноцінну загрозу для регіональної та міжнародної безпеки. Клани Хафтара і Дабайби продовжуватимуть зміцнювати свій вплив доти, доки держава не відновить контроль над власними ресурсами. Без цього Лівія ризикує залишитися у пастці нескінченного економічного виснаження, а її народ — заручником чужих інтересів.

Моніторинг онлайн-торгівлі нелегальною дикою природою: стратегія виживання чорного ринку в умовах глобальних заборон і санкцій⁹

Під егідою Глобальної ініціативи проти транснаціональної організованої злочинності вийшов п'ятий випуск серії Global Trend Reports, підготовлений проектом ECO-SOLVE. Це дослідження стало, без перебільшення, одним з найґрунтовніших аналізів світового онлайн-ринку нелегальної торгівлі дикою природою, яке не лише фіксує масштаби проблеми, а й демонструє, як цифрова екосистема створює абсолютно нову архітектуру злочинності.

Звіт охоплює період із квітня 2024 по серпень 2025 року і спирається на дані десяти регіональних хабів моніторингу, які проаналізували 13 254 оголошення про продаж захищених видів тварин. Цей масив інформації дозволив авторам показати, що онлайн-торгівля дикою природою давно вийшла за межі вузькоспеціалізованих ринків і перетворилася на глобальну кримінальну інфраструктуру, тісно пов'язану з конфліктами, культурними практиками, економічними шоками та санкційним тиском на окремі держави.

Авторам вдалося продемонструвати, що зростання цих злочинних практик неможливо оцінити без створення системного підходу до збору та аналізу даних. Саме тому Глобальна система моніторингу (GMS), запущена ECO-SOLVE, стала критичним інструментом у розумінні сучасних тенденцій. На відміну від фрагментованих попередніх ініціатив, GMS функціонує як децентралізована мережа національних вузлів у державах, де онлайн-ринок нелегальної дикої природи є найбільшим або найвпливовішим. Поступове розширення мережі з трьох до десяти хабів дозволило охопити Бразилію, Південну Африку, Таїланд, Індонезію, Нігерію, Колумбію, Мексику, Камерун, Південну Азію та регіон MENA. Моніторинг ведеться на 54 цифрових платформах, поєднуючи інструменти штучного інтелекту з ручною верифікацією. Методологія побудована за принципом «кошика товарів» — кожна точка відстежує стандартизований набір видів, включених до CITES, списків IUCN та відповідного національного законодавства. Такий підхід дозволяє не лише рахувати оголошення, а й аналізувати, як на ринок впливають зміни регуляції, міграція попиту, сезонні та культурні фактори, а також реакції злочинних мереж на зростання контролю.



⁹ <https://globalinitiative.net/wp-content/uploads/2025/11/Monitoring-illegal-wildlife-trade-Featuring-rhino-horn-pills-and-wildlife-substitutions-GI-TOC-November-2025.pdf>

Звіт показує різке зростання кількості оголошень — з 3192 до 13 254. Домінуючим залишається Facebook, на який припадає 83,8% виявлень, хоча його частка зменшилася з 95% після посилення модерації. Натомість значно зросла активність на e-commerce платформах (12,8%) та в сегменті B2B-постачальників і месенджерів. Це зміщення сигналізує про адаптивність злочинців: вони водночас використовують глобальні платформи та переходять у менш регульовані середовища — від Line і Kaidee до Tokopedia, Shopee, WhatsApp, Junkmail, Gumtree, TikTok, Instagram, Mercado Libre, Amazon, OpenSooq і TradeFord. Торівля полягає переважно у продажу частин тіл та продуктів із захищених видів (67%), тоді як частка живих тварин складає близько третини. Найчастіше зустрічаються оголошення про ссавців (7668 випадків) — слонів, тигрів, левів, ягуарів; на другому місці птахи (2973, особливо африканський сірий папуга), далі рептилії (1732), водні види (857) і амфібії.

Ключовим аспектом є те, що 84% оголошень стосуються видів з Додатків I та II CITES, тобто таких, торівля якими жорстко регулюється або фактично заборонена. Проте абсолютна більшість продавців не надає жодних документів чи дозволів, і це свідчить про системну відсутність дотримання правил у глобальному масштабі.

Особливості торівлі мають яскраво виражений регіональний характер: у Таїланді переважають слонова кістка, частини тигрів і ведмедів, які використовуються у традиційній медицині, як амулети або статусні предмети; в Індонезії популярні морські коники й молоді видри для домашнього утримання; у Бразилії та Колумбії продають частини кайманів і піраруку як елемент ритуальних практик та місцевої комерції; у Південній Африці й Нігерії — леопардів і панголінів для культурних церемоній та кустарної індустрії одягу; у Мексиці — ягуарів, мавп і папуг для екзотичних домашніх тварин і таксидермії; у Південній Азії торівля виходить на дитячі YouTube-канали, нормалізуючи утримання рідкісних тварин; у регіоні MENA процвітає торівля фальконами, слоною кісткою й папугами як символами статусу; у Камеруні додатково фіксуються випадки продажу людських черепів поряд із рештками левів і панголінів. Поєднання культурних, економічних і кримінальних мотивів формує складну соціально-економічну екосистему, яку правозастосовні органи не встигають контролювати. Водночас злочинці активно обходять алгоритми модерації: використовують емодзі, кодові слова, навмисні помилки, публікації у форматі 24-годинних сторіз та приховані канали комунікації.

Особливе місце у звіті займає аналіз ролі Північної Кореї, яка за останні роки значно активізувала виробництво пігулок Angong Niuhuang Wan (ANW), відкрито маркуючи їх як такі, що містять ріг носорога. На відміну від легальних китайських виробників, які з 1990 року замінили ріг носорога на ріг буйвола, КНДР свідомо продовжує використовувати заборонений інгредієнт, перетворюючи його на високомаржинальний товар. Вартість рогу, що на «чорному ринку» становить 10,7–22,3 тис. доларів за кілограм, у пігулках зростає до 420–830 доларів за грам, а роздрібна ціна коробки сягає 300–600 доларів. Виробництво контролюється Бюро 39 — ключовою структурою, відповідальною за генерацію валюти для режиму, — а географія збуту охоплює Китай, Японію, Гонконг, Малайзію, Таїланд, В'єтнам, Сінгапур і Камбоджу. Ланцюги постачання детально описані: пігулки надходять із фабрик у Пхеньяні до прикордонних міст, звідти — до китайських посередників, після чого морем розходяться по регіону. Важливу роль відіграють корумповані дипломати КНДР, причетні до щонайменше 18 відомих випадків контрабанди, включно зі скандалом у ПАР у 2022 році, коли була виявлена партія рогу носорога вартістю 65 млн доларів.

Для Пхеньяна нелегальна торівля ANW має стратегічне значення: вона дозволяє генерувати валюту для фінансування ядерної та ракетної програм. Кожне випробування оцінюється у 3–10 мільйонів доларів, і дохід від ANW є прямим способом обходити міжнародні санкції. Попит на ці пігулки різко зростає під час епідемій, що підтверджують тренди пошуку — від H1N1 у 2005 році до сезонних спалахів інфекцій у 2010-х. Цей сегмент ринку перетинає одразу кілька

критичних сфер: кримінальну економіку, масову міфологізацію традиційної медицини, системи фінансування режимів, що перебувають під санкціями, та глобальну безпеку.

Висновки:

- Глобальна система моніторингу (GMS) виявила значне зростання онлайн-торгівлі нелегальною дикою природою, підкреслюючи необхідність адаптації стратегій модерації платформ до регіональних варіацій.
- Виробництво Північною Кореєю пігулок ANW з справжнім рогом носорога слугує механізмом обходу міжнародних санкцій, генеруючи тверду валюту для фінансування заборонених програм, що пов'язує охорону природи з питаннями глобальної безпеки та вимагає форензичного тестування продуктів.
- Торговці адаптуються до заборон шляхом заміни видів, що переносить тиск на нові екосистеми та ускладнює контроль.
- Лазівки в регуляціях, вимагають реформ CITES, посилення моніторингу, інвестицій у кампанії зі зменшення попиту, щоб запобігти подальшій адаптації нелегальної торгівлі.

У підсумку звіт показує, що онлайн-торгівля дикою природою стала багаторівневою кримінальною системою, де поєднуються культурні норми, економічні стимули, політичні інтереси й високотехнологічні методи уникнення контролю. GMS демонструє, що без глобальної, стандартизованої та постійної системи моніторингу уряди та правоохоронні органи фактично не мають інструментів для стримування цієї індустрії. Лише поєднання аналітики, міжнародної координації, санкційних механізмів і реформ цифрової модерації може створити умови, за яких ринки незаконної дикої природи перестануть розширюватися. Наразі ж ми спостерігаємо протилежну тенденцію — проникнення цієї торгівлі в буденні онлайн-практики мільйонів людей, від соціальних

мереж до торговельних платформ. І це робить проблему не лише екологічною, а й безпековою, економічною та геополітичною.

Незаконна торгівля панголінами та її глобальні наслідки для збереження видів у контексті міжнародного права та організованих мереж контрабанди¹⁰



Екологічна розслідувальна агенція (EIA) опублікувала доповідь, яка ґрунтується на аналізі 169 судових рішень китайських судів у період з 2014 по червень 2024 року, доступних через China Judgments Online. Ця робота не просто констатує факти нелегальної торгівлі панголінами — одними з найбільш загрожених ссавців у світі, всі види яких перебувають під високим ризиком вимирання через браконьєрство та комерційне використання м'яса, лусок і частин тіла — але й глибоко досліджує динаміку цієї торгівлі, її організований характер, маршрути контрабанди, роль традиційної китайської медицини (TCM) як ключового драйвера попиту та ефективність правоохоронних органів Китаю.

Доповідь показує, що в період 2014–2024 років було зафіксовано щонайменше 42 744 кг лусок панголінів і 5 465 цілих особин у 139 унікальних випадках. При цьому легальний внутрішній ринок Китаю для використання лусок у TCM безпосередньо стимулює глобальне браконьєрство,

¹⁰ <https://eia-international.org/wp-content/uploads/2025-EIA-A-View-from-the-Courts.pdf>

відмивання нелегальних поставок та порушення міжнародних зобов'язань за CITES, перетворюючи локальну проблему на глобальну загрозу біорізноманіттю. Відтак попит у Китаї призводить до виснаження популяцій на двох континентах, що вимагає невідкладного міжнародного втручання для закриття ринків, які стимулюють цей деструктивний цикл.

Історичний контекст, викладений у доповіді, свідчить про те, що панголіни — ссавці родини Manidae, що населяють ліси, савани, луки і чагарники Африки та Азії — стали об'єктом масштабної експлуатації через попит на традиційні ліки та їжу. Луски панголінів традиційно вважаються ефективними для лікування різноманітних захворювань, хоча наукових підтверджень цього немає. Три азіатські види (сундський, китайський та філіппінський) класифіковані як критичні, а інші — як вразливі, причому головною загрозою залишається браконьєрство для комерційної торгівлі. З 2016 по 2024 рік конфіскації панголінів у 49 країнах еквівалентні щонайменше 553 042 особинам, з лусками, що становлять майже 99% обсягів торгівлі. Китай виступає основним пунктом призначення як легальних, так і нелегальних поставок, а оцінки конфіскацій у країні за період 2015–2024 років сягають 160 000 кг лусок або 92 844 еквівалентів панголінів, тоді як реальні обсяги, ймовірно, значно вищі.

Китайська роль у торгівлі панголінами є домінуючою: попит на луски для ТСМ, що сягає щонайменше 480 року н.е., виснажив азіатські популяції та переорієнтував браконьєрство на африканські види. Легальний експорт африканських лусок з 2013 по 2017 рік становив приблизно 13 тонн, переважно до Китаю, тоді як нелегальні маршрути охоплюють Західну, Центральну та Східну Африку, Південно-Східну Азію та ключові країни-джерела та транзиту. Після внесення всіх видів панголінів до Додатку I CITES у 2017 році легальний внутрішній ринок Китаю сприяє відмиванню нелегальних поставок, що ставить під сумнів дотримання Конвенції та перетворює проблему на глобальне питання комплаєнсу.

Контроль за торгівлею панголінами еволюціонував: від початкового включення до CITES у 1975 році до повного захисту всіх видів у 2017 році, забороняючи комерційну торгівлю. У Китаї панголіни захищені з 1989 року, а з 2020 року віднесені до категорії I, з заборобою на торгівлю для їжі з 2023 року, проте з винятками для розведення, виставок і «інших спеціальних обставин». Це створює лазівки для комерційного використання лусок під схемою China National Wildlife Mark, з щонайменше 53 ліцензованими продуктами ТСМ, що містять луски, доступними онлайн у 2023 році. Попри заходи 2024 року щодо скорочення використання, ринок залишається відкритим, підтримуючи попит, підриваючи зусилля CITES.

Методологія EIA передбачала аналіз 188 судових рішень з ключовим словом «панголін», з яких після видалення дублікатів і нерелевантних залишилися 169, що стосуються 139 унікальних інцидентів. Судові дані дозволяють відновити реальні обсяги торгівлі, включаючи випадки, де конфіскації були мінімальними або відсутні, а доказами виступають цифрові записи, банківські транзакції та експертизи видів.

Обсяги торгівлі, виявлені через судові рішення, демонструють тривожні тенденції: 42 744 кг лусок і 5 465 цілих панголінів, з переважанням африканських лусок у конфіскаціях (35 521 кг) і азіатських особин серед цілих панголінів (1 726 особин). Це свідчить про зсув тиску браконьєрства на Африку, тоді як виявлені випадки — лише вершина айсберга, що підкреслює необхідність посилення моніторингу та оцінки впливу на популяції.

Маршрути контрабанди охоплюють 17 країн, включаючи Нігерію, В'єтнам, Ефіопію, Малайзію, М'янму та інші, де Нігерія лідирує за обсягами, а В'єтнам — за кількістю інцидентів. Методи контрабанди варіюються: великі партії транспортуються контейнерами, менші — авіа-, морським і наземним транспортом, із приховуванням у товарах, використанням «мулів» та корупцією на митниці. Організовані мережі координують постачання, зберігання та транспорт, тоді як опортуністичні випадки — малі партії в багажі, що потребує комплексного розслідування.

Зв'язок контрабанди з медичним використанням є центральним: 105 випадків торгівлі лусками для ТСМ, 35 — цілими панголінами для їжі і ліків, із численними прикладами участі ліцензованих трейдерів і фармакологічних компаній. Це демонструє, що легальний ринок ТСМ підтримує попит і відмивання, роблячи його ключовим фактором, який стимулює незаконну торгівлю.

Китайські правоохоронці та прокурори демонструють передові методи розслідування: використання свідчень, цифрових записів, банківських транзакцій, дослідження видів, що дозволяє встановлювати великі обсяги торгівлі навіть без повної конфіскації. Проте системні проблеми, пов'язані з існуванням ринку ТСМ, підбивають ефективність, а без зменшення попиту зусилля залишаються неповними.

Доповідь EIA підкреслює, що Китай значно просунувся у виявленні та переслідуванні злочинів, але без закриття ринку лусок для комерції, включно з ТСМ, і без зменшення попиту глобальна торгівля продовжуватиме загрожувати панголінам. Рекомендації включають: закриття комерційного ринку, кампанії зі зменшення попиту серед користувачів і громадськості, заохочення альтернатив, посилення міжнародної співпраці з джерелами і транзитерами, а також впровадження строгого скринінгу на приватних маршрутах.

Доповідь також наголошує на потребі подальших досліджень і інвестицій у технології та глобальні бази даних, оскільки зменшення конфіскацій може відображати лише кращі методи приховування, а не реальний спад торгівлі. Водночас аналіз EIA демонструє, що внутрішня політика Китаю безпосередньо впливає на глобальне біорізноманіття, і лише баланс між культурними традиціями та екологічною стійкістю може забезпечити виживання цих унікальних ссавців.

Висновки:

- **Легальний ринок Китаю для медичних потреб є основним паливом для глобальної незаконної торгівлі та створює потужний стимул для браконьєрства в Африці та Азії та канали для легалізації контрабандної сировини.**
- **Торгівля має одночасно високоорганізований транснаціональний і дрібний опортуністичний характер.** Ключові транскордонні маршрути пролягають через В'єтнам та М'янму.
- **Китайська правоохоронна та судова система демонструє значні можливості у викритті та покаранні, використовуючи сучасні методи розслідування.** Однак ця ефективність не усуває кореневу причину — попит, підтримуваний легальним ринком.
- **Всім восьми видам панголінів загрожує зникнення, а документовані судами обсяги контрабандної торгівлі — лише "верхівка айсбергу".**

Острів Маргаріта: трансформація наркотрафіку від кримінального феодалізму до керованої монополії¹¹

Венесуельський острів Маргаріта протягом десятиліть слугував місцем відпочинку для туристів, що шукають ідеальні карибські пляжі. А паралельно формувалася як один з найважливіших стратегічних вузлів у глобальній наркотичній логістиці. Однак починаючи приблизно з 2023 року, ця територія переживає фундаментальну трансформацію, яка може слугувати прикладом того, як держави з ослабленими інституціями адаптуються до зовнішніх тисків та внутрішніх криз, не ліквідуючи злочинну економічну діяльність, а інтегруючи її в нову систему влади.

Золотий вік незалежних кримінальних авторитетів, таких як Теофіло Родрігес Касорла на прізвище «Кролик», який відверто контролював місцеву в'язницю Сан-Антоніо як свою штаб-

¹¹ <https://insightcrime.org/news/shifting-tides-drug-trafficking-on-venezuela-margarita-island/>

квартиру, закінчився. На його місце прийшла більш дискретна, але не менш могутня архітектура, де ключову роль грають уже не окремі «королі наркотиків», а державні установи та менші, підконтрольні їм мережі. Цей перехід від кримінального феодалізму до керованої державної монополії відбувається на тлі двох потужних зовнішніх факторів: посиленої військової присутності США в



Карибському морі та цільового правоохоронного співробітництва європейських держав, головним чином Франції. Історія зникнення та подальшого викриття риболовецького судна «Седна», перехопленого Береговою охороною США з 1 тоною кокаїну та 1,5 тонами марихуани на борту, стає символічною ілюстрацією нових правил гри, де кожен вихід у море перетворюється на складну партію з непередбачуваними наслідками, а кордон між легальним рибальством і незаконним трафіком розмивається до невпізнанності під тиском обставин.

Протягом багатьох років Маргаріта була класичним кримінальним анклавом, де локальні боси, часто маючи зв'язки на найвищих рівнях уряду в Каракасі, створювали автономні зони впливу. Згідно з розслідуваннями, «Кролик» підтримував стосунки з колишнім міністром ув'язнень Іріс Варелою, що дозволило йому буквально жити та керувати бізнесом з-за тюремних стін. Після його смерті контроль перейшов до інших фігур, таких як Джонні Александер Сільва Родрігес на прізвище «Джастін», але модель залишалася незмінною: острів служив надійним пунктом збору, зберігання та відправлення наркотиків, що прямували до Карибського басейну, Центральної Америки та, що особливо важливо, до Європи. Затримання на острові у вересні 2023 року громадянина Польщі, який перебував у міжнародному розшуку за Interpol, стало прямим підтвердженням триваючих трансатлантичних зв'язків.

Проте сьогодні, за даними InSight Crime, явні ознаки великих, публічно відомих організованих злочинних груп на острові відсутні. Штат Нуева-Еспарта, до якого належить Маргаріта, демонструє один з найнижчих у Венесуелі рівнів насильницької злочинності. Але ця статистична «стабільність» є оманливою. Вона не свідчить про зникнення наркотрафіку, а скоріше про його професіоналізацію та інституціоналізацію. Держава, представлена різними силовими структурами, поступово витіснила або підпорядкувала собі незалежних кримінальних підприємців, перетворивши хаотичний ринок на регульовану, хоча й нелегальну, монополію.

Механізми цього захоплення контролю є витонченими та всеохоплюючими. З 2023 року венесуельський уряд розгорнув на острові мережу постів Дирекції водних просторів Національної поліції Болівару, паралельно посиливши присутність Берегової охорони та Військово-морських сил. Формальною метою цих дій оголошено боротьбу з незаконним трафіком і забезпечення безпеки. На практиці, як розповідають місцеві рибалки, ці заходи створили багаторівневу систему дозволів та обмежень, що дає чиновникам та силовикам широкі можливості для вилучення ренти. Тепер, щоб вийти в море, капітан повинен не тільки отримати стандартний дозвіл Національного інституту водних просторів (INEA), але й пройти обов'язкову інспекцію судна та отримати схвалення від поліції водних просторів або представників флоту. Цей процес перетворює кожен вихід у море на потенційну угоду, де «правильна» плата може забезпечити не тільки дозвіл, але й запобігання надмірним перевіркам або навіть гарантії захисту.

Надзвичайно показовим є запровадження жорстких обмежень на видачу пального — не більше 120 літрів на судно на тиждень. Номінально це має перешкоджати далеким незаконним рейсам, але реальним наслідком є параліч легального рибного промислу. Як пояснює один із рибалок із Ель-Тірано, такого запасу недостатньо для ефективного виходу на угіддя, що змушує їх повертатися з порожніми сітями, позбавляючи основного джерела існування. Таким чином, держава не ліквідує наркотрафік; вона створює штучний дефіцит легальних можливостей, тим самим збільшуючи залежність населення від тієї ж незаконної економіки, яку нібито контролює. У такій системі лише ті, хто має доступ до «спеціальних дозволів» та додаткових ресурсів (тобто хто сплачує), можуть вести будь-яку значущу морську діяльність, будь то рибальство чи транспортування наркотиків.

Ситуацію істотно ускладнює активна зовнішня присутність, яка представлена двома різними підходами. З одного боку, Європа, головним чином через Францію, діє в рамках правоохоронної парадигми. Французькі та венесуельські органи безпеки демонстрували співпрацю, що призводила до перехоплення великих партій наркотиків біля берегів Мартиніки та Гваделупи. Наприклад, у травні 2024 року судно, що вийшло з Маргаріти, було виявлено біля Мартиніки з 2,4 тоннами кокаїну на борту. Таке співробітництво вигідно режиму Мадуро, оскільки дозволяє йому демонструвати зовнішньому світову готовність боротися з трафіком, водночас ліквідуючи конкурентні мережі, що працюють поза його контролем та не сплачують «податків» на місцевому рівні. Це вибіркове співробітництво є інструментом консолідації внутрішнього контролю під прикриттям міжнародної боротьби зі злочинністю.

З іншого боку, Сполучені Штати з серпня 2025 року обрали силовий, військовий підхід. Адміністрація президента Трампа розгорнула в Карибському морі кораблі та авіацію, проводячи ракетні удари по суднам, ідентифікованим як учасники наркотрафіку. Станом на 12 листопада 2025 року було проведено 19 таких ударів, в результаті яких загинуло понад 70 осіб. Ця тактика прямого стримування має миттєві, але непрогнозовані наслідки. З одного боку, вона, безсумнівно, підвищує ризики для будь-кого, хто займається транспортуванням наркотиків морським шляхом, тимчасово пригнічуючи активність. З іншого боку, вона створює колатеральну шкоду для всього морського співтовариства. Рибалка, який виходить у море на легальний промисл, тепер ризикує не тільки стикнутися з корумпованими венесуельськими патрулями, але й бути помилково ідентифікованим системами спостереження США як ціль. Це призводить до глибокої соціально-економічної та гуманітарної кризи на острові, де тисячі родин втрачають останнє джерело існування. Військова присутність США, таким чином, діє як таран, який руйнує крихку економічну екосистему, не вдаючись при цьому до кореню проблеми — системі інституціоналізованої державної корупції, що породжує та живить трафік.

Отже, сучасний острів Маргаріта представляє собою складний гібридний простір, де переплелися кілька рівнів контролю. На місцевому рівні держава через свої силові структури встановила режим детального регулювання та вилучення ренти, перетворивши наркотрафік з вільної злочинної діяльності на керовану державну монополію. Цей контроль супроводжується паралічем легальної економіки, що робить населення ще більш залежним від тієї ж системи. На регіональному рівні діють дві протилежні зовнішні сили: Франція та ЄС, які працюють через канали співпраці, часто сприяючи консолідації контролю Каракаса, і США, які застосовують силове стримування, що несе загрозу для всього морського руху.

Така конфігурація створює патову ситуацію. Режим Мадуро отримує можливість монетизувати трафік та зміцнювати внутрішній контроль, але ціною глибокої гуманітарної кризи серед власного населення та міжнародної ізоляції. США можуть демонструвати короткострокові оперативні успіхи у вигляді знищених суден, але не можуть вплинути на структурні причини, що роблять Венесуелу наркодержавою. А європейські споживачі продовжують отримувати наркотики, адже мережі адаптуються, знаходячи нові маршрути та способи.

Висновки:

- Відбувся перехід від контролю наркотрафіку незалежними кримінальними групами до системного захоплення цього бізнесу державними структурами. Через корупційні механізми видачі дозволів, інспекцій суден та обмеження ресурсів держава не ліквідує трафік, а перетворює його на керовану монополію.
- Жорсткі обмеження, введені під виглядом боротьби з трафіком, паралізують традиційне рибальство. Це змушує місцеве населення залежати від незаконної діяльності, посилюючи його вразливість та залежність від корумпованих державних схем.
- Поєднання державної корупції, паралічу легального заробітку та зовнішніх військових ударів призводить до глибокої гуманітарної кризи серед місцевих жителів.

Острів Маргаріта, таким чином, є яскравим прикладом більшої глобальної дилеми: як боротися з транснаціональною злочинністю, коли вона переплітається з корумпованими державними інститутами, а зовнішні втручання часто породжують більше страждань для цивільного населення, ніж реальних перешкод для злочинців.

Майбутнє острова та подібних хабів залежить від того, чи зможуть суб'єкти міжнародного права вийти за межі простої силової логіки чи вибіркової кооперації з корумпованими режимами та розробити комплексну стратегію, спрямовану на відновлення легальної економіки, боротьбу з корупцією та захист цивільних, які опинилися в епіцентрі цієї неоголошеної війни.

 Інші новини**Заява ESMA щодо перехідних заходів MiCA¹²**

Даний документ є офіційною заявою Європейського органу з цінних паперів та ринків (ESMA), оприлюдненою 4 грудня 2025 року, та присвячений завершенню перехідних періодів, передбачених Регламентом ЄС про ринки криптоактивів (MiCA), для

постачальників послуг у сфері криптоактивів (CASPs). У заяві ESMA послідовно нагадує, що MiCA встановив спеціальний перехідний режим для тих CASPs, які надавали свої послуги відповідно до національного законодавства до 30 грудня 2024 року, дозволяючи їм протягом обмеженого часу перейти від національних регуляторних режимів до повної відповідності вимогам MiCA. Водночас документ чітко підкреслює, що стаття 143(3) MiCA надала державам-членам повну дискрецію щодо застосування такого перехідного режиму, включно з правом не застосовувати його взагалі або скоротити його тривалість з міркувань фінансової стабільності та захисту інвесторів, що призвело до фрагментованої та неоднорідної картини перехідних періодів у межах ЄС.

ESMA нагадує, що ще у жовтні 2023 року вона закликала CASPs завчасно готуватися до імплементації MiCA та активно взаємодіяти з національними компетентними органами (NCAs) щодо своїх планів авторизації, а у грудні 2024 року окремо звернула увагу на ризики, пов'язані з різною тривалістю перехідних періодів у державах-членах. У цій заяві логічно продовжується

¹² [https://www.esma.europa.eu/sites/default/files/2025-12/ESMA75-113276571-1631 Statement on end of MiCA transitional periods.pdf](https://www.esma.europa.eu/sites/default/files/2025-12/ESMA75-113276571-1631%20Statement%20on%20end%20of%20MiCA%20transitional%20periods.pdf)

ця лінія, але з акцентом на те, що значна частина перехідних періодів уже завершилася, а решта добігає кінця, і що ринкові учасники мали достатньо часу для підготовки та подання заяв на авторизацію за MiCA. У цьому контексті ESMA формулює чітке очікування, що CASPs, які станом на кінець перехідного періоду не отримали авторизацію за MiCA, повинні мати та реалізовувати впорядковані плани згортання діяльності у тих державах-членах, де перехідний період уже сплив, а також заздалегідь підготовлені плани на випадок, якщо авторизацію не буде отримано до завершення інших перехідних періодів або взагалі. Особливо підкреслюється, що такі плани мають бути спрямовані на мінімізацію шкоди для клієнтів, зокрема шляхом організації передачі криптоактивів клієнтів до інших авторизованих CASPs, і водночас мають забезпечувати дотримання вимог у сфері ПВК/ФТ.

Документ також містить чіткі сигнали для національних наглядових органів. ESMA наголошує, що NCAs повинні з особливою обережністю ставитися до так званих заявок «останньої хвилини» на авторизацію за MiCA та оцінювати їх за тими самими високими стандартами, що й будь-які інші заявки, навіть якщо це означатиме необхідність згортання діяльності CASP на національному або загальноєвропейському рівні на час розгляду заявки. Крім того, ESMA прямо очікує від наглядових органів готовності до координації та правозастосування у випадках несанкціонованого надання криптопослуг після завершення перехідних періодів, що фактично підкреслює завершення «регуляторної поблажливості» та перехід до повноцінного режиму нагляду і примусу. Завершальна частина заяви адресована інвесторам і має характер превентивного попередження: ESMA наголошує, що діяльність CASPs після завершення перехідного періоду не означає автоматичної авторизації за MiCA, і рекомендує інвесторам самостійно перевіряти статус постачальників послуг у Проміжному реєстрі MiCA ESMA, щоб упевнитися у застосуванні до них захисних механізмів, передбачених регламентом.

Крипто-загроза демократії¹³

У коментарі RUSI порушується принципова теза: ризик для виборчої безпеки Великої Британії полягає не лише (і не стільки) у тому, що політичні пожертви можуть надходити *безпосередньо* у криптоактивах, а в тому, що криптоінфраструктура радикально підсилює здатність ворожих держав і пов'язаних із ними посередників



«відмити» політичне походження коштів і далі завести їх у політичну систему вже у фіаті, формально як «дозволені» внески. Автор наполягає, що урядовий підхід «просто прирівняти криптопожертви до фіатних» концептуально хибний і може залишити дірки, бо ключова загроза — це **політичне відмивання коштів** (political money laundering): процес, у якому «брудним» є не предикатний злочин (наркоторгівля тощо), а **зв'язок фінансування з ворожою державою**, який необхідно приховати, аби зробити донорство «прийнятним» для виборчого законодавства. Типовий механізм, який описує автор: посередник отримує, наприклад, значну суму у Bitcoin/USDT, утримує винагороду й переводить решту як політичний внесок уже у фіаті, тобто «дозволений донор» фактично виступає платним каналом впливу.

Звідси впливає перший проблемний блок: **вузьке трактування “крипторизику” у виборчому праві**. Якщо законодавство буде сфокусоване на контролі лише тих жертв, які технічно зайшли

¹³ <https://www.rusi.org/explore-our-research/publications/commentary/uk-election-security-threatened-political-money-laundering-cryptocurrency>

«криптою», значна частина реальної загрози пройде поза радаром — тому що кошти, пройшовши через криптоканали й конвертацію/шари посередників, з'являться у звітності як банківський переказ від формально допустимого донора. Автор прямо формулює: криптоактиви — це насамперед **«технологічний стрибок» у можливостях відмивання**, тому протидія має будуватися як протидія відмиванню (з урахуванням специфіки політичного контексту), а не як косметичне «вирівнювання правил» для крипто і фіату.

Другий блок — **інституційна слабкість контролю та верифікації походження коштів**, де центральною є ланка HMRC ↔ Electoral Commission. Автор підкреслює, що навіть коли донор є британським платником податків, реальна перевірка може бути неефективною без дієвого та законодавчо забезпеченого обміну даними: податкові декларації (як мінімум у потенційно підозрілих кейсах) мають бути доступні для перевірки, але на практиці HMRC може обмежувати співпрацю з правоохоронними та іншими органами, посиляючись на захист даних/приватність. Пропозиція RUSI — **закріпити взаємодію HMRC та виборчого регулятора на статутній (законодавчій) основі** для кейс-бай-кейс розслідувань. Це важливо саме у логіці ПВК/ФТ: якщо підозра стосується «відмитого» іноземного впливу, без доступу до релевантних фінансово-податкових даних перевірка перетворюється на формальність.

Третій блок — **офшорні донори та “нерезидентська” сіра зона**, яка в криптосередовищі стає ще більш небезпечною через швидкість і непрозорість ланцюгів транзакцій. Автор звертає увагу на те, що розслідувати походження коштів, коли донор живе поза юрисдикцією HMRC, практично «майже неможливо», а розрахунок на підтримку розвідслужб у виборчих справах ускладнений традиційною політичною чутливістю таких втручань. У результаті виникає вразливість: навіть якщо номінально заборонено іноземне фінансування, у системі залишаються реалістичні шляхи завести гроші через посередників/структури, які не піддаються швидкій перевірці. Тому серед найжорсткіших, але логічних з точки зору ризик-менеджменту, ідей — вимога, щоб **усі індивідуальні донори були платниками податків у Великій Британії** (“No (financial) representation without taxation”).

Четвертий блок — **корпоративна “дірка” у правилах пожертв**: можливість для активно діючих компаній робити внески незалежно від структури власності. Автор називає це «надмірною» і давньою прогалиною: формально “UK company that is actively trading” є допустимим донором, навіть якщо кінцевий контроль/власність — офшорні чи потенційно ворожі інтереси. У термінах ПВК це класичне використання корпоративних оболонок для маскування джерела/контролю коштів, але у політичному фінансуванні наслідок ще гірший: підривається легітимність демократичного процесу. Тому рекомендація — **закрити можливість донатів від британських компаній незалежно від власності** (тобто прив'язати допустимість донорства до прозорості та бенефіціарного контролю).

П'ятий блок — **регуляторний арбітраж у криптоплатежах і доступ до даних**, який проявляється, зокрема, у виборі платіжних провайдерів/криптопроцесорів з іншої юрисдикції. Автор наводить кейс, що криптодонати у британській політиці поки що «у зародку», але вже з'являються ознаки залежності від іноземної інфраструктури обробки криптоплатежів, що може ускладнювати доступ наглядових органів до даних і забезпечення єдиних AML-стандартів. Тому одна з ключових пропозицій — **дозволити обробку криптодонатів лише через зареєстрованих в Сполученому Королівстві VASP**, щоб AML-вимоги застосовувалися послідовно й щоб у регулятора/правоохоронців був реалістичний шлях отримати дані для перевірок.

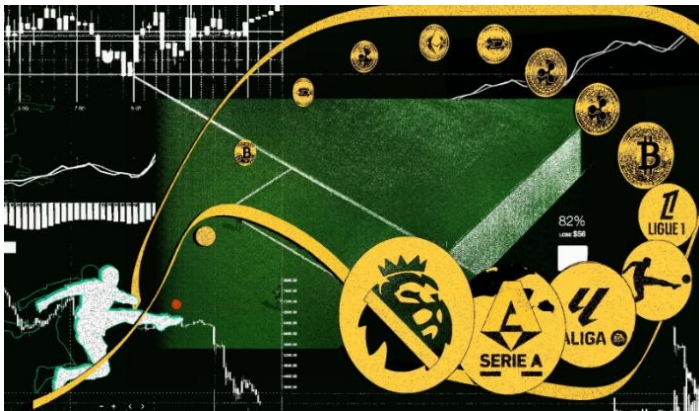
Шостий блок — **“останній рубіж” контролю: тягар доведення походження коштів**. Автор пропонує модель, коли у випадку ознак непрозорих криптотранзакцій або складних офшорних конструкцій виборчий регулятор (за участю HMRC) має право вимагати додаткове розкриття, а якщо достовірність походження коштів не може бути встановлена — пожертву слід блокувати.

Це фактично перенесення в сферу політичного фінансування AML-логіки enhanced due diligence але адаптовано до демократичних ризиків.

Окремим, але показовим елементом аналізу є аргументація через **“порівняльну регуляторну реальність”**: автор ілюструє, що певні інструменти, які полегшують анонімну конвертацію готівки в крипто (наприклад, крипто-АТМ), у Великій Британії є незаконними без реєстрації та були об’єктом системних дій FCA, тоді як в інших країнах подібна інфраструктура може бути значно більш поширеною. Це важливо не як критика конкретної юрисдикції, а як демонстрація того, що **виборче фінансування, “прив’язане” до зовнішньої криптоінфраструктури**, автоматично піддається ризикам слабших AML-бар’єрів та складнішого доступу до доказів.

Підсумовуючи, коментар RUSI розглядає криптовалюту не як “новий спосіб донатити”, а як **мультиплікатор спроможностей для прихованого іноземного фінансування**, який оголює старі слабкості системи (донори нерезиденти, корпоративні оболонки, слабка міжвідомча співпраця, недоукомплектований/«недоуповноважений» регулятор) і додає нові (швидкість, транскордонність, децентралізація, технологічні інструменти). Власне тому пакет із шести запропонованих заходів автор подає як “взаємопов’язану оборону”: від концептуального визнання політичного відмивання через криптоактиви, до конкретних правових і процедурних запобіжників.

Футбол під цифровим пресом: як системна залежність від нерегульованих фінансових спонсорів формує нову арену ризику для мільйонів європейців ¹⁴



Феноменальне вторгнення криптовалютних бірж та трейдингових онлайн-платформ в екосистему європейського футболу слід розглядати не як ізольований маркетинговий тренд, а як глибокий системний зсув, що відображає кризові явища як у спортивному бізнесі, так і в регуляторній архітектурі глобальних фінансів.

Цей симбіоз народився на перетині двох потужних потоків: з одного боку,

відчайдушної потреби футбольних клубів у нових джерелах капіталу на тлі поступового витіснення традиційних спонсорів з азартних ігор через законодавчі обмеження, а з іншого — агресивної експансії фінансових технологій, що пропонують високоприбуткові, але вкрай спекулятивні інструменти мільйонам дрібних інвесторів. Однак за блискучими логотипами на футболках, що з’являються на екранах по всьому світу, та за урочистими прес-релізами про «стратегічне партнерство» ховається тривожна реальність, детально документована розслідуванням Investigate Europe.

Значна частина цих нових «меценатів футболу» оперує в юридичних сірих зонах, не має необхідних ліцензій для діяльності на території Європейського Союзу, а в деяких випадках має історію серйозних правопорушень перед регуляторами інших країн. Таким чином, футбольні клуби, які є одними з найпотужніших культурних та соціальних інституцій континенту, мимоволі або свідомо перетворюються на канали легалізації та масштабування потенційно ризикованих,

¹⁴ <https://www.investigate-europe.eu/posts/revealed-fans-at-risk-as-crypto-and-trading-sponsors-flood-european-football>

а інколи й відверто небезпечних фінансових продуктів, цілеспрямовано націлених на найбільш лояльну та емоційно вразливу частину своєї аудиторії — вболівальників.

Масштаби цього явища демонструють його вже не периферійний, а центральний характер у фінансовій моделі сучасного футболу. Згідно з даними, у сезоні 2025/26 року понад третина всіх команд із п'яти найпрестижніших європейських чемпіонатів — Англійської Прем'єр-ліги, іспанської Ла Ліги, італійської Серії А, німецької Бундесліги та французької Ліги 1 — мають угоди з компаніями з сектору криптовалют або онлайн-трейдингу.

Абсолютним лідером за рівнем проникнення є Прем'єр-ліга, де цілих 70% клубів розраховують на фінансову співпрацю з такими партнерами. Це означає, що мільйони уболівальників щотижня стикаються з логотипами бірж та трейдингових платформ на формах гравців, бордах стадіонів, в цифровому контенті клубів та в рекламних інтеграціях. Така розповсюдженість формує ефект нормалізації: продукти, які за своєю суттю є високоризиковими фінансовими інструментами, починають сприйматися як легітимна та невід'ємна частина футбольної культури, а авторитет і емоційний капітал клубу несвідомо переносяться на комерційного партнера. Експерт із футбольних фінансів Кіран Магуайр з Ліверпульського університету точно окреслює цю механіку, зазначаючи, що футбольні клуби розглядаються як бренди з репутаційним капіталом, а компанії прагнуть «причепитися» до цього капіталу, щоб досягти демографічної групи, яка часто володіє вільними коштами та вже має зв'язки з традиційною азартною індустрією. Таким чином, футбол виконує роль потужного соціального верифікатора, що надає сумнівним з точки зору регуляції операторам відчуття надійності та стабільності.

Проте загроза криється не в самій ідеї фінансового спонсорства, а в конкретному профілі значної частини цих компаній. Розслідування виявляє тривожну закономірність: багато з фірм, які укладають мільйонні угоди з топ-клубами, не мають необхідних ліцензій для надання фінансових послуг на територіях, де розташовані ці клуби та де проживають їхні вболівальники. Класичним прикладом слугує випадок з «Манчестер Сіті» та криптобіржею OKX, офіційним криптовалютним партнером клубу. Ця біржа, зареєстрована на Сейшельських островах, одному з найпопулярніших офшорів у світі, була визнана винною у систематичному порушенні законодавства США про боротьбу з відмиванням коштів і сплатила штраф у розмірі понад півмільярда доларів. Незважаючи на цей гучний скандал та відсутність реєстрації в британському Управлінні з фінансового регулювання та нагляду (FCA), OKX продовжує бути партнером одного з найсильніших клубів світу, а її логотип регулярно з'являється на аренах та в медіа. Для британського вболівальника, який бачить цю асоціацію, вона слугує непрямою рекомендацією, хоча на практиці будь-які інвестиції через OKX не захищені британськими механізмами компенсації фінансових послуг у разі зникнення або банкрутства компанії.

Ще більш показовий випадок пов'язаний з «Ньюкаслем» та трейдинговою платформою VT Markets. Ця австралійська компанія, яка пропонує торгівлю на валютному ринку форекс, дорогоцінними металами та іншими похідними інструментами, з 2023 року перебуває в офіційному списку попереджень FCA через відсутність будь-якої британської ліцензії. Аналогічні попередження про неї опубліковані регуляторами Італії, Бельгії та Данії. Проте VT Markets не лише уклала угоду з «Ньюкаслем», але й активно використовує цю асоціацію в таргетованій рекламі на платформі Facebook, спрямованій на аудиторію Великої Британії. Коли потенційний клієнт із Великобританії намагається зареєструватися на сайті VT Markets, йому показують дисклеймер, де йдеться, що компанія регулюється лише органами Південної Африки та що користувач діє на «власний розсуд та ініціативу». Подібні формулювання, як виявило розслідування, стали стандартним інструментом для цілого ряду подібних фірм. Представник FCA чітко зазначив, що просте попередження про відсутність захисту не звільняє компанію від відповідальності, особливо якщо вона пропонує або рекламує регульовані фінансові продукти без належних дозволів.

Структурні причини цього масового явища глибоко вкорінені в економічній логіці сучасного професійного спорту. По-перше, футбольні клуби, особливо ті, що не мають доступу до астрономічних доходів від прав на трансляції або стабільних власників-олігархів, перебувають під постійним фінансовим тиском. Обмеження на спонсорство з боку індустрії азартних ігор, яка була одним з основних донорів протягом десятиліть, створили величезну фінансову прогалину. Криптовалютні біржі та трейдингові платформи, які переживають період бурхливого зростання та мають великі бюджети на маркетинг, виявилися ідеальними кандидатами для заповнення цієї прогалини.

Маркетингове дослідження компанії SportQuake показує, що лише за один сезон криптобіржі вклали 565 мільйонів доларів як спортивні спонсори по всьому світу, причому 59% цієї суми припало саме на футбол. Витрати платформ онлайн-трейдингу на спортивні партнерства з 2019 року потроїлися, досягнувши 183 мільйонів доларів. Ці цифри ясно демонструють фінансову вагу нового сектора для спортивної індустрії. По-друге, демографічний портрет середньостатистичного вболівальника топ-клубу ідеально збігається з цільовою аудиторією цих фінансових компаній: це переважно чоловіки віком від 18 до 45 років, зі стабільним доходом, технологічно підковані, схильні до адреналіну та конкуренції, а також часто вже знайомі з механізмами ставок на спорт. Таким чином, перехід від пропозиції ставок до пропозиції інвестицій у криптовалюту або CFD (контракти на різницю) є для цих користувачів логічним кроком, а для компаній — ефективним способом конвертувати лояльність до клубу в лояльність до бренду. Самі продукти, як зауважує Магуайр, за своєю суттю є високоспекулятивними, а їхня ризикованість наближає їх до азартних ігор, що робить ці галузі природними союзниками в новій реальності.

Однак найбільші питання викликає не економічна логіка, а етична позиція та рівень відповідальності самих футбольних клубів. Здається, що в гонитві за швидкими грошима багато клубів проводять поверхневу або взагалі ігнорують процедуру належної перевірки (due diligence) своїх комерційних партнерів. Експерт зі спортивного маркетингу Тім Кроу зазначає, що, асоціюючи клуб з певним брендом, керівництво неявно рекомендує його фанатам, передаючи їм частину довіри, заробленої командою на полі. Тому клуб повинен бути впевнений на всі сто відсотків, що провів ретельну перевірку, щоб потім фанам не довелося жалкувати про цю асоціацію.

Наслідки цього безконтрольного футбольного спонсорства можуть бути далекосяжними та глибокими. Найочевидніший ризик — це пряма фінансова шкода для вболівальників, які, довіряючи авторитету клубу, можуть інвестувати свої заощадження в продукти, що не мають належного регуляторного захисту, а отже, є вразливими до махінацій, раптових банкрутств платформ або різких злетів і падінь ринків. Оскільки футбольна аудиторія включає людей різного віку та рівня фінансової грамотності, особливо вразливими можуть виявитися молоді фанати, які тільки починають свій шлях у світі фінансів.

По-друге, це серйозно підриває суспільну довіру до футбольних клубів як соціальних інституцій, які традиційно були центрами громадського життя та носіями певних цінностей. Коли клуб стає промоутером потенційно шкідливих фінансових продуктів, це розмиває його соціальну місію та перетворює його на звичайну комерційну корпорацію, що прагне максимізувати прибуток будь-якою ціною.

По-третє, ця ситуація свідчить про серйозні прогалини в транскордонному фінансовому регулюванні ЄС. Компанії з офшорних юрисдикцій можуть вільно укладати угоди з європейськими клубами, використовувати європейські бренди для маркетингу, але при цьому уникати нагляду європейських регуляторів, перекладаючи всі ризики на споживачів. Це створює несправедливу конкурентну перевагу для нерегульованих гравців і ставить під загрозу єдиний фінансовий ринок ЄС.

Вирішення цієї комплексної проблеми вимагає консолідованих зусиль з боку різних інституцій. Насамперед, національні фінансові регулятори, такі як британський FCA, повинні активізувати діалог з футбольними асоціаціями та клубами, надаючи їм прозорі списки компаній, які мають ліцензії, а також тих, що перебувають під попередженням. Санкції за сприяння нелегальній фінансовій діяльності мають бути чіткими та суворими. По-друге, УЄФА та національні ліги повинні розробити та запровадити обов'язкові єдині стандарти належної перевірки комерційних партнерів для всіх клубів, які беруть участь у їхніх змаганнях. Ці стандарти мають містити обов'язкову вимогу підтвердження діючих ліцензій у всіх юрисдикціях, де будуть діяти рекламні кампанії, а також оцінку репутаційних ризиків. По-третє, самим футбольним клубам необхідно взяти на себе моральний обов'язок щодо фінансової освіти своїх фанатів. Партнерство з фінансовою компанією має супроводжуватися не лише рекламою, а й чіткими попередженнями про ризики, посиланнями на офіційні регуляторні сайти та інформаційними кампаніями про основи фінансової грамотності.

Вибір, зроблений зараз між короткостроковою вигодою та довгостроковою довірою мільйонів, визначить, чи залишиться європейський футбол громадським благом, чи остаточно перетвориться на інструмент фінансової експлуатації найвідданіших своїх прихильників.

Ваша думка важлива!

1. Нова Стратегія нацбезпеки США 2025 року фокусується на ізоляціонізмі та захисті власної економіки, ігноруючи глобальну корупцію, якщо вона не шкодить США прямо. Чи готові ми до того, що "парасолька" глобального тиску США може згорнутися, і нам доведеться покладатися лише на власні та європейські стандарти?
2. Звіт Казначейства Великої Британії показує зростання витрат на 24% до £57 млн, але Basel Index фіксує "системну стагнацію". Ми витрачаємо все більше ресурсів на технології та звітність. Чи відчуваєте ви на практиці, що це конвертується в реальне зменшення злочинності?
3. Кейси Лівії (контрабанда палива) та Венесуели (острів Маргаріта) показують, що державні структури та нацкомпанії можуть бути головними бенефіціарами схем відмивання. Стандартні процедури КУС/AML базуються на довірі до офіційних документів та державних реєстрів. Як ви дієте, коли контрагентом є державна компанія? Які маркери ви використовуєте?
4. Шахраї використовують vIBAN, де код країни не відповідає реальній юрисдикції. Чи вважаєте ви, що поточні налаштування моніторингу транзакцій у ваших установах здатні виявити невідповідність між IBAN та реальним географічним ризиком?
5. Наскільки вразливою є Україна до використання її території або цифрової інфраструктури як транзитного хабу для міжнародних кіберзлочинних груп? Чи достатньо наявних заходів кібербезпеки та фінансового моніторингу?
6. Чи існує в Україні ризик формування «керованих монополій» на окремих ринках нелегальної економіки (наприклад, контрабанда, тіньова торгівля)? Як окремі представники силових або адміністративних структур на місцях можуть використовувати надзвичайні повноваження та обмеження для встановлення контролю над незаконними потоками замість їх блокування?

Контакуйте щодо цього документу з Міністерством фінансів України:

- Email: aml_bulletin@minfin.gov.ua
- Поштова адреса: Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- Ідентифікація контакту: стосовно Методологічного Бюлетеня № МінФін-AML-2025-50

Бюлетень є розробкою методологічної команди Міністерства фінансів України відповідно до частини 8 статті 18 Закону України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

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