Методологічний бюлетень

Серійний номер: МінФін-AML-2026-08

Лютий 2026

“Знати недостатньо – потрібно діяти”

Йоганн Ґете

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.

П'яте пленарне засідання FATF під головуванням Мексики: результати, ризики та критичний погляд з позиції України [1]

П'яте пленарне засідання Групи з розробки фінансових заходів боротьби з відмиванням коштів під головуванням Елісі де Анди Мадрасо відбулося 11–13 лютого 2026 року в Мехіко. У зібранні взяли участь делегати з більш ніж 200 юрисдикцій та спостережних організацій Глобальної мережі FATF. З точки зору формальних результатів, пленарне засідання ухвалило ряд рішень, що відображають поступальну еволюцію стандартів FATF у напрямку більш ефективного та результатоорієнтованого підходу до взаємних оцінок та управління ризиками.

Першим і найбільш значущим для практики ПВК/ФТ технічним результатом є ухвалення звітів взаємних оцінок Австрії, Італії та Сінгапуру. Ці три звіти стали одними з перших в рамках нового, переглянутого раунду методологічних оцінок FATF, що розпочався у грудні 2025 року. Нова методологія принципово відрізняється від попередньої: акцент зміщено з технічного комплаєнсу (де-юре наявність законодавства) на вимірювані практичні результати (де-факто ефективність правозастосування). Кожна оцінена юрисдикція отримує тепер не лише формальні

[1] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/outcomes-FATF-plenary-february-2026.html

рейтинги відповідності за 40 Рекомендаціями, але й обмежену за часом «Дорожню карту ключових рекомендованих дій» з очікуванням суттєвого прогресу протягом трьох років. Цей механізм є значним кроком уперед порівняно з попереднім циклом, де слабкий прогрес можна було роками «компенсувати» законодавчими реформами без реального поліпшення ефективності.

Другим помітним рішенням стало включення Кувейту та Папуа Нової Гвінеї до «сірого списку» FATF. Кувейт опинився на ньому вдруге (перший раз — 2012–2015), що свідчить про системні труднощі з утриманням досягнутого рівня ефективності. Головні недоліки включають: формальне, а не ризик-орієнтоване розуміння загроз ФТ; низьку кількість розслідувань та обвинувальних вироків у складних справах з ВК; нерозвинутий нагляд у секторі ВНУП. Папуа Нова Гвінея повертається у список вперше після виходу у 2016 році. Серед юрисдикцій, що наближаються до виходу з сірого списку, Алжир та Намібія досягли попереднього визначення про суттєве виконання планів дій, що відкриває можливість для виїзних оцінок FATF з метою верифікації прогресу.

Пленарне засідання затвердило дві нових публікації щодо віртуальних активів, заплановані до виходу у березні 2026 року. Перший — «Understanding and Mitigating the Risk of Offshore Virtual Asset Service Providers» — присвячений аналізу регуляторних прогалин, що дозволяють злочинцям використовувати офшорні VASP, які оперують за межами будь-якого ефективного нагляду. Другий — «Targeted Report on Stablecoins and Unhosted Wallets» — аналізує ризики, пов'язані зі стрімким зростанням ринку стейблкоїнів та P2P-транзакцій через некастодіальні гаманці. Обидва документи є прямою відповіддю на кризу регуляторного охоплення крипторинку, яка була зафіксована у численних звітах протягом 2024–2025 рр. Паралельно пленарне засідання схвалило стратегічний документ щодо кібершахрайства (cyber-enabled fraud), зафіксувавши цю загрозу як один із пріоритетів FATF на наступний дворічний цикл.

У сфері інституційного розвитку FATF пленарне засідання призначило Джайлса Томсона з Великої Британії новим президентом організації на дворічний термін, що розпочнеться 1 липня 2026 року. Томсон обіймав посаду віце-президента FATF з 1 липня 2025 року. Також було погоджено заходи щодо підвищення ролі та участі Регіональних органів у стилі FATF (FSRBs) у роботі організації — крок, що є частиною ширшої стратегії зміцнення єдності і узгодженості Глобальної мережі FATF.

Попри ці формально позитивні результати, пленарне засідання у Мехіко продемонструвало критичне та системне слабке місце FATF — неспроможність організації ефективно реагувати на геополітично чутливі загрози. Це обмеження наочно виявляється у питанні росії: FATF продовжує формально підтримувати режим призупинення членства РФ, запроваджений у лютому 2023 року у зв'язку з повномасштабним вторгненням в Україну, однак не робить жодних кроків назустріч переведенню росії до чорного списку, незважаючи на системне та задокументоване порушення нею стандартів FATF.

Саме ця тема стала центральною у критичному коментарі Олександра Глущенка, директора Департаменту антилегалізаційної політики (AML) Міністерства фінансів України та одного з провідних національних експертів з питань ПВК/ФТ. У своєму дописі в LinkedIn Глущенко характеризує результати зустрічі у Мехіко як майстер-клас з інституційного безсилля. Його критика зосереджена на кількох ключових аргументах. По-перше, членство росії хоч і було призупинено, її представники все ще долучаються до пленарних засідань та робочих груп через Євразійську Групу (EAG) – FSRB, який відображає «особливий погляд» москви на ПВК/ФТ. Більш того, FATF очікує, що росія продовжить платити свої членські внески, що ставить серйозні моральні питання.

По-друге, FATF попереджає про те, що КНДР має все більше доступу до глобальної фінансової системи і висловлює жаль з приводу припинення роботи Панелі Експертів ООН 1718, при цьому

замовчуючи факт того, що саме росія наклала вето на продовження роботи цієї Панелі Експертів. По-третє, FATF бере до уваги ратифікацію Іраном Палермської конвенції та конвенції про боротьбу з фінансуванням тероризму, зосереджуючись на «надто широких застереженнях». При цьому, FATF ігнорує відчутну підтримку Іраном війни росії шляхом постачання безпілотників Shahed та технологій, які щодня використовуються проти українських цивільних осіб та інфраструктури.

Зі свого боку, команда Методологічного бюлетеня, висловлює власну думку стосовно того, що росія відповідає всім об'єктивним критеріям чорного списку: систематичне ухилення від санкцій, фінансування тероризму через державні канали (Wagner Group, постачання зброї), сприяння незаконному розповсюдженню зброї масового знищення у взаємодії з КНДР та Іраном — юрисдикціями, що вже перебувають у чорному списку. Але FATF вже протягом чотирьох років не може досягти консенсусу щодо ескалації заходів проти РФ. Механізм призупинення членства без реальних наслідків для міжнародних фінансових відносин росії насправді легітимізує модель поведінки, за якої держава може відкрито порушувати міжнародне право та стандарти FATF, але при цьому продовжувати функціонувати в міжнародній фінансовій системі через треті юрисдикції — передовсім ОАЕ, Туреччину, Китай та ряд країн Центральної Азії. Відсутність конкретного рішення щодо росії підриває довіру до FATF як органу, здатного протистояти не лише «малим» порушникам, але і системним загрозам з боку великих держав. Таке вибіркове застосування стандартів деформує всю архітектуру міжнародного AML-режиму.

Призупинення членства РФ у 2023 році стало важливою, але лише проміжною перемогою. Невключення росії до чорного списку попри накопичений масив доказів свідчить, не про недостатність фактологічної бази, а про політичну неспроможність FATF долати геополітичні протиріччя між членами за допомогою процедури консенсусу.

Звіти міжнародних організацій та окремих юрисдикцій

Ризики відмивання коштів у середовищі віртуальних IBAN: новий аналітичний погляд ПФР Італії [2]

Публікація ПФР Італії відображає зростаючу стурбованість наглядових та правоохоронних органів ЄС практикою використання множинних ідентифікаторів банківських рахунків, що технологічно трансформує традиційну чотиристоронню модель платіжних відносин (платник, банк платника, отримувач, банк отримувача) у значно складніші ланцюги, принципово нові для систем AML. Дослідження є спробою комплексної таксономізації конфігурацій так званих віртуальних IBAN — і вже з цієї причини заслуговує на особливу увагу практиків у сфері фінансового моніторингу.

Центральним поняттям документа є «additional IBAN» (aIBAN) — числово-літерний ідентифікатор, який доповнює основний (primary) IBAN рахунку, але не є самостійним рахунком. Автор принципово переосмислює загальноприйнятий термін «virtual IBAN» і пропонує більш точне визначення — «additional IBAN», оскільки ця назва адекватніше відображає юридичну та технічну природу інструменту: додатковий ідентифікатор залишається прив'язаним до того самого основного рахунку, не

[2] https://uif.bancaditalia.it/pubblicazioni/quaderni/2026/quaderno-33-2026/QAR-33.pdf

створюючи окремого платіжного зобов'язання. Ця, на перший погляд, суто термінологічна деталь насправді має критичне значення для регулювання: якщо регулятор неправильно кваліфікує vIBAN як окремий рахунок, то виникають прогалини у вимогах щодо ідентифікації клієнта, бенефіціарного власника та моніторингу транзакцій.

Таксономія, запропонована Манною, є оригінальним внеском документа й будується на трьох ключових критеріях. Перший — збіг банківського ідентифікатора vIBAN з ідентифікатором основного рахунку або його відмінність від нього. Другий — збіг коду країни в структурі vIBAN з кодом країни основного рахунку або його відмінність. Третій — і найважливіший з точки зору ризиків ВК — питання про те, кому належить основний рахунок: безпосередньо платнику або отримувачу, чи ним володіє третій посередник. Ця тривимірна класифікація породжує вісім категорій конфігурацій, які суттєво різняться за своїм ризик-профілем. Саме конфігурації, де основний рахунок утримується посередником, а не кінцевим платником або отримувачем, становлять найбільшу небезпеку: в таких схемах ланцюг транзакцій переривається на рівні посередника, і реальна особа платника стає практично невидимою для банку-отримувача.

Методологічний підхід автора поєднує нормативний аналіз (детальний розбір ISO 13616, регламенту ЄС 2012/260 та звіту EBA 2024 щодо vIBANs) з емпіричним дослідженням ринку. Автор аналізує бізнес-моделі провідних постачальників vIBANs у ЄС, зокрема платіжних установ, зареєстрованих переважно в юрисдикціях з відносно ліберальним регуляторним режимом. Статистика, зібрана з відкритих джерел та бази EBA, свідчить про виражену географічну асиметрію у розподілі платіжних установ по ЄС: непропорційно велика кількість таких суб'єктів зареєстрована в окремих невеликих юрисдикціях, що само по собі є індикатором регуляторного арбітражу. Станом на жовтень 2025 року IBAN є обов'язковим у 80 країнах, з яких 51 розташована повністю або частково в Європі (64%), а серед них 73% вимагають IBAN як для внутрішніх, так і для міжнародних переказів.

Документ детально аналізує взаємозв'язок між vIBANs та двома паралельними трансформаційними трендами фінансової індустрії — Open Banking та Banking-as-a-Service (BaaS). Обидва ці явища, засновані на відкритті банківських API для третіх сторін та «аутсорсингу» базових банківських функцій небанківським провайдерам, фундаментально змінюють структуру платіжних відносин і ускладнюють ідентифікацію кінцевого бенефіціара транзакції. В умовах BaaS-моделі дрібна фінтех-компанія, зареєстрована в одній юрисдикції ЄС і використовуючи платіжну ліцензію банку-партнера, може надавати vIBANs клієнтам по всьому ЄС, при цьому банк-партнер часто не має повноцінного уявлення про кінцевого клієнта. Це породжує проблему «субделегованої ідентифікації», за якої реальне KYC-зобов'язання розмивається між кількома суб'єктами ланцюга та де-факто не виконується жодним з них у повному обсязі.

Окрема увага приділяється феномену «IBAN discrimination» — незаконній, але поширеній практиці, за якої банки або платіжні системи відмовляються приймати перекази на IBAN з кодом країни, відмінним від країни платника. Стаття 9 SEPA Regulation прямо забороняє цю практику, проте вона зберігається де-факто. Парадоксально, але саме боротьба з цією дискримінацією є одним з легальних підстав для запиту vIBAN: домогосподарство з рахунком у країні A, яке працює в країні B, може запросити vIBAN з кодом країни B, щоб уникнути відмов від роботодавця. Автор ретельно досліджує, наскільки ця легальна функціональність може використовуватися як обгортка для схем ВК, в яких злочинці навмисно конструюють транзакційні ланцюги з розривом між кодом країни в IBAN і реальним місцезнаходженням рахунку.

Регуляторні висновки документа формулюються навколо трьох пріоритетних напрямів дій. По-перше, необхідно усунути IBAN discrimination на рівні імплементації, оскільки саме вона є каталізатором попиту на vIBANs у сірих і чорних схемах. По-друге, слід суттєво підвищити

прозорість у складних транзакційних ланцюгах — зокрема, запровадити вимогу до платіжних установ передавати в повідомленні про переказ повну інформацію про первинний рахунок, а не лише vIBAN, що фактично реалізує логіку «Travel Rule». По-третє, необхідно вирішити проблему нерівномірного розподілу платіжних установ по юрисдикціях ЄС, яка є симптомом регуляторного арбітражу: частина постачальників vIBANs свідомо обирає юрисдикції з менш суворим наглядом, а тоді надає послуги клієнтам по всьому ЄС.

Дослідження Манни є надзвичайно своєчасним у контексті переходу ЄС до нового AML-пакету та початку роботи AMLA. Практика vIBANs — це один із прикладів, де технологічна інновація об'єктивно випереджає регуляторне мислення: SEPA Regulation 2012 року та Директива PSD2 просто не передбачали такого масштабу поширення vIBANs та складних BaaS-ланцюгів. Звіт закликає AMLA включити до майбутнього Єдиного зводу правил спеціальні вимоги до прозорості ланцюга ідентифікаторів платіжних транзакцій та до верифікації бенефіціарної власності в умовах BaaS.

Висновки:

- vIBANs у конфігураціях, де основний рахунок утримується третьою стороною, а не кінцевим платником / отримувачем, є структурно непрозорими для стандартних AML/KYC-процедур — СПФМ необхідно розробити окремі правила верифікації таких транзакцій та запити до контрагентів щодо природи ідентифікатора.
- Принцип «Travel Rule» фактично має бути розширений аналогічними вимогами до непрозорих платіжних ланцюгів у SEPA-просторі: передача повної інформації про первинний рахунок-джерело в повідомленні про переказ є необхідним мінімальним стандартом для запобігання легалізації через vIBANs.
- Подальша еволюція Open Banking та BaaS неминуче збільшить масштаб і складність vIBAN-екосистем — СПФМ необхідно вже зараз адаптувати свої системи моніторингу транзакцій (TMS) для ідентифікації транзакцій, де отримувач або платник може бути «схований» за vIBAN посередника.

Індекс сприйняття корупції 2025: глобальна корупція набирає обертів на тлі демократичного регресу [3]

Transparency International (TI) опублікувала черговий щорічний Індекс сприйняття корупції (Corruption Perceptions Index, CPI) за 2025 рік, охоплюючи 182 країни та території. Документ фіксує найбільш тривожну тенденцію за останнє десятиліття: глобальний середній показник впав до 42 балів зі 100 можливих — це перше реальне погіршення середнього значення після кількох років відносної стабілізації. Що особливо тривожно для аналітиків у сфері ПВК/ФТ/ФР — 122 країни, тобто дві третини охоплених юрисдикцій, набрали менше 50 балів, що за методологією TI відповідає рівню системної корупції. Це безпосередньо корелює зі збільшенням ризику відмивання коштів, оскільки системна корупція є класичним предикатним злочином та інфраструктурним фактором для ВК-схем.

Методологія CPI базується на 13 незалежних джерелах даних від восьми міжнародних організацій, включаючи Світовий банк, Transparency International Business

[3] https://files.transparencycdn.org/images/CPI-2025-Report-EN.pdf

Principles та Varieties of Democracy (V-Dem). Кожен індикатор вимірює сприйняття корупції в публічному секторі з боку бізнес-спільнот, експертів та широкої громадськості. Індекс не вимірює прямі акти корупції чи обсяги корупційних потоків, натомість фіксує інституційний контекст — стан судової незалежності, контролю над державними закупівлями, захисту від хабарництва та ефективності антикорупційних установ. Для практиків ПВК/ФТ низький бал CPI означає підвищений ризик відповідної юрисдикції, а також необхідність посиленої належної перевірки контрагентів та бенефіціарних власників з таких країн.

Географічний аналіз результатів 2025 року виявляє тривожну деградацію навіть у юрисдикціях, традиційно зразкових з точки зору управління. Данія зберегла першість із 89 балами, проте серед розвинених демократій зафіксоване суттєве зниження: Сполучені Штати Америки отримали 64 бали (зниження порівняно з попередніми роками), Канада — 75, Велика Британія — 70, Франція — 66, Швеція — 80. Найнижчі позиції традиційно займають Сомалі та Південний Судан (по 9 балів), проте аналітична цінність звіту полягає не в константних аутсайдерах, а у динаміці погіршення в середній та верхній частинах рейтингу. Зокрема, зниження показників розвинених демократій пов'язується з підривом незалежності судових систем, послабленням законодавства про фінансування партій та звуженням простору для громадянського суспільства.

Звіт TI встановлює прямий причинно-наслідковий зв'язок між звуженням громадянського простору та погіршенням антикорупційних показників: у двох третинах країн, де відзначено погіршення CPI, одночасно зафіксовано обмеження свободи преси, переслідування НПО та обмеження права на мирні зібрання. Цей зв'язок є критично важливим для розуміння ризиків у сфері ПВК/ФТ/ФР, оскільки саме незалежна журналістика та активне громадянське суспільство є ключовими позаінституційними механізмами виявлення корупційних схем, що передують кримінальному переслідуванню. Звуження цього простору означає подовження латентного часу виявлення корупційних операцій, що збільшує час і масштаб відмивання коштів. Особливо критична ситуація у 2025 році спостерігається в контексті міжнародних підривних впливів: TI фіксує масштабне втручання росії у демократичні процеси в 20+ країнах через фінансування маргінальних партій, дезінформаційні кампанії та корупційні мережі, що системно підриває антикорупційні інституції.

Детальний аналіз регіональних тенденцій виявляє значущі для практики ПВК/ФТ/ФР патерни. В Азійсько-Тихоокеанському регіоні Сінгапур (83) та Гонконг (75) зберігають лідируючі позиції, проте рейтингові агентства фіксують зростання ризиків у другому ешелоні юрисдикцій (М'янма, Камбоджа, Лаос), де корупційна інфраструктура активно використовується для легалізації доходів від незаконної торгівлі. У Латинській Америці особливо тривожна ситуація в Перу (30 балів), де молодіжні протести 2025 року виникли на тлі системної корупції в судовій системі та державних закупівлях. Африканський регіон показує неоднорідну картину: поряд з відносним прогресом Руанди (53) та Ботсвани (59), більшість субсахарських держав залишається в зоні критичного ризику з показниками нижче 30 балів. Такі країни як Греція, Угорщина, Болгарія фіксують стагнацію або регрес, що має прямі наслідки для оцінки ризиків транзитних потоків у межах ЄС.

Доповідь TI містить розгорнутий аналіз впливу міжнародних факторів на корупційну динаміку, що безпосередньо стосується сфери транскордонних фінансових потоків. Зокрема, TI відзначає деградацію американської системи FCPA (Foreign Corrupt Practices Act) внаслідок зміни правозастосовної пріоритетності, що вже знижує стримуючий ефект цього ключового механізму протидії транснаціональній корупції. Скорочення міжнародної допомоги на розвиток, включаючи програми зміцнення потенціалу у сфері ПВК/ФТ, TI кваліфікує як системний ризик для глобальної архітектури протидії відмиванню коштів — особливо в країнах із низьким рівнем доходів, де ці програми були основним джерелом операційних можливостей фінансових розвідок. Рекомендації TI зосереджуються на чотирьох стратегічних напрямах: зміцненні незалежності судових та правоохоронних систем; реформуванні правил фінансування

політичних партій; захисті простору для громадянського суспільства та журналістських розслідувань; посиленні міжнародного співробітництва у протидії транскордонним нелегальним фінансовим потокам. Зокрема, TI наполягає на повноцінній імплементації Директиви ЄС 2024/1762 про боротьбу з корупцією та прискоренні ратифікації Конвенції ООН проти корупції (UNCAC) державами, які досі цього не зробили.

З практичної точки зору для СПФМ та регуляторів, Індекс CPI 2025 свідчить про необхідність переосмислення підходу до ризиків. Традиційна логіка "юрисдикція має високий / середній / низький ризик" поступається місцем більш детальному аналізу: погіршення показників у "надійних" юрисдикціях (США, Франція, Угорщина) вимагає від комплаєнс-підрозділів переглядати автоматичні виключення з EDD-процедур. Водночас концентрація 122 країн нижче 50-балового порогу означає, що стандартна належна перевірка є недостатньою для більшості транскордонних транзакцій. TI також вказує на зростаючу складність схем з використанням підставних компаній в юрисдикціях з частково задовільними показниками CPI (40-55 балів) як проміжних ланок для легалізації коштів, отриманих у юрисдикціях з критично низькими показниками. Реєстри бенефіціарного права власності та автоматичний обмін податковою інформацією (AEOI/CRS) у цьому контексті набувають критичного значення як контрзаходи проти багатоярусних корупційних схем.

Висновки:

- Глобальний середній показник CPI 2025 (42/100) при 122 країнах нижче порогу 50 балів вимагає від СПФМ переходу до варіативної оцінки юрисдикційного ризику: автоматичні виключення з EDD-процедур для юрисдикцій з «традиційно позитивною» репутацією є неприйнятними без актуальної верифікації їх поточних інституційних показників.
- Задокументоване послаблення американського механізму FCPA та скорочення міжнародної допомоги на зміцнення систем ПВК/ФТ у країнах, що розвиваються, є системними сигналами для глобальних фінансових установ: операційне середовище ставатиме менш регульованим, що підвищує власну відповідальність за виявлення корупційних транзакцій.
- Прямий кореляційний зв'язок між обмеженням громадянського простору та погіршенням CPI є практичним індикатором для оцінки ризиків: обмеження свободи преси та переслідування НПО у конкретній юрисдикції мають автоматично підвищувати рівень моніторингу транзакцій, пов'язаних з нею.

Європейський досвід регулювання блокчейн-рішень за звітом European Blockchain Sandbox [4]

Документ є комплексним підсумковим аналітичним звітом третього раунду пан’європейської регуляторної пісочниці Європейського Союзу, спрямованої на формування узгодженого підходу до правового регулювання блокчейн- і DLT-рішень у різних секторах економіки. Звіт відображає результати системних регуляторних діалогів між розробниками інноваційних цифрових продуктів і національними та європейськими компетентними органами, які проводилися у 2024–2025 роках у межах ініціативи, що функціонує з 2023 року та фінансується в рамках Digital Europe Programme.

[4] https://blockchain-observatory.ec.europa.eu/document/download/4f633a49-02a2-4001-8799-d09e74c74839_en?filename=Abstract%20%20Exec%20summary%20%28final%20January%202026%29.pdf

Центральною ідеєю документа є закріплення ролі Європейської блокчейн-пісочниці (European Blockchain Sandbox) як інструменту превентивного регуляторного узгодження, який не створює винятків із чинного законодавства, але дозволяє на практиці тестувати правозастосування нових і складних нормативних режимів у безпечному та контрольованому середовищі. У звіті підкреслюється, що пісочниця не є механізмом легалізації експериментів поза межами права, а виступає платформою спільного навчання регуляторів і ринку, де інновації аналізуються крізь призму реального регуляторного навантаження.

Третій раунд охопив двадцять відібраних проєктів, що представляють широкий спектр галузей, включно з фінансовим сектором, цифровими активами, енергетикою, охороною здоров'я, кібербезпекою, управлінням даними, логістикою, митним контролем, екологічною звітністю та цифровою ідентифікацією. При цьому звіт фіксує тенденцію поступового перетворення блокчейну з вузькоспеціалізованої фінансової технології на горизонтальну цифрову інфраструктуру, яка використовується для забезпечення простежуваності, довіри, автоматизації комплаєнсу та міжсекторального обміну даними. Методологія роботи в межах третього набору передбачала багаторівневі консультації, що включали попередню підготовку регуляторів, два основні раунди діалогу з розробниками, а також окремі координаційні зустрічі між наглядовими органами, що дозволяло виробляти узгоджені правові позиції та мінімізувати фрагментацію підходів.

Змістовно звіт побудований навколо концепції багаторівневого та кумулятивного регулювання DLT-рішень, відповідно до якої кожен технологічний продукт одночасно підпадає під дію кількох нормативних режимів. У документі послідовно демонструється, що сучасні блокчейн-системи не можуть оцінюватися ізольовано в межах одного правового акта, а мають аналізуватися з урахуванням GDPR, eIDAS 2.0, Data Act, Digital Services Act, Data Governance Act, NIS2, DORA, Cyber Resilience Act, AMLR, MiCAR, DLT Pilot Regime, податкових директив DAC7 і DAC8 та секторального законодавства. Такий підхід формує нову модель правового ризику, за якої основною проблемою стає не відсутність регулювання, а його надмірна концентрація та складність інтеграції вимог.

Особливе місце у звіті займає аналіз захисту персональних даних у блокчейн-середовищі. Автори детально розглядають проблематику кваліфікації ончейн-даних як персональних, застосування принципів мінімізації та обмеження строків зберігання, а також наслідки неможливості повного видалення інформації з розподілених реєстрів. Значну увагу приділено впливу судової практики Суду ЄС, зокрема справи Єдиної ради з врегулювання (Single Resolution Board), на тлумачення понять ідентифікованості та псевдонімізації. Звіт фіксує, що для більшості DLT-проєктів проведення оцінки впливу на захист даних фактично стає обов'язковим елементом регуляторної відповідності, а використання криптографічних методів саме по собі не звільняє від застосування GDPR.

У блоці, присвяченому eIDAS та цифровій ідентичності, документ розглядає блокчейн як компонент нової європейської екосистеми довірчих сервісів, пов'язаної з Європейським цифровим гаманцем ідентичності та майбутніми бізнес-гаманцями. Наголошується на необхідності технічної та правової сумісності DLT-рішень із кваліфікованими електронними підписами, атрибутами автентифікації та корпоративними повноваженнями, а також на тісному зв'язку цієї сфери з вимогами фінансового моніторингу та корпоративного права.

Суттєвий обсяг звіту присвячено кібербезпеці та операційній стійкості цифрових систем. Уперше в межах пісочниць на такому рівні систематизовано взаємодію NIS2, DORA, CRA та Cybersecurity Act у контексті блокчейн-архітектур. Смарт-контракти розглядаються як повноцінні інформаційно-комунікаційні технологічні активи (ІКТ-активи), які підлягають оцінці вразливостей, сертифікації, контролю ланцюгів постачання та управлінню інцидентами. Звіт підкреслює, що відсутність належного кіберуправління дедалі частіше розцінюється як регуляторний ризик, а не лише технічна проблема.

Фінансово-регуляторний блок документа демонструє послідовне закріплення функціонального підходу до кваліфікації цифрових активів і сервісів. DAO, DeFi-протоколи, токенізовані депозити, стабількоїни та інвестиційні токени аналізуються з погляду економічної сутності, розподілу контролю та ризиків, а не задекларованого рівня децентралізації. Звіт детально розглядає співвідношення MiCAR, MiFID II та AIFMD, а також проблематику ідентифікації емітента, застосування винятків та регулювання послуг, що надаються через смарт-контракти.

Окрему увагу приділено питанням протидії відмиванню коштів і фінансуванню тероризму. У документі блокчейн і DLT розглядаються не лише як об'єкти фінансового моніторингу, а й як інструменти підвищення ефективності контролю у сфері ПВК, зокрема через використання аналітики транзакцій, RegTech-рішень та штучного інтелекту. Водночас наголошується, що застосування AI у сфері ПВК/ФТ автоматично створює перетин із режимом регулювання високоризикових систем відповідно до AI Act, що істотно підвищує вимоги до управління моделями, якості даних та прозорості прийняття рішень.

Секторальні розділи, присвячені енергетиці, батарейним паспортам, цифровим паспортам продукції, EHDS, митному регулюванню та цифровій спадщині, демонструють тенденцію використання блокчейну як інфраструктури регуляторного контролю, звітності та забезпечення виконання політик ЄС у сфері сталого розвитку, охорони здоров'я та внутрішнього ринку. У цих кейсах DLT дедалі більше виступає не як бізнес-інновація, а як технічний інструмент реалізації публічної політики.

Висновки:

- **Регулювання блокчейн-рішень у ЄС остаточно перейшло до моделі багаторівневої кумуляції,** за якої кожен проєкт одночасно підпадає під декілька горизонтальних і секторальних режимів, що робить попередню правову кваліфікацію критично необхідною.
- **У сфері захисту даних блокчейн більше не сприймається як «виняткова технологія»:** більшість DLT-рішень розглядаються як такі, що обробляють персональні дані, із відповідним обов'язком проведення оцінки впливу на захист даних та впровадження архітектурних механізмів мінімізації ризиків.
- **У фінансовому секторі функціональний підхід остаточно домінує над формальним:** DAO, DeFi та токенізовані структури оцінюються за економічною сутністю, а не за заявленим рівнем децентралізації.
- **Використання блокчейну та штучного інтелекту для цілей ПВК/ФТ одночасно підпадає під вимоги AMLR та AI Act,** що формує новий клас комплексних регуляторних ризиків для фінансових установ і постачальників RegTech-рішень.

У підсумковій частині звіту European Blockchain Sandbox розглядається як елемент довгострокової архітектури регулювання цифрової економіки ЄС, що дозволяє зменшувати фрагментацію національних підходів, формувати спільні стандарти правозастосування та забезпечувати поступовий перехід від експериментального регулювання до стабільної нормативної системи. Документ фіксує трансформацію пісочниці із пілотного проєкту в стратегічний інструмент формування регуляторної політики, орієнтованої на баланс

між інноваціями, фінансовою стабільністю, захистом прав громадян та безпекою цифрового середовища.

Інформаційна війна та відповідальність держави: практичні механізми атрибуції російського впливу [5]

Звіт присвячений комплексному аналітичному дослідженню, що спрямоване на формування системного, доказово обґрунтованого та юридично стійкого підходу до встановлення відповідальності за інформаційно-впливові операції рф, спрямовані проти України, її сусідів та європейських партнерів. Документ розглядає атрибуцію не як суто технічний або експертний інструмент, а як складову стратегічної політики безпеки, яка безпосередньо впливає на санкційні рішення, дипломатичні процеси, регуляторні механізми та міжнародно-правову відповідальність держави-агресора. Автори виходять із того, що в умовах гібридної війни, зростання ролі інформаційного простору та посилення правового регулювання цифрових платформ будь-яка атрибуція повинна відповідати підвищеним стандартам доказовості, прозорості та процедурної коректності.

В основі дослідження лежить Рамкова модель атрибуції інформаційного впливу (IIAF), яка пропонується як уніфікована методологічна система для аналізу походження, координації та управління інформаційними кампаніями. Ця модель інтегрує чотири ключові виміри: технічний, поведінковий, контекстуальний та юридично-етичний. Автори детально пояснюють, що сучасні інформаційні операції навмисно будуються як багаторівневі та фрагментовані структури, які поєднують офіційні канали, проксі-ресурси, анонімні майданчики та псевдоорганічні спільноти. У таких умовах встановлення відповідальності неможливе без системного аналізу різнорідних даних, які доповнюють і взаємно підтверджують одне одного.

Технічний вимір аналізу у звіті розглядається як первинна основа виявлення та картування інформаційних операцій. Автори приділяють особливу увагу дослідженню цифрової інфраструктури, доменних реєстрацій, хостингових сервісів, записів системи доменних імен, сертифікатів захищеного з'єднання, платформних метаданих, ідентифікаторів аналітичних систем та фінансових слідів. На прикладі домену fondfbr.ru показано, як через аналіз реєстраційних даних, використання масового хостингу, анонімізованих сервісів та автоматизованих центрів сертифікації можна виявляти спроби приховування власності та централізованого управління. Водночас аналіз обходу санкцій телеканалів «Раша Тудей» і «Спутнік» після їх заборони в Європейському Союзі демонструє, як через створення альтернативних доменів, використання спільних систем веб-аналітики, синхронізоване просування посилань та перенаправлення аудиторії забезпечується збереження доступу до європейського інформаційного простору. Автори підкреслюють, що жоден окремий технічний індикатор не може розглядатися як прямий доказ державної участі, однак системне повторення інфраструктурних патернів формує переконливий профіль операції.

5 https://stratcomcoe.org/pdfjs/?file=/publications/download/Attribution_Russian_Information_Influence.pdf?zoom=page-fit

Поведінковий аналіз у звіті спрямований на дослідження організаційної логіки інформаційних кампаній, способів їхнього масштабування та механізмів імітації спонтанної підтримки. Через використання Рамкової моделі аналізу дезінформаційних загроз (DISARM) автори систематизують тактики, техніки та процедури, які застосовуються у впливових операціях. Особливу увагу приділено поширенню контенту через декілька цифрових платформ, синхронізації публікацій у різних каналах, використанню ідентичних або мінімально змінених формулювань, створенню мереж псевдорегіональних ресурсів, підробки першоджерел та маскуванню реального походження інформації. На прикладах кампаній, пов'язаних із дискредитацією мобілізації, корупційною тематикою та міжнародною підтримкою України, показано, як повторювані поведінкові патерни дозволяють ідентифікувати централізоване управління, наявність координаційних центрів та довгострокове стратегічне планування.

Контекстуальний аналіз у звіті розкриває ідеологічний, політичний і соціокультурний вимір російських інформаційних операцій. Автори досліджують структуру російської інформаційної екосистеми, яка включає державні медіа, ресурси, пов'язані з олігархічними групами, проксі-платформи, мережі псевдоекспертів, блогерів та закордонні канали ретрансляції. Окремо аналізуються стратегічні наративи, спрямовані на делегітимізацію української державності, дискредитацію західної підтримки, експлуатацію релігійних, мовних і регіональних тем, а також формування образу «зовнішнього управління». Значну увагу приділено моделі «потоку неправдивих повідомлень», яка передбачає масове поширення суперечливих наративів для різних аудиторій, та механізму «відмивання наративів», за допомогою якого фейкова інформація поступово легітимізується через послідовне поширення на різних майданчиках. Контекстуальний підхід дозволяє пов'язувати інформаційні кампанії з конкретними політичними, військовими та дипломатичними подіями, розкриваючи їхню стратегічну доцільність.

Висновки:

- **Надійна атрибуція інформаційних операцій можлива лише за умови поєднання технічних, поведінкових і контекстуальних доказів у єдиній стандартизованій моделі.** Окремі індикатори не забезпечують достатньої доказової сили; лише їх системна інтеграція дозволяє формувати юридично стійкі висновки.
- **російські інформаційні кампанії проти України мають стабільні інфраструктурні та операційні патерни, що свідчить про централізовану координацію.** Повторюваність доменних, мережевих і дистрибуційних механізмів підтверджує їх належність до організованої державної або квазідержавної екосистеми впливу.
- **Використання шкал впевненості та спектру державної відповідальності є необхідною умовою правової захищеності атрибуційних рішень.** Формалізація рівня впевненості дозволяє обґрунтовувати пропорційні санкційні, дипломатичні та регуляторні заходи.
- **Обмежений доступ до платформних і фінансових даних суттєво знижує доказову спроможність атрибуції.** Без інституційних механізмів обміну такими даними неможливо системно досягати високого рівня впевненості щодо державної участі.

Суттєвим елементом звіту є аналіз рівня впевненості атрибуційних висновків. Автори наголошують, що атрибуція за своєю природою є імовірнісною та повинна супроводжуватися чітким визначенням ступеня достовірності. Запропоновані шкали впевненості покликані унеможливити перебільшення результатів та забезпечити коректне використання висновків у політичних і правових процесах. Паралельно адаптується модель спектра державної відповідальності, яка дозволяє диференціювати різні рівні залученості держави — від мовчазного ігнорування до прямого командування операціями. Такий підхід формує підґрунтя для

пропорційного реагування у вигляді дипломатичних кроків, санкцій, регуляторних заходів або міжнародно-правових процедур.

Важливе місце у звіті займає юридично-етичний вимір атрибуції. Автори аналізують ризики судових оскаржень, проблеми захисту персональних даних, питання легітимності використання прихованих методів збору інформації, а також необхідність збереження довіри до аналітичних інституцій. Підкреслюється, що в умовах активного використання «правового тиску» з боку пов'язаних із росією структур слабко обґрунтовані атрибуції можуть не лише втратити юридичну силу, а й завдати шкоди міжнародній репутації України та її партнерів.

У фінальних розділах звіту демонструється практична інтеграція всіх видів доказів у єдину аналітичну модель. На прикладі комплексної кампанії з дискредитації України через тему корупції показано, як поєднання інфраструктурних зв'язків, синхронізованої дистрибуції, поведінкових патернів та наративної узгодженості з офіційною риторикою російської федерації дозволяє досягти високого рівня впевненості щодо державної координації. Водночас автори визнають суттєві обмеження сучасної аналітичної роботи, пов'язані зі скороченням доступу до програмних інтерфейсів платформ, закритістю внутрішніх систем обробки даних та обмеженим доступом до фінансової інформації, що ускладнює доведення прямих командно-контрольних зв'язків.

У підсумку звіт формує цілісну концепцію атрибуції інформаційного впливу як інституційного, міжсекторального та доказово орієнтованого процесу, який має бути інтегрований у систему національної та європейської безпеки. Він демонструє, що протидія російським інформаційним операціям потребує не фрагментарних розслідувань, а стандартизованих методик, постійного розвитку аналітичних спроможностей, глибокої координації між державними органами, цифровими платформами та громадянським суспільством. Документ позиціонує атрибуцію як ключовий елемент демократичної стійкості України та її міжнародних партнерів, здатний забезпечити як системне викриття маніпулятивних кампаній, так і легітимність довгострокових заходів реагування в умовах тривалої гібридної агресії.

Залучення партнерств і технологій для боротьби з грошовими мулами [6]

Аналітичний матеріал Королівського об'єднаного інституту оборонних досліджень (RUSI), підготовлений за підсумками третьої зустрічі Робочої групи з державно-приватного партнерства у грудні 2025 року, є комплексним дослідженням сучасного стану, структурних причин та інституційних механізмів протидії використанню грошових мулів у фінансових злочинах в Україні в умовах воєнного часу та трансформації фінансової системи.

У центрі аналізу перебуває твердження про те, що діяльність грошових мулів не може розглядатися як периферійне явище або сукупність поодиноких порушень, а є системним елементом злочинних екосистем, пов'язаних із шахрайством, ухиленням від оподаткування, тіньовою економікою та транснаціональною організованою злочинністю. Автори підкреслюють, що після початку повномасштабної агресії російської федерації масштаби проблеми суттєво зросли, а

[6] https://cfi-ua.org/uk/%D0%B7%D0%B0%D0%BB%D1%83%D1%87%D0%B5%D0%BD%D0%BD%D1%8F-%D0%BF%D0%B0%D1%80%D1%82%D0%BD%D0%B5%D1%80%D1%81%D1%82%D0%B2-%D1%96-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D0%B9-2/

втрати державного бюджету, спричинені такими схемами, безпосередньо впливають на обороноздатність, соціальну сферу та процеси відновлення.

У вступній частині документа грошові мули визначаються як фізичні особи, рахунки, платіжні інструменти або персональні дані яких використовуються для переміщення незаконних коштів, незалежно від рівня їх усвідомленої участі в злочинній діяльності. Автори наголошують, що значна частина таких осіб не до кінця усвідомлює правові та фінансові наслідки своєї участі, що формує окремий вимір проблеми, пов'язаний із фінансовою грамотністю, соціальною вразливістю та маніпулятивними практиками злочинних мереж. Водночас визнається, що істотна частина грошових мулів діє свідомо, розглядаючи надання доступу до рахунків як джерело додаткового доходу, що вказує на недостатню ефективність стримувальних механізмів.

У розділі, присвяченому розумінню загрози, детально аналізуються типології грошових мулів та механізми їх вербування. Документ демонструє, що усталені уявлення про домінування молоді або людей похилого віку не відповідають сучасній реальності, оскільки дедалі частіше до схем залучаються особи працездатного віку з базовими цифровими та фінансовими навичками. Вербування здійснюється через соціальні мережі, месенджери, фальшиві оголошення, псевдогуманітарні ініціативи та інші форми соціальної інженерії, які адаптуються до суспільних настроїв та кризових обставин. Особливо підкреслюється, що висока цифровізація України, з одного боку, створює передумови для розвитку фінансових технологій, а з іншого — значно полегшує масштабування злочинних схем.

Подальший аналіз фокусується на зв'язку грошових мулів із предикатними злочинами та структурою злочинних мереж. Автори наголошують, що діяльність мулів є інструментом маскування та фрагментації фінансових потоків, який дозволяє відокремити організаторів від безпосередніх виконавців та ускладнити роботу правоохоронних і наглядових органів. Учасники зустрічі звертають увагу на те, що транснаціональні злочинні групи свідомо обирають юрисдикції з прискореними процедурами відкриття рахунків та обмеженими початковими перевірками, що робить актуальним перегляд українських практик дистанційної ідентифікації та онбордингу. Водночас визнається відсутність єдиного бачення щодо напрямів руху незаконних коштів, що свідчить про недостатній рівень агрегованої аналітики та міжвідомчої координації.

Значну частину дослідження присвячено аналізу чинних механізмів виявлення та реагування. Описується ризик-орієнтована модель, яку застосовують українські банки під наглядом Національного банку України, що поєднує дані державних реєстрів, BankID, застосунку «Дія», агрегаторів, відкритих джерел та транзакційного моніторингу. Автори підкреслюють, що попри розвиток сценарного аналізу та RegTech-рішень, зокрема інструментів аналізу пристроїв і поведінкових патернів, ефективність індивідуальних банківських заходів залишається обмеженою через можливість переміщення схем між установами. У цьому контексті розглядаються міжбанківський меморандум щодо обмеження карткових переказів та ідея створення реєстру грошових мулів як інструменти колективного реагування, які водночас несуть ризики надмірної фінансової ізоляції та порушення прав клієнтів за відсутності належних гарантій.

Окремий концептуальний блок документа присвячено мережевій аналітиці як ключовому інструменту переходу від реактивного до системного протидіяння. Автори докладно пояснюють, як аналіз зв'язків між рахунками, пристроями, клієнтами та контрагентами дозволяє ідентифікувати організаторів схем, а не лише виконавців. Наводяться практичні індикатори, пов'язані з кількістю пристроїв на один рахунок, кількістю клієнтів на один пристрій, характером транзакційних ланцюгів та поведінковими аномаліями. Водночас підкреслюється, що ефективність мережевих моделей прямо залежить від повноти та міжінституційної інтеграції даних, що знову актуалізує питання партнерств і правових механізмів обміну інформацією.

У розділі, присвяченому розвитку партнерств, детально аналізується міжнародний досвід Європейського Союзу та Великої Британії. Стаття 75 Регламенту ЄС про протидію відмиванню коштів 2024 року розглядається як фундамент для легітимного державно-приватного співробітництва, а британські моделі на основі POCA та ECCTA — як приклад інституціоналізованого обміну інформацією через ф'южн-центри та спільні аналітичні платформи. Автори наголошують, що головною перешкодою для подібної взаємодії в більшості юрисдикцій є не формальні заборони, а правова невизначеність, страх відповідальності та відсутність чітких регуляторних настанов, що негативно впливає на якість фінансових розслідувань і формування SAR.

Важливим аспектом документа є аналіз технологічних рішень для безпечного обміну інформацією, включно з українськими платформами обміну ризиковими індикаторами, захищеними міжбанківськими каналами, системами моніторингу швидких платежів та перспективами використання федеративного машинного навчання. Автори демонструють, що такі інструменти дозволяють поєднувати аналітичні можливості різних установ без прямої передачі персональних даних, підвищуючи ймовірність раннього блокування коштів і їх повернення потерпілим.

Документ також містить аналіз міжнародних практичних кейсів, зокрема кампанії Europol EMMA та робочої групи EFIPPP, які ілюструють ефективність централізованого збору даних, координації операцій та агрегованої оцінки вразливостей банківського сектору. Ці приклади використовуються для аргументації необхідності переходу України від фрагментарних ініціатив до сталих інституційних форматів співпраці.

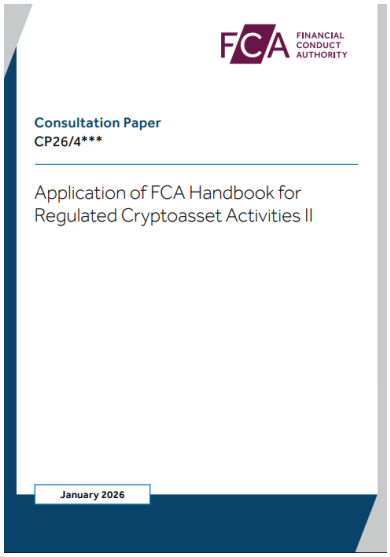
Висновки:

- **Ізольовані заходи окремих банків є недостатніми —** ефективна протидія грошовим мулам потребує системної міжбанківської координації та механізмів обміну інформацією.
- **Мережева аналітика та аналіз ідентифікаторів пристроїв є критично важливими** для виявлення організаторів злочинних мереж, а не лише окремих грошових мулів.
- **Правова визначеність щодо допустимого обміну інформацією (з урахуванням вимог захисту даних)** є необхідною умовою розвитку державно-приватного партнерства.
- **Превентивні заходи — освітні кампанії, фінансова грамотність та підвищення обізнаності — повинні доповнювати правоохоронні та моніторингові механізми** для зменшення масштабів вербування грошових мулів.

Завершальні розділи присвячені превентивним заходам і стримуванню. Автори детально аналізують роль фінансової освіти, інформаційних кампаній, діяльності кіберполіції та використання поведінкових інсайтів для зменшення вразливості населення до вербування. Паралельно розглядається питання кримінально-правової відповідальності та можливого перегляду статті 200 Кримінального кодексу України, при цьому підкреслюється ризик надмірної криміналізації молоді та соціально вразливих груп. У фіналі документа формується висновок про необхідність переходу від ситуативної взаємодії до інституціоналізованої, операційно орієнтованої системи державно-приватного партнерства, що поєднує правову визначеність, спільну аналітику, технологічну інтеграцію та довгострокову стратегічну координацію у сфері протидії відмиванню коштів і фінансовому шахрайству.

Регулювання

Регуляторна архітектура FCA для криптоактивів: аналіз Консультаційного документа CP26/4 [7]



Орган фінансового регулювання та нагляду Сполученого Королівства (FCA) опублікував Консультаційний документ CP26/4 «Застосування Довідника FCA до регульованої діяльності з криптоактивами — частина II». Цей документ є логічним продовженням масштабної регуляторної реформи, розпочатої після прийняття у грудні 2025 року законодавства, яке вперше комплексно вводить діяльність із криптоактивами під повноцінний нагляд FCA, прирівнюючи її за регуляторним статусом до традиційних фінансових послуг. Кінцевий термін подання консультаційних зауважень — 12 березня 2026 року. Для розуміння значущості цього документа критично важливо усвідомити регуляторний контекст: Сполучене Королівство, вийшовши з ЄС і втративши автоматичне застосування регламенту MiCA, формує власний регуляторний шлях для криптоактивів, і CP26/4 фіксує конкретну операційну архітектуру цього шляху.

Центральним елементом консультаційного документа є застосування принципу Consumer Duty (Принцип 12 Довідника FCA) до регульованої діяльності з криптоактивами. Consumer Duty — це не просто стандарт «не завдавай шкоди», а позитивне зобов'язання фірм досягати добрих результатів для споживачів, що складається з трьох наскрізних зобов'язань та чотирьох правил. Три наскрізні зобов'язання охоплюють: (i) дії в інтересах споживача; (ii) уникнення заподіяння шкоди; (iii) надання підтримки для досягнення фінансових цілей споживача. Чотири правила регулюють якість продуктів і послуг, ціноутворення та цінність, комунікацію та підтримку споживачів. Для криптовалютних бірж, кастодіальних провайдерів та ринків токенів це означає перехід від disclosure-based парадигми до outcomes-based standard, що підвищує вимоги до внутрішнього комплаєнсу.

Особливу увагу з точки зору ПВК/ФТ/ФР заслуговує блок положень щодо захисту клієнтських криптоактивів та кастодіальної діяльності над криптоактивами. CP26/4 пропонує детальні вимоги до сегрегації активів клієнтів, технічних стандартів збереження (включаючи вимоги до cold/hot wallet розподілу), процедур аварійного відновлення та управління ризиком контрагента при зберіганні. Регулятор вводить поняття «specified investment cryptoasset» для кастодіальної діяльності — це технічна категоризація, яка визначає, до яких активів застосовуються найвищі стандарти захисту. Для ПВК/ФТ-комплаєнсу ці вимоги є критичними: вони визначають, де фізично зберігаються активи, які процедури передачі існують, та яка відповідальність фірми при крадіжці або нестачі.

Проблематика роздрібного кредитування та позик у криптоактивах є одним із найбільш аналітично насичених розділів CP26/4. FCA визнає, що ринок криптопозик є якісно новим ризиком для споживачів, що не вкладається в традиційні категорії фінансового ризику. Документ встановлює особливі вимоги для використання роздрібними споживачами власних криптоактивів як забезпечення, включаючи вимоги до волатильності, маржинальних вимог та процедур примусової ліквідації. Принципово важливою нормою є заборона придбання криптоактивів за кредитними картками — FCA розглядає це як неприйнятне поєднання споживчого кредитного ризику з інвестиційним ризиком у сфері, де волатильність активів може

[7] https://www.fca.org.uk/publication/consultation/cp26-4.pdf

призводити до миттєвої нездатності погасити кредитну заборгованість. З перспективи ПВК/ФТ, вимоги до роздрібного кредитування криптоактивів встановлюють додатковий рівень ідентифікації джерела коштів, що може використовуватися для виявлення незвичних моделей поведінки.

Системний підхід до регулювання персональної відповідальності займає значне місце в CP26/4. FCA пропонує диференційований підхід до оцінки криптофірм у рамках SM&CR залежно від обсягу та складності регульованої діяльності. Для великих платформ передбачається повноцінне застосування SM&CR категорії «Enhanced», тоді як для менших фірм — спрощена «Core» категорія. Це має безпосередні наслідки для ПВК/ФТ/ФР: режим SM&CR встановлює персональну відповідальність конкретних керівників за відповідність системам комплаєнсу, включаючи функцію MLRO (Money Laundering Reporting Officer). У поєднанні з вимогами до навчання та компетентності (Training & Competence, T&C), що містяться в CP26/4, це формує цілісну систему персональної підзвітності, де недотримання ПВК/ФТ-процедур може мати безпосередні наслідки для персональних ліцензій керівників криптофірм.

Вимоги до регуляторної звітності (SUP 16) та міжнародне вимірювання консультаційного документа є особливо значущими для транскордонної діяльності. CP26/4 встановлює детальні вимоги до регулярного регуляторного звітування, включаючи операційні дані, скарги споживачів, показники ліквідності та технічні збої. Для фірм із транскордонною діяльністю принципово важливою є «політика розміщення»: FCA вимагає від іноземних фірм, що обслуговують британських клієнтів, реєстрації юридичної особи у Сполученому Королівстві. Це напряму кореспондує з рекомендаціями FATF щодо розміщення регульованих VASP у юрисдикціях, де забезпечується ефективний нагляд. FCA підтверджує відповідність CP26/4 міжнародним стандартам FATF, рекомендаціям IOSCO щодо регулювання криптоактивів (CDA Recommendations) та рекомендаціям Ради фінансової стабільності (FSB). Особливо важливою є демографічна деталь звіту: власники криптоактивів у Великій Британії непропорційно молоді (переважно до 34 років), чоловічої статі та з доходами вище середнього — ця характеристика впливає на профілювання ризиків та таргетування освітніх програм для споживачів.

Метрики успіху, зазначені в CP26/4, є показовими для розуміння регуляторних пріоритетів FCA: індикатори конкуренції (ринкові частки, бар'єри входу), дослідження споживчої довіри, моніторинг рівня злочинності (включаючи криптошахрайство та ВК), кількість авторизованих фірм. Визначення рівня злочинності як явного індикатора успіху регуляторної реформи є принципово важливим сигналом: FCA розглядає боротьбу з криптозлочинністю не лише як побічну мету, а як центральний критерій ефективності регулювання. Це означає, що ПВК/ФТ-вимоги є не обтяженням, а ключовою метрикою

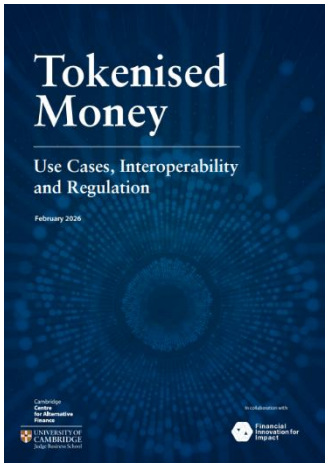
Висновки:

- **Бюджетування регуляторних витрат:** Фінансові установи мають закласти в бюджети на 2026/27 роки зростання зборів, особливо в сегментах високого ризику (крипто, перекази), що вимагає оптимізації внутрішніх комплаєнс-процесів для зниження ризик-профілю.
- **Інвестиції в якість даних:** З огляду на перехід FCA до дата-центричного нагляду, фірми повинні провести аудит своїх систем звітності, щоб забезпечити «data integrity» та уникнути штрафних нарахувань за некоректні дані.
- **Синхронізація ПВК та кібербезпеки:** Необхідно інтегрувати протоколи кіберзахисту в загальну систему фінансового моніторингу, оскільки FCA розглядає ці сфери як єдиний контур операційної стійкості.
- **Адаптація до Consumer Duty:** Комплаєнс-стратегія має включати механізми захисту клієнтів від шахрайства як частину регуляторної відповідності, що впливає на розмір внесків до компенсаційних фондів.

регуляторної відповідності для криптофірм у Великій Британії. Для українських СПФМ та регуляторів, що спостерігають за міжнародними підходами, CP26/4 є важливим прикладом для порівняльного аналізу власних підходів до регулювання надавачів послуг із криптоактивами в контексті вимог Рекомендації FATF 15.

Звіти окремих інституцій та експертів

Токенізовані гроші у глобальній фінансовій системі: регуляторні виклики та ризики нового покоління платіжних інструментів [8]



Cambridge Centre for Alternative Finance (CCAF) Кембриджської школи бізнесу спільно з організацією Financial Innovation for Impact (Fii) опублікував масштабне дослідження «Tokenised Money: Use Cases, Interoperability and Regulation». Документ є результатом дев'ятимісячного дослідницького проекту, що включав 21 структуроване інтерв'ю з представниками провідних учасників ринку (великі інвестиційні та комерційні банки, платіжні мережі, емітенти стейблкоїнів, блокчейн-інфраструктурні компанії), регуляторів та міжнародних органів стандартизації — зокрема, BIS, EBA, IOSCO, Fed, MAS, HKMA. Методологія поєднує якісний аналіз на основі глибинних інтерв'ю з кількісною обробкою відповідей за шкалою від 1 до 10, що дозволяє формалізувати суб'єктивні оцінки ринкових гравців. Базою порівняльного регуляторного аналізу стали п'ять ключових юрисдикцій: ЄС, Гонконг, Японія, Сінгапур та США.

Концептуальна основа дослідження виходить з необхідності чіткої таксономії токенізованих грошових інструментів, відсутність якої дотепер є однією з ключових перешкод для ефективного регулювання. Автори пропонують двошарову класифікаційну рамку, що оцінює інструменти за чотирма базовими вимірами: природа вимоги (claim), характер забезпечення (backing), форма (form) та рівень доступу (access). На цій основі виокремлюються чотири широкі категорії: цифрові гроші центральних банків (CBDC), вимоги до комерційних банків / токенізовані депозити, вимоги, забезпечені фіатними коштами (стейблкоїни з фіатним забезпеченням) та активи прив’язані до фіатної валюти. Ця таксономія принципово важлива для AML-регулювання, оскільки кожна з категорій має різну архітектуру ризиків відмивання коштів: CBDC перебувають під прямим контролем центрального банку, тоді як стейблкоїни, особливо за умов операцій через публічні блокчейни із відкритим доступом (public permissionless blockchains), можуть функціонувати у практично повністю дерегульованому середовищі.

Документ ідентифікує чотири первинних варіанти використання токенізованих грошей, що визначають їхню актуальність для фінансового сектору: транскордонні платежі та розрахунки; управління казначейством та ліквідністю; цифровізація торгового фінансування; та інфраструктура ринків капіталу. Для кожного з варіантів автори проводять двовимірну оцінку — стратегічний пріоритет ринку та готовність до імплементації — що дозволяє виявити кейси «зрілих» і «незрілих» застосувань. Стейблкоїни, перш за все USDT Tether та USDC Circle, що разом сформували ринок обсягом понад 250 млрд доларів США, демонструють найвищий рівень готовності саме для транскордонних платежів і торгових розрахунків в децентралізованих фінансах (DeFi). Токенізовані депозити (tokenised deposits), натомість,

[8] https://www.jbs.cam.ac.uk/wp-content/uploads/2026/02/2026-ccaf-tokenised-money-use-cases-interoperability-and-regulation.pdf

позиціонуються як перспективний інструмент для інституційного казначейства, що поєднує знайомі банківські відносини з цифровою ефективністю.

Аналіз інтероперабельності є одним з методологічно найбільш опрацьованих розділів дослідження. Автори розрізняють п'ять вимірів інтероперабельності: транскордонна ефективність, крос-платформена взаємодія, крос-активна інтеграція, регуляторна гармонізація та координація управління. Аналізуються чотири конкретних ініціативи: Partior, Project Guardian (MAS), Regulated Settlement Network (RSN) та Project Agorá (BIS). Ці проекти ілюструють дві принципово різних архітектурних стратегії — консорціумні приватні мережі та публічні блокчейни з доданими шарами конфіденційності — кожна з яких має специфічні компроміси між ефективністю, прозорістю та контрольованістю для AML-цілей. Консорціумні мережі забезпечують кращу ідентифікацію учасників, але обмежені вузьким колом авторизованих учасників. Публічні блокчейни з «privacy layers» дозволяють більш широку участь, але потенційно розмивають ланцюг ідентифікації транзакцій.

Програмованість розглядається авторами як акселератор впровадження — не самоціль, а механізм реалізації більш складних фінансових операцій у автоматизованому режимі. Вже функціонують пілотні застосування: автоматизація торгового фінансування (trade-finance automation), параметричне страхування та оптимізація казначейства на базі штучного інтелекту. Регуляторний ракурс аналізу програмованості є особливо цінним: смарт-контракти, що вбудовують правила AML/CFT безпосередньо в протокол транзакцій (compliance-by-design), є перспективним, але поки що неурегульованим підходом. Питання про те, яким чином вбудований комплаєнс взаємодіє з вимогами FATF щодо моніторингу транзакцій у режимі реального часу та зупинення платежів на вимогу регуляторів, залишається відкритим.

Регуляторний ландшафт, змальований у четвертому розділі, визначається кількома ключовими тезами. AML/CFT та ризики незаконного фінансування ідентифіковані регуляторами як топ-пріоритет поряд із кібербезпекою та операційною стійкістю і фінансовою стабільністю. Ризики для монетарного суверенітету — зокрема, домінування

Висновки:

- Відсутність загальновизнаної таксономії токенізованих грошей залишається основним структурним бар'єром для ефективної AML-регуляції: фахівці з комплаєнсу мають вже зараз формувати власне розуміння категоріальних відмінностей між токенізованими депозитами, стейблкоїнами та tokenised MMFs — оскільки кожен із цих інструментів вимагає різного підходу до верифікації клієнта та моніторингу транзакцій.
- Домінування USD-деномінованих стейблкоїнів у транскордонних платежах і торговому розрахунку є не лише монетарно-суверенним ризиком, але і ризиком ВК/ФТ: USDT та USDC широко використовуються для обходу фінансових санкцій та розрахунків у тіньовій торгівлі, що вимагає від СПФМ підвищеної уваги до транзакцій з цими активами через неліцензовані або офшорні VASP.
- Compliance-by-design через смарт-контракти є перспективним, але регуляторно неурегульованим підходом — і до появи чіткої правової рамки його не можна розглядати як замінник традиційних AML-контролів; пілотні проєкти (Project Guardian, Project Agorá) слід відстежувати як орієнтири розвитку стандартів.
- Прискорення регуляторних процесів після прийняття Genius Act у США та запровадження MiCA в ЄС неминуче призведе до «регуляторної гонки» у токенізованих фінансах, що вимагає від підрозділів комплаєнсу постійного моніторингу змін у 5 ключових юрисдикціях-лідерах (ЄС, США, Гонконг, Сінгапур, Японія) та оперативного коригування внутрішніх процедур.

деномінованих у доларах США стейблкоїнів — набувають особливої актуальності для регуляторних дискусій в країнах, що розвиваються, де ризик доларизації та виходу капіталу є невід'ємними від широкого поширення USDT/USDC. Прийняття в 2025 році американського Genius Act, який легалізує і регулює платіжні стейблкоїни з явно задекларованою метою просування міжнародного використання долара США, стало каталізатором прискорення регуляторних процесів в інших юрисдикціях, спонукавши до конкурентної регуляторної гонки.

Порівняльний аналіз регулювання стейблкоїнів у п'яти юрисдикціях виявляє суттєві розбіжності, зокрема у вимогах до резервних активів та вимогах щодо створення дочірньої компанії іноземними емітентами. ЄС у рамках MiCA запровадив строгі пруденційні вимоги та принцип обов'язкового отримання ліцензії CASP, тоді як низка інших юрисдикцій зберігає менш жорсткий реєстраційний режим. Гармонізація цих підходів є критичним завданням — саме регуляторна фрагментація створює структурне підґрунтя для офшорних VASP, які, як зазначено у доповіді FATF від лютого 2026 року, являють собою одну з ключових загроз ВК.

Документ CCAF є вичерпним академічним свідченням того, що регуляторне мислення у сфері AML/CFT щодо токенізованих грошей ще значно відстає від темпів розвитку ринку. Відкриті питання, які визначать наступний цикл регуляторної відповіді, включають: правовий статус смарт-контрактів у транзакціях; режим нагляду за публічними permissionless блокчейнами як інфраструктурою для системно значущих платіжних інструментів; та механізми «технологічно нейтрального» застосування вимог KYC/CDD до операцій з токенізованими депозитами.

Аналіз ефективності санкційної політики: Структурні лазівки та геополітика обходу [9]

Звіт інституту ifo є одним з найґрунтовніших економічних аналізів сучасної системи міжнародних обмежень. Автори використовують методологію порівняльного аналізу торговельних потоків, зосереджуючись на феномені «mirror statistics discrepancies». Логіка дослідження полягає в тому, що санкції не можуть бути ефективними, поки існують юрисдикції, які готові виконувати роль «чорних ходів» для підсанкційної економіки. Аналіз демонструє, що після запровадження масштабних санкцій проти РФ, експорт з ЄС до таких країн як Туреччина, ОАЕ, Казахстан та Киргизстан зріс на сотні відсотків. Юридичний нюанс, який висвітлюють автори, полягає в тому, що ці товари (часто подвійного призначення) офіційно прямують до місцевих споживачів у Центральній Азії, але фактично реекспортуються до РФ або навіть не перетинають кордони заявлених країн призначення, що класифікується як «ghost trade».

Глибокий аналіз «ghost trade» (примарної торгівлі) виявляє системні прорахунки в митному контролі ЄС та системі фінансового моніторингу банків-кореспондентів. Регуляторна логіка, за якою працюють фінансові установи, часто обмежується перевіркою санкційних списків, тоді як реальний ризик полягає в товарній номенклатурі. Звіт ifo наводить статистику щодо товарів групи «Common High Priority Items» (мікросхеми, датчики, навігаційне обладнання), експорт яких до країн-посередників аномально зріс саме в періоди посилення санкцій. Для фахівця з ПВК/ФТ це означає, що традиційний KYC (Know Your Customer) є недостатнім, і необхідно переходити до KYCC (Know Your Customer's Customer) та аналізу логістичних ланцюжків. Документ впроваджує термін «circumvention hubs» (хаби обходу), які стають критичними

[9] https://www.ifo.de/DocDL/EconPol_PolicyBrief_80.pdf

точками ризику. Статистичні дані показують, що понад 80% критичних компонентів для російської оборонної промисловості все ще є складовими західних технологій, легалізованих через треті країни.

Юридичні нюанси санкційного режиму також стосуються визначення «контролю» над юридичними особами. Звіт ifo вказує на те, що російські олігархи та державні компанії успішно використовують номінальних власників у «дружніх» юрисдикціях для управління активами в Європі. Логіка регулятора (зокрема OFAC та DG FISMA) починає схилятися до принципу «substance over form», де реальна економічна вигода є визначальною для накладення санкцій. Однак, звіт критикує повільність цього процесу. Аналіз нафтових танкерів тіньового флоту демонструє, як РФ вдається обходити цінову стелю на нафту. Використання старих суден з невідомими страховиками та складною структурою власності дозволяє перевозити нафту без залучення західних сервісів. Для банківського сектора це створює величезні ризики при фінансуванні морської торгівлі, оскільки ідентифікація приналежності судна до «тіньового флоту» вимагає специфічної розвідки.

Статистика, наведена в документі, вказує на те, що ВВП РФ скоротився значно менше, ніж прогнозувалося, саме завдяки адаптації торговельних мереж. Автори впроваджують концепцію «sanctions fatigue» (втоми від санкцій) серед приватного сектора, де компанії шукають будь-які юридичні шпарини для збереження ринків збуту. Регуляторна логіка майбутніх пакетів санкцій, на думку ifo, має зміститися в бік «вторинних санкцій» (secondary sanctions) проти фінансових установ третіх країн. Це радикально змінює ландшафт для комплаєнс-офіцерів: тепер банк у Казахстані або ОАЕ може втратити доступ до доларових розрахунків лише за проведення транзакції на користь російського контрагента. Звіт детально описує механізм «re-export markup», де посередники додають 20–50% до ціни товару за ризик, що створює величезні корупційні капітали в країнах-хабах, які згодом також потребують відмивання.

Особлива увага приділяється ролі криптовалют у обході фінансових обмежень. Хоча обсяги крипто-транзакцій все ще менші за традиційні банківські перекази, їхнє використання для розрахунків за паралельний імпорт стабільно зростає. Юридичні нюанси використання стейблкоїнів (наприклад, USDT) дозволяють здійснювати миттєві транскордонні платежі поза системою SWIFT. Логіка регуляторів тепер вимагає від криптобірж блокування не лише адрес підсанкційних осіб, а й цілих кластерів гаманців, що демонструють ознаки зв'язку з російськими операторами. Статистичні дані звіту підтверджують, що використання децентралізованих фінансів (DeFi) для обходу санкцій є зростаючим

Висновки:

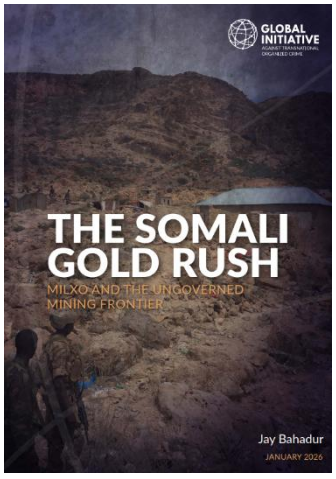
- **Торговельний комплаєнс (TBML):** Фінансові установи повинні інтегрувати перевірку кодів HS (Harmonized System) у свої системи моніторингу транзакцій, блокуючи платежі за критичні компоненти, якщо отримувач знаходиться в країні-хабі без реальних виробничих потужностей.
- **Управління ризиками вторинних санкцій:** Необхідно провести повний аудит банків-кореспондентів у країнах СНД, Туреччині та ОАЕ, вимагаючи від них підтвердження наявності суворих санкційних фільтрів, еквівалентних стандартам G7.
- **Моніторинг логістики (Know Your Logistics):** Для операцій з торговельного фінансування обов'язковим стає надання документів, що підтверджують фактичне прибуття товару в країну призначення (митна декларація імпорту), для виявлення схем «ghost trade».
- **Технологічний скринінг:** Комплаєнс-системи мають бути налаштовані на виявлення компаній оболонок, створених після лютого 2022 року, які займаються торгівлею високотехнологічними товарами в регіонах, межуючих з підсанкційними територіями.

трендом, який поки що важко контролювати через відсутність єдиного регуляторного органу в цьому просторі.

Звіт ifo також аналізує вплив санкцій на технологічний суверенітет. Попри успішний обхід, РФ стикається з деградацією промислового обладнання, оскільки сервісне обслуговування та оновлення ПЗ неможливо повністю замінити через посередників. Для ПВК-аналітиків це важливий індикатор: транзакції на великі суми за «запчастини» від компаній, що існують менше року, є класичним «червоним прапорцем». У документі підкреслюється, що ефективність санкцій залежить не від кількості заборон, а від якості їхнього виконання (enforcement). Автори закликають до створення єдиного санкційного агентства ЄС з широкими повноваженнями, аналогічного американському OFAC. Це призведе до уніфікації вимог та зникнення можливостей для «forum shopping» — вибору юрисдикції ЄС з найм'якшим наглядом.

Країна-посередник	Зростання експорту з ЄС (%)	Ключові групи товарів	Рівень ризику обходу (High/Medium)
Киргизстан	+800%	Електроніка, автозапчастини	High (Ghost trade)
Вірменія	+400%	Мікросхеми, побутова техніка	High (Re-export)
Туреччина	+150%	Промислове обладнання	Medium (Complex supply chains)
ОАЕ	+200%	Предмети розкоші, золото	High (Financial layering)

Нелегальний видобуток золота в Сомалі у контексті ПВК/ФТ та регіональної безпеки [10]



Документ присвячений комплексному аналізу стрімкого розвитку нелегального золотодобувного сектору в районі Мілксо на північному сході Сомалі та його інтеграції у міжнародні торговельні й фінансові ланцюги через інфраструктуру країн Перської затоки, насамперед Об'єднаних Арабських Еміратів. Дослідження розглядає цей регіон як приклад некерованого ресурсного простору, у якому поєднуються слабкість державних інституцій, політико-територіальна фрагментація, міжкланова конкуренція, елітна корупція та вплив збройних угруповань, що в сукупності створює сприятливе середовище для розвитку тіньової економіки.

У звіті показано, що трансформація Мілксо з невеликого старательського поселення у великий гірничий центр відбулася протягом відносно короткого періоду без будь-якої системної участі держави. Зростання чисельності населення, поява десятків видобувних майданчиків, неформальних переробних пунктів і торговельних мереж відбувалися в умовах повної відсутності ліцензування, просторового планування та екологічного контролю. Територія перебуває у зоні конкуренції між

[10] https://globalinitiative.net/wp-content/uploads/2026/01/Jay-Bahadur-The-Somali-gold-rush-Milxo-and-the-ungoverned-mining-frontier-GI-TOC-January-2026.pdf

федеральним урядом Сомалі, адміністрацією Пунтленду та іншими регіональними структурами, що призвело до формування правового вакууму, в межах якого жоден орган влади не здатний ефективно реалізувати свої повноваження.

Особливу увагу автор приділяє аналізу нормативно-правового середовища. Конституційна модель Сомалі передбачає спільне управління природними ресурсами між центром і регіонами, однак у сфері надрокористування відсутні узгоджені рамкові акти, процедури ліцензування та механізми розподілу доходів. У Пунтленді не сформовано повноцінну систему гірничого регулювання, а відповідні міністерства мають обмежені кадрові та фінансові ресурси. Федеральний уряд формально вважає більшість операцій у Мілксо незаконними, проте не володіє інструментами для їх припинення. У результаті формується ситуація множинної юрисдикції без реального управління.

У таких умовах у Мілксо склалася напівформальна економіка видобутку, у якій домінують тимчасові об'єднання підприємців, місцевих посередників і технічних спеціалістів. Більшість так званих компаній не має чітко визначеного юридичного статусу, не веде системного бухгалтерського обліку та не підпадає під податковий нагляд. Видобуток і первинна переробка здійснюються з використанням ртуті, ціанідів та інших небезпечних реагентів, що створює довгострокові загрози для здоров'я населення та довкілля. Екологічні наслідки, зокрема забруднення водних ресурсів і деградація ґрунтів, залишаються поза межами будь-якого державного реагування.

Важливим аналітичним блоком документа є дослідження феномену елітного захоплення ресурсів. Автор демонструє, що ключові позиції у секторі займають компанії та посередницькі структури, пов'язані з політичним керівництвом Пунтленду та впливовими кланами. Через мережу проксі-власників, родинних зв'язків і непрозорих корпоративних схем відбувається концентрація контролю над видобутком і торгівлею золотом. Це супроводжується використанням доступу до державних контрактів, донорських програм і адміністративних ресурсів для зміцнення приватних економічних позицій, що перешкоджає формуванню конкурентного та прозорого ринку.

Окремий розділ присвячено ролі збройних угруповань у функціонуванні золотого сектору. У звіті задокументовано системні спроби «Аш-Шабаб» інтегрувати Мілксо у власну фінансову інфраструктуру шляхом запровадження примусового «оподаткування», рекету, викрадень та тиску на операторів. Наводяться приклади телефонних перехоплень, свідчень місцевих мешканців і даних

Висновки:

- **Видобуток золота в районі Мілксо здійснюється в умовах інституційної фрагментації та відсутності узгодженої системи регулювання** між федеральним і регіональними рівнями влади, що унеможливлює ефективний державний контроль, ліцензування та оподаткування сектору.
- **Золотодобувний сектор характеризується домінуванням напівформальних компаній і пов'язаних із політичними елітами структур,** що призводить до системного елітного захоплення ресурсів і блокування формування прозорої моделі управління надрами.
- **Збройні угруповання, насамперед «Аш-Шабаб», використовують золотий сектор як джерело фінансування через примусове «оподаткування» та тиск на операторів,** що створює сталий зв'язок між видобутком ресурсів і безпековими ризиками.
- **Експорт золота з Мілксо до ОАЕ здійснюється через кур'єрські канали зі спрощеним документальним супроводом і відсутністю належної перевірки походження,** що дозволяє інтегрувати нерегульоване золото у глобальний ринок із мінімальним рівнем простежуваності.

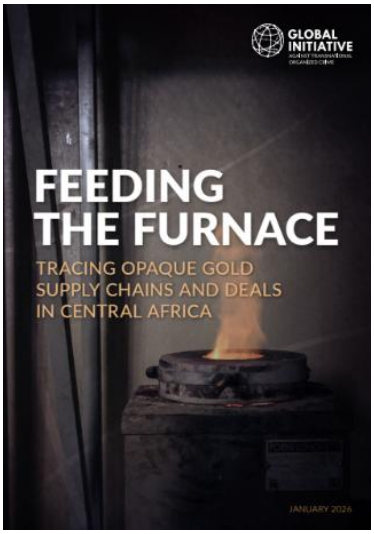
безпекових структур, які підтверджують регулярність таких практик. Хоча прямий територіальний контроль угруповання є нестабільним, його фінансовий вплив залишається постійним фактором ризику.

Значну частину дослідження присвячено аналізу ланцюга постачання золота від місця видобутку до міжнародних ринків. Основний маршрут проходить через портове місто Босасо та далі авіарейсами до Дубаю. Перевезення здійснюється індивідуальними кур'єрами, які транспортують напівоброблені злитки без маркування та сертифікації. Документація обмежується мінімальними митними деклараціями, що не містять інформації про джерело походження, законність видобутку чи екологічну відповідність. У Дубаї золото потрапляє до торговців і переробників у межах спрощених процедур, після чого втрачає будь-які ознаки ризикового походження.

На основі інтерв'ю з учасниками ринку автор показує, що формальна легальність імпортних процедур підміняє реальний комплаєнс і належну перевірку. Попри задекларовані зобов'язання щодо відповідального постачання та протидії торгівлі конфліктними ресурсами, практичний контроль за сомалійським золотом залишається обмеженим. Це створює структурну можливість для інтеграції нелегального ресурсу у глобальну фінансову систему без істотних бар'єрів.

У підсумку звіт інтерпретує феномен Мілксо як прояв глибших проблем сомалійської державності, зокрема незавершеного федералізму, слабкості фіскальних інститутів, дефіциту верховенства права та хронічної залежності від неформальних економічних мереж. Відсутність доходів від видобутку для державного бюджету, поєднання економічних і безпекових ризиків, деградація довкілля та інституційна корупція формують замкнене коло нестабільності. Документ демонструє, що золотий бум у Мілксо не є локальним явищем, а інтегрований у глобальні торговельні та фінансові процеси, що робить його важливим прикладом для аналізу взаємозв'язку між природними ресурсами, фінансовою злочинністю та слабкими державами.

Золота лихоманка по-африканськи: Як ОАЕ, Руанда та ДР Конго перетворили конфлікт на бізнес-модель [11]



У січні-лютому 2025 року, коли повстанці руху M23 за підтримки Руанди увійшли до Гоми, а згодом і до Букаву — столиці золотоносної провінції Південне Ківу, міжнародна спільнота знову зосередила увагу на кривавому конфлікті на сході Демократичної Республіки Конго (ДРК). Звичні наративи про етнічну напруженість та політичну нестабільність, однак, часто маскують справжню рушійну силу цієї війни: боротьбу за доступ до надзвичайно прибуткових ресурсів. Звіт Глобальної ініціативи проти транснаціональної організованої злочинності (GI-TOC) проливає світло на складний, опортуністичний і часто цинічний ринок золота, головними дійовими особами якого виступають не лише регіональні гравці, але й глобальний фінансовий гігант — Об'єднані Арабські Емірати (ОАЕ).

Все почалося наприкінці 2022 року, коли ДРК, відчуваючи гостру військову загрозу з боку M23, розпочала переговори з ОАЕ. Результатом стало створення спільного підприємства Primera Gold DRC SA, де 55% отримала зареєстрована в ОАЕ компанія

[11] https://globalinitiative.net/wp-content/uploads/2026/01/feeding-the-furnace-tracing-gold-supply-chains-and-deals-in-central-africa-gitoc-january-2026.pdf

Primera Group Limited, а 45% — уряд ДРК. На папері це виглядало як ідеальна угода: президент Фелікс Чісекеді особисто презентував перший злиток «справедливої торгівлі», стверджуючи, що проєкт має на меті подолати багаторічну контрабанду золота до Руанди та очистити галузь.

За лаштунками угоди стояли не лише декларації про співпрацю, а й конкретні військові домовленості. Ключову роль у формуванні партнерства відіграв радник президента ДРК Кахумбу Мандунгу Була (відомий як Као), який, за даними джерел, був причетний до залучення військової допомоги з ОАЕ для боротьби з М23. Емірати постачали зброю, гелікоптери та транспорт, фактично купуючи собі доступ до конголезького золота. Водночас структура самого підприємства була глибоко вплетена в елітні кола Абу-Дабі. Представником Primera Group Limited виступив бізнесмен Сібтейн Алібхай, який, за іронією долі, ще у 2012 році фігурував у звітах експертів ООН через компанію AR Gold, яка, за даними слідства, купувала золото з районів, контрольованих збройним угрупуванням NDC, чий лідер згодом був засуджений за воєнні злочини.

Корпоративна структура Primera Group Limited вказує на ще глибші зв'язки. Адресою компанії значилася штаб-квартира Royal Group, конгломерату, який очолює шейх Тахнун бін Заїд Аль Нагаян, радник з національної безпеки ОАЕ та брат президента. Інвестором виступила компанія International Holding Company (IHC), також під головуванням шейха Тахнуна. У липні 2023 року Алібхая та конголезького міністра Адель Каїнду на посадах директорів змінили два громадяни ОАЕ, один з яких, Алі Рашид, був директором з розвитку бізнесу в IHC та директором золотопереробного заводу Auric Hub Ltd — єдиного номінованого покупця золота Primera. Таким чином, контроль над спільним підприємством став безпосереднім.

Але поки ОАЕ поглиблювали співпрацю з ДРК, вони не забували і про альтернативний маршрут. Дані свідчать, що десятки тонн золота продовжували надходити до ОАЕ з Руанди, яку звіти ООН прямо звинувачують у підтримці М23. Частина цього золота проходила через компанії, пов'язані з бельгійським бізнесменом Аленом Гьотцем, який перебуває під санкціями США та ЄС за торгівлю золотом зі збройними групами. Його колишнє підприємство в Руанді, Gasabo Gold Refinery, також потрапило під санкції ЄС у березні 2025 року. І попри це, 1 лютого 2025 року, коли М23 вже контролювали Гому, високопоставлений дипломат ОАЕ шейх Шахбут бін Нахаян зустрівся в Кігалі з президентом Руанди Полем Кагаме, щоб обговорити зміцнення двосторонньої співпраці. Це виглядає як відверте хеджування ставок: поки один проєкт занепадав через війну, Емірати готувалися до співпраці з переможцем.

Зрештою, у серпні 2024 року, на фоні успіхів М23, ОАЕ вийшли з угоди, залишивши Primera Gold (перейменовану на DRC Gold Trading) у руках конголезького уряду, який тепер шукав нових інвесторів. Однак справжні масштаби проблеми розкриваються не в політичних маневрах, а на землі — там, де видобувалося це золото. Польові дослідження GI-TOC у трьох ключових районах Південного Ківу, звідки Primera отримувала сировину, демонструють системне нехтування обіцянками.

У районі Лухіхі, який став пілотним проєктом, дослідники зафіксували масштабне використання дитячої праці. Діти віком від 14 років працювали в шахтах, займаючись копанням, промиванням та транспортуванням руди. Місцеві вчителі скаржилися на зростання рівня відсіву в школах та поширення шкідливих звичок серед підлітків. Хоча в березні 2023 року Міністерство гірничої справи надало копальням навколо Лухіхі статус «блакитних», що дозволяло Primera купувати там золото, це не зупинило порушень. Попри обіцянки компанії інвестувати в соціальну сферу, місцева школа L'Institut Bwimika залишалася в жалюгідному стані з дірявими стінами та земляною підлогою. Крім того, старателі масово використовували ртуть для вилучення золота, що призводило до забруднення земель та водойм, роблячи їх непридатними для сільського господарства — традиційного заняття місцевих громад.

Ще більш тривожна ситуація склалася в районі Місісі, одному з найбільших центрів кустарного видобутку в провінції. Саме тут, за даними GI-TOC, Primera Gold купила понад тонну золота з копалень сектору Нганджа та десятки кілограмів з сектору Мутамбала. І саме тут дослідники зібрали численні докази того, що видобуток контролювався та оподатковувався збройним угрупуванням «Маї-Маї Якутумба», яке входить до коаліції CNPSC під проводом Вільяма Амурі Якутумби. Останній був внесений до санкційного списку Ради Безпеки ООН у лютому 2024 року за незаконну торгівлю ресурсами, зґвалтування та інші форми сексуального насильства.

GI-TOC отримала копії документів CNPSC, які підтверджують систематичне оподаткування гірничих робіт у 2022-2024 роках. Крім того, свідчення місцевих старателів, торговців та членів кооперативів описують регулярну сплату податків «на військові зусилля» бійцям Якутумби. Торговці сплачували фіксовані щомісячні суми, власники шахт платили за використання помп, а простих копачів обкладали даниною на блокпостах, іноді застосовуючи насильство. Люди платили зі страху, визнаючи, що держава не здатна їх захистити. Таким чином, Primera Gold, формально купуючи золото в офіційних кооперативах, де-факто стала частиною ланцюжка постачання, який фінансував збройне угрупування, що чинило насильство.

Найбільш кричущим прикладом нехтування обіцянками та законодавством став видобуток у лісовому заповіднику Ітомбве. Ця територія, створена для захисту рідкісних видів, включаючи рівнинну горилу, та визнана охоронюваною зоною, з вересня 2023 року стала ареною промислового видобутку золота за допомогою днопоглиблювальних машин (драг). Ці плавучі установки, керовані, за непідтвердженою інформацією, бізнесменами з Букаву, використовують потужні насоси для всмоктування золотоносного піску з дна річок, завдаючи незворотної шкоди екосистемі. Драги працювали цілодобово в зоні заповідника, що прямо заборонено законом про охорону природи. Водолази пірнали кожні дві години, видобуваючи до 18 грамів золота за одне занурення, а для амальгамації знову використовувалася ртуть. Місцеві жителі вирубували дерева в заповіднику для будівництва плотів, що обслуговували драги.

Висновки:

- **Об'єднані Арабські Емірати стали головним світовим покупцем африканського золота, значна частина якого є нелегальною або походить із зон конфліктів.** Виключення ОАЕ з "сірого списку" FATF було передчасним, оскільки не врахувало реальних ризиків, пов'язаних із золотим сектором.
- **Дослідження демонструє цинічний опортунізм ОАЕ**, які одночасно підтримували і законний уряд ДРК, і його супротивників. Це свідчить про те, що для Еміратів доступ до ресурсів є пріоритетом, що виправдовує співпрацю з усіма сторонами конфлікту, поглиблюючи нестабільність у регіоні.
- **Ні уряд ДРК, ні банки, що обслуговували угоду, ні міжнародні наглядові органи не виконали належним чином свої функції.** Міжнародна спільнота, включно з FATF та ЄС, фактично "відмила" репутацію ОАЕ, не звернувши уваги на кричущі порушення в її золотому секторі.

Дані внутрішньої звітності Primera Gold свідчать про те, що з травня 2023 по квітень 2024 року компанія 76 разів купувала золото з Ітомбве. Причому після появи драг у вересні обсяги закупівель різко зросли: за п'ять місяців до вересня було придбано 65 кг, а за наступні п'ять — майже 90 кг. Хоча неможливо довести, що компанія купувала золото безпосередньо у власників драг, збіг у часі та зростанні обсягів є надто промовистим.

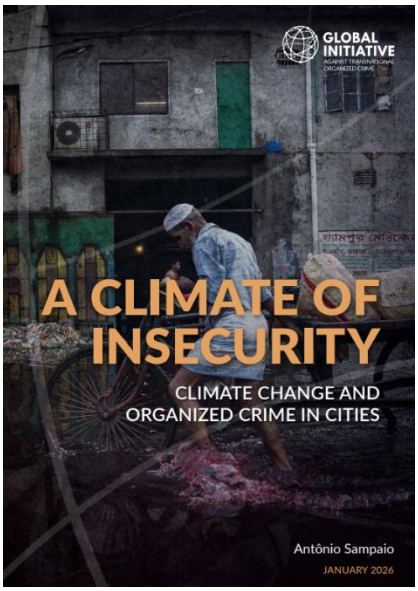
Усі ці порушення — дитяча праця, фінансування збройних груп, екологічний злочин — відбувалися на тлі повної бездіяльності або навіть потурання з боку відповідальних інституцій. Незважаючи на вимоги законодавства ДРК, Primera Gold жодного разу не опублікувала звіт про комплексну перевірку своїх ланцюгів постачання. Міжнародна

конференція регіону Великих озер (ICGLR), яка має проводити аудит усіх компаній-експортерів, так і не здійснила перевірку Primera. Банки, що обслуговували підприємство — Rawbank та Equity Bank — отримали на свої рахунки сотні мільйонів доларів, але немає жодних доказів того, що вони проводили незалежну оцінку ризиків, пов'язаних із походженням цих коштів.

Нарешті, питання про те, куди поділися прибутки, залишається відкритим. У 2023 році Primera Gold експортувала понад 5 тонн золота на суму понад 300 мільйонів доларів. Однак в офіційних бюджетних документах ДРК, де мають обліковуватися доходи державних підприємств, не було жодної згадки про надходження від цього спільного підприємства. Незрозуміло, чи пішли ці кошти на погашення військового боргу перед ОАЕ, чи осіли в інших кишенях. Мінімальний експортний податок у 0,25%, прописаний в угоді, також позбавив місцеві громади належної їм частки відрахувань.

Таким чином, історія Primera Gold є яскравим прикладом того, як глобальний попит на ресурси може посилювати локальні конфлікти та страждання. ОАЕ, прагнучи забезпечити собі доступ до золота, продемонстрували вражаючий опортунізм, підтримуючи одночасно і уряд ДРК (через військову допомогу), і його противників (через торгівлю з Руандою). Оголошена мета — очистити ланцюги постачання — виявилася фікцією, прикриттям для бізнесу, який не зупинявся перед співпрацею з тими, хто використовує дитячу працю, фінансує збройні угруповання та знищує унікальні природні екосистеми. Те, що FATF у 2024 році виключила ОАЕ з «сірого списку», фактично схваливши її зусилля з боротьби з відмиванням грозей, виглядає щонайменше недалекоглядно.

Тіні майбутнього: Як зміни клімату живлять організовану злочинність [12]



Світ опинився перед новою, гнітючою реальністю, де кліматична криза перестала бути лише питанням екології або далекої абстрактної загрози, перетворившись на потужний та невблаганний каталізатор соціальної дестабілізації, економічної нерівності та стрімкого поширення організованої злочинності.

Доповідь, опублікована Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC), є, по суті, першим глибоким та системним дослідженням тривожного перетину двох визначальних глобальних трендів сучасності: безпрецедентної за масштабами урбанізації, спричиненої кліматичними змінами, та експансії, адаптації та посилення впливу організованих злочинних угруповань. Саме мегаполіси стають одночасно і єдиним рятівним притулком для мільйонів людей, і жорстоким полем битви за виживання, де організована злочинність, з її хижацькими методами та здатністю швидко адаптуватися до нових умов, пожинає найкривавіші врожаї.

Міста завжди, впродовж усієї історії людства, були магнітами для тих, хто шукає кращої долі, економічних можливостей та соціальних ліфтів. Однак сьогодні цей традиційний потік набуває трагічних рис масової міграції виживання, спричиненої не надією на краще, а відчаєм через втрату всього. За даними Світового банку, навіть за помірними сценаріями, до 2050 року лише в країнах Африки на південь від Сахари, Південній Азії та Латинській Америці понад 143 мільйони людей можуть бути змушені покинути свої домівки через повільні кліматичні зміни —

[12] https://globalinitiative.net/wp-content/uploads/2026/01/Anto%CC%82nio-Sampaio-A-climate-of-insecurity-Climate-change-and-organized-crime-in-cities-GI-TOC-January-2026.pdf

посухи, опустелювання, підвищення рівня моря, неврожаї. Якщо ж додати до цього раптові катастрофи — руйнівні повені, як-от у Пакистані 2022 року, що змістили 8 мільйонів осіб, урагани, що стирають з лиця землі цілі містечка, — цифри стають воістину апокаліптичними. Дослідження впливової глобальної мережі міст C40 прогнозує, що до того ж 2050 року лише десять найбільших мегаполісів світу приймуть щонайменше 8 мільйонів таких «кліматичних мігрантів».

Автор звіту, спираючись на десятки польових досліджень, академічних статей та звітів міжнародних організацій, виокремлює три ключові, глибинно та тісно переплетені між собою сфери, де кліматичні зрушення безпосередньо та найбільш руйнівно посилюють позиції криміналітету, трансформуючи самі основи міського життя. Це, по-перше, неконтрольована торгівля людьми та сучасне рабство, яке стає тіньовим ринком праці для мільйонів зневірених мігрантів; по-друге, кримінальний контроль над водними ресурсами, що перетворює базову потребу на розкіш, доступну лише за ціною боргу та покори; і по-третє, масштабні земельні махінації та рейдерство, які стають найприбутковішим бізнесом в умовах шаленого попиту на житло.

Перший і найгостріший виклик, що безпосередньо впливає на долі мільйонів людей, — це екстремальна вразливість сільських мігрантів до експлуатації. Люди, чиї фермерські господарства знищені катастрофічними повенями, засоленням ґрунтів або багаторічними посухами, прибувають до міста, не маючи жодних заощаджень, часто без професійних навичок, потрібних в урбаністичній економіці, і, що найважливіше та найтрагічніше, без жодних соціальних зв'язків та підтримки. Вони стають ідеальними жертвами. І саме цю прогалину в безпеці та інформації миттєво заповнюють злочинні угруповання.

Вербувальники, які часто діють ще в селах, обіцяючи престижну роботу та високі заробітки в місті, заманюють людей у пастку боргової кабали. Найбільш показовим, детально описаним у звіті прикладом є Бангладеш — країна, яка системно потерпає від циклонів, річкових повеней, підвищення рівня моря, особливо в регіоні Сундарбану. Тисячі знедолених людей щодня прибувають до столиці Дакки, яка вже задихається від перенаселення, налічуючи понад 20 мільйонів мешканців, значна частина з яких, за оцінками, є саме кліматичними мігрантами. Тут, у перенаселених нетрях із жахливими санітарними умовами та відсутністю правопорядку, вони стають легкою здобиччю для торговців людьми. Чоловіки та підлітки потрапляють у рабські умови на небезпечних будівництвах або в цегляних печах, де панує важка фізична праця. Окремої уваги заслуговує доля дітей — дослідження у восьми нетрях Дакки показало, що сотні дітей віком від 8 років працюють по 12 годин на день, часто потрапляючи в боргову кабалу через аванси, отримані їхніми зневіреними батьками. Жінки та дівчата є найбільш вразливою категорією: їх систематично продають у сексуальне рабство на вулицях або в борделях, примушують до фіктивних шлюбів, які насправді є формою торгівлі людьми, або жорстоко експлуатують у домашньому господарстві, де вони стають повністю ізольованими та безправними.

Дослідження Глобального фонду боротьби з сучасним рабством 2022 року, наведене у звіті, показало приголомшливу цифру: 86% неформальних працівників швейної промисловості в двох районах Дакки відповідають критеріям сучасного рабства, а дві третини з них зазнавали фізичного або сексуального насильства. Місцеві кримінальні авторитети, відомі в Бангладеш як «мастаани», не лише контролюють цей ринок праці та експлуатації, а й створили цілу систему паралельної влади в нетрях. Вони надають «послуги» з вирішення суперечок, захисту та навіть постачання води й електрики, фактично заповнюючи вакуум державної присутності, але роблять це ціною постійного насильства, вимагання, контролю над землею та жорстокого придушення будь-якої непокори. Їхня роль амбівалентна — вони і захисники, і головна загроза, що робить життя мешканців нетрів ще більш нестабільним.

Подібна, хоча й з іншими культурними та соціальними особливостями, динаміка простежується і в Центральній Америці, зокрема в Гондурасі та Гватемалі, які входять до так званого Сухого коридору. Тут багаторічні посухи та неврожаї руйнують сільське господарство, змушуючи молодь, яка втратила будь-які перспективи вдома, тікати до міст або намагатися дістатися США через небезпечні маршрути. У бідних районах міст на них чекають могутні банди, які не лише вербують зневірених юнаків у свої ряди як солдатів, а й контролюють цілі райони, обкладаючи даниною місцевий бізнес — від дрібних крамничок до вуличних торговців. В Гаїті після руйнівного землетрусу 2021 року банди просто захоплювали вантажівки з гуманітарною допомогою, демонструючи, що в умовах слабкої держави стихійне лихо стає не часом для консолідації, а додатковою можливістю для збагачення та посилення влади криміналу.

Друга критична сфера, де перетинаються клімат і злочинність — це ресурсний тиск, найяскравіше та найболючіше виражений у виснажливій боротьбі за воду, яка стає все дорожчою. Зміна клімату робить посухи не просто частішими, а інтенсивнішими та тривалішими, а стрімке, часто хаотичне зростання міст лише багаторазово загострює хронічний дефіцит. За прогнозами Міжурядової групи експертів зі зміни клімату, до 2050 року кількість міських жителів, які зіштовхнуться з нестачею води, зросте до астрономічних 2,4 мільярда осіб. Найбільше постраждає Індія. І там, де державні комунальні служби виявляються неефективними, корумпованими або просто не в змозі дотягнутися до нетрів, де офіційно прокладати труби нібито «невигідно», на сцену виходять так звані «водні мафії». У Карачі, Пакистан, де, за оцінками, ще у 2016 році злочинці щодня відкачували 10 мільйонів галонів води, ці угруповання діють із цинічною відвертістю. Вони встановлюють незаконні насоси (гідранти) на державних магістральних трубопроводах, часто за мовчазної згоди або навіть за активної участі корумпованих чиновників з водоканалів та місцевої влади. Вони виснажують підземні водоносні горизонти, погіршуючи й без того критичну ситуацію, і продають воду мешканцям нетрів у цистернах за цінами, що в рази, а то й на порядок перевищують офіційні тарифи для заможних кварталів. Бідні верстви населення змушені витрачати левову частку свого мізерного щоденного доходу на купівлю води сумнівної якості, яка до того ж часто спричиняє кишкові інфекції та інші хвороби, створюючи ще більше навантаження на і так перевантажену систему охорони здоров'я. Це не просто економічна експлуатація, а пряма загроза життю та здоров'ю.

Нарешті, третя, і, мабуть, найприбутковіша сфера злочинної діяльності в умовах кліматичної міграції — це земля та нерухомість. Нестримний, хаотичний наплив людей створює шалений, небачений раніше попит на житло, будь-яке житло, що, у свою чергу, роздмухує ціни до небес та провокує безсоромні спекуляції. У цю високоприбуткову гру вступають потужні «земельні мафії», які часто діють не на вулицях, а в кабінетах, використовуючи корупційні зв'язки з державними реєстраторами, нотаріусами та місцевими політиками. Їхні методи надзвичайно різноманітні: від прямого, брутального силового захоплення публічних земель (в Бангладеш, як зазначається у звіті, таким чином було привласнено понад 1,3 мільйона гектарів так званих «кхас» — державних земель, часто через насильницьке виселення селян) до складних, технологічно оснащених шахрайських схем із підробкою правовстановлюючих документів, фальшивими договорами купівлі-продажу та рейдерським захопленням цілих житлових кварталів.

Злочинні угруповання, часто у змові з забудовниками та чиновниками, витісняють бідних мігрантів з відносно придатних районів на небезпечну периферію — схили пагорбів, заплави річок, зони відчуження. Там люди будують халупи, знову опиняючись у зоні підвищеного ризику від зсувів, повеней та інших кліматичних катастроф. Це замикає трагічне порочне коло: люди тікають від кліматичних негараздів у селі, а опиняються в ще більш вразливих місцях у місті, до того ж під контролем злочинців, які стягують з них плату за саме існування.

Звіт робить набагато більше, ніж просто констатує факти. Він руйнує спрощене, примітивне уявлення про те, що організована злочинність є лише пасивним «тіньовим бенефіціаром» кліматичних змін. Він переконливо демонструє, як кримінальні структури стають активними, впливовими гравцями, що формують нову урбаністичну реальність XXI століття. Вони не просто паразитують на дефіциті, а свідомо поглиблюють його, створюючи складні, багаторівневі системи паралельної влади та неформального, часто жорстокого управління. Вони пропонують «послуги» там, де держава відсутня, але ціна цих послуг — свобода, гідність, здоров'я, а іноді й життя. Їхня діяльність системно підриває соціальну стійкість міст, роблячи зусилля з адаптації до змін клімату, які фінансуються міжнародними донорами, набагато складнішими, а часто й просто неможливими. Злочинність стає частиною екосистеми міста, вбудованою в його економіку та соціальні відносини.

Висновки:

- **Зміна клімату змушує мільйони людей тікати з сільської місцевості до міст,** де відсутність соціальних зв'язків та коштів робить їх легкою здобиччю для торговців людьми та сучасних рабовласників. Жінки та діти опиняються в найбільш вразливому становищі.
- **Дефіцит води, спричинений кліматичними змінами та стрімкою урбанізацією,** породжує "водну мафію", яка незаконно видобуває ресурс і продає його бідним верствам населення за непомірними цінами, часто у змові з корумпованими чиновниками.
- **Наплив мігрантів провокує шалене зростання цін на землю та житло, чим користується "земельна мафія".** Вона захоплює ділянки, підробляє документи та витісняє бідних на небезпечні території, де ті знову потерпають.
- **Там, де держава не справляється з наданням базових послуг, її місце займають злочинні угруповання,** створюючи паралельні системи влади, засновані на насильстві, вимаганні та контролі над ресурсами.

Автор наголошує на нагальній необхідності кардинально змінити підхід до проблеми на глобальному рівні. Досі існує стійке «сільське упередження» в дослідженнях безпекових аспектів клімату, тоді як міста, де вже зараз живе більшість населення планети, залишаються на периферії уваги політиків та аналітиків, які займаються кліматичною безпекою. Подолання цього фатального розриву потребує термінових, скоординованих та рішучих дій на всіх рівнях. По-перше, необхідно на законодавчому та програмному рівні інтегрувати глибокий аналіз загроз організованої злочинності у всі міські стратегічні плани сталого розвитку. По-друге, кардинальне розширення доступу найбідніших верств населення та мігрантів до легальних, захищених ринків праці, доступного житла, чистої питної води та формальних механізмів кредитування є не просто соціальною політикою чи благодійністю, а прямою, стратегічною інвестицією в національну та міську безпеку. По-третє, потрібна жорстка, невідворотна та системна боротьба з корупцією, особливо в органах, що відповідають за землекористування, будівництво, реєстрацію нерухомості та водопостачання. Саме корупція є тим мастилом, яке дозволяє безперебійно працювати складним механізмам «водних» та «земельних» мафій, роблячи їх практично невразливими для правосуддя.

Від того, чи зможуть уряди, міжнародні організації, місцеві громади та правоохоронні органи об'єднати зусилля, щоб розірвати цей фатальний, смертоносний зв'язок між кліматичним лихом і криміналом, залежить не просто майбутнє окремих міст чи регіонів, а глобальна стабільність та соціальний мир у найближчі десятиліття. Ігнорування цього глибинного зв'язку, намагання вирішувати проблеми клімату та злочинності окремо, остаточно перетворить міста, які за визначенням мали б бути двигунами прогресу та центрами інновацій, на епіцентри неконтрольованого хаосу.

Як працює нелегальний ринок диких тварин Центральної Азії і чому регіон став епіцентром контрабанди [13]

Поки світова громадськість зосереджена на гучних кампаніях із порятунку слонів від браконьєрів або на припиненні контрабанди рогів носорога, значно менш помітна, але не менш руйнівна торгівля пульсує в надрах онлайн-месенджерів, на стихійних ринках та в затишних, на перший погляд, приватних домівках Центральної Азії. Цей регіон, розташований на перехресті шляхів між Європою, Азією та Близьким Сходом, десятиліттями залишався "білою плямою" на карті моніторингу незаконної торгівлі дикою природою.

Масштабне дослідження, проведене авторитетною організацією TRAFFIC у Казахстані, Киргизстані та Узбекистані, вперше так детально розкрило анатомію цього ринку, продемонструвавши, що регіон став не просто транзитним хабом на шляху до заможних покупців у Перській затоці чи росії, а й потужним споживачем рідкісних та зникаючих видів фауни, сформувавши власний стійкий попит на екзотику.

Задокументовані результати вражають своїми масштабами та глибиною: загалом було виявлено 1753 пропозиції про продаж, які охоплювали 6355 живих тварин, що належать до 96 різних видів. Це не просто суха статистика, а відображення глибоко вкоріненої соціально-економічної та правової проблеми, де переплітаються бідність, жага до володіння унікальним "аксесуаром", прогалини в законодавстві, корупційні ризики та майже повна безкарність. Безумовним лідером за обсягами торгівлі став Узбекистан, на який припало приголомшливі 85% усіх пропозицій та 94% виставлених на продаж тварин. Це позиціонує країну як головний хаб регіону, своєрідну "живу біржу", куди стікаються товари з різних куточків світу — від вологих екваторіальних лісів Африки до холодних гірських масивів Тянь-Шаню.

Домінування цифрового простору в цій торгівлі є беззаперечним та показовим: 80% оголошень було знайдено в інтернеті, що підкреслює глобальний тренд на цифровізацію навіть таких архаїчних злочинів, як браконьєрство. Найпопулярнішою платформою виявився Telegram, де зосередилося 68% усіх онлайн-пропозицій, переважно в Узбекистані. Анонімність, яку надають месенджери, легкість створення закритих каналів з аукціонами та можливість миттєвого видалення контенту роблять їх ідеальним середовищем для продавців, які прагнуть будь-що уникнути уваги контролюючих органів. Водночас традиційні фізичні ринки, попри значно менше розмаїття видів (лише 20), продовжують відігравати ключову роль у продажах. На них припало 55% усіх задокументованих особин, що свідчить про те, що "живий товар" найчастіше продається оптом, гуртом, у клітках, наставлених одна на одну в тісних крамницях старих базарів Ташкента, Бішкека чи Алмати.

Асортимент цього "живого товару" вражає своєю різноманітністю. Понад 40% виявлених видів внесено до Додатків I та II Конвенції CITES, що регулює міжнародну торгівлю видами, які перебувають під загрозою зникнення. Серед них — справжні перлини дикої природи: чутливий та інтелектуальний папуга жако (сірий африканський папуга), могутній тигр, яскравий жовточубий какаду та швидкий, як вітер, балобан. Ці тварини класифікуються Міжнародним союзом охорони природи як вразливі, зникаючі або такі, що перебувають на межі зникнення. Найпоширенішим видом, однак, став зовні непоказний, але надзвичайно популярний у регіоні

[13] https://www.traffic.org/site/assets/files/29597/out-of-the-wild_uncovering_the_live_animal_trade_in_central_asia.pdf

щиглик європейський, внесений до Додатку III CITES. Його пропозиції склали 35% від усіх оголошень, що вказує на величезний, майже промисловий попит на місцевих диких птахів, яких масово виловлюють у природі сітками. Торгівля щигликами, яких продають десятками в одному оголошенні, стала своєрідним маркером байдужості суспільства до виснаження власних природних ресурсів.

Ціни на цих тварин формують справжній "чорний ринок розкоші", де вартість живих істот вимірюється тисячами доларів. Найдорожчими виявилися види з Додатку I CITES: великі кішки, екзотичні папуги та примати. Більше чверті пропозицій щодо таких тварин перевищували позначку в 1000 доларів США за одну особину. За один екземпляр просили від кількох тисяч до 35 000 доларів США. Наприклад, в Узбекистані через Telegram пропонували дитинча тигра за 35 000 доларів, а в Казахстані на платформі OLX пальмового какаду оцінили у 15 000 доларів. Навіть менш рідкісні, але все ще екзотичні види, як-от сервал, коштували до 5500 доларів. Такі суми перетворюють торгівлю тваринами на надприбутковий бізнес, який за прибутковістю може конкурувати з наркоторгівлею, де ризики нелегального вилову та контрабанди виправдовуються високою маржею.

Одним із найбільш тривожних висновків дослідження стала майже повна відсутність прозорості щодо походження тварин. Лише 20% пропозицій містили бодай якусь інформацію про джерело походження — чи то дика природа, чи розведення в неволі. Це створює ідеальний "сірий" ринок, де неможливо відрізнити законний товар від незаконного. З тих же оголошень, де дані були доступні, приголомшливі 84% тварин, за заявами самих продавців, були виловлені безпосередньо в дикій природі. Це викликає серйозні занепокоєння щодо масштабів вилучення рідкісних видів з їхніх природних середовищ існування та ставить під сумнів сталість таких популяцій.

Ще більше проблем додає той факт, що майже в жодному з оголошень не згадувалася наявність дозволів CITES. Лише один продавець з усіх 1753 зробив посилання на такі документи. Натомість поширеними є розпливчасті заяви про "розведення в неволі", які в умовах слабкого контролю та відсутності генетичної експертизи можуть слугувати ідеальним прикриттям для "відмивання" диких тварин, виловлених браконьєрами. Це глобальна проблема, відома як "wildlife laundering", і Центральна Азія, як показує дослідження, стала її невід'ємною частиною. Ситуацію кардинально ускладнює існування Євразійського економічного союзу (ЄАЕС), який гарантує вільний рух товарів між Казахстаном, Киргизстаном та росією. Це створює величезну "сіру зону" для переміщення живих тварин без належного прикордонного ветеринарного та CITES-контролю. Тварину, ввезену, скажімо, до Киргизстану без документів, можна легально, з точки зору митниці ЄАЕС, перевезти до Казахстану, хоча з точки зору міжнародного екологічного права це є грубим порушенням.

Відвідування центрів розведення тварин лише підтвердило неоднорідність та серйозні прогалини в регулюванні цього сектору. Якщо казахстанські центри розведення соколів, такі як Sunkar LLP, демонстрували відносно високі стандарти роботи, ведучи племінні книги та співпрацюючи з науковими інститутами, то в Киргизстані картина виявилася зовсім іншою. Там було виявлено дрібних приватних заводчиків папуг, які працюють буквально на дому, у житлових будинках, без жодної реєстрації, державного нагляду чи підтвердження законності походження їхнього племінного поголів'я. Це створює прямий канал для легалізації диких птахів, виловлених десь у тропіках. В Узбекистані ж існує найбільш структурована система для розведення степових черепах, із реєстрацією та інвентаризацією, однак і там зберігаються проблеми з верифікацією походження племінного поголів'я та забезпеченням сталого управління ресурсами, що призводило до міжнародних санкцій у вигляді нульових квот на експорт.

Законодавча база всіх трьох країн, попри те, що вони є сторонами CITES, виявилася фрагментованою, застарілою та, що найгірше, неефективною на практиці. Ключові недоліки включають відсутність обов'язкової реєстрації диких тварин у приватних руках, що робить неможливим облік того, хто і яких тварин тримає вдома. Спостерігається катастрофічно недостатній моніторинг як фізичних ринків, так і, особливо, розплідників. Слабка координація між різними відомствами — екологами, митницею, ветеринарами, поліцією — призводить до того, що кожен орган перекладає відповідальність на іншого. Окремою проблемою є ветеринарні сертифікати: вони підтверджують лише здоров'я тварини, але аж ніяк не законність її походження, що дозволяє браконьєрській тварині з "липовою" довідкою виглядати цілком легально. Це створює ідеальні умови для функціонування тіньового ринку, де незаконно добуті тварини отримують "легальний" статус завдяки прогалинам у системі.

Висновки:

- **Масштабний та неврегульований ринок.** В Казахстані, Киргизстані та Узбекистані зафіксовано продаж понад 6300 тварин 96 видів, з яких понад 40% перебувають під загрозою зникнення.
- **80% продажів відбувається через інтернет, переважно в анонімних Telegram-каналах.** Інформація про походження тварин відсутня у 80% випадків, а там де вона є — 84% тварин, за словами продавців, виловлені в дикій природі.
- **В країнах регіону відсутня обов'язкова реєстрація диких тварин,** а ветеринарні сертифікати підтверджують лише здоров'я, але не законність походження. Це створює ідеальні умови для "відмивання" особин під виглядом розведених у неволі.
- **Ціни на рідкісні види сягають десятків тисяч доларів,** що робить контрабанду тварин надприбутковим бізнесом. Вільне переміщення товарів у межах ЄАЕС додатково ускладнює контроль на кордонах.

Результати дослідження змушують кардинально переглянути роль Центральної Азії в глобальній торгівлі дикою природою. Це вже не просто транзитна зона на Шовковому шляху контрабанди, а величезний, самодостатній ринок збуту з власними усталеними каналами, високим платоспроможним попитом та значними фінансовими оборотами. Ігнорування цієї проблеми матиме катастрофічні, незворотні наслідки для біорізноманіття планети. Це призведе до скорочення популяцій місцевих видів та до підтримки глобального браконьєрства.

Вихід із цієї кризової ситуації потребує комплексу невідкладних, системних та скоординованих дій на регіональному рівні. Насамперед, необхідно терміново гармонізувати та кардинально посилити національні законодавства, запровадивши обов'язкову реєстрацію, чипування та документальне підтвердження законності походження для всіх без винятку диких тварин, що перебувають у неволі. Потрібен жорсткий контроль за діяльністю центрів розведення з обов'язковим ліцензуванням, регулярними позаплановими перевірками та генетичною верифікацією племінного поголів'я. Нагальною потребою є навчання співробітників правоохоронних органів, суддів та митників сучасним методам виявлення нелегальної торгівлі, зокрема моніторингу даркнету, месенджерів та соціальних мереж. І нарешті, без тісної регіональної співпраці, створення спільних слідчих груп та обміну інформацією в реальному часі, зупинити цей руйнівний потік буде неможливо.

Центральна Азія стоїть перед доленосним вибором: стати регіоном, де закон, свідомість громадян і міжнародне співробітництво нарешті перемагають, чи назавжди залишитися "диким ринком" у самому центрі Євразії.

Тіньовий флот: Як іранське пальне потрапляє в М'янму [14]

У ніч на 13 жовтня 2025 року мешканці віддаленого села Ванха, затиснутого між лісистих гір штату Чин на заході М'янми, прокинулися від завивання літака. За кілька секунд перша бомба, скинута з військового літака хунти, рознесла дах єдиної в селі школи. Друга бомба, скинута з безпілотника за кілька хвилин, вдарила по людях, які вибігли на подвір'я. Того ж дня, за тисячі кілометрів звідти, іранський танкер Reef узяв курс додому, завершивши чергову операцію з доставки понад 16 000 тонн авіаційного пального режиму в Неп'їдо. Цей збіг у часі – не випадковість, а символ нового рівня співпраці двох ізольованих режимів, яка змінює перебіг громадянської війни в М'янмі та коштує життів сотням цивільних.

Масштабне журналістське розслідування Reuters, засноване на аналізі суднових документів, супутникових знімках та даних трекінгових систем, відкриває завісу над механізмами цієї таємної торгівлі. Іран, чия власна економіка задихається під тягарем міжнародних санкцій, а регіональні союзники один за одним зазнають поразок чи втрачають владу, знайшов несподіваного, але дуже прибуткового покупця. Військова хунта М'янми, яка після перевороту 2021 року намагається придушити народний спротив, відчайдушно потребує ресурсів для ведення війни. Іран заповнив цю прогалину, ставши з жовтня 2024 року головним постачальником авіаційного пального.

Два танкери-близнюки, Reef та Noble, внесені США до санкційних списків ще у 2024 році, перетворилися на регулярний човниковий маршрут між Іраном та М'янмою. За 15 місяців вони здійснили щонайменше дев'ять рейсів, доставивши близько 175 000 тонн авіаційного пального. Цифра може здатися не надто вражаючою в масштабах світової нафтової торгівлі, але для М'янми, чиї ВПС налічують близько 100 літаків (радянські МіГ-29 та Су-30, китайські JF-17 Thunder), це означає можливість проводити тисячі бойових вильотів. І хунта не змусила себе чекати. За даними моніторингової групи Myanmar Peace Monitor, з моменту першого іранського постачання і до кінця 2025 року військова авіація завдала ударів по 1022 цивільних локаціях. Це більш ніж удвічі перевищує показники попередніх 15 місяців.

Але як іранські танкери можуть непомітно перетинати океани в епоху супутникового стеження та глобальних систем моніторингу? Відповідь криється в технології, яка стала візитівкою тіньового флоту Ірану – спуфінгу, або підміні сигналів. Комерційні судна зобов'язані транслювати своє місцезнаходження через автоматичну ідентифікаційну систему (AIS). Reef та Noble навчилися обманювати цю систему, транслюючи фейкові координати. 15 вересня 2025 року AIS Reef показувала, що він стоїть біля іракського нафтового терміналу Басра. Супутникові знімки цього району, зроблені того ж дня компанією SynMax Intelligence, не зафіксували жодного судна. Насправді Reef перебував за сотні кілометрів звідти, в іранському порту Бендер-Аббас, де розташований нафтопереробний завод, що виробляє авіаційне пальне. Найбільш промовистим доказом обману став епізод 16 вересня: о 17:28 AIS показувала танкер за 330 кілометрів від порту, а вже о 17:31 – безпосередньо в порту. Таку відстань неможливо подолати й за 10 годин, не те що за три хвилини. Це класичний спуфінг: судно вимикає справжній сигнал і вмикає заздалегідь запрограмований фейковий маршрут. Після завантаження Reef вирушив у путь, і десь після проходження південного узбережжя Індії знову ввімкнув обманку, імітуючи рух до бангладешського порту Читтагонг. Та 2 жовтня 2025 року система дала збій: фейковий сигнал показував танкер біля Читтагонга, а справжній раптово проявив його за 800 кілометрів звідти – біля терміналу Myan Oil неподалік Янгона. Вантаж прибув за адресою.

[14] https://www.reuters.com/graphics/IRAN-MYANMAR/JET-FUEL/jnpwkonqrpw/

Термінал Myan Oil (колишній Puma) став ключовим хабом для прийому іранського пального. Це не просто нафтобаза, а ціла мережа компаній та бізнесменів, тісно пов'язаних з військовим режимом. Компанії Myan Oil, Swan Energy, Shoon Energy, Asia Sun Group та двоє їхніх власників, Зав Мін Тун і Він К'яв Аун, вже потрапили під санкції США, Канади, ЄС та Британії за постачання пального військовим. Санкції, втім, не зупиняють потік пального – вони лише підвищують ціну та роблять ланцюжки постачання більш заплутаними. Іран, з його досвідом обходу санкцій, стає для хунти ідеальним партнером.

Але паливо – це лише частина смертоносної формули. Розслідування Reuters виявило, що Іран таємно постачає М'янмі не лише пальне для літаків, а й сотні тисяч тонн карбаміду. Ця хімічна речовина у мирному житті є цінним азотним добривом. Але в умовах війни вона стає ключовим інгредієнтом для виробництва вибухівки. За оцінками трьох аналітиків, які відстежують імпорт М'янми, щорічний обсяг поставок може сягати від 400 до 600 тисяч тонн. Танкери для сипучих вантажів, такі як Golden ES та Rasha, доставляють її до портів М'янми, так само вдаючись до спуфінгу, щоб приховати своє справжнє походження.

Двоє колишніх військовослужбовців Татмадо, які дезертирували, аби не вбивати цивільних, підтвердили журналістам, куди саме прямує ця речовина. Вона надходить на два державні заводи з виробництва боєприпасів, розташовані в центральній частині М'янми. Там її використовують для виготовлення вибухових речовин, якими начиняють авіабомби, артилерійські снаряди, а також боєприпаси для безпілотників.

Цей альянс є не просто вигідною комерційною угодою, а свідченням глибокого геополітичного переформатування. Іран, який ще у 2017 році вустами президента Хасана Роугані різко засуджував переслідування мусульман-рохінджа в М'янмі, а міністр закордонних справ Джавад Заріф закликав світ не допустити геноциду, кардинально змінив риторику. Після військового перевороту 2021 року, коли армія усунула від влади уряд Аун Сан Су Чжі, Тегеран побачив потенційного союзника. У січні 2022 року, за даними регіонального джерела з безпеки, іранська урядова делегація таємно відвідала М'янму для зустрічі з військовим керівництвом. Тема переговорів, як повідомляло Asia Times, була далекою від гуманітарної – продаж іранської зброї, включаючи керовані ракети.

Цей поворот експерти пояснюють прагматизмом Тегерана. Традиційні союзники Ірану опинилися в скрутному становищі: Башар Асад втратив владу в Сирії, Ніколас Мадуро більше не контролює Венесуелу так, як раніше, а Хезболла та ХАМАС ослаблені війною з Ізраїлем. Ірану потрібні нові партнери, нові ринки збуту та нові джерела доходу, щоб вижити під тиском санкцій. М'янма, багата на ресурси, але ізольована країна з великою армією, стала ідеальним кандидатом.

Висновки:

- **Іран став головним постачальником авіаційного пального для військової хунти М'янми,** що дозволило режиму вдвічі збільшити кількість авіаударів по цивільних об'єктах, вбиваючи мирних жителів.
- **Постачання здійснюються через "тіньовий флот"** із використанням технології спуфінгу (підміни сигналів AIS), що дозволяє обходити міжнародні санкції та залишатися непоміченими для глобальних систем моніторингу.
- **Окрім пального, Іран таємно експортує до М'янми сотні тисяч тонн хімікатів**, які використовуються військовими заводами для виробництва вибухівки, що робить Іран співучасником не лише авіаударів, а й наземних операцій.
- **Цей альянс демонструє цинічний геополітичний прагматизм Тегерана,** який заради економічної вигоди та пошуку нових союзників відмовився від колишньої критики та налагодив тісну співпрацю з ізольованим військовим режимом.

З поглибленням торговельних зв'язків активізувалися і політичні контакти. У грудні 2025 року президент Ірану Масуд Пезешкіан провів зустріч із прем'єр-міністром М'янми Мьо Све на полях саміту в Туркменістані. Згідно з іранським звітом, Мьо Све наголосив на бажанні розширювати співпрацю в імпорті нафти та технологіях її видобутку. Іран навіть отримав запрошення надіслати спостерігачів на сфальсифіковані загальні вибори, які хунта провела наприкінці грудня 2025 року. Вибори, які ООН та міжнародна спільнота назвали невільними та нечесними, отримали схвалення Тегерана.

Наприкінці січня 2026 року, коли в самому Ірані були жорстоко придушені чергові антиурядові протести, супутникові дані SynMax знову зафіксували знайому картину: Noble, транслюючи фейковий сигнал про стоянку біля узбережжя Іраку, насправді готувався до відплиття біля Бендер-Аббаса. Reef уже був завантажений і знову прямував до Янгона.

Цей безкінечний кругообіг пального, грошей та смерті є найкращою ілюстрацією того, як працює тіньова глобальна економіка в епоху санкцій. Вона не зупиняє війни, а лише робить їх більш заплутаними та цинічними. В той час як дипломати в ООН закликають притягнути винних до відповідальності, а санкційні списки поповнюються новими назвами компаній та іменами бізнесменів, реальність на місцях залишається незмінною. Тіньовий флот продовжує плисти, залишаючи за собою кривавий слід.

Інші новини

Наркокартелі та гіг-економіка: нова архітектура легалізації кримінальних доходів через криптоактиви [15]

Стаття Bloomberg Businessweek, авторства Джесіки Брайс, є важливим журналістським дослідженням, що документує фундаментальний зсув у методології легалізації наркодоходів мексиканських та латиноамериканських картелів. Матеріал відкривається конкретним кейсом Девіда Скотезе — типового «незалежного крипто-брокера», який між 2021 та 2023 роками здійснив понад 4 000 транзакцій за схемою «готівка за крипту», пропонуючи свої послуги через онлайн-платформу LocalMonero.co. Угоди укладалися у публічному місці — паркінгу місцевого парку — і не вимагали жодних запитань щодо походження коштів. Скотезе не був особою, пов'язаною з картелями безпосередньо: він позиціонував себе як пасивного учасника «гіг-економіки» у фінансовій сфері. Саме ця модель — децентралізованої, анонімізованої, горизонтальної мережі незалежних брокерів — і є предметом аналізу Bloomberg.

Стаття ілюструє стратегічну еволюцію схем відмивання картельних коштів від традиційного «bulk cash smuggling» та відмивання через нерухомість і підставні компанії до використання криптоактивів як первинного інструменту конвертації готівки. Ключовим каталізатором цієї трансформації є стейблкоїни (насамперед USDT), що вирішили проблему волатильності,

[15] https://www.bloomberg.com/news/features/2026-02-11/drug-cartel-money-laundering-shifts-to-crypto-and-the-gig-economy?srnd=phx-crypto

притаманну першим поколінням крипто-схем ВК. Стейблкоїн деномінований у доларах є практично еквівалентним готівковому долару, але повністю оцифрованим і потенційно анонімним на рівні адрес гаманців.

Паралельно Bloomberg аналізує роль китайських брокерських мереж як ключового інфраструктурного елемента нової системи. Ці мережі, за даними FinCEN, є зараз одними з найбільш значущих загроз для американської фінансової системи. Їхня роль у схемі є структурно асиметричною: картелі є постачальниками доларової готівки, накопиченої на вулицях американських міст; китайські мережі — посередниками, що конвертують цю готівку у криптоактиви і перенаправляють відповідні кошти клієнтам у Китаї, які обходять валютні обмеження КНР. Таким чином, дві незалежні злочинні інфраструктури утворюють «симбіотичні» відносини, за визначенням FinCEN — взаємовигідний альянс, що базується не на прямому кримінальному партнерстві, а на спільній фінансовій логіці.

Матеріал Bloomberg також документує структурні недоліки правоохоронного реагування. Колишній керівник DEA Дерек Мальтц констатує, що агентства «не готові до такого масштабу незаконної діяльності». Основні проблеми включають: нестачу кадрів зі спеціалізованими знаннями криптоаналітики; обмежений доступ до адрес гаманців та приватних ключів без повноважень на вилучення пристроїв; залежність від спеціалізованих комерційних аналітичних блокчейн-інструментів (Chainalysis, TRM), доступ до яких не є стандартним у всіх слідчих відділах. Скотт Грейтак з Transparency International US поставив під сумнів, чи повністю законодавці розуміють функціонування нової екосистеми.

Стаття відображає суттєву зміну ринкової структури нелегальних послуг з конвертації грошей: замість ієрархічних організацій, де відмивач є штатним співробітником кримінальної організації, виникла децентралізована «платформа» незалежних контракторів — аналог Uber або Fiverr для нелегальних фінансових послуг. Ця структура принципово стійкіша до правоохоронного тиску, ніж ієрархічна: арешт одного брокера не зачіпає функціональності всієї мережі.

Велика Британія оголошує глобальне лідерство у боротьбі з дипфейками: регуляторні та правоохоронні виміри нової ініціативи [16]

Уряд Великої Британії 5 лютого 2026 року оприлюднив пресрелізи та анонси заходів, що визначають Сполучене Королівство першим у світі регулятором, який системно вирішує проблему шкідливого вмісту, створеного з допомогою штучного інтелекту (deepfakes). Ключовим елементом ініціативи є розробка «deepfake detection evaluation framework» — першої у світі рамкової методології для оцінки ефективності технологій виявлення синтетичних медіа. Рамка розроблена у партнерстві з Microsoft та іншими провідними технологічними компаніями за участі INTERPOL, представників «Альянсу п'яти очей» (Five Eyes) та великих технологічних корпорацій.

За тиждень до оголошення уряд провів «Deepfake Detection Challenge» — чотириденний хакатон з участю понад 350 фахівців. Учасники у режимі реального часу вирішували задачі ідентифікації реального, сфабрикованого та частково маніпульованого аудіовізуального контенту в умовах, наближених до реальних загроз — зокрема, сценаріїв для цілей ідентифікації

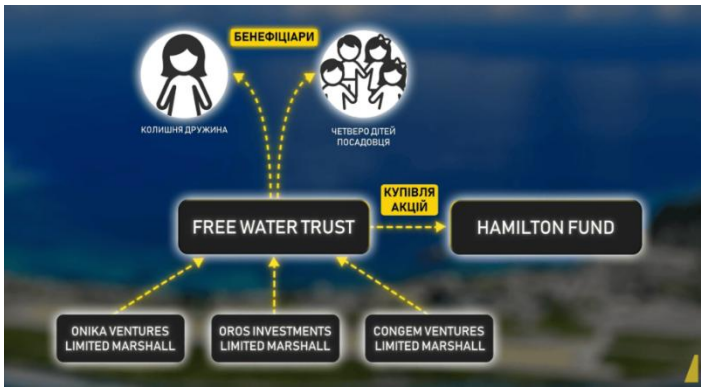
[16] https://www.gov.uk/government/news/government-leads-global-fight-against-deepfake-threats

жертв, безпеки виборів, організованої злочинності та шахрайської документації. За наявними оцінками, у 2025 році у світі було поширено 8 мільйонів діпфейків — порівняно з 500 тисячами у 2023 році, що означає зростання більш ніж у 16 разів за два роки.

З точки зору кримінального права, уряд прискорив набуття чинності законодавством, що криміналізує створення та запит на створення діпфейків інтимного характеру без згоди особи. Державний секретар DSIT також оголосила про надання цьому правопорушенню статусу «пріоритетного» у рамках Online Safety Act, що зобов'яже платформи вживати проактивних, а не лише реактивних заходів. Заплановано також заборону інструментів «nudification» — програмного забезпечення, що автоматично видаляє одяг із зображень реальних людей.

Ця ініціатива безпосередньо пов'язана зі сферою AML/CFT/CPF: діпфейки вже активно використовуються у фінансових шахрайствах, схемах соціальної інженерії для обходу KYC-верифікації при відкритті рахунків та для авторизації транзакцій, а також у схемах корпоративного шахрайства (CEO fraud/Business Email Compromise) де відеозапис підтвердження є частиною верифікаційного процесу. Заступник комісара поліції Лондона Нік Адамс наголосив, що «злочинці дедалі активніше використовують ШІ для обману жертв, уособлення довірених осіб та масштабування шкоди». Розробка стандартизованих методів виявлення діпфейків є, таким чином, не лише правозахисною, але і фундаментальною AML-інфраструктурною ініціативою, спрямованою на захист цілісності цифрових KYC-процедур.

Справа «Мідас»: НАБУ розкрило деталі схеми відмивання $12,9 млн з використанням криптовалют [17]



16 лютого 2026 року Національне антикорупційне бюро України офіційно повідомило про підозру у участі у злочинній організації та відмиванні незаконних доходів колишньому міністру енергетики України та екс-міністру юстиції. Матеріали справи, оприлюднені НАБУ 20 лютого 2026 року в деталізованому відеоматеріалі, розкривають повну анатомію корупційної схеми на загальну суму USD 12,9 млн. Підозрюваний фігурує в матеріалах кримінального провадження під кодовим ім'ям «Сигізмунд.

Предикатний злочин у схемі «Мідас» — хабарництво та зловживання службовим становищем у державному секторі ядерної енергетики. Механізм дії схеми, відомий як «шлагбаум» («barrier»), функціонував таким чином: підрядники державного підприємства «Енергоатом» (монополіст атомної генерації України) могли отримати розрахунок за виконаними державними контрактами лише після виплати «відкату» у розмірі від 10% до 15% від суми контракту. За версією НАБУ, підозрюваний, використовуючи своє міністерське становище, особисто сприяв введенню мораторію на погашення заборгованостей підприємства перед підрядниками — штучно створюючи стан фінансової залежності підрядників від власного рішення, що і становило «шлагбаум». Загальний обсяг корупційних надходжень у злочинну організацію, за даними НАБУ, міг сягати USD 112 млн готівкою за весь строк перебування підозрюваного на посаді.

[17] https://www.youtube.com/watch?v=zaNMXgyecYQ

Структура схеми відмивання, розкрита НАБУ, є класичним прикладом багатоярусної легалізації з використанням юрисдикцій з пільговим корпоративним режимом та офшорних фондів. На першому рівні схеми у лютому 2021 року на острові Ангілья (британська заморська територія з пільговим корпоративним правом) було зареєстровано фонд із заявленим капіталом USD 100 млн. Очолював структуру професійний посередник — громадянин Сейшельських Островів та Сент-Кітс і Невіс, якого НАБУ кваліфікує як особу, що надавала «послуги з відмивання коштів» на професійній основі. На Маршаллових островах (ще одна офшорна юрисдикція) зареєстровано дві компанії, номінальними бенефіціарами яких оформлено екс-дружину та четверо дітей підозрюваного. Ці компанії стали «інвесторами» фонду шляхом придбання його акцій, а кошти переказувалися на рахунки фонду у трьох швейцарських банках.

Роль криптовалют у схемі «Мідас», виходячи з оприлюднених матеріалів НАБУ, полягала в одному з декількох паралельних каналів легалізації. За наявними даними, використовувався стейблкоїн USDT (Tether). Стейблкоїни на відміну від волатильних криптовалют зберігають функціональну еквівалентність фіатним грошам і мінімізують конверсійний ризик при переміщенні великих сум. Криптовалютний канал в справі «Мідас» функціонував паралельно з «фондовим» каналом (через рахунки у швейцарських банках) та готівковим каналом (USD 4 млн видано готівкою безпосередньо у Швейцарії). Транзакції здійснювалися через довірену особу підозрюваного під кодовим ім'ям «Рокет».

Кінцеве використання відмитих коштів, зафіксоване у матеріалах НАБУ, є показовим з типологічної точки зору. USD 7,4 млн, отримані на рахунки двох маршаллових компаній, розміщувалися на банківських депозитах у Швейцарії (що приносили «легальний» відсотковий дохід), а також витрачалися на навчання дітей підозрюваного у дорогих швейцарських закладах, медичні послуги та придбання преміального одягу за кордоном. Залучення системи освітнього фінансування як механізму приховування джерел статків є класичною типологією ВК, оскільки платежі за навчання формально є «споживчими витратами» і не підлягають жорсткій перевірці джерел у більшості юрисдикцій. Для СПФМ-банків та платіжних систем ця типологія є прямою вказівкою на необхідність посиленого моніторингу значних освітніх платежів за кордон від фізичних осіб без чіткого джерела доходів або з доходами, несумісними з обсягами платежів.

Для загального розвитку

Санкційний контроль як елемент корпоративної стійкості: управлінський та технологічний вимір [18]

Документ присвячений формуванню комплексної, довгостроково стійкої та регуляторно захищеної системи санкційного скринінгу, яка розглядається не як окремий технічний інструмент, а як інтегрований елемент загальної системи управління ризиками фінансової установи.

Автор виходить із того, що в сучасному середовищі санкційного регулювання, яке характеризується постійним розширенням списків, ускладненням типологій обходу санкцій та зростанням обсягів транзакцій, формальний підхід до скринінгу є недостатнім. Натомість пропонується модель «самопідтримуваного» фреймворку, здатного функціонувати з мінімальним ручним втручанням, постійно

[18] https://media.licdn.com/dms/document/media/v2/D4D1FAQGlOieoVmi6gw/feedshare-document-pdf-analyzed/B4DZxgK.AVIoAY-/0/1771140017129?e=1772064000&v=beta&t=g7s40TYMWtPzCM0_RusZIefmz6I2i6v8lN2PKsRhCMA

адаптуватися до змін регуляторних вимог і зберігати високу операційну ефективність.

Центральним елементом запропонованої моделі є формалізоване визначення цілей санкційного контролю та рівня прийнятного ризику, які повинні бути безпосередньо пов'язані з регуляторними зобов'язаннями установи та її бізнес-профілем. Документ підкреслює, що саме рівень прийнятного ризику визначає логіку побудови всієї системи: від налаштування алгоритмів і порогів спрацювання до порядку ескалації та розподілу ресурсів. Автор демонструє, що без чітко зафіксованого та погодженого на рівні керівництва підходу до допустимого співвідношення між хибними спрацюваннями та пропущеними збігами санкційний контроль неминуче стає нестабільним, непослідовним і вразливим для наглядових органів.

Подальший розвиток фреймворку ґрунтується на формуванні розвиненої системи корпоративного управління санкційними ризиками, у межах якої чітко розмежовуються повноваження операційних підрозділів, комплаєнсу та внутрішнього аудиту. Санкційний скринінг інтегрується в модель трьох ліній захисту, що забезпечує як операційну ефективність, так і незалежний контроль. Особлива увага приділяється формалізації процедур ескалації, прийняття рішень щодо потенційних порушень, управління санкційними списками та внесення змін до налаштувань системи. У цьому контексті система управління розглядається не як формальна вимога, а як ключовий механізм забезпечення стабільності, послідовності та відтворюваності санкційного контролю.

Важливим блоком документа є аналіз технологічної складової санкційного скринінгу. Автор підкреслює, що вибір програмного забезпечення має здійснюватися з урахуванням масштабованості, гнучкості, можливостей інтеграції та підтримки складних моделей співставлення даних. Окремо підкреслюється, що результативність системи визначається не назвою постачальника програмного забезпечення, а якістю її налаштування, тестування та постійної оптимізації. Значна увага приділяється інтеграції санкційного скринінгу з основною банківською системою, платіжними платформами, системами управління взаємовідносинами з клієнтами та системами управління справами, що забезпечує безперервність контролю на всіх етапах взаємодії з клієнтами та контрагентами.

Документ детально розкриває концепцію інтелектуального управління повідомленнями про спрацювання системи, відповідно до якої всі такі повідомлення класифікуються за рівнем ризику та обробляються в межах стандартизованої системи первинного аналізу та пріоритизації. Такий підхід дозволяє мінімізувати навантаження на аналітиків, зосередити ресурси на високоризикових випадках і водночас забезпечити повну аудиторську простежуваність рішень. Система управління справами розглядається як обов'язковий компонент, що забезпечує фіксацію всіх дій, строків, рішень і їх обґрунтування, а також формує основу для здійснення внутрішнього контролю якості.

Окремий акцент зроблено на якості даних та управлінні санкційними списками, які визначають фактичну результативність будь-якої системи скринінгу. Автор аргументує, що більшість помилок у санкційному контролі виникає через неповні, застарілі або некоректно структуровані клієнтські дані, а також через несвоєчасне оновлення списків. Тому фреймворк передбачає впровадження централізованих механізмів стандартизації, очищення та збагачення даних, а також жорстких процедур версіонування й аудиту змін у списках.

Вагомою складовою запропонованої моделі є система безперервного тестування, налаштування та контролю якості, яка забезпечує підтримання балансу між результативністю та операційною доцільністю. Регулярне сценарне тестування, регресійні перевірки після внесення змін, аналіз першопричин виявлених помилок та системні перевірки якості формують механізм постійного вдосконалення санкційного контролю. Зазначений процес розглядається як невід'ємний елемент системи управління ризиками, а не як допоміжна або другорядна функція.

Документ також приділяє значну увагу людському фактору та формуванню культури комплаєнсу. Автор підкреслює, що навіть за умов високого рівня автоматизації остаточна відповідальність за прийняття рішень залишається за фахівцями. Тому система повинна спиратися на постійне навчання, розвиток компетенцій, сценарне моделювання та підтримку з боку керівництва. Комплаєнс розглядається як організаційна цінність, а не лише як регуляторний обов'язок.

У контексті сталого розвитку системи особливе місце відводиться використанню штучного інтелекту та машинного навчання. Автор розглядає технології штучного інтелекту та машинного навчання як інструмент підвищення точності пріоритизації повідомлень про спрацювання системи, зменшення кількості повторюваних помилкових спрацювань та вдосконалення виявлення складних схем. Водночас підкреслюється необхідність запровадження жорсткої моделі управління моделями, яка передбачає контроль алгоритмічної упередженості, забезпечення пояснюваності прийнятих рішень, моніторинг погіршення якості функціонування моделей та постійний людський нагляд за їх застосуванням.

Завершальним елементом фреймворку є впровадження системи управлінської візуалізації через спеціалізовані дашборди, які дозволяють керівництву та комплаєнс-функції в режимі реального часу відстежувати ефективність санкційного контролю, стан списків, результати налаштувань і рівень регуляторної готовності. Таким чином, санкційний скринінг трансформується з реактивного механізму у стратегічний інструмент управління ризиками.

У підсумку документ формує цілісну методологічну модель, у межах якої санкційний контроль постає як поєднання управління ризиками, технологій, якісних даних, професійної експертизи та корпоративної культури. Запропонований фреймворк орієнтований на забезпечення не лише формальної відповідності вимогам регуляторів, а й довгострокової стійкості фінансової установи до санкційних ризиків у мінливому геополітичному та нормативному середовищі.

Анатомія шахрайства з інвойсами у сучасному бізнес-середовищі [19]

У світі, де фінансові потоки переміщуються з неймовірною швидкістю, а довіра є основою ділових відносин, виникає парадоксальна вразливість: чим простіше стає платити, тим легше стати жертвою тих, хто цією простотою зловживає. Шахрайство з рахунками-фактурами, або інвойсне шахрайство, міцно утримує позицію одного з найпоширеніших видів економічних злочинів, що вражають не лише корпорації, а й звичайні сім'ї та малі підприємства. Це явище — не просто технічний збій у системі безпеки, а складний соціально-інженерний механізм, що грає на найсвятішому для бізнесу — довірі між партнерами.

Сутність цього злочину, на перший погляд, є оманливо простою: зловмисники спонукають жертву здійснити платіж на підроблений рахунок або ж перенаправити легальний платіж на власний банківський рахунок. Однак за цією простотою ховається ціла індустрія обману. Злочинці можуть виступати в ролі давніх постачальників, перехоплювати електронне листування або створювати настільки переконливі фальшиві інвойси, що вони здатні ввести в оману навіть досвідчених бухгалтерів. Їхня мета — змусити жертву діяти швидко, не роздумуючи, використовуючи для цього психологічний тиск, терміновість та імітацію авторитетності.

Головна зброя у боротьбі з цим явищем — це знання. Розуміння того, як саме діють шахраї, є фундаментом, на якому будується будь-яка стратегія захисту. Першим і найважливішим кроком

[19] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/787-invoice-fraud-infosheet/file

є тотальна перевірка. Будь-яка, навіть найменша зміна в реквізитах рахунку, банківських даних або раптова вимога термінового платежу має сприйматися не як дрібна незручність, а як потенційний сигнал тривоги. Досвід свідчить, що шахраї часто покладаються на людську звичку ігнорувати деталі, сподіваючись, що отримувач рахунку просто не помітить підміни символу в електронній адресі постачальника або незначної зміни у фірмовому стилі листа.

Звідси випливає друге золоте правило — верифікація. В епоху цифрових комунікацій електронний лист перестав бути надійним джерелом інформації. Зловмисники можуть не лише надсилати фальшиві листи зі схожих адрес, а й перехоплювати легітимне листування, втручаючись у діалог між двома сторонами в найбільш невідповідний момент. Саме тому єдиним надійним способом підтвердити зміну платіжних реквізитів є телефонний дзвінок. Але дзвінок не за номером, вказаним у підозрілому листі, а за перевіреним, давно відомим номером телефону, який ви використовували для зв'язку з контрагентом раніше. Лише почувши знайомий голос і отримавши підтвердження, можна з чистою совістю переказувати кошти. Ніколи не слід переказувати гроші, доки не буде стовідсоткової впевненості в точності всіх деталей.

Важливо підкреслити, що стати жертвою інвойсного шахрайства — це не ознака недбалості чи професійної непридатності. Це свідчення надзвичайно високого рівня підготовки злочинців, які використовують витончені тактики соціальної інженерії. Вони ретельно вивчають свою жертву: структуру компанії, імена ключових співробітників, графік платежів, навіть стиль спілкування керівництва. Вторгаючись у цей контекст, вони будують своє повідомлення таким чином, щоб воно виглядало природно і не викликало підозр. Тому захист має бути багаторівневим: знання, ретельна перевірка та, найголовніше, впровадження надійних бізнес-процесів.

Для захисту бізнесу вкрай важливо розпізнавати попереджувальні сигнали на ранніх стадіях. Шахраї завжди намагатимуться створити відчуття терміновості — «терміновий платіж», «прострочена заборгованість», «останній шанс уникнути пені». Вони повідомлятимуть про зміну банківських реквізитів постійного постачальника, часто пояснюючи це «модернізацією системи» або «переходом на нове обслуговування». Сам рахунок-фактура може містити невідповідності: суми, номери референсів або контактні імена, які трохи відрізняються від попередніх, справжніх документів. Звертайте увагу на дрібні зміни в електронних адресах — наприклад, заміна літери або додавання дефісу, які роблять адресу шахрая майже ідентичною адресі справжнього постачальника. Несподівані рахунки за товари чи послуги, які ви не замовляли, а також незвична манера письма, граматичні помилки або дивні мовні звороти, що не властиві вашій звичній контактній особі, також мають викликати негайну підозру. Пам'ятайте головне правило: якщо ви маєте сумніви або відчуваєте тиск, не піддавайтеся емоціям. Зупиніться і перевірте.

Захист власних фінансів починається з утвердження принципу «довіряй, але перевіряй» на рівні внутрішньої політики компанії. Зміни банківських реквізитів мають підтверджуватися виключно через опубліковані офіційні номери телефонів або через особистий контакт із менеджером, з яким ви працювали роками. Впровадження системи «двох рук» для авторизації великих платежів, коли платіжне доручення мають підписати дві відповідальні особи, значно ускладнює завдання шахраям. Корисною звичкою є крос-перевірка кожного нового рахунку з попереднім, справжнім зразком, особливо якщо йдеться про велику суму або нового постачальника. Освіта ж є безперервним процесом: необхідно регулярно проводити тренінги для співробітників, особливо для фінансового відділу та відділу закупівель, нагадуючи їм про актуальні схеми шахрайства та методи протидії.

Окрема увага має приділятися кібербезпеці. Вразливі IT-системи — це відкриті двері для зловмисників. Забезпечення надійного захисту комп'ютерних мереж, регулярна зміна паролів (бажано з використанням багатофакторної автентифікації) та своєчасне оновлення

антивірусного програмного забезпечення є не просто технічними рекомендаціями, а критично важливими елементами фінансової безпеки. Зламана електронна пошта бухгалтера може коштувати компанії мільйони.

Нарешті, якщо ви підозрюєте, що вже стали жертвою шахрайства або ж маєте справу зі спробою обману, час стає вашим найлютішим ворогом. Негайно зв'яжіться зі своїм банком. Першочергове завдання — вимагати замороження коштів та рахунку отримувача на час проведення розслідування. Кожна хвилина зволікання зменшує шанси на повернення грошей. Після цього необхідно офіційно повідомити про шахрайство, подавши заяву або зателефонувавши на спеціальну лінію. І в жодному разі не видаляйте жодних доказів: збережіть усі електронні листи, підроблені рахунки-фактури та історію листування. Ці цифрові сліди стануть основою для слідства і можуть допомогти не лише вам, а й запобігти злочинам проти інших. Інвойсне шахрайство — це виклик, який вимагає від сучасного суспільства не лише технологічної обізнаності, а й культури фінансової обачності, де перевірка стає такою ж природною, як сам платіж.

Ваша думка важлива!

1. Чергове пленарне засідання FATF знову не зробило кроків до переведення росії до «чорного списку», незважаючи на накопичений масив доказів системного порушення нею міжнародних стандартів ПВК/ФТ. Якою має бути відповідь міжнародної спільноти на цю інституційну неспроможність FATF? Яку роль у цьому процесі повинні відіграти такі країни, як Україна?
2. Понад 80% критичних компонентів для російської оборонної промисловості досі проходять через юрисдикції-«хаби». Яким чином фінансові установи, що проводять транзакції з контрагентами в цих країнах, мають перебудувати свої AML-процедури, щоб не стати мимовільними ланками ланцюгів санкційного обходу? Чи запровадження «вторинних санкцій» змінить поведінку фінансового сектору в цих юрисдикціях?
3. Індекс CPI 2025 фіксує зниження антикорупційних показників навіть у традиційно «надійних» юрисдикціях. Чи вважаєте Ви, що стандартні підходи до оцінки юрисдикційного ризику потребують суттєвого перегляду? Якими практичними індикаторами, крім балів CPI, Ви б доповнили систему оцінки ризиків при роботі з клієнтами та контрагентами з юрисдикцій, що демонструють негативну динаміку?
4. Як інтеграція України до європейського простору ПВК/ФТ та імплементація статті 75 AMLR можуть змінити архітектуру національної системи протидії фінансовим злочинам, і чи готові українські інституції до такого рівня відповідальності та прозорості?
5. Яким чином українські програми підтримки внутрішньо переміщених осіб враховують ризики потрапляння переселенців у трудове рабство або боргову кабалу на неформальних ринках праці у великих містах, і які додаткові механізми запобігання могли б бути запроваджені?
6. Як впливає високий рівень цифровізації державних послуг та банкінгу в Україні на чутливість бізнесу до інвойсного шахрайства? Чи створює звичка швидко вирішувати питання онлайн «гіпер-довіру» до електронних документів, що робить український бізнес більш вразливим до фішингу та підроблених рахунків?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-08

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

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