Методологічний бюлетень

Серійний номер: МінФін-AML-2025-51

Грудень 2025

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

Джим Рон

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Глобальна податкова прозорість в епоху криптоактивів: Впровадження CARF як відповідь на нові виклики [1]

У відповідь на швидке поширення криптоактивів як нового глобального фінансового феномену, що несе в собі як економічні перспективи, так і суттєві ризики для податкової прозорості, Глобальний форум з питань прозорості та обміну інформацією з метою оподаткування опублікував оновлення щодо моніторингу та впровадження Звітного механізму щодо криптоактивів (Crypto-Asset Reporting Framework, CARF). Цей документ, схвалений Групою CARF та прийнятий членами Глобального форуму, є логічним продовженням багаторічної міжнародної роботи з протидії ухиленню від сплати податків та забезпеченню автоматичного обміну інформацією (AEOI). Він детально описує політичну динаміку, інституційні процеси та практичні кроки, необхідні для інтеграції

[1] https://www.oecd.org/content/dam/oecd/en/networks/global-forum-tax-transparency/crypto-asset-reporting-framework-monitoring-implementation-update-2025.pdf

криптосектору в глобальну систему податкової прозорості, прагнучи запобігти його використанню як опори для приховання доходів і активів за кордоном.

Основним імпульсом для створення CARF стало усвідомлення міжнародним співтовариством, зокрема «Групою двадцяти» (G20), того, що швидкий ріст ринку криптоактивів ставить нові виклики перед податковими адміністраціями. Традиційні механізми обміну інформацією, такі як Стандарт спільного звітування (Common Reporting Standard, CRS), що успішно впроваджений з 2014 року, виявилися недостатніми для охоплення транзакцій з цифровими активами. Це створювало небезпеку того, що капітал міг перетікати з регульованого фінансового сектора в менш прозорий криптосектор, тим самим підриваючи досягнуті успіхи в боротьбі з міжнародним ухиленням від сплати податків. У відповідь на ці ризики OECD спільно з G20 розробила CARF – спеціалізовану рамку, яка поширює принципи AEOI на операції з криптоактивами, вимагаючи від постачальників послуг (Reporting Crypto-Asset Service Providers) збирати та повідомляти інформацію про транзакції своїх клієнтів (Reportable Users) податковим органам країни їхнього резидентства.

Документ підкреслює надзвичайно сильну політичну підтримку CARF на найвищому рівні, що виступає критичною умовою його успішної імплементації. Посилання на комюніке міністрів фінансів G20 ще з 2021 року та декларації лідерів G20 в Балі (2022) та Нью-Делі (2023) демонструють послідовний і невпинний тиск з боку провідних економік світу на необхідність швидкого розроблення, завершення та впровадження цього механізму. Цей політичний консенсус дозволив Глобальному форуму, якому було доручено забезпечити широкомасштабне впровадження, розпочати активну інституційну роботу.

Ключовим досягненням станом на кінець 2025 року є те, що 75 юрисдикцій, включаючи більшість світових центрів обігу криптоактивів, вже взяли на себе політичні зобов'язання щодо імплементації CARF в рамках спеціального процесу зобов'язань Глобального форуму. Ця цифра свідчить про значний прогрес у створенні критичної маси учасників, необхідної для ефективності системи.

Для забезпечення всеосяжності та уникнення спроб обійти нові правила Глобальний форум запровадив складний та динамічний процес визначення «Юрисдикцій, що мають значення» для CARF (CARF Jurisdictions of Relevance). Цей щорічний процес спрямований на ідентифікацію всіх країн і територій, де діють або можуть з'явитися значні постачальники послуг з криптоактивів. Він ґрунтується на аналізі даних FAFT, національних регуляторних звітів та інформації з приватного сектору. Критерії включення є широкими та враховують різні типи зв'язків постачальника послуг з юрисдикцією: резидентство для цілей оподаткування, місце реєстрації, місце управління або наявність постійного місця ведення бізнесу. Така широта покликана закрити потенційні лазівки та гарантувати, що постачальник послуг, який намагається змінити юрисдикцію на ту, що не бере участі в CARF, все одно залишиться під дією звітних вимог, якщо у нього збережуться зв'язки з іншою юрисдикцією-учасницею. Цей аспект підкреслює проактивний та технічно виважений підхід розробників до мобільності криптосектору.

Окрему увагу в документі приділено практичним аспектам імплементації, яка розгортається за триєдиною схемою: правові рамки, адміністративно-технологічна інфраструктура та гарантії конфіденційності. На внутрішньодержавному рівні юрисдикції повинні прийняти законодавство, яке зобов'язує постачальників послуг проводити належну перевірку клієнтів та звітувати. Для перших обмінів, запланованих на 2027 рік, таке законодавство має набрати чинності вже з початку 2026 року, оскільки обмінюватися будуть даними за попередній рік.

Документ констатує, що багато юрисдикцій вже мають або знаходяться на завершальній стадії прийняття необхідних законів. На міжнародному рівні основним правовим інструментом для обміну є Конвенція про взаємну адміністративну допомогу у податкових справах (MAAC), учасниками якої є майже всі юрисдикції, що взяли зобов'язання щодо CARF. Додатково 53

юрисдикції вже підписали Багатосторонню угоду уповноважених органів щодо CARF (CARF MCAA), що спрощує встановлення двосторонніх адміністративних процедур.

Технічна інфраструктура будується з розрахунком на синергію з наявними системами CRS. Більшість країн планують розширити свої портали для автоматичного обміну інформацією, щоб включити звітування за CARF. Для безпечного міжнародного обміну даними буде використовуватися вже існуюча Система загальної трансмісії (Common Transmission System, CTS), що керується Глобальним форумом. Всі дані повинні відповідати спеціальній XML-схемі CARF, що забезпечує стандартизацію та можливість валідації інформації.

Ключовим завданням для національних адміністрацій стає розробка пропорційних, заснованих на оцінці ризиків стратегій дотримання вимог та їх примусового виконання, спрямованих на ідентифікацію всіх постачальників послуг, що підлягають звітуванню, та перевірку повноти і точності наданих ними даних. При цьому Глобальний форум зберігає механізм оцінки стандартів конфіденційності та захисту даних, запроваджений для CRS, який може призвести до припинення обміну з юрисдикціями, що не забезпечують належного рівня захисту інформації.

Висновки:

- **Рамка звітності щодо криптоактивів (CARF) отримала надзвичайно сильну політичну підтримку на найвищому рівні**, зокрема від G20, що дозволило Глобальному форуму швидко розпочати процес її впровадження. Станом на кінець 2025 року 75 юрисдикцій, включаючи більшість світових криптоцентрів, вже взяли на себе політичні зобов'язання.
- **Глобальний форум розробив складні інституційні механізми для забезпечення ефективності CARF:** щорічний процес ідентифікації «Юрисдикцій, що мають значення», широкі критерії зв'язку для постачальників послуг, що унеможливлюють легке уникнення правил, та триєдину модель впровадження.
- **Документ фіксує перехід від стадії розробки стандартів до стадії їх практичної імплементації.** Багато юрисдикцій, які планують почати обмін даними з 2027 року, вже приймають необхідне внутрішнє законодавство та розбудовують технологічну інфраструктуру.
- **Кінцева мета CARF — не просто збір даних, а запобігання перетіканню капіталу** з традиційного фінансового сектору в менш прозорий криптосектор для ухилення від оподаткування.

Реалізація такого амбітного міжнародного проекту неможлива без всебічної підтримки. Глобальний форум розробив комплексну стратегію нарощування потенціалу, що включає створення типового законодавства, запити на яке надійшли від понад 50 юрисдикцій, проведення масштабних навчальних заходів для понад 1500 службовців з більш ніж 140 країн, а також запуск спеціальної програми «майстер-класів» для детального вивчення технічних правил CARF. Ця підтримка спрямована на забезпечення однорідного та якісного впровадження стандарту в різних правових і адміністративних системах.

Таким чином, звіт фіксує перехід міжнародної спільноти від фази політичного узгодження та розробки правил до фази їх практичної імплементації. Створена система є амбітною спробою закріпити принципи податкової прозорості й справедливості в динамічному й децентралізованому середовищі цифрових активів. Успіх цього проекту залежатиме від узгодженості дій великої кількості юрисдикцій, ефективності їх адміністративних механізмів та здатності системи адаптуватися до постійної еволюції крипторинку. Остаточним випробуванням стане початок перших автоматичних обмінів даними у 2027 році, який має продемонструвати, чи справді вдалося інтегрувати криптосектор у глобальну архітектуру фіскальної прозорості, закривши одну з останніх значущих лазівок для міжнародного ухилення від сплати податків.

Прозорість контролю над компаніями: Аналіз британського механізму реєстрації осіб, що мають суттєвий контроль (PSC) [2]

Впровадження Реєстру осіб, що мають суттєвий контроль (People with Significant Control, PSC), у Великій Британії є ключовою ланкою в глобальній трансформації фінансової прозорості, спрямованої на протидію відмиванню коштів, ухиленню від сплати податків та прихованій власності на корпоративні структури.

Видана Міністерством бізнесу та торгівлі п'ята редакція керівництва є не просто технічним довідником — це всеосяжний стратегічний документ, що відображає зрілість та динаміку британського регуляторного підходу після дев'яти років існування цього режиму. Документ аналізує його як прояв системної еволюції, від ранніх спроб запровадити прозорість до складного, технологічно інтегрованого механізму, центральну роль у якому відіграє Companies House, що перетворюється з пасивного репозитарію даних на активного учасника у забезпеченні дотримання вимог.

Філософською основою режиму PSC є перехід від формалізованої структури власності до розкриття реальних бенефіціарних власників — фізичних осіб, які остаточно володіють або контролюють юридичні особи. Це виходить далеко за рамки традиційних реєстрів акціонерів. Документ деталізує п'ять квантифікованих та якісних критеріїв визначення PSC:

- володіння понад 25% акцій або прав на активи при ліквідації (умова i),
- понад 25% голосуючих прав (умова ii),
- право призначати або звільняти більшість керівників (умова iii),
- право здійснювати або фактичне здійснення суттєвого впливу чи контролю (умова iv),
- контроль над трастами чи фірмами, які, у свою чергу, відповідають першим чотирьом умовам (умова v).

Особливу увагу приділено саме умовам (iv) та (v), що вимагають від компаній не лише механічного аналізу документів, а й глибокого розуміння фактичних відносин впливу, звертаючись до окремого статутного керівництва. Цей підхід визнає, що реальний контроль часто здійснюється не через пряме володіння акціями, а через складні мережі домовленостей, трастів, номінальних осіб та неформальних каналів впливу.

Ключовою новиною 2025 року, відображеною в документі, є фундаментальна зміна архітектури реєстру: скасування вимоги про ведення компаніями «локальних» реєстрів PSC та повна централізація даних в єдиному реєстрі Companies House, що набуло чинності 18 листопада 2025 року. Ця зміна, передбачена Законом про економічні злочини та корпоративну прозорість 2023 року, значно підвищує ефективність та доступність інформації. Вона усуває ризик розбіжностей між внутрішніми та публічними даними та закладає основу для більш активної перевірки даних реєстратором.

Паралельно з цим впроваджується обов'язкова верифікація особи PSC, що є іншим революційним кроком. Особи з суттєвим контролем тепер повинні підтвердити свою особу безпосередньо в Companies House або через авторизованого корпоративного постачальника послуг (ACSP), отримуючи унікальний персональний код. Це перетворює реєстр з колекції потенційно анонімних записів на базу даних, де кожен ключовий бенефіціар ідентифікований

[2] https://assets.publishing.service.gov.uk/media/691c9c97e39a085bda43ef2b/register-of-people-with-significant-control-guidance-for-registered-unregistered-companies.pdf

та перевірений державою, що є потужним інструментом протидії використанню підставних осіб та складних схем.

Документ ретельно структурує обов'язки компаній навколо концепції «розумних кроків» (reasonable steps). Він не лише описує ідеальний сценарій, але й надає детальну дорожню карту дій у разі спротиву або небажання розкривати інформацію з боку PSC. Система повідомлень (notices) за розділами 790D, 790DA, 790E, 790EA Закону про компанії 2006 року є формалізованим механізмом взаємодії. Якщо особа ігнорує запит, компанія зобов'язана пройти триетапну процедуру: попередження, а потім — накладення обмежень на відповідну частку або права. Обмеження є суворим заходом, який фактично заморожує активи: заборони на передачу, голосування, виплату дивідендів або випуск нових акцій. Цей примусовий механізм перетворює компанію з пасивного на активного учасника в процесі виявлення бенефіціарів, який має реальні повноваження для впливу на недобросовісних осіб.

Важливим аспектом режиму, детально розглянутим у Додатку 1, є баланс між прозорістю та захистом. Визнаючи, що розкриття інформації про бенефіціарів може створити серйозні ризики для окремих осіб, система передбачає механізм захисту інформації PSC у «виключних обставинах», а саме — при серйозній загрозі насильства чи залякування. Захист може стосуватися як приховування адреси місця проживання, так і повного вилучення всієї інформації про PSC з публічного реєстру. Проте, навіть у разі захисту, дані залишаються доступними для правоохоронних органів і податкових служб, що підкреслює першочергову мету режиму — боротьбу зі злочинністю, а не безпідставне вторгнення в приватне життя.

Особливу цінність керівництву надає його практична спрямованість. Воно містить детальні додатки для різних організаційних форм: товариств з обмеженою відповідальністю (LLP) та відповідних шотландських партнерств (SLP, SQP). У цих додатках адаптовані критерії контролю: наприклад, для LLP замість володіння акціями розглядаються права на понад 25% активів, що залишаються після ліквідації. Крім того, документ містить зразки всіх необхідних юридичних повідомлень, фактично надаючи компаніям готові інструменти для дотримання вимог, що знижує операційні бар'єри та ризик помилок.

Висновки:

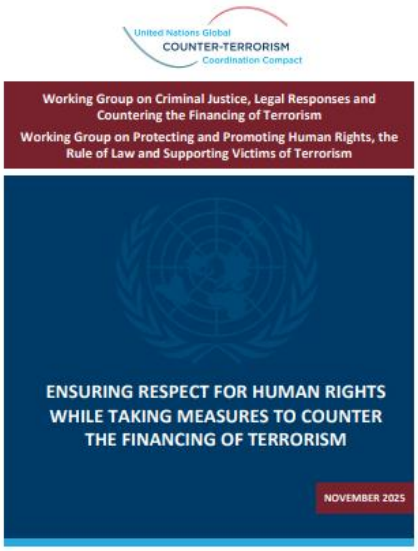
- **Британський режим PSC пройшов довгий шлях.** Скасування локальних реєстрів та повна централізація в Companies House означає радикальну зміну: державний реєстр стає єдиним, активним джерелом перевіреної істини, а не пасивним архівом.
- **Серцевиною системи є п'ять критеріїв визначення PSC**, особливо умови (iv) та (v), що стосуються «суттєвого впливу чи контролю». Це дозволяє виявляти не лише формальних власників акцій, але й реальних бенефіціарів.
- **Документ деталізує прогресивну модель зобов'язань:** компанія має вжити «розумних кроків» для виявлення PSC; PSC зобов'язані співпрацювати та пройти верифікацію особи; у разі опору закон передбачає сувору процедуру ескалації.
- **Режим визнає, що публічне розкриття інформації про бенефіціарів може створити серйозні ризики для окремих осіб.** Тому в екстремальних випадках (серйозна загроза насильства чи залякування) передбачено механізм захисту (приховування) даних з публічного реєстру.

Таким чином, оновлене керівництво з реєстру PSC є свідченням того, як Велика Британія інтегрує боротьбу з економічною злочинністю в самі основи корпоративного права. Режим еволюціонував від відносно простої вимоги про розкриття інформації до комплексної екосистеми, що поєднує централізований перевірений реєстр, чіткі процедурні кроки для компаній, суворі механізми примусу та обмежені, але реалістичні гарантії безпеки для осіб, що перебувають під загрозою. Ця система будується на принципі спільної відповідальності:

держава (через Companies House) забезпечує інфраструктуру та верифікацію, компанії мають активний обов'язок розслідування та звітування, а PSC зобов'язані співпрацювати та підтверджувати свою особу.

Успіх цього підходу робить британський реєстр PSC одним із найбільш просунутих інструментів бенефіціарної прозорості у світі, модель якого можуть, з урахуванням національного контексту, вивчати інші юрисдикції, включаючи Україну, в руслі її євроінтеграційних зобов'язань щодо протидії відмиванню коштів.

Баланс між безпекою та свободою: дотримання прав людини в контексті протидії фінансуванню тероризму [3]



У листопаді 2025 року в рамках Глобального пакту ООН з координації боротьби з тероризмом (UN Global Counter-Terrorism Coordination Compact) було опубліковано керівні настанови, присвячені критично важливому питанню: як забезпечити дотримання прав людини під час впровадження заходів щодо протидії фінансуванню тероризму (ПФТ).

Цей документ, розроблений спільною робочою групою з кримінального правосуддя, правових відповідей та протидії фінансуванню тероризму та робочою групою з захисту та сприяння правам людини, верховенству права та підтримки жертв тероризму, є результатом широких консультацій з державами-членами, неурядовими організаціями, експертами з прав людини та іншими зацікавленими сторонами.

На тлі глобальної боротьби з тероризмом, яка часто призводить до впровадження жорстких фінансових обмежень, виникає напруга між необхідністю забезпечення безпеки та обов'язком дотримання міжнародного права в галузі прав людини. Керівні настанови відзначають, що заходи ПФТ, спрямовані на виявлення, блокування та конфіскацію коштів, що використовуються для терористичних цілей, нерідко реалізуються за рахунок обмеження фундаментальних свобод. Перебільшено широкі визначення тероризму та його фінансування, масова фінансова розвідка, цільові фінансові санкції з обмеженими гарантіями правової процедури, а також надмірне регулювання некомерційного сектору — все це може призвести до серйозних порушень прав людини, включаючи право на приватність, свободу асоціації, мирних зібрань, справедливий суд та економічні права.

Документ ґрунтується на комплексній міжнародній правовій основі, яка включає Міжнародний пакт про громадянські та політичні права, Міжнародну конвенцію про боротьбу з фінансуванням тероризму, резолюції Ради Безпеки ООН (зокрема 1373 (2001), 2462 (2019)), Рекомендації Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) та інші інструменти. Ключовим принципом, що пронизує весь документ, є необхідність дотримання державами принципів законності, необхідності, пропорційності та недискримінації під час впровадження будь-яких обмежувальних заходів.

Однією з найбільш проблемних зон, детально розглянутих у керівній записка, є криміналізація фінансування тероризму. Відзначається, що через відсутність універсального визначення тероризму багато держав прийняли національні закони з надмірно широкими та розмитими

[3] https://www.ohchr.org/sites/default/files/documents/issues/terrorism/respect-measures-financing-terrorism-1-en.pdf

формулюваннями. Це створює ризик свавільного застосування законів проти політичних опонентів, правозахисників, неурядових організацій та навіть медичних і гуманітарних працівників. Документ наголошує, що визначення «фінансування тероризму» має бути чітким, передбачуваним і точно відповідати міжнародним стандартам, зокрема статті 2 Конвенції 1999 року, а кримінальна відповідальність повинна виникати лише за наявності прямого умислу («mens rea»).

Значну увагу приділено конфлікту між заходами фінансової розвідки та правом на приватність і захист даних. Фінансові розвідувальні підрозділи, правоохоронні та розвідувальні органи збирають та аналізують величезні масиви даних про транзакції, часто з використанням автоматизованих систем моніторингу. Документ констатує, що такі практики, особливо коли вони здійснюються без належного судового контролю, чіткої правової основи та ефективних механізмів захисту, можуть становити свавільне втручання в приватне життя. Також висловлюється стурбованість щодо масового стеження, профілювання за расовою, релігійною або політичною ознакою та обміну даними між державами з різним рівнем захисту прав людини. Як рішення пропонуються посилення внутрішнього та незалежного зовнішнього нагляду, обов'язкові оцінки впливу на права людини та призначення уповноважених із захисту даних у відповідних органах.

Питання справедливого судового розгляду є особливо гострим у справах, пов'язаних із фінансуванням тероризму. Документ зазначає, що у деяких випадках судочинство відбувається у спеціальних судах з обмеженим доступом до доказів, адвоката та гласності з посиланням на національну безпеку. Такі практики, як наголошується, часто суперечать стандартам, встановленим у статті 14 Міжнародного пакту про громадянські та політичні права, включаючи презумпцію невинуватості та право на ефективний захист. Особливу проблему становить використання в якості доказів інформації від розвідувальних служб, доступ до якої для захисту може бути обмеженим. Для вирішення цих проблем документ закликає до посилення судового контролю за спеціальними слідчими методами, надання обвинуваченому всієї необхідної інформації для оскарження та підвищення кваліфікації правоохоронців і прокурорів у галузі прав людини.

Окремий розділ присвячений впливу заходів ПФТ на цивільний простір, зокрема на діяльність некомерційних організацій (НКО). За останні роки НКО по всьому світу стикаються зі зростаючими труднощами через посилення фінансового моніторингу, обтяжливі звітні вимоги, обмеження на отримання іноземного фінансування та практику «де-рискінгу» з боку банків. Остання полягає в тому, що фінансові установи, намагаючись уникнути ризиків, масово закривають рахунки НКО або відмовляють у послугах, особливо тим організаціям, які працюють у конфліктних регіонах. Це не тільки паралізує життєво важливу гуманітарну та правозахисну діяльність, але й безпосередньо порушує право на свободу асоціацій.

FATF, визнаючи цю проблему, переглянула Рекомендацію 8, наголосивши на необхідності виваженого, ризик-орієнтованого підходу, який не повинен безпідставно перешкоджати законній діяльності НКО. Документ закликає держави залучати громадянське суспільство до розробки заходів ПФТ, уникати підходу «однаковий розмір санкцій для всіх» та встановлювати механізми оскарження свавільних дій фінансових установ.

Критично важливим є аналіз впливу заходів ПФТ на гуманітарну діяльність. Медичні працівники та гуманітарні організації, які надають життєво необхідну допомогу населенню в зонах конфліктів, де часто діють терористичні угруповання, самі можуть стати мішенями для переслідувань. Широкі визначення «підтримки тероризму» можуть криміналізувати надання медичної допомоги, продовольства чи притутку цивільним особам на підконтрольних терористам територіях. Хоча Рада Безпеки у резолюції 2664 (2022) запровадила виняток для гуманітарної діяльності, на практиці його імплементація залишається складною через надмірну

обережність банків та нечіткі національні законодавства. Керівна записка наполягає на необхідності чітких і безпечних юрисдикційних винятків, які б дозволяли безперешкодне надання гуманітарної допомоги відповідно до принципів міжнародного гуманітарного права.

Документ також висвітлює гендерний аспект заходів ПФТ, який часто залишається поза увагою. Санкції, що застосовуються до «асоційованих осіб», непропорційно впливають на жінок і дітей, які можуть бути фінансово залежними від зазначених членів сім'ї та не мати доступу до коштів для задоволення базових потреб. Жіночі правозахисні організації, особливо невеликі та місцеві, стикаються з найбільшими труднощами у доступі до фінансування через сприйняття їхньої роботи як «ризикованої». Крім того, гендерно-нейтральні оцінки ризиків можуть призвести до неадекватного розуміння ролі жінок як у фінансуванні тероризму, так і у боротьбі з ним. Закликається систематично інтегрувати гендерну перспективу у всі заходи ПФТ, збирати розділені за статтю дані та забезпечувати рівний доступ до правосуддя.

Висновки:

- **Протидія фінансуванню тероризму повинна невідступно дотримуватися міжнародного права** та прав людини. Це основа всього керівного документа.
- **Заходи ПФТ часто мають серйозні непрямі наслідки, особливо для громадянського суспільства.** Надмірно широкі заходи призводять до звуження громадянського простору, перешкоджають роботі неурядових організацій (НУО) та обмежують надання життєво необхідної гуманітарної допомоги у зонах конфліктів.
- **Підхід, заснований на оцінці ризиків, є центральним для ефективної ПФТ.** Держави повинні ідентифікувати та оцінювати реальні, підтверджені фактами ризики фінансування тероризму, а не застосовувати загальні обмежувальні заходи до цілих секторів.
- **Заходи ПФТ мають значний гендерний вплив, який часто ігнорується.** Гендерно-нейтральні на перший погляд закони можуть дискримінувати на практиці.

Окремо розглядається роль приватного сектору, зокрема фінансових установ, які стали «на передовій» у впровадженні заходів ПФТ. На них покладаються обов'язки з ідентифікації клієнтів, моніторингу транзакцій та подання підозрілих звітів. Однак, відсутність чіткого державного керівництва та страх перед суворими штрафами призводять до практик надмірної обережності та де-рискінгу.

Документ нагадує, що відповідно до Керівних принципів ООН з бізнесу та прав людини, приватні компанії несуть відповідальність за повагу до прав людини навіть за відсутності чітких державних регуляцій. Держави ж зобов'язані забезпечити ефективне регулювання та нагляд, щоб діяльність приватного сектору не призводила до порушень прав.

У висновку можна сказати, що ці настанови ООН є своєчасним та всебічним інструментом, який нагадує міжнародній спільноті про необхідність дотримання балансу між безпекою та свободою. Вони не заперечують важливості боротьби з фінансуванням тероризму, але наголошують, що ця боротьба буде ефективною лише в тому випадку, якщо вона ведеться в рамках верховенства права та з повагою до гідності кожної людини.

Реалізація рекомендацій вимагає політичної волі, міжвідомчої координації, постійного діалогу з громадянським суспільством та нарощування потенціалу правозахисних інститутів. Тільки тоді заходи, спрямовані на позбавлення терористів фінансових ресурсів, не будуть одночасно підривати демократичні основи суспільства, цивільний простір та захист найвразливіших верств населення.

Economic Crime Survey 2024: Економічна злочинність у британському бізнесі [4]

На тлі глобальної нестабільності та цифрової трансформації економічна злочинність перетворилася з нішевої загрози на системний виклик для національної безпеки та фінансової стійкості. Проте, незважаючи на політичні декларації та медійну увагу, реальний масштаб цього явища, особливо крізь призму безпосереднього досвіду бізнесу, залишався в значній мірі невідомим, прихованим за межами офіційної статистики та фрагментарних досліджень. Масштабне опитування, проведене Міністерством внутрішніх справ Великої Британії, намагається розвіяти цю завісу, пропонуючи безпрецедентно детальну та репрезентативну картину того, як шахрайство, корупція та відмивання коштів торкаються компаній зі співробітниками по всій країні.

Шахрайство постає як наймасовіша та найбільш відчутна форма економічної злочинності, справжня епідемія, що охопила корпоративну Британію. Цифри викликають тривогу: кожна четверта компанія із співробітниками (27%, або приблизно 389 тисяч бізнесів) стала жертвою шахрайських дій протягом лише одного року. Однак справжній масштаб розкривається, коли аналіз переходить від поширеності до інтенсивності. Загальна кількість інцидентів перевищує 6 мільйонів, що свідчить про надзвичайно високу частоту атак. Середня постраждала компанія пережила 16 окремих випадків шахрайства, а це означає, що бізнес стикається не з одноразовим інцидентом, а з постійним, нав'язливим тиском, що вимагає безперервних ресурсів для відсічі. Структура шахрайства дедалі більше зміщується у цифрову площину: 40% останніх інцидентів були спричинені кібератаками, причому фішингові атаки виступають основним механізмом. Це підкреслює симбіоз традиційного шахрайства з сучасними кіберзагрозами, створюючи гібридні ризики, для боротьби з якими багатьом компаніям бракує спеціалізованих навичок.

Фінансовий тягар є колосальним. Хоча безпосередні грошові втрати від шахраїв оцінюються в £486 мільйонів, повна економічна вартість, що включає витрати на персонал, розслідування, нові системи захисту та втрачені можливості, сягає £812 мільйонів. Ще більш показовим є той факт, що витрати бізнесу на превентивні заходи — страхування, програмне забезпечення, навчання, співробітників — перевищують вартість самих інцидентів майже втричі, складаючи додаткові £2,57 мільярда. Це формує парадоксальну економіку страху, де витрати на запобігання злочинам стають значущою статтею операційних витрат, особливо для середніх і великих компаній, які несуть пропорційно більше тягарів.

При цьому, незважаючи на масштаб проблеми, лише третина компаній повідомляє про інциденти зовнішнім органам. Банки залишаються основним адресатом скарг (41% тих, хто повідомляв), тоді як правоохоронна система — поліція та Підрозділ з протидії шахрайству — отримує сигнали лише від 22%. Це розкриває глибоку кризу довіри або сприйняття ефективності: більшість бізнесів вважає, що звернення до правоохоронців не принесе ніякої користі або що інцидент недостатньо серйозний для такої дії. Така позиція фактично створює імунітет для дрібного та середнього шахрайства, дозволяючи йому процвітати в тіні.

У той час як шахрайство діє масово та часто відкрито, корупція, зокрема хабарництво, існує у витонченій, прихованій сфері, що робить її складнішою для виявлення та вимірювання, але не менш руйнівною. Дослідження зосередилося на хабарництві як найбільш вимірюваному прояві корупції, виявивши, що 3% компаній (близько 40 500) мали досвід участі в таких інцидентах. Оцінки загальної кількості пропозицій хабарів сягають 117 тисяч на суму близько £309

[4] https://www.gov.uk/government/publications/economic-crime-survey-2024/economic-crime-survey-2024

мільйонів, із середнім розміром £2 640. Однак найсуттєвішим відкриттям є не статистика, а культурний та процедурний контекст. Майже 70% пропозицій або вимог висловлювалися усно, без жодного документального сліду, що перетворює боротьбу з корупцією на складну гру, де докази практично відсутні. Більш того, виявлення цих інцидентів покладається не на внутрішні контрольно-ревізійні механізми (лише 5% випадків), а на особисту чесність та мужність окремих співробітників, які самостійно повідомляють про отримані пропозиції.

Ще більш тривожним є виявлений рівень байдужості або навіть нормалізації: 61% компаній, яким пропонували хабар, та 59% тих, хто мав його дати, заявили, що інцидент не справив жодного впливу на їхній бізнес. Це може свідчити про те, що в окремих секторах — будівництві, сфері послуг, адміністративному та транспортному секторах, де рівні хабарництва найвищі — певні неформальні платежі або обміни послугами сприймаються як невід'ємна, навіть якщо й небажана, частина бізнес-процесів.

Однак ця нормалізація має чіткі вторинні ефекти: 5% компаній вважають, що програвали тендери через те, що конкурент дав хабар, а серед компаній, що ведуть міжнародну торгівлю, цей показник зростає до 7%, особливо в регіонах, що сприймаються як такі, що мають високий ризик, — Африці, країнах Азіатсько-Тихоокеанського регіону, країнах Перської затоки. Готовність до боротьби з корупцією залишається кричущою недостатньою: понад половина компаній (55%) не мають жодних, навіть формальних, антикорупційних механізмів, таких як кодекси поведінки, політики або механізми інформування. Це свідчить про глибоке розходження між усвідомленням корупції як абстрактної загрози та сприйняттям її як актуального операційного ризику, що потребує конкретних механізмів реакції.

Відмивання коштів, на відміну від шахрайства, виглядає як нішева, але надзвичайно витончена загроза. Дослідження, яке вперше кількісно оцінило досвід бізнесу в цій сфері, показує, що лише 2% компаній (близько 33 500) ідентифікували інциденти, пов'язані з відмиванням. Проте ці компанії стали свідками приблизно 225 тисяч окремих підозрілих дій, що вказує на систематичний характер спроб інтеграції незаконних коштів у легальну економіку. Найпоширенішими схемами виступають виплата зарплат у готівці для уникнення оподаткування та контролю (26%) та маніпуляції з платіжними документами (20%). Ключовою проблемою є надзвичайно низький рівень усвідомлення ризику: 95% компаній не вважають себе ціллю для відмивання грошей, посилаючись на невеликі розміри, відсутність роботи з готівкою або довіру до клієнтів. Ця ілюзія безпеки розвіюється при поглибленому аналізі: нерегульовані компанії, які становлять більшість бізнесу, виявляють більше інцидентів у абсолютних цифрах (приблизно 23 300), ніж регульовані (10 200), хоча останні мають вищі показники поширеності через кращу підготовленість до виявлення.

Процес виявлення відмивання грошей часто покладається не на автоматизовані системи моніторингу (їх використовує лише 10% бізнесів), а на досвід, інтуїцію та «відчуття» співробітників (40% випадків). Бізнес, особливо нерегульований, опиняється в складному становищі: з одного боку, відсутність чітких доказів ускладнює звернення до правоохоронців, з іншого — побоювання репутаційних втрат, юридичної відповідальности та навіть фізичних загроз змушують їх уникати будь-якої участі в підозрілих операціях. Досвід подання Повідомлень про підозрілу діяльність (SAR) серед регульованих компаній характеризується як бюрократично складний, що вимагає значних трудовитрат, і часто завершується інформаційним вакуумом через відсутність зворотного зв'язку від національних агентств, що знижує мотивацію до подальшого інформування.

Таким чином, дослідження малює складний та багаторівневий ландшафт загроз. З одного боку, існує масове, майже рутинне шахрайство, що наносить мільярдні збитки та сприймається як постійна операційна витрата. З іншого — глибоко вкорінена, таємна культура корупції в окремих секторах, що спотворює конкуренцію та підриває довіру до інституцій. І, нарешті, — складна,

технологічно витончена загроза відмивання грошей, яку більшість бізнесу ігнорує через помилкове відчуття безпеки. Об'єднує ці різні форми економічної злочинності кілька ключових тем: значне недоінформування бізнесу про реальні ризики, брак довіри або віри в ефективність формальних механізмів звітності, переважання неформальних методів виявлення над структурованими процесами, а також критична залежність від розміру та сектору компанії. Маленький, нерегульований бізнес часто залишається найбільш вразливим і найменш підготовленим, тоді як великі та регульовані компанії несуть найбільші фінансові втрати, але й мають більше ресурсів для захисту.

Висновки:

- **Шахрайство стало масовим явищем** — кожна четверта компанія стикається з ним щороку, з загальною кількістю понад 6 мільйонів інцидентів, що завдає мільярдних прямих і непрямих збитків, однак лише третина бізнесів повідомляє про це правоохоронцям.
- **Корупція існує у тіні, але є системною проблемою —** близько 3% компаній стикаються з хабарництвом, суми якого оцінюються в сотні мільйонів фунтів. Переважна більшість пропозицій або вимог висловлюється усно, а бізнес демонструє байдужість або нормалізацію таких практик.
- **Відмивання коштів недооцінюється бізнесом** — 95% компаній не вважають себе під загрозою, хоча нерегульований малий бізнес виявляє більше інцидентів, ніж регульований. Виявлення частіше покладається на інтуїцію, а не на формальні процеси.
- **Підготовленість бізнесу до протидії значно відрізняється** — великі та регульовані компанії мають значно більше заходів захисту, тоді як малий і середній бізнес часто не має жодних механізмів протидії, особливо в сферах корупції та відмивання коштів.

Результати дослідження чітко вказують на необхідність парадигмальної зміни в підході до боротьби з економічною злочинністю. Замість універсальних рішень потрібні секторально-специфічні стратегії, що враховують унікальні вразливості. Критично важливим є спрощення процесів звітності, особливо для SAR, надання бізнесу чітких, практичних інструкцій та гарантованого зворотного зв'язку. Необхідно подолати розрив між великим бізнесом, який інвестує у безпеку, і малим, який залишається практично беззахисним, можливо, через цільові програми підтримки та спрощені, доступні інструменти.

Нарешті, ключовим завданням є трансформація корпоративної культури — від байдужості та нормалізації окремих злочинів до активної, усвідомленої відповідальності, де етична поведінка та дотримання закону сприймаються не як витрати, а як стратегічні інвестиції в довгострокову стійкість та репутацію бізнесу. Лише такий комплексний, диференційований та інституційний підхід зможе протистояти тій складній хвилі економічної злочинності, яка сьогодні загрожує самій основі здорового бізнес-середовища.

Звіти окремих інституцій та експертів

Розкриття тіней: методологія OSINT у протидії фінансовій непрозорості та виявленню кінцевих бенефіційних власників [5]

У сучасному глобалізованому фінансовому середовищі, де капітал легко перетинає кордони, а корпоративні структури можуть набувати неймовірної складності, здатність простежити ланцюжок власності до реальної людини, що стоїть за юридичними обличчями компаній, перетворилася з нішевої навички фахівців на критичний інструмент публічної відповідальності.

Навчальний посібник, опублікований Eurovision News Spotlight дає змогу не лише окреслити конкретний шестикроковий алгоритм дій, але й глибше зрозуміти філософські, етичні та практичні основи боротьби за фінансову прозорість. Цей документ є своєрідним маніфестом, що поєднує в собі технічну інструкцію, етичний кодекс і стратегічне бачення того, як відкриті дані можуть бути зведені в потужну систему протистояння корупції, ухиленню від сплати податків та відмиванню коштів.

Фундаментальним викликом, на який відповідає методологія, є навмисне розмежування юридичного та бенефіціарного власництва, інституціоналізоване через мережі офшорних компаній, номінальних директорів та юрисдикцій із захищеною таємницею. Юридичний власник – це лише вивіска, закріплена в офіційному реєстрі, тоді як кінцевий бенефіційний власник (КБВ) – це жива людина, яка отримує вигоду від активів і контролює прийняття рішень. Саме ця роздвоєність створює ідеальне середовище для злочинних схем: від привласнення бюджетних коштів через фіктивні тендери до міжнародного відмивання коштів, отриманих злочинним шляхом. Історія з контрактом місцевої ради, який дістався новій компанії без персоналу, чий КБВ виявився подругою високопосадовця, є не гіпотетичним, а одним з типових прикладів, через які відбувається розкрадання суспільних ресурсів. Боротьба з цими явищами вимагає не лише правових механізмів, але й активних дослідницьких зусиль, заснованих на публічно доступній інформації.

Однак така розслідувальна діяльність розгортається в чутливому правовому та етичному полі. Посібник чітко окреслює кордони, що відокремлюють законне розслідування від вторгнення в приватне життя. Ключовим принципом є "правило зупинки на логіні": дослідник має право працювати лише з даними, що знаходяться у відкритому доступі за законом, не намагаючись обходити платні перепони чи отримувати доступ до закритих баз даних без відповідної санкції. Це розмежування між публічною сферою та приватним життям є священною межею. Крім того, підкреслюється необхідність критичного ставлення до якості даних, особливо в регіонах зі слабким регулюванням, де інформація може бути застарілою або навмисно спотвореною. Консультація з юристами перед публікацією будь-яких звинувачень є обов'язковим кроком, оскільки помилка в ідентифікації КБВ може мати серйозні правові наслідки.

Серцевиною запропонованої методології є системний, ітераційний процес, що нагадує археологічні розкопки через шари корпоративних утворень. Він починається з цільової компанії та послідовного просування вглиб, використовуючи як агреговані платформи типу OpenCorporates, так і офіційні національні реєстри, такі як Companies House у Великій Британії. OpenCorporates виступає в ролі потужного навігатора, дозволяючи швидко знаходити зв'язки між компаніями в різних юрисдикціях, виявляти спільних директорів і переходити до материнських або дочірніх структур через вбудовані посилання. Однак, що особливо важливо,

[5] https://spotlight.ebu.ch/p/tracing-beneficial-ownership-with

кожен критичний факт, знайдений в агрегованій базі, повинен бути верифікований шляхом звернення до першоджерела – офіційного реєстраційного документу в відповідній юрисдикції. Це запобігає поширенню помилок, властивих будь-яким вторинним базам даних.

Практична реалізація включає низку специфічних тактик. Пошук за адресою може виявити, що один номінальний офіс у Панамі чи на Британських Віргінських островах є "домом" для сотень ніяк не пов'язаних між собою компаній, що є класичною ознакою послуг номінального сервісу. Перехресна перевірка імен компаній та директорів у базах даних витоків інформації, таких як OCCRP Aleph (що інтегрує дані з Panama Papers, Paradise Papers та інших), може надати беззаперечні докази використання офшорних інструментів.

Але, можливо, найважливішим аспектом є скрупульозна документація та збереження доказів. Запис кожного кроку в таблицю з посиланнями, архівування веб-сторінок за допомогою спеціальних інструментів та фіксація хеш-суми збережених файлів створюють ланцюжок збереження доказів (chain of custody). Це не лише полегшує написання матеріалу, але й захищає журналіста або дослідника у разі юридичних викликів, роблячи процес повністю прозорим і відтворюваним.

Процес не закінчується на складанні схеми. Верифікація – ось що перетворює набір даних на надійний доказ. Ідентифікувавши кандидата на роль КБВ, необхідно знайти незалежні джерела для підтвердження його особистості: дані з інших реєстрів, публічні виборчі списки, інформацію з профілів у соціальних мережах. Контекстуальний аналіз також має ключове значення: чи має виявлена людина будь-яке відношення до галузі діяльності цільової компанії? Чи проживає вона в країні, де зареєстрована компанія? Неможливість знайти такі зв'язки часто вказує на використання номінальної особи. В ідеалі, найкращим підтвердженням є звернення до офіційних реєстрів бенефіційних власників (як-от реєстр PSC у Великій Британії), які стають все більш поширеними у світі.

Трансформація технічних даних у переконливу публіцистичну розповідь є мистецтвом, якому в посібнику приділено значну увагу. Наочна візуалізація складних зв'язків за допомогою інструментів, таких як Maltego або навіть прості майнд-карти, стає мостом між сухою таблицею реєстру та розумінням аудиторії. Схема, що показує, як досліджувана компанія через ланцюжок компаній у юрисдикціях із високим рівнем секретності з'єднується з конкретною особою, сама по собі розкриває історію. Виявлення професійного номінального директора, який фігурує в сотнях фірм, або збіг юридичної адреси компанії з домашньою адресою КБВ – це не просто технічні деталі, а наріжні камені журналістського наративу, що демонструють намір приховати інформацію та відсутність реальної діяльності.

Цікавим аспектом сучасного підходу, описаного в матеріалі, є обережне використання штучного інтелекту (AI). Великі мовні моделі можуть виконувати рутинну, але трудомістку роботу: аналізувати довгі установчі документи, кластеризувати великі набори даних за спільними адресами або іменами, перекладати іноземномовні документи. Однак посібник супроводжує це суворими застереженнями. Небезпека "галюцинацій" AI, тобто генерації неправдивої інформації, робить абсолютно неприйнятним використання її як першоджерела для ідентифікації UBO. Кожен факт повинен бути перевірений людиною. Крім того, категорично заборонено завантажувати в публічні AI-сервіси конфіденційні або навіть чорнові дані розслідування, що не є частиною офіційного публічного реєстру. AI тут – це лише допоміжний інструмент для обробки вже отриманих публічних даних, а не «детектив».

На завершення, ключові висновки посібника формують міцну філософію розслідувальної роботи. Головна мета – слідувати за живою людиною, а не зупинятися на черговій юридичній особі. Візуалізація є обов'язковим кроком для осмислення складності. Номінальні фігури – це червоний прапор, що вказує на намір приховати власність. І, нарешті, OpenCorporates та подібні інструменти – це лише воронка для початкового пошуку, а не остання інстанція.

Цей методологічний комплекс, поєднуючи технічну майстерність, етичну обережність і системне мислення, надає журналістам та фахівцям із дотримання законодавства практичний інструментарій для демонтажу фасадів корпоративної таємниці. У світі, де фінансові злочини носять глобальний характер, здатність розплутувати мережі за допомогою відкритих даних стає однією з найважливіших гарантій підзвітності влади та захисту суспільних інтересів. Боротьба за фінансову прозорість – це боротьба за справедливість.

Висновки:

- **Виявлення кінцевого бенефіційного власника (КБВ) є системним процесом, що потребує поетапного просування крізь шари корпоративних структур,** починаючи з цільової компанії та використовуючи агреговані бази даних (наприклад, OpenCorporates) та офіційні національні реєстри для послідовного встановлення ланцюга власності аж до живої людини.
- **Етичні та правові кордони є невід'ємною частиною розслідування —** дослідник повинен працювати виключно з публічно доступними даними, не порушуючи приватне життя, обов'язково верифікувати інформацію по першоджерелах та консультуватися з юристами перед публікацією.
- **Візуалізація складних корпоративних зв'язків і скрупульозна документація кожного кроку є критично важливими** для аналізу, побудови переконливого журналістської наративу та забезпечення ланцюжка збереження доказів (chain of custody), що захищає дослідника.
- **Штучний інтелект (AI) може використовуватися лише як допоміжний інструмент** для обробки великих масивів публічних даних, але його застосування супроводжується ризиками «галюцинацій», тому будь-які висновки AI потребують обов'язкової перевірки людиною.

Золота лихоманка: як нелегальний видобуток підриває Ефіопію [6]

THE BUREAU OF INVESTIGATIVE JOURNALISM

Регіон Тіграй на півночі Ефіопії, який ще не оговтався від наслідків однієї з найкривавіших громадянських воєн XXI століття, опинився в епіцентрі нової руйнівної кризи — неконтрольованої та нелегальної золотої лихоманки. Розслідування The Bureau of Investigative Journalism (TBIJ) розкриває моторошну картину: масштабні незаконні видобутки золота, що ведуться за підтримки місцевих військових, за фінансування та за участю іноземних інвесторів, зокрема китайських та канадських компаній. Ця діяльність не тільки збагачує вузьке коло осіб, але й призводить до масштабного екологічного лиха, порушень прав людини, отруєння населення та загрожує повторною дестабілізацією регіону.

Після закінчення війни між федеральним урядом Ефіопії та владою Тіграю в 2022 році регіон опинився у вакуумі влади та закону. Саме цим скористалися тіньові «інвестори», які разом із місцевими військовими командирами розпочали швидке та неконтрольоване освоєння золотих родовищ. Два найбільші з них, Мато Була та Да Тамбук, перетворилися на гігантські кар'єри, видимі з космосу. Незважаючи на те, що ліцензії на промислову розробку цих ділянок офіційно належать канадській компанії East Africa Metals (EAM) та її партнерам, фактично тут більше року ведуться масові незаконні роботи з використанням важкої техніки та отруйних речовин.

[6] https://www.thebureauinvestigates.com/stories/2025-11-13/inside-ethiopias-illegal-gold-trade

Розслідування вказує на складну мережу взаємозв'язків. Канадська EAM формально володіє правами, але її китайські бізнес-партнери, такі як Tibet Huayu та пов'язана з нею Silk Road Investments, фінансують операції на місцях. Важку техніку на об'єкти доставляють китайські гірники, які почали активізацію робіт у 2024 році — приблизно в той же час, коли EAM оголосила про початок будівництва. Ключовою ланкою є місцеві військові, які не лише охороняють шахти, але й контролюють канали контрабанди видобутого золота за кордон, переважно через Еритрею. Таким чином, зловживання відбувається за схемою «іноземний капітал — китайська техніка та експертиза — місцеве силове прикриття».

Однією з центральних фігур цієї мережі є бізнесмен Цзінбін Ван. Він обіймає керівні посади одночасно в кількох компаніях: голова Sinotech Minerals Exploration, голова Nickel North Exploration, колишній голова Beijing Donia Resources (з якою EAM отримала ліцензії) та голова ради директорів самої East Africa Metals. Крім того, він є головним геологом китайського гірничого гіганта Zijin Mining Group. Ця концентрація впливу в руках однієї особи, яка також має зв'язки з державними органами Китаю, відповідальними за стратегію видобутку корисних копалин, вказує на глибоку інтеграцію приватних інтересів із державною політикою в сфері ресурсів.

Наслідки цієї нелегальної діяльності для місцевого населення та екології катастрофічні. Для видобутку золота в кустарних умовах масово використовуються ртуть та ціанід. Ртуть, яка накопичується в організмі, спричиняє неврологічні розлади, ураження шкіри та втрату зору, особливо небезпечна для вагітних та дітей. Ціанід руйнівно впливає на мозок, серце та нервову систему. Хімікати потрапляють у ґрунтові води та річки, отруюючи джерела питної води. Мешканці навколишніх сіл розповідають про дивні хвороби шкіри, масову загибель худоби та врожаїв. Засвідчені випадки смертей дітей від хвороб, які місцеві жителі однозначно пов'язують із отруєнням ціанідом.

Соціальні наслідки також глибокі. Золота лихоманка не принесла добробуту простим ефіопцям. Безробіття та злидні після війни змусили тисячі людей, включаючи жінок, працювати на небезпечних шахтах за мізерну плату. Більшу частину прибутку забирають іноземні інвестори та військові посередники, залишаючи гірникам мінімум для виживання. Як описав один з місцевих дослідників, вони — «рабська робоча сила». Протести місцевого населення проти знищення їхньої землі жорстоко придушуються, а журналісти та інформатори, які намагаються розкрити правду, стикаються з загрозами, залякуванням та насильством.

Висновки:

- **Нелегальний видобуток золота фінансується та здійснюється за участю іноземних компаній** (переважно китайських та канадських) у змові з місцевими військовими, що призводить до формування тіньових мереж, які контролюють видобуток, контрабанду та розподіл прибутків.
- **Діяльність має катастрофічні наслідки для екології та здоров'я місцевого населення:** масове використання токсичних речовин призводить до отруєння, хвороб і смертей.
- **Навіть урядові структури Ефіопії опинилися втягнутими в систему легалізації контрабандного золота**, що свідчить про системну корупцію та розмивання меж між законною та нелегальною економікою.
- **Золота криза не лише поглиблює соціально-економічні проблеми регіону**, але й створює загрозу повторної дестабілізації, оскільки злочинці зацікавлені у продовженні хаосу для збереження контролю над ресурсами.

Парадоксальним є той факт, що значна частина нелегально видобутого золота тепер легалізується через державні структури самої Ефіопії. За минулий рік Національний банк Ефіопії придбав понад 18 000 кг

золота в гірників Тіграю — що майже в 30 разів перевищує легально прогнозований обсяг видобутку для регіону. Це означає, що федеральний уряд, формально борючись із нелегальним видобутком, фактично став основним покупцем контрабандного металу, генеруючи мільярдні доходи від експорту. Така ситуація створює корупційні зв'язки на всіх рівнях влади — від місцевих командирів до федеральних чиновників, розмиваючи межі між законністю та злочинністю.

Спроби нового тимчасового президента Тіграю встановити контроль над гірничою галуззю та призупинити незаконну діяльність поки що мають обмежений успіх. Хоча на деяких великих об'єктах китайську техніку було передано місцевим операторам, це не вирішує корінних проблем — відсутності верховенства права, екологічної безпеки та справедливого розподілу доходів. Колишній президент тимчасової адміністрації Тіграю Гетачев Реда попереджає, що криза набуває регіонального масштабу, а ті, хто отримує вигоду від торгівлі золотом, зацікавлені в подальшій дестабілізації, адже «в каламутній воді легше рибу ловити».

Історія золотої лихоманки в Тіграї — це класичний приклад «прокляття ресурсів» у дії. Замість того, щоб стати джерелом відновлення та розвитку для постраждалого від війни регіону, золото перетворилося на інструмент збагачення вузької групи, посилення конфлікту та системного руйнування. Це криза колосальних масштабів: екологічна, гуманітарна, політична та економічна. Вона демонструє, як слабкі інститути, корупція та зовнішній капітал, що прагне швидкого прибутку без відповідальності, можуть перетворити багатства надр на отруту для землі та народу. Майбутнє Тіграю залежить від того, чи вдасться порвати цей пагубний ланцюг і знайти шлях до легального, прозорого та сталого управління природними ресурсами, яке слугувало б інтересам його мешканців, а не тих, хто панує над руїнами.

Тіньові мільйони: як повсякденна корупція та відмивання коштів формують альтернативну реальність Великої Британії [7]

У свідомості міжнародної спільноти та власного населення Велика Британія десятиліттями підтримувала імідж політично стабільної, правової та фінансово надійної юрисдикції. Цей образ підкріплювався міцними інститутами, прозорими регуляторними рамками та постійною риторикою політиків про неприйняття корупції. Проте ґрунтовне дослідження, проведене нещодавно заснованим Міжнародним товариством економічної кримінології (ISEC), завдає серйозного удару цій концепції, відкриваючи глибокі та широко поширені форми економічної злочинності, які пустили коріння в повсякденному житті мільйонів британців. Отримані дані малюють картину не поодиноких зловживань, а скоріше нормалізованих практик, що існують паралельно з офіційними уявленнями про доброчесність, формуючи тіньову реальність, масштаби якої залишалися невидимими для традиційних методів вимірювання.

Результати анонімного онлайн-опитування, що охопило репрезентативну за віком, статтю та регіоном вибірку з 1000 дорослих жителів Великої Британії в липні 2023 року, є глибоко тривожними. Шістнадцять відсотків респондентів — еквівалент приблизно 7,5 мільйонам дорослих громадян — повідомили, що протягом останніх дванадцяти місяців до них зверталися

7 https://cdn.roxhillmedia.com/production/email/attachment/1770001_1780000/8e36cdfbf9bbfdff5bfaba7b07b5eb06b29161b1.pdf

з вимогою дати хабар. Ще більш значущим є той факт, що 56% тих, хто отримав таку пропозицію, погодилися виконати вимогу, що складає 9% від загальної вибірки, або приблизно 5 мільйонів осіб. Ці цифри не тільки значно перевищують офіційну статистику поліції, що реєструє лише кілька сотень корупційних злочинів на рік, але й різко контрастують із загальноєвропейськими показниками. Середній рівень зіткнення з вимогами хабарів у ЄС становить 9%, тоді як Велика Британія зі своїми 16% опиняється на одному рівні з такими країнами, як Бельгія та Австрія. Це ставить під сумнів усталене переконання про те, що корупція є переважно проблемою менш розвинених держав.

Соціально-демографічний аналіз даних розкриває ще більш складну та тривожну картину. Корупція в Британії не є універсальним явищем; вона розподілена нерівномірно, виявляючи чіткі гендерні розриви. Чоловіки виявляються вдвічі більш вразливими до корупційних вимог, ніж жінки (23% проти 10%). Ця диспропорція може відображати різницю в професійних середовищах, соціальних мережах або культурних очікуваннях щодо поведінки.

Однак найбільш разючий розкол спостерігається між поколіннями. Серед молоді віком від 18 до 40 років з вимогою дати хабар зіткнулися 29%, що є надзвичайно високим показником. На противагу цьому, серед осіб віком 61+ рік ця частка падає до всього 3%. Така різниця не може бути пояснена лише різним життєвим досвідом або кар'єрним шляхом. Вона може свідчити про глибоку соціокультурну зміну: для цілого покоління британців корупційні взаємодії, схоже, стають не винятком, а скоріше прийнятною, хоча й небажаною, частиною соціальної та економічної реальності. Це може бути наслідком поєднання факторів: фінансової невизначеності, яка робить людей більш схильними до пошуку нечесних переваг; нормалізації певних практик у конкретних секторах економіки; або впливу цифрових платформ, що спрощують непрозорі угоди.

Важливо відзначити, що арена корупції значною мірою змістилася з державних установ у сферу приватного бізнесу. На частку приватного сектора припадає 56% усіх зафіксованих вимог хабарів, тоді як на публічний сектор — лише 25%. Беззаперечним лідером серед галузей є фінансовий сектор (23%), що особливо іронічно, враховуючи його центральну роль у боротьбі з відмиванням грошей та підтримці економічної стабільності. Це свідчить про те, що корупція просочилася в саме серце капіталістичної системи країни. Окрім фінансів, значну активність демонструють будівництво, виробництво, інженерія (8%), агенти з нерухомості (7%) та професійні послуги, такі як юридичні та бухгалтерські фірми (6%). Наведений у звіті приклад агента з нерухомості, який відверто пропонує клієнту дати хабар у розмірі 1000 фунтів для отримання знижки у 10 000 фунтів на будинок, є кричущим прикладом такої зухвалості. Ця історія не лише демонструє механізм дії, але й натякає на системний характер проблеми в галузі, де щорічно відбуваються мільйони високо вартісних угод, створюючи безліч можливостей для зловживань.

Форми хабарів також різноманітні. Хоча готівка залишається найпоширенішим засобом (48% випадків), істотну частку становлять подарунки (25%) та, що викликає особливу тривогу, сексуальні послуги (15%). Це розширює традиційне розуміння хабарництва за межі фінансових трансакцій, включаючи особисті та морально деградуючі форми обміну, що ускладнює виявлення та протидію.

Паралельно з корупцією дослідження виявляє масштабну проблему сприяння відмиванню коштів через схеми з "грошовими мулами". 11% опитаних (еквівалент 5,8 мільйонам дорослих) протягом року пропонували стати ланкою для отримання та перерахування коштів з метою приховання їхнього злочинного походження. Майже дві третини (64%) тих, кому робили пропозицію, погодилися взяти участь, що становить 7% від загальної популяції дорослих, або близько 3,7 мільйона осіб. Як і у випадку з хабарництвом, тут виражена гендерна та вікова динаміка: чоловіків (16%) залучають частіше, ніж жінок (6%), а молодь віком 18-40 років (22%) є

найбільш цільовою групою. Ці дані узгоджуються з попередженнями британських правоохоронних органів про те, що "мули" переважно молоді. Організація фінансової розвідки CIFAS повідомляє, що в 2023 році понад 37 000 банківських рахунків демонстрували ознаки використання мулами, причому 65% причетних осіб були молодші 30 років, а 23% — молодші 21 року.

Розрив між інформацією отриманою в рамках дослідження та офіційною статистикою приголомшливий. Поліція щорічно реєструє всього від 100 до 170 корупційних злочинів та від 2000 до 3700 злочинів, пов'язаних із відмиванням грошей. Ці цифри, ймовірно, є лише найбільш очевидними та легко доведеними випадками, тоді як маса повсякденних порушень залишається в тіні. Глобальні дослідження, на які посилається ISEC, свідчать, що щорічно у світі даються хабарі на суму понад 1 трильйон доларів США, більшість із яких ніколи не розкриваються. У контексті Великої Британії, Національне агентство з боротьби зі злочинністю (NCA) оцінює, що щорічно в країні відмивається понад 100 мільярдів фунтів стерлінгів. Ці астрономічні суми можуть циркулювати лише завдяки тисячам або мільйонам окремих транзакцій та участі великої кількості людей, свідомо чи несвідомо.

Глибоке значення цих відкриттів виходить за рамки кримінології. Вони торкаються самих основ соціального договору, громадянської довіри та економічної справедливості. Поширеність цих явищ серед молоді загрожує формуванню цілого покоління, для якого корупція та участь у фінансових махінаціях можуть сприйматися не як моральні провали, а як прагматичні стратегії виживання чи досягнення успіху в умовах, які вони сприймають як несправедливі або конкурентні. Коли мільйони людей вважають за краще дати хабар, щоб отримати послугу, контракт або перевагу, це підриває принципи чесної конкуренції та рівності перед законом. Це створює систему паралельного доступу, де благополуччя залежить не від таланту чи наполегливої праці, а від готовності до компромісів.

Звіт ISEC також вказує на серйозні прогалини в національній системі моніторингу та реагування. На відміну від багатьох європейських країн, офіційне щорічне опитування про злочинність в Англії та Уельсі (Crime Survey for England and Wales), яке охоплює десятки тисяч респондентів, не включає питання про досвід корупції та відмивання грошей. Це означає, що уряд та громадськість не мають систематичного, науково обґрунтованого уявлення про масштаби проблеми, покладаючись лише на дані про зареєстровані злочини, які, як з'ясовується, є лише вершиною айсбергу.

Висновки:

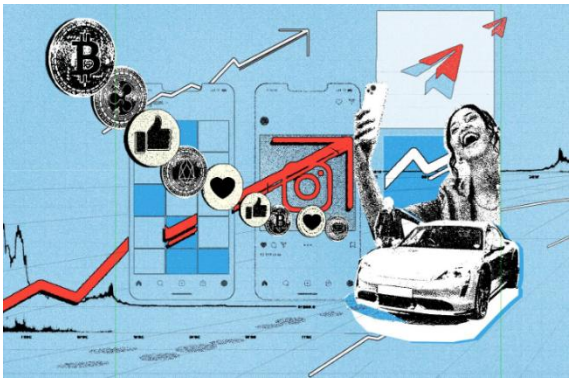
- **Корупція в Великій Британії набагато поширеніша, ніж показує офіційна статистика.** 16% дорослих (близько 7,5 млн осіб) стикалися з вимогою хабаря протягом останнього року, а 9% (близько 5 млн) погодилися його дати.
- **"Грошові мули" — масована проблема, особливо серед молоді.** 11% дорослих (5,8 млн) пропонували стати ланкою для відмивання грошей, причому 64% з них погодилися. Найбільш вразлива група — молодь 18–40 років.
- **Корупція змістилася в приватний сектор,** зокрема у фінансову галузь (23% випадків), будівництво, нерухомість та професійні послуги, тоді як публічний сектор загалом становить лише 25% випадків.
- **Офіційна статистика суттєво недооцінює масштаби явища.** Поліція фіксує лише 100–170 корупційних злочинів на рік, тоді як соціологічні опитування виявляють мільйони випадків.

Отримані результати вимагають не лише подальших досліджень, але й фундаментального перегляду підходів до боротьби з економічною злочинністю. Правові інструменти, такі як Закон про боротьбу з хабарництвом 2010 року, хоч і прогресивні на папері (зокрема, завдяки статті про "невжиття заходів для запобігання хабарництву" компаніями), на практиці застосовуються вкрай обмежено. Потрібен перехід від

реактивного переслідування окремих злочинів до проактивної, системної стратегії. Така стратегія повинна включати: масштабні кампанії з підвищення фінансової та правової грамотності, особливо серед молоді та вразливих груп; посилення корпоративної відповідальності та внутрішнього контролю в ключових секторах, таких як фінанси, нерухомість та професійні послуги; розвиток безпечних та анонімних каналів для повідомлення про корупційні вимоги; інтеграцію питань досвіду корупції та відмивання грошей до національних систем моніторингу злочинності; а також глибший аналіз соціально-економічних умов, що сприяють нормалізації цих практик.

Висновок звіту однозначний: Велика Британія стикається з серйозною, хоча й частково прихованою, проблемою повсякденної економічної злочинності. Це не абстрактна загроза на рівні високої політики чи міжнародних корпорацій; це реальність, що торкається мільйонів звичайних громадян у їхніх спробах отримати роботу, укласти угоду, отримати послугу чи просто покращити своє матеріальне становище. Ігнорування цієї реальності, приховування її за риторикою про чесність та верховенство права, не просто лицемірно — це небезпечно, оскільки дозволяє хворобі глибоко вкорінюватися в соціум, підриваючи довіру, погіршуючи соціальну згуртованість та створюючи умови для більш серйозних системних криз у майбутньому. Це потужний сигнал тривоги, що вимагає негайної уваги, чесного суспільного діалогу та рішучих дій на всіх рівнях влади та громадянського суспільства.

Поза наглядом: як соціальні мережі стають загрозою для фінансової безпеки молоді [8]



Сучасний цифровий простір, особливо завдяки соціальним мережам, перетворився на потужний канал впливу не лише на суспільну думку, але й на фінансову поведінку мільйонів людей, зокрема молоді. Проте за привабливою оболонкою фінансової свободи, розкішних автомобілів та екзотичних подорожей часто ховається складний клубок нерегульованої діяльності, який може мати риси не лише шахрайства, але й витончених схем з потенційним відмиванням коштів. Явище— «фінансових інфлюенсерів» (finfluencers), які активно пропагують інвестиційні стратегії та конкретні платформи — стало масовим, але його наслідки виходять далеко за межі окремих втрачених заощаджень. Це питання системного характеру, що стосується цілісності фінансових ринків, ефективності нагляду та захисту від легалізації доходів, отриманих злочинним шляхом.

Розслідування Investigate Europe на прикладі португальського інфлюенсера Джеймса Перейри вказує на типовий шаблон дій. Створення іміджу успішного мільйонера, який «зробив себе сам» та досяг усього завдяки «розумним інвестиціям», служить потужним магнітом для аудиторії, що шукає швидких рішень. Однак реальний механізм заробітку такого інфлюенсера часто ґрунтується не на власній торгівлі, а на партнерських комісіях від залучення клієнтів до конкретних брокерських платформ. У випадку Перейри це був IronFx — платформа, яка неодноразово потрапляла в поле зору регуляторів від Малайзії до Італії через відсутність необхідних ліцензій. Ключовою деталю є те, що домен ironfx.com, на який направлялися користувачі, не був авторизований Комісією з цінних паперів та бірж Кіпру, хоча саме на цю юрисдикцію посилався Перейра. Натомість він був зареєстрований на компанію з Британських

[8] https://www.investigate-europe.eu/posts/the-rogue-finfluencers-pushing-risky-investments-to-young-followers

Віргінських Островів — територію з послабленим регулюванням, високою конфіденційністю і відому як один із центрів офшорних операцій.

Саме тут виникають гострі питання. Неавторизовані брокери, такі як IronFx, часто не підпадають під жорсткі міжнародні стандарти «знай свого клієнта» (KYC) та моніторингу підозрілих транзакцій. Коли користувачі вносять кошти на такі платформи, траєкторія руху цих коштів може стати непрозорою. Кошти можуть бути переведені через низку юрисдикцій, змішані з іншими потоками або виведені через криптобіржі з мінімальною ідентифікацією. Таким чином, соціальні мережі, через інфлюенсерів, стають ефективним каналом для залучення «чистих» грошей від масових інвесторів у нерегульовані системи, де вони можуть бути використані для легалізації незаконних активів. Комісії інфлюенсерів, які часто виплачуються через ті ж офшорні схеми або криптовалюти, ще більше ускладнюють фінансове відстеження.

Масштаб впливу наражає на думку про системні ризики. Дані показують, що понад третина молодого покоління покладається на YouTube та TikTok у пошуку фінансових порад. Це означає, що мільйони молодих людей, які часто не мають досвіду та критичного фінансового мислення, отримують інформацію з джерел, що не несуть жодної професійної відповідальності. Дослідження Barclays констатує, що 42% тих, хто інвестував за порадами з соцмереж, зазнали збитків. Ці втрати можуть бути не лише наслідком ринкової волатильності, а й прямим результатом шахрайства, маніпуляцій або направлення на неспроможні платформи. З точки зору AML, ці мільйони євро втрачених коштів фактично випадають з офіційного фінансового поля зору, можучи стати частиною тіньових потоків.

Висновки:

- **Фінансові інфлюенсери часто є частиною схеми залучення коштів до нерегульованих брокерів**, які можуть діяти через і не підпадати під стандарти AML/KYC, що створює ризики легалізації доходів.
- **Молодь є основною цільовою аудиторією та найбільш вразливою групою:** понад третина представників молодого покоління шукає фінансові поради в соцмережах.
- **Регулятори відстають від динаміки цифрового середовища:** багато неавторизованих платформ продовжують роботу, а юридичні дисклеймери не звільняють від відповідальності за фактичне фінансове посередництво.
- **Проблема має транскордонний характер і потребує поглибленої міжнародної координації,** оскільки така діяльність і потік коштів легко перетинають юрисдикції, ускладнюючи нагляд і захист інвесторів.

Реакція регуляторів, хоч і активізується, все ще фрагментарна та відстає від динаміки інтернет-середовища. Розслідування показує, що навіть після попереджень національних органів, як це було двічі з Перейрою з боку португальського CMVM, багато каналів та платформ відновлюють роботу під іншими назвами або доменами.

Аналіз Investigate Europe виявив, що половина URL-адрес, внесених CMVM у список блокування за останні п’ять років, досі доступні. Ця стійкість неавторизованої діяльності свідчить про наявність значних регуляторних прогалин та технічних складнощів у блокуванні таких ресурсів на міжнародному рівні.

Окремої уваги заслуговує юридична казуїстика, якою користуються такі інфлюенсери. Вони часто прикриваються дисклеймерами про те, що надають лише «освітній» чи «інформаційний» контент, а не фінансові поради. Проте, як пояснює юрист Ізабель Пінейру Торреш, якщо фактично через їхні канали надається доступ до фінансових послуг або присутнє пряме залучення до конкретного брокера, такі дисклеймери не знімають відповідальності. Це створює сіру зону, в якій діють одночасно правила щодо свободи слова, реклами та фінансового

регулювання. Для AML-фахівців така невизначеність ускладнює кваліфікацію дій: де закінчується легальна фінансова освіта і починається неліцензоване фінансове посередництво?

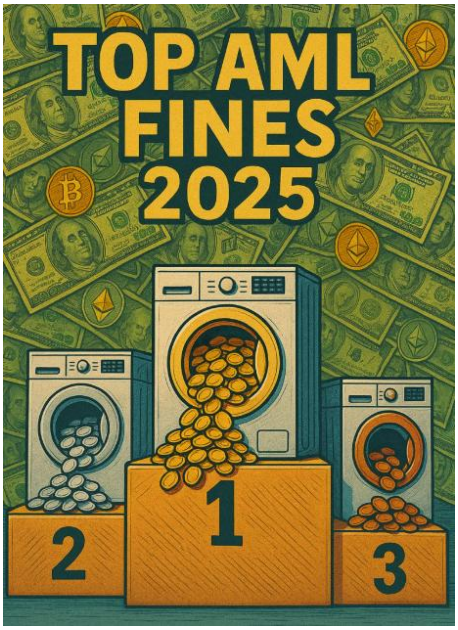
Проблема також має європейський вимір. Хоча існують чіткі директиви (наприклад, MiFID II), що вимагають ліцензування фінансових послуг, їхня імплементація та нагляд залишаються в компетенції національних органів. Крім того, така діяльність легко перетинає кордони. Інфлюенсер з однієї країни може залучати клієнтів для брокера, зареєстрованого в іншій, який, у свою чергу, обслуговує клієнтів з третіх країн. Це робить будь-які спроби національного регулятора зупинити таку діяльність неефективними без глибокої міжнародної координації, обміну даними та спільних оперативних дій.

Таким чином, феномен «фінансових інфлюенсерів», особливо в його нерегульованому вигляді, перетворюється з проблеми захисту прав окремих інвесторів на серйозний виклик для фінансової безпеки та цілісності. Він створює паралельні, не прозорі потоки капіталу, залучає великі маси людей у системи з мінімальним AML-контролем і створює ідеальні умови для змішування легальних коштів дрібних інвесторів з незаконними активами.

Боротьба з цим вимагає не лише посилення покарань та блокувань, але й комплексного підходу: інтеграції моніторингу соціальних мереж у роботу фінансових розвідок, розвитку міжнародних механізмів швидкого реагування на зміни доменів та схем, а також масштабної кампанії з підвищення фінансової та цифрової грамотності, яка навчила б молодих людей розпізнавати ознаки потенційно небезпечного та злочинного контенту. Поки ці заходи не будуть реалізовані, тіньова економіка продовжуватиме процвітати, використовуючи довіру та мрії мільйонів.

Інші новини

Топ-10 AML-штрафів у 2025 році: аналіз глобальних трендів та регуляторних пріоритетів [9]



2025 рік продемонстрував безкомпромісну та жорстку позицію регуляторів у всьому світі щодо дотримання вимог проти відмивання коштів (AML) та протидії фінансуванню тероризму (CFT). Сумарний обсяг штрафів, накладених на фінансові установи, фінтех-компанії та криптовалютні біржі, сягає мільярдів доларів, що свідчить про систематичне посилення нагляду та зростання відповідальності за порушення. Аналізуючи топ-10 найбільших штрафів, можна чітко простежити кілька ключових тенденцій, які формують сучасний регуляторний ландшафт.

Перш за все, очевидним є абсолютна домінація США у примусових заходах. Більшість позицій у рейтингу займають американські регулятори, причому лідирують Міністерство юстиції США (DOJ) та прокуратура Південного округу Нью-Йорка. Саме вони наклали найбільші штрафи на криптовалютні платформи: $504 мільйони на OKX (Aux Caves Fintech Co. Ltd) та $297 мільйонів на KuCoin (Peken Global Limited). Ці колосальні суми не лише показують серйозність порушень, але й сигналізують про те, що криптоіндустрія залишається в центрі уваги регуляторів. Причини вказують на системні недоліки в програмі дотримання вимог AML/BSA (Закон про банківську таємницю), що включає, ймовірно, неадекватну перевірку клієнтів (KYC), неспроможність виявляти та повідомляти про підозрілі операції. Це свідчить про те, що регулятори вже не розглядають криптобізнес як експериментальний, а вимагають від нього того ж рівня відповідальності, що й від традиційних фінансових установ.

Окремої уваги заслуговує той факт, що компанія Block, Inc. (Cash App) потрапила до рейтингу двічі: на п'ятому місці зі штрафом у $80 мільйонів від державних фінансових регуляторів США (CSBS) та на дев'ятому місці зі штрафом у $40 мільйонів від Нью-Йоркського департаменту фінансових послуг (NYDFS). Це є безпрецедентним випадком, коли одна й та сама компанія отримує два значні штрафи протягом одного року за суміжні порушення. NYDFS у своєму рішенні прямо вказує, що це вже друга примусова міра щодо Cash App у 2025 році, що свідчить про хронічні та невиправлені слабкості в їхній програмі AML-комплаєнсу. Така ситуація може вказувати на системну проблему в інтеграції комплаєнс-культури в швидкозростаючі фінтех-компанії, де бізнес-процеси часто випереджають створення належних контрольних механізмів.

Глобальний характер нагляду підкреслюється включенням до рейтингу штрафів від неамериканських регуляторів. Канадський FINTRAC наклав штраф у $126 мільйонів на Cryptomus (Xeltox Enterprises Ltd), що є одним з найбільших адміністративних грошових штрафів за недотримання вимог AML/CFT для компаній, що надають грошові послуги (MSB). У Великій Британії FCA оштрафувала Barclays Bank UK PLC на $55 мільйонів за недоліки в рамках національного AML-регулювання, а німецький BaFin призначив штраф у $52 мільйони J.P. Morgan SE за недоліки в обов'язкових внутрішніх контролях AML. Ці випадки демонструють, що

[9] https://www.linkedin.com/posts/pietro-odorisio-30ab009a_aml-antimoneylaundering-topamlfines-activity-7402611160522399744-zMZB?utm_source=share&utm_medium=member_desktop&rcm=ACoAAENvx0QB2ErUZ9-ViGo_HTMEo4OpWHlquxQ

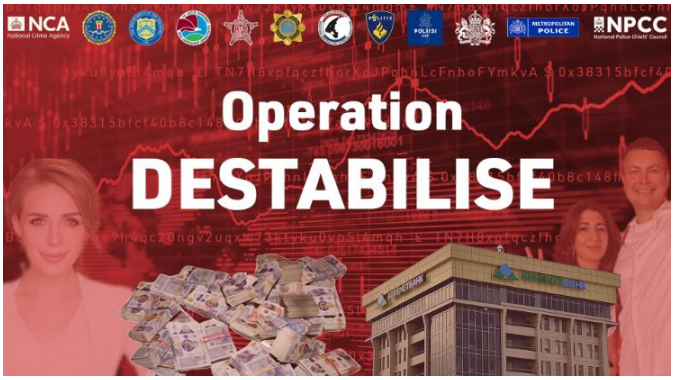
європейські регулятори також посилюють тиск, зосереджуючись як на національних банках, так і на локальних підрозділах міжнародних фінансових гігантів.

Важливо відзначити різноманітність регуляторних органів, які беруть участь у примусових заходах. Окрім кримінальних переслідувань DOJ, активну роль відіграють і цивільні, та адміністративні органи. FinCEN наклав цивільний грошовий штраф у $37 мільйонів на Brink's Global Services USA, Inc., спеціалізовану компанію з логістики та інкасації, що підкреслює, що вимоги AML поширюються далеко за межі банківського сектору. NYDFS, будучи державним регулятором, продемонстрував свою незалежність та строгість, оштрафувавши Paxos Trust Company на $48.5 мільйонів. Така багаторівнева система регулювання (федеральна, державна, міжнародна) створює складне, але дуже щільне поле вимог, де слабкість на одному рівні може призвести до наслідків на іншому.

У висновку, аналіз топ-10 штрафів за AML у 2025 році ясно показує, що ера поблажливого ставлення до порушень у сфері фінансової безпеки закінчилася. Регулятори воліють застосовувати превентивні та показові заходи, а розміри штрафів мають не лише компенсаційний, але й стримуючий характер для всієї індустрії. Криптовалютний сектор, фінтех-компанії та традиційні банки опинилися під однаковою мікроскопічною лінзою нагляду.

Головний урок для будь-якої установи, що працює в фінансовій сфері, полягає в тому, що інвестиції в надійну, проактивну та ресурсно забезпечену систему комплаєнсу AML/CFT більше є не вибором, а обов'язковою умовою виживання та легальної діяльності на сучасному глобальному ринку. Невиконання цієї вимоги може призвести не лише до руйнівних фінансових втрат, але й до непоправної шкоди репутації та втрати довіри клієнтів і партнерів.

Розкрита глобальна мережа: як відмивали мільярди для фінансування війни [10]



Національна агенція з боротьби зі злочинністю Великої Британії (NCA) оприлюднила результати масштабної міжнародної операції під кодовою назвою «Дестабілізація». Розслідування виявило мільярдну схему відмивання коштів, яка діяла на території Сполученого Королівства та за його межами, а її кінцевою метою було фінансування російських військових зусиль та обхід міжнародних санкцій. Особливістю цієї мережі стало пряме придбання банку в Киргизстані для створення легального каналу переказу коштів.

Як з'ясували слідчі, мережа, що складалася з низки організованих груп, спеціалізувалася на перетворенні «брудної» готівки, отриманої від торгівлі наркотиками, постачання зброї та організованої нелегальної міграції, на «чисті» криптовалютні активи. Цей процес слугував життєво важливою ланкою глобальної екосистеми організованої злочинності. Він поєднував локальні злочини в британських громадах з транснаціональною діяльністю найвищого рівня, включаючи послуги з відмивання коштів на користь російської держави.

Операція «Дестабілізація», розпочата ще у 2021 році, була спрямована на розрив цього ланцюга. В ході другого етапу операції було заарештовано 45 підозрюваних у відмиванні коштів, а також конфісковано понад 5,1 мільйона фунтів стерлінгів готівкою менш ніж за рік. Загалом з

[10] https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-exposes-billion-dollar-money-laundering-network-that-purchased-bank-to-fund-russian-war-effort

моменту старту операції здійснено 128 арештів, а сума конфіскованих коштів у Великій Британії (як готівкою, так і в криптовалюті) перевищила 25 мільйонів фунтів. Міжнародним партнерам, завдяки розвідувальним даним NCA, вдалося вилучити ще 24 мільйони доларів США та понад 2,6 мільйона євро.

Ключовим відкриттям розслідування стало виявлення двох основних мереж – «TGR» та «Smart». Група «Smart» контролювалася Єкатериною Ждановою, яка тісно співпрацювала з Хаджі-Муратом Магомедовим та Микитою Красновим. Улітку 2023 року до цієї групи звернулися особи, пов'язані з російськими спецслужбами, з метою фінансування агентів у Великій Британії та Європі, зокрема групи болгарських громадян на чолі з Орліном Русевим, які були згодом засуджені за шпигунство на користь росії. Мережа «TGR» очолювалася Джорджем Россі, його помічницею Оленою Чиркінян та Андреєм Браденсом (також відомим як Андрейс Царенокс). Усі шість вищевказаних членів обох мереж у грудні 2024 року потрапили під санкції Управління з контролю за іноземними активами Міністерства фінансів США (OFAC), а сама Жданова наразі перебуває під слідством у Франції.

Найбільш вражаючим аспектом діяльності мережі стало придбання банку. У серпні 2024 року британські санкції були накладені на компанію «Altair Holding SA», пов'язану з Джорджем Россі, яка виявилася власником контрольного пакету акцій киргизького «Керемет Банку». Як з'ясувалося, угода з купівлі 75% акцій банку була укладена на Різдво 2024 року. Цей фінансовий інститут був використаний для полегшення міжнародних платежів на користь російського державного «Промсвязьбанку», який, у свою чергу, фінансує підприємства військово-промислового комплексу росії. Таким чином, мережа створила офіційний банківський канал для обходу санкцій та фінансування війни.

У схему також був втягнутий російсько-молдовський олігарх Ілан Шор, який раніше був засуджений за виведення мільярда доларів з молдовських банків. Пов'язана з ним платіжна компанія «A7», також підпала під санкції Великої Британії та ЄС. Разом із «Промсвязьбанком» вона анонсувала випуск стейблкоїна A7A5, нібито першої в світі криптовалюти, що забезпечується російським рублем. Цей інструмент, ймовірно, був розроблений саме для здійснення підсанкційних платежів.

Операція «Дестабілізація» наочно продемонструвала взаємозв'язок між дрібною вуличною злочинністю, транснаціональною організованою злочинністю та державною підтримкою такої діяльності. Кур'єри, які збирають готівку по всій Великій Британії (активність зафіксована в 28 містах), отримуючи за це мізерну оплату та ризикуючи довічним ув'язненням, є лише найнижчою ланкою в складній ієрархії. Їхня робота дозволяє «відбілювати» прибутки, які потім реінвестуються в нові злочини або пряму підтримку агресії.

У відповідь на це NCA розгорнула безпрецедентну комунікаційну кампанію, спрямовану безпосередньо на кур'єрів. Плакати та повідомлення англійською та російською мовами розміщуються на автозаправних станціях та в інших місцях їхньої відомої активності, наголошуючи на неминучості арешту та довготривалих тюремних ув'язнень. Мета – психологічно тиснути на виконавців, змусити їх полишити цю діяльність, розриваючи таким чином живлення кримінальної екосистеми.

Британські правоохоронці та їхні міжнародні партнери – поліція США, Франції, Фінляндії, Нідерландів, Ірландії, Іспанії та інших країн – продемонстрували здатність ефективно протидіяти настільки складним та глобалізованим загрозам. Однак, як зазначають в NCA, це лише одна розкрита мережа. Висока прибутковість та політичне покровительство подібних схем продовжують стимулювати їх виникнення.

Боротьба з відмиванням коштів, особливо в контексті фінансування міжнародної агресії, залишається пріоритетним і безперервним викликом для всього світового співтовариства.

Невидимі архітектори злочину: чому арешт брокера прекурсорів більше шкодить наркотрафіку, ніж ліквідація “королів” [11]

У жовтні 2025 року Мексика екстрадувала до США китайського громадянина Чжі Дун Чжана, відомого під псевдонімом “Брат Ван”. Ця подія, на перший погляд лише черговий епізод у нескінченній війні з наркоторгівлею, насправді розкриває глибші структурні зміни в глобальних злочинних мережах. Арешт Чжана, який діяв не як класичний наркобарон, а як міжнародний брокер та логіст, завдав значно більшої шкоди потокам фентанілу, ніж захоплення багатьох “королів” наркобізнесу. Його справа стає наочним прикладом того, як сучасний транскордонний злочин функціонує через децентралізовані мережі високоспеціалізованих посередників, кожен з яких є критично важливою ланкою у набагато більшій і складній системі.

Чжі Дун Чжан не перший раз опиняється у руках правоохоронців. Вперше його затримали в Мехіко у жовтні 2024 року за звинуваченнями у міжнародному наркотрафіку, відмиванні коштів та встановленні альянсів з кримінальними групами по всьому світу. Проте, отримавши домашній арешт, у червні він зумів втекти з країни, перш ніж був повторно схоплений на Кубі та виданий США. Тепер йому загрожує суд у федеральних судах Джорджії та Нью-Йорка за вісьмома пунктами обвинувачень, пов’язаних із торгівлею кокаїном, фентанілом та метамфетаміном, а також 15 пунктами за фінансові злочини.

За даними американських обвинувачів, Чжан керував організацією, яка щонайменше з 2016 року координувала виробництво, підготовку та транспортування цих наркотиків з Мексики до Лос-Анджелеса та Атланти, звідки вони розповсюджувалися по всій території Сполучених Штатів. Мексиканська влада оцінює масштаби його діяльності у щонайменше одну тонну кокаїну, 1.8 тонни фентанілу та 600 кілограмів метамфетаміну щорічно, що генерувало близько 150 мільйонів доларів прибутку. Важливо, що він підтримував зв’язки з ключовими гравцями мексиканського наркокартелю, такими як Картель Сіналоа та Картель Халіско Нового Покоління (CJNG), виступаючи для них незамінним постачальником послуг.

Справжня значущість фігури Чжана полягає не в масштабах торгівлі, а в його специфічній ролі в екосистемі наркобізнесу. Він був типовим “брокером повного пакету” – ключовою ланкою, що забезпечувала зв’язок між легальним світом хімічної промисловості та підпільними лабораторіями. Як зазначає InSight Crime, такі оператори часто виступають мостами між постачальниками прекурсорних хімікатів з Азії (переважно з Китаю) та виробниками синтетичних наркотиків у Мексиці. Їх функції виходять далеко за рамки простої посередницької угоди: вони ведуть переговори, забезпечують доступ до хімікатів, організовують логістику, керують платежами та навіть безпосередньо постачають прекурсори та обладнання.

Така роль вимагає унікального поєднання навичок: доступ до міжнародних мереж, спеціалізовані знання в галузі хімії та логістики, а також легальний бізнес-фасад, що дозволяє уникати пильної уваги правоохоронних органів. Брокери, такі як Чжан, зазвичай мають можливість отримувати дозволи на імпорт, оформляти документацію та забезпечувати доставку вантажів. Їхня діяльність часто балансує на межі законності, що забезпечує їм правдоподібне

[11] https://insightcrime.org/news/chinese-brokers-arrest-hits-mexicos-fentanyl-trade-harder-than-kingpin-captures/

прикриття, але водночас робить їх неймовірно важливими для функціонування всієї наркоіндустрії.

Арешт Чжана демонструє стратегічну вразливість сучасних злочинних мереж. На відміну від наркокур'єрів або навіть видимих лідерів картелів, яких часто швидко замінюють, такі високоспеціалізовані посередники є рідкісним ресурсом. Їхні зв'язки, експертиза та репутація формуються роками, і їхня ліквідація може призвести до серйозних перебоїв у ланцюгах постачання. Як зауважує професор Національного автономного університету Мексики Ядіра Гальвес Сальвадор, справу Чжана можна розглядати як "критичний вузол", захоплення якого дійсно порушує операції мережі. Однак вона також попереджає про надзвичайну здатність цих мереж адаптуватися та знаходити нові шляхи для підтримки своєї діяльності.

Боротьба з такими посередниками є надзвичайно складною. Розслідування проти Чжана тривало майже десятиліття, і лише після багатьох років збору доказів вдалося досягти успіху. Частина проблеми полягає в тому, що ці фігури часто ведуть подвійне життя, маскуючись під законних бізнесменів, що ускладнює встановлення чіткого зв'язку між їхньою легальною діяльністю та злочинними операціями.

Справа Чжі Дун Чжана не є ізольованим випадком. Вона вписується в загальну тенденцію, яку демонструють останні арешти по всьому регіону. У 2023 році в Гватемалі була затримана Габріела Рубіо Сеа, яка, незважаючи на образ бізнес-леді та інфлюенсера, працювала посередником між постачальниками хімікатів у Китаї та фракцією "Чапітос" картелю Сіналоа. У період між 2021 та 2024 роками мексиканські та американські правоохоронці розгромили мережу на чолі з братами Карлосом і Хав'єром Алгредо, які роками керували низкою фіктивних хімічних компаній, включаючи деякі в США, щоб постачати прекурсори для CJNG. Ці приклади свідчать про систематичну спробу правоохоронних органів перерізати життєво важливі артерії, що живлять індустрію синтетичних наркотиків.

Екстрадиція Чжана до США, де його справу вестиме суддя Браян М. Коган, який розглядав справи таких гігантів наркобізнесу, як Хоакін "Ель Чапо" Гусман та Ісмаель "Ель Майо" Замбада, символізує зміну акцентів у боротьбі з організованою злочинністю. Все частіше цільовими стають не ті, хто знаходиться на вершині піраміди, а ті, хто забезпечує її стабільність та функціональність — невидимі архітектори та інженери глобального наркотрафіку. Хоча їхні імена рідко потрапляють на шпальти таблоїдів, їхня діяльність є основним каталізатором "синтетичної наркореволюції", що охопила Північну та Південну Америку.

Отже, арешт Чжі Дун Чжана — це не просто чергова перемога в нескінченній війні. Це сигнал про те, що ефективна боротьба з такими складними та глобалізованими явищами, як трафік фентанілу, вимагає глибшого розуміння його внутрішньої структури, логістики та тих, хто забезпечує його безперебійне функціонування. Поки що захоплення такого брокера є серйозним, але, ймовірно, тимчасовим ударом. Справжнє випробування полягатиме в здатності міжнародної спільноти не лише ліквідовувати окремі критичні вузли, але й системно руйнувати механізми, які постійно відтворюють їх на заміну.

ТікТок та тіньовий бізнес: як соцмережі знищують популяцію сірих папуг [12]

На тлі стрімкої цифровізації суспільства та розквіту візуальних платформ, зокрема TikTok, які перетворили повсякденність на безперервний потік контенту, виник парадоксальний і водночас трагічний феномен: соціальні мережі, прагнучи розважати та об'єднувати, стали невмисною рушійною силою екологічної катастрофи. Африканські сірі папуги, колись численні мешканці тропічних лісів Центральної та Західної Африки, опинилися в епіцентрі цього шторму. Їхня

[12] https://www.rollingstone.com/culture/culture-features/african-grey-parrot-tiktok-black-market-1235460022/

неймовірна здатність імітувати людську мову, розпізнавати форми, кольори та навіть демонструвати зачатки самоусвідомлення — все те, що робить їх об'єктом наукових досліджень та захоплення, — тепер перетворює їх на товар, предмет розкоші та символ статусу в цифрову епоху. Попит, розпещений безліччю вірусних відео, де папуги спілкуються, жартують або виконують складні трюки, сформував гігантський, жорстокий та ефективний ринок, ланцюги постачання якого простягаються від найвіддаленіших куточків конголезьких джунглів до розкішних вілл у Дубаї та передмістях США.

Цей ринок функціонує за власною, зловісною логікою. На початку ланцюга — браконьєри, часто представники місцевих спільнот, які опинилися в умовах крайньої бідності та відсутності альтернатив. Ризикуючи життям, вони вилазять на неймовірну висоту, використовуючи примітивне обладнання, щоб вихопити пташенят із гнізд або зловити дорослих птахів на липкі гілки. Процес вилову кривавий і травматичний: птахи ламають крила, втрачають пір'я, отримують глибокі стресові ушкодження. Далі — довгий і нелегкий шлях на мотоциклах, човнах, а потім і вантажівках до переправних пунктів. У дорозі багато хто гине від зневоднення, голоду чи травм. Ті, хто виживають, продаються за безцінь — близько 10 доларів за птаха — посередникам, які вже формують великі партії для подальшого транспортування. Ціна зростає на кожній проміжній ланці, досягаючи на кінцевому ринку сум у тисячу, а іноді й сім тисяч доларів за одну особу.

Особливу роль у цій системі відіграють країни, такі як Південна Африка, які мають легальні, сертифіковані CITES (Конвенція про міжнародну торгівлю видами дикої фауни і флори, що перебувають під загрозою зникнення) канали для експорту папуг, розведених у неволі. Саме через ці канали, як вважають слідчі та активісти, відбувається «відмивання» тисяч птахів, незаконно вивезених із дикої природи. Механізм досить простий: до легальної партії від розплідника додаються «чисті» птахи без необхідних ідентифікаційних кілець (або з підробленими документами), після чого вся партія отримує видимість законності. Проведені розслідування, включаючи ретельний аналіз баз даних експорту та свідчення колишніх правоохоронців, свідчать про тисячі невідповідностей, фальсифікацій та корупційних схем за участю інспекторів в аеропортах та чиновників. Торговці, на кшталт Гідеона Фурі, який має кримінальну історію за контрабанду, відкрито говорять про те, що державні регулятори «не знають усіх трюків торгівлі» і що бізнес залишається високоприбутковим через низькі ризики та мізерні покарання.

Паралельно з цим в інформаційному просторі формується абсолютно інший, ідеалізований образ життя домашньої папуги. TikTok, YouTube та Instagram наповнені яскравими, ретельно відредагованими роликами, де розумні птахи взаємодіють із господарями, смішно відповідають на запитання або демонструють неймовірні здібності. Цей контент, безсумнівно, викликає захоплення та пізнавальний інтерес, але водночас він створює спотворене уявлення. Користувачі бачать лише кульмінацію — гармонійну взаємодію, але не бачать нічого з того, що їй передувало: ні жорстокого вилову, ні стресу транспортування, ні тривалого та складного процесу адаптації, який потребує від власника експертних знань, неймовірного терпіння та бажання, порівнянного з вихованням дитини. Соцмережі продають мрію про готового, «запрограмованого» друга, тоді як насправді вони опосередковано фінансують криваву індустрію та прирікають тисячі живих істот на страждання.

Наслідки для виду катастрофічні. За оцінками вчених, з 1975 по 2015 рік з природи було вилучено щонайменше 1,3 мільйона африканських сірих папуг, причому реальна цифра,

ймовірно, наближається до трьох мільйонів, якщо врахувати колосальну смертність під час транспортування. У таких країнах, як Гана, популяція скоротилася на 90%, а в Демократичній Республіці Конго, колись головному «постачальнику», щільність птахів у лісах різко впала. Міжнародна спільнота спробувала ввести заборони: у 2016 році вид був переведений у категорію «під загрозою зникнення» (Endangered) в Червоному списку МСОП, що суттєво обмежило міжнародну торгівлю. Однак, як це часто буває, заборони не ліквідували попит, а лише зробили його більш підпільним, вигідним для організованої злочинності, яка часто займається одночасно контрабандою зброї, наркотиків та людей. Новою тенденцією стала контрабанда яєць, які набагато легше приховати від митників, а вилучення великих партій яєць у Східній Азії свідчить про нові масштаби проблеми.

Протидія цій системі розпорошена, несистемна, але героїчна. У Конго подружжя Хартів не тільки документує злочини, але й організовує рятувальний центр, де потерпілі птахи проходять реабілітацію перед поверненням у ліс. У ПАР активістка Смарагда Лув і колишній агент «Зелених Скорпіонів» Юджин Сварт намагаються розплутати клубок корупції в системі експорту. У наукових лабораторіях розробляються інноваційні методи, такі як аналіз мікробіому, який може стати судовим доказом походження птаха. Але їхні зусилля нагадують спробу заткнути пальцем безліч дір у греблі.

Без глибокої зміни законодавства, що буде передбачати жорсткі кримінальні покарання для всіх учасників ланцюга, без значного збільшення фінансування та підготовки природоохоронних органів у країнах походження та транзиту, і, що найголовніше, без фундаментальної зміни свідомості мільйонів споживачів контенту, які своїми відео неусвідомлено підтримують цей попит, ситуація не зміниться.

Феномен «папуги в TikTok» — це не просто історія про моду на екзотичних домашніх улюбленців. Це глибокий симптом нашої епохи, де цифрові технології, прискорюючи та глобалізуючи всі процеси, збільшують і масштаб наслідків наших дій. Ми опинилися в ситуації, коли один дотик до екрану для перегляду смішного ролика може бути пов’язаний зі смертю розумної істоти за тисячі кілометрів.

Це виклик не лише до екологічної етики, але й до нашої здатності як суспільства усвідомити складні, часто невидимі зв’язки між нашим щоденним цифровим споживанням і реальними, матеріальними трагедіями в природному світі. Майбутнє залежить не лише від зусиль правоохоронців, але й від того, чи зможемо ми, користувачі соцмереж, перейти від пасивного споживання контенту до критичного осмислення його ціни.

Чорна лінія розвитку: як інфраструктурні проєкти породжують епіцентри злочинності [13]

Колись спокійне узбережжя провінції Гуаяс в Еквадорі зараз являє собою криваву картину того, як інфраструктурний прогрес, позбавлений всебічного управління ризиками та міцних інституційних опор, може призвести до соціальної та економічної катастрофи. Відкриття глибоководного порту Посорха в 2019 році, задумане як локомотив економічного зростання та інтеграції регіону в глобальні ланцюги поставок, на практиці спричинило зворотний ефект: воно перетворило сусідні містечка Плаяс і

[13] https://insightcrime.org/news/how-new-port-created-latest-criminal-epicenter-ecuador/

Посорха в один з найнебезпечніших регіонів не лише країни, а й всього континенту. Ця трансформація є наочним та похмурим кейсом для світу фінансової безпеки, наголошуючи на невід'ємному зв'язку між великими інвестиційними проєктами, організованою злочинністю та викликами, які стоять перед системою протидії відмиванню коштів (AML). Історія, детально описана InSight Crime, розкриває не просто сплеск насильства, а формування цілої злочинної екосистеми, вбудованої в логістику легальної торгівлі, що генерує потоки «брудних» грошей, які потребують інтеграції в фінансову систему.

До появи порту статистика вбивств у цих прибережних населених пунктах була мізерною. Проте вже за кілька років крива насильства різко пішла вгору, досягнувши у 2023 році показника в 168 вбивств на 100 тисяч мешканців. Ця цифра не просто абстрактна, за кожною такою подією стоїть жорстока боротьба за контроль над стратегічним активом — портом, здатним обслуговувати найбільші контейнеровози світу класу post-Panamax. Його значення для глобальної логістики важко переоцінити: він скорочує шлях для суден, що прямують до Гуаякіля, і став ключовим транзитним вузлом.

Саме ця ефективність і привабливість для легального бізнесу парадоксально зробили порт ідеальним інструментом для організованої злочинності. За даними розслідувань, Посорха швидко перетворилася на головну точку відправлення кокаїну до Європи, зокрема через такі хаби, як Антверпен і Роттердам. Різке зростання обсягів вилучених наркотиків у регіоні — з 5-6 тонн у 2023 до понад 15 тонн у 2024 році — лише підтверджує цей статус.

Однак наркотрафік, попри свої колосальні обсяги, є лише верхівкою айсберга злочинної економіки, що розквітла навколо порту. Справжньою проблемою місцевого бізнесу та суспільства, стало систематичне вимагання. Практика «захисту» перетворилася на рутинну процедуру. Злочинці діють методично: спочатку проводять розвідку, оцінюючи потенційний дохід бізнесу (кількість номерів у готелі, відвідувачів ресторану), а потім переходять до прямого звернення або відправлення погрозливих повідомлень.

Ця схема має декілька критично важливих аспектів для AML-фахівців. По-перше, вона створює постійний, передбачуваний потік менших за розміром, але численних грошових надходжень, які набагато складніше ідентифікувати та відрізнити від легальних операцій, ніж великі одноразові суми від продажу наркотиків. Ці кошти можуть легше інтегруватися в оборот через мережі малого та середнього бізнесу, транспортні компанії або сферу послуг. По-друге, часто це роблять дрібні групи або навіть окремі «скаути», які діють під прапором більших і відомих угруповань, таких як «Чонерос» чи «Лобос». Це створює додатковий рівень непрозорості, ускладнюючи відстеження бенефіціарів і встановлення зв'язків між фактичними виконавцями, організаторами та кінцевими одержувачами коштів.

Сама структура злочинних угруповань у регіоні є джерелом додаткової складності. Класичні ієрархічні організації, такі як «Чонерос», зазнали фрагментації, розпавшись на локальні фракції, що конкурують між собою за території впливу та ресурси. Угрупування «Сіленсіосос» та «Плайєрос» фактично ведуть міжусобну війну. Така внутрішня конкуренція вимагає постійних витрат на ведення «війни» — закупівлю зброї, оплату найманців, хабарі правоохоронцям, — що генерує додаткові, часто екстрені, фінансові операції, спрямовані на підтримку збройного конфлікту. Крім того, обидві групи внесені США до списку іноземних терористичних організацій, що автоматично накладає санкційні ризики на будь-які фінансові операції, пов'язані з ними, зобов'язуючи міжнародні банки та компанії до посиленої перевірки клієнтів та контрагентів, пов'язаних із регіоном.

Найбільшою загрозою для глобальної системи AML є не сам порт як такий, а його синергія з легальним бізнесом. Активність таких гігантів, як Maersk, надає криміналітету тінь законності. Контейнери з наркотиками або готівкою можуть переміщатися тими самими логістичними маршрутами, що й легальні товари, використовуючи фальшиві документи або корумпованих

співробітників. Кошти, отримані від злочинної діяльності, можуть інвестуватися в бізнеси, що безпосередньо обслуговують порт і його інфраструктуру: вантажні перевезення, ремонтні майстерні, склади, готельні комплекси для моряків. Це створює ідеальні умови для відмивання коштів через торгові операції (trade-based money laundering), коли шляхом завищення або зниження вартості товарів у документах гроші переміщуються через кордони та легалізуються. Порт Посорха, таким чином, стає не лише фізичним, а й фінансовим шлюзом для незаконних активів.

Ця ситуація яскраво ілюструє системну неспроможність, коли інфраструктурне будівництво випереджає створення інституційних бар'єрів. Відсутність ефективного фінансового моніторингу на місцевому рівні, слабкість судової системи, корупція та брак координації між різними правоохоронними органами призвели до того, що порт став епіцентром не торгівлі, а злочинності. Для міжнародних банків та корпорацій, які прямо чи опосередковано працюють з цією зоною, це означає підвищені репутаційні, операційні та нормативні ризики. Будь-які транзакції, пов'язані з бізнесом у регіоні, потребують посиленої належної перевірки, оскільки висока ймовірність того, що контрагенти можуть бути під впливом або контролем злочинних груп.

Отже, урок еквадорської трагедії виходить далеко за межі національного контексту. Він говорить про те, що при плануванні масштабних інфраструктурних проєктів, особливо в країнах з високим рівнем вразливості до злочинності, оцінка ризиків AML має бути не додатковим, а обов'язковим і центральним елементом. Необхідно заздалегідь створювати механізми фінансової розвідки, навчати місцеві правоохоронні органи виявленню ознак відмивання коштів, впроваджувати прозорі процедури закупівель і контролю за бенефіціарними власниками компаній, що працюють навколо об'єкта. Міжнародні фінансові інституції, які фінансують такі проєкти, повинні вимагати дотримання цих умов як частини кредитних угод.

Як ми бачимо на прикладі Еквадору, протидія відмиванню коштів у таких умовах починається не з аналізу банківських даних, а з розуміння соціально-економічного та кримінального ландшафту, що формується в умовах глобалізації.

Ваша думка важлива!

1. Як впровадження суворих звітних вимог може вплинути на розвиток національного ринку криптоактивів та фінтеху? Чи може це створити додаткове регуляторне навантаження та як, на вашу думку, держава має забезпечити баланс між досягненням податкової прозорості та створенням сприятливого середовища для інноваційних бізнесів?
2. Британська система КБВ покладає значне адміністративне навантаження на директорів компаній з обов'язком проведення розслідувань. Чи мають українські підприємства достатній кадровий, юридичний та фінансовий ресурс для належного виконання аналогічних обов'язків? Як запобігти тому, щоб складність процедур ідентифікації КБВ не перетворилася на стимул до участі в тіньових схемах?
3. Як Україна може протистояти впливу іноземних корпорацій, які можуть прагнути використовувати слабкість інститутів або корупційні зв’язки для отримання контролю над стратегічними ресурсами? Яку роль у цьому може відігравати громадський нагляд та міжнародна співпраця?
4. Чи може досвід Великої Британії, де корупція більш поширена в приватному секторі, бути актуальним для України, яка традиційно фокусується на боротьбі з корупцією в державному управлінні? Які механізми запобігання корупції в бізнес-середовищі мають бути пріоритетними для України?
5. Яким чином держава може сприяти українським компаніям, особливо малому і середньому бізнесу, який опинився в умовах воєнного стану та підвищених ризиків, в побудові ефективних механізмів виявлення та протидії шахрайству, яке також є масовим в Україні?
6. Чи є, на вашу думку, ризик повторення сценарію Еквадору в Україні під час відбудови? Яким чином ми можемо забезпечити прозорість при великих інфраструктурних інвестиціях, щоб уникнути перетворення нових об’єктів на осередки тіньової економіки?

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-2025-51

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

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