Методологічний бюлетень

Серійний номер: МінФін-AML-2025-37

Вересень 2025

“Любіть те, що робите — тоді робитимете це якнайкраще”

Кетрін Джонсон

Мета

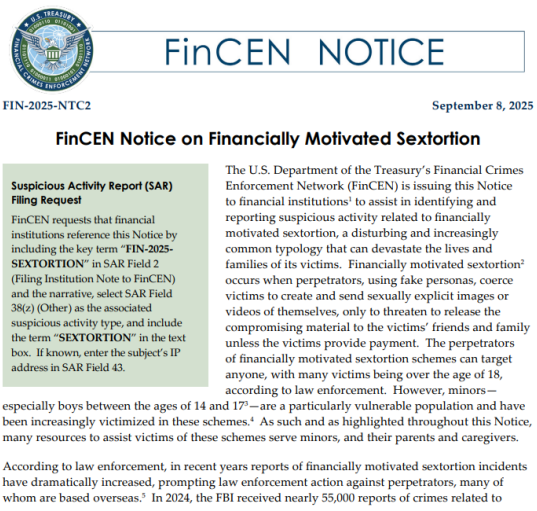
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено 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

FinCEN публікує повідомлення про сексуальне вимагання з фінансових мотивів [1]



FinCEN NOTICE

FIN-2025-NTC2 September 8, 2025

FinCEN Notice on Financially Motivated Sextortion

Suspicious Activity Report (SAR) Filing Request

FinCEN requests that financial institutions reference this Notice by including the key term “**FIN-2025-SEXTORTION**” in SAR Field 2 (Filing Institution Note to FinCEN) and the narrative, select SAR Field 38(z) (Other) as the associated suspicious activity type, and include the term “**SEXTORTION**” in the text box. If known, enter the subject’s IP address in SAR Field 43.

The U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to financial institutions[1] to assist in identifying and reporting suspicious activity related to financially motivated sextortion, a disturbing and increasingly common typology that can devastate the lives and families of its victims. Financially motivated sextortion[2] occurs when perpetrators, using fake personas, coerce victims to create and send sexually explicit images or videos of themselves, only to threaten to release the compromising material to the victims’ friends and family unless the victims provide payment. The perpetrators of financially motivated sextortion schemes can target anyone, with many victims being over the age of 18, according to law enforcement. However, minors—especially boys between the ages of 14 and 17[3]—are a particularly vulnerable population and have been increasingly victimized in these schemes.[4] As such and as highlighted throughout this Notice, many resources to assist victims of these schemes serve minors, and their parents and caregivers.

According to law enforcement, in recent years reports of financially motivated sextortion incidents have dramatically increased, prompting law enforcement action against perpetrators, many of whom are based overseas.[5] In 2024, the FBI received nearly 55,000 reports of crimes related to

Документ є офіційним повідомленням Мережи по боротьбі з фінансовими злочинами (FinCEN) Міністерства фінансів США, яке має на меті надання фінансовим установам допомоги у виявленні та звітуванні про підозрілу діяльність, пов'язану з фінансово вмотивованим сексуальним вимаганням. Документ наголошує, що ця злочинна діяльність є дедалі поширенішою типологією, яка завдає руйнівної шкоди жертвам та їхнім родинам, а також зловживає фінансовою системою США. Ця ініціатива відповідає національним пріоритетам США у сфері ПВК/ФТ, зокрема боротьбі з кіберзлочинністю та шахрайством. Суть фінансово вмотивованого

[1] https://www.fincen.gov/system/files/2025-09/FinCEN-Notice-FMS-508C.pdf

сексуального вимагання полягає в тому, що зловмисники, використовуючи фальшиві особистості в Інтернеті, змушують жертв створювати та надсилати сексуально відверті зображення чи відео, а потім погрожують їх оприлюднити, якщо не отримають грошову винагороду. Хоча жертвою може стати будь-хто, особливо вразливою групою є неповнолітні, переважно хлопці віком від 14 до 17 років. Масштаби проблеми вражають: у 2024 році ФБР отримало майже 55 000 звітів про такі злочини із загальними фінансовими втратами у $33,5 мільйона, що на 59% більше, ніж у 2023 році. Наслідки є трагічними, включаючи самогубства серед підлітків-жертв.

У повідомленні детально розкривається механізм злочину. Зловмисники створюють підроблені акаунти в соціальних мережах або зламують існуючі, видаючи себе за привабливих однолітків протилежної статі. Вони вивчають профілі потенційних жертв, щоб знайти точки дотику, ініціюють контакт на публічних платформах, а потім переводять спілкування у приватні чати. Процес шантажу може розпочатися в лічені хвилини після отримання компрометуючих матеріалів, причому злочинці часто вимагають повторних платежів. Злочинні угруповання переважно діють з-за кордону, зокрема з країн Західної Африки (Кот-д'Івуар, Нігерія, Бенін) та Південно-Східної Азії (Філіппіни). Новим небезпечним трендом є використання генеративного штучного інтелекту для створення реалістичних фальшивих зображень і відео («діпфейків») жертв, які відмовляються надсилати справжні матеріали.

Особлива увага в документі приділяється фінансовим аспектам злочину. Платежі від жертв, особливо неповнолітніх, зазвичай невеликі (від $10 до $50), тоді як дорослі можуть платити суми від $500 до $2,500. Для отримання та відмивання коштів зловмисники активно використовують мережі «грошових мулів». Жертвам дають вказівку надсилати гроші через P2P-платформи, поштові перекази, чеки або конвертовану віртуальну валюту (CVC). Грошові мули, які можуть бути як свідомими співучасниками, так і жертвами, що діють під примусом, отримують ці кошти на свої рахунки.

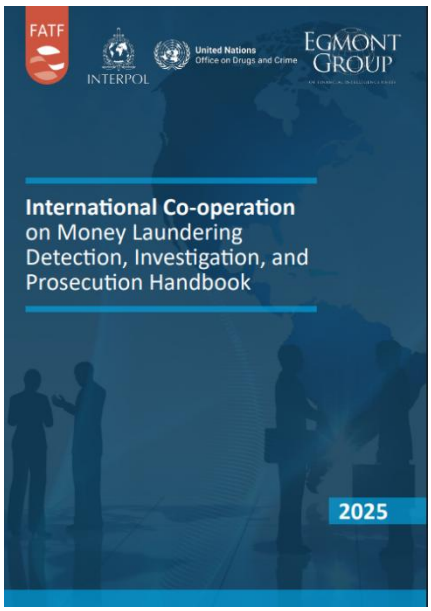
Висновки:

- **Калібрування моніторингових систем на виявлення мікроплатежів.** Системи моніторингу мають бути налаштовані на ідентифікацію патернів, характерних для сексуального вимагання, а саме: серій невеликих, часто округлених, P2P-платежів (особливо в діапазоні $10–$50 від неповнолітніх або молодих людей) на користь раніше невідомих отримувачів. Особливу увагу слід приділяти рахункам, на які надходять такі кошти, якщо вони одразу ж переказуються далі, конвертуються у віртуальні активи або знімаються готівкою.
- **Посилена увага до географічних ризиків та активності «грошових мулів».** Схеми мають чітко виражений міжнародний характер з операційними центрами переважно у країнах Західної Африки (Кот-д'Івуар, Нігерія, Бенін) та Південно-Східної Азії (Філіппіни). Необхідно посилити контроль за рахунками, які отримують численні P2P-платежі від різних непов'язаних відправників, а потім консолідують кошти та здійснюють транскордонні перекази або купують віртуальну валюту для відправки на іноземні гаманці.
- **Ідентифікація нових загроз, пов'язаних зі штучним інтелектом.** Спеціалістам з фінмоніторингу слід враховувати зростаючу загрозу використання генеративного ШІ для створення «діпфейків» з метою шантажу. Це означає, що підозра може виникати навіть за відсутності доказів реальної передачі компрометуючих матеріалів. Транзакції, пов'язані з оплатою за створення такого контенту, часто здійснюються анонімними методами, як-от через віртуальні валюти або передплачені картки, що вимагає пильності при аналізі таких операцій.

Потім гроші проходять через декілька рахунків для ускладнення відстеження, конвертуються у CVC або знімаються готівкою, після чого агрегуються та відправляються за кордон організаторам схеми. У полях до P2P-платежів іноді можна побачити приховані прохання про допомогу (наприклад, «видали фото»), хоча злочинці все частіше інструктують жертв вказувати нейтральні призначення платежу, як-от «для сім'ї».

FinCEN надає фінансовим установам чіткі інструкції щодо звітування про підозрілу діяльність (SAR). Документ містить перелік «червоних прапорців» для виявлення потенційних жертв та грошових мулів. Для жертв це можуть бути серії невеликих P2P-платежів у юрисдикції, що викликають занепокоєння, нехарактерні покупки віртуальних валют чи передплачених карток, а також платежі з підозрілими коментарями. Для грошових мулів характерним є отримання численних P2P-платежів від непов'язаних осіб з подальшим швидким переказом цих коштів на інші рахунки, їх конвертацією у CVC або виведенням у готівку. Наостанок, FinCEN наголошує на важливості обміну інформацією між фінансовими установами в рамках програми USA PATRIOT Act Section 314(b) для ефективного виявлення та припинення таких злочинних схем.

FATF, Егмонтська група, Інтерпол та УНЗ ООН закликають до тіснішої співпраці між країнами, випускаючи посібник з протидії ВК [2]



Цей комплекс документів є всеосяжним ресурсом, розробленим для практиків ПФР, правоохоронних органів (ПО), прокурорів та інших компетентних органів. Головна мета – надати практичні інструменти та рекомендації для оптимізації неформального міжнародного обміну розвідувальною інформацією, інтеграції новітніх технологій та забезпечення відповідності глобальним передовим практикам. Загальний меседж полягає в тому, що "міжнародна загроза вимагає міжнародної відповіді" і що успішні результати боротьби з ВК залежать від синергії неформальних та формальних механізмів співпраці.

Основний "Посібник із міжнародної співпраці з виявлення, розслідування та переслідування у справах про відмивання коштів" поділений на дві частини:

Частина I: Розуміння операційного середовища. Ця частина надає компетентним органам спільне розуміння операційного ландшафту неформальної міжнародної співпраці. Вона починається з розгляду взаємозв'язку між неформальною та формальною співпрацею, підкреслюючи, що остання часто повільна та процедурно складна, тоді як неформальні обміни між ПФР заповнюють цю прогалину, дозволяючи швидкий обмін розвідувальними даними. Документ деталізує ключові характеристики неформальної співпраці: швидкість, гнучкість, цілеспрямованість, оперативність та довіру, яка ґрунтується на операційній незалежності ПФР. Розглядаються чотири основні типи неформальної співпраці: багатостороння (наприклад, через Egmont Secure Web, INTERPOL I-24/7), двостороння (через MoU, офіцерів зв'язку), діагональна (між різними типами органів) та спільний аналіз/розслідування. Також у Частині I обговорюються зміни у злочинному середовищі (глобалізація, цифровізація, віртуальні активи) та виклики, які вони створюють для співпраці, такі як швидкість реагування, обсяг обмінів, якість запитів та доступ до інформації. Завершується частина викладом інформаційних потреб компетентних органів (кримінальна, фінансова,

[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/International-Cooperation-ML-Detection-Investigation-Prosecution.pdf.coredownload.pdf

AML/CFT, відкриті джерела, регуляторна та цифрова інформація) та описом основних багатосторонніх мереж, таких як Egmont Group, FIU.net, INTERPOL, Europol, AMON, Eurojust, IberRed та UNODC CRIMJUST.

• Частина II: Найкращі практики, інструменти та механізми. Ця частина зосереджена на практичних рішеннях для зміцнення міжнародної співпраці. Вона починається з викладу загальних найкращих практик: забезпечення високої якості запитів (чітка мета, обґрунтування, уникнення "рибальських експедицій"), безперервна комунікація (зворотний зв'язок), стандартизація (шаблони, єдина термінологія), дотримання принципів управління та конфіденційності (правило "третьої сторони", операційна незалежність ПФР) та міцна внутрішня координація. Далі розглядаються інструменти та механізми для виявлення та розслідування, включаючи використання багатосторонніх мереж, цифрові інструменти (шифрування, ШІ, PETs) та підтримка діагональної співпраці (пряма та опосередкована). Окрема увага приділяється переходу до фази розслідування та судового переслідування, де неформальна співпраця підтримує формальні запити взаємної правової допомоги (ВПД) шляхом збору розвідувальних даних для уточнення, виявлення невідомих зв'язків та визначення місцезнаходження осіб (наприклад, через повідомлення INTERPOL). Детально описуються приклади успішної неформальної співпраці, такі як спільний аналіз ПФР Італії, Іспанії та Нідерландів, операція AVARUS-X в Австралії та координація США й Індії щодо віртуальних активів. Також розглядається тема спільного аналізу та розслідувань, їх переваги (інтегрований підхід, пряма комунікація, об'єднання ресурсів) та виклики, пов'язані з побудовою довіри та створенням спільних умов. У висновку "Посібник" наголошує на гнучкості вибору каналів співпраці та визначає ключові фактори успіху, включаючи внутрішню координацію, технологічні інвестиції та проактивний підхід.

Три практичні посібники доповнюють основний посібник, надаючи цільові вказівки для відповідних груп практиків.

Практичний посібник для підрозділів фінансової розвідки (ПФР) [3]

Цей практичний посібник, підготовлений спільно Egmont Group, FATF, INTERPOL та UNODC у 2025 році, адресований фахівцям ПФР та партнерським організаціям. Він слугує як покрокове керівництво для покращення неформального міжнародного обміну розвідувальною інформацією (як оперативною, так і стратегічною), інтеграції новітніх технологій та забезпечення відповідності глобальним найкращим практикам.

ПФР знаходяться на передовій боротьби з фінансовими злочинами. Одним з найпотужніших інструментів, доступних ПФР, є можливість обмінюватися розвідувальною інформацією через кордони. Неформальна співпраця є критично важливою, оскільки вона заповнює прогалини формальної міжнародної допомоги, яка може бути повільною та не завжди ефективною, дозволяючи швидкий обмін розвідувальними даними при збереженні конфіденційності та правових рамок. Вона дозволяє швидке виявлення транскордонних злочинних мереж, своєчасне втручання до розсіювання активів, обмін інформацією на етапі досудового розслідування, ефективне застосування ризик-

[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Informal%20Int%20Cooperation%20Brochure%20-%20For%20FIUs.pdf.coredownload.pdf

орієнтованого підходу та підтримку стратегічної розвідки для виявлення тенденцій та нових загроз.

Побудова довіреної мережі для неформальної співпраці є фундаментальною. Співпраця ґрунтується на довірі та операційній незалежності та автономії ПФР, відповідно до стандартів FATF та принципів Egmont Group. Ключові кроки для побудови довіри включають: регулярну участь у міжнародних зустрічах ПФР, вступ до робочих груп (наприклад, Egmont Group, FATF), призначення спеціалізованих контактних осіб, встановлення двосторонніх/багатосторонніх відносин з ключовими партнерами на основі спільних ризиків та пріоритетів, нарощування потенціалу через спільні тренінги та використання безпечних комунікаційних каналів, таких як Egmont Secure Web (ESW) або FIU.net. Також варто розглянути спільний набір правил для обміну інформацією, захисту даних та правил конфіденційності.

Ефективний обмін інформацією передбачає п’ять кроків. Перший крок – визначення мети та оцінка потреби у співпраці. Перед запитом інформації необхідно чітко з’ясувати точну потребу (оперативна чи стратегічна розвідка). Не всі повідомлення про підозрілі операції з міжнародним елементом повинні автоматично призводити до запиту інформації. Такі запити слід робити лише після того, як запитуючий ПФР проведе попередню оцінку, яка вказує, що запитувана інформація, ймовірно, суттєво сприятиме збору розвідувальних даних та аналізу справ. ПФР, що надсилають інформацію, повинні намагатися враховувати, як надана інформація узгоджується з пріоритетами та операційними потребами одержувачів, і можуть ініціювати неформальний діалог для виявлення спільних сфер інтересів.

Другий крок – це створення ефективного запиту. Він має бути чітким та лаконічним, включати імена суб'єктів, ідентифікатори, деталі транзакцій, обґрунтування запиту (наприклад, предикатний злочин, транскордонний зв'язок), бажаний термін відповіді (з обґрунтуванням терміновості) та запит на попередню згоду на розповсюдження для компетентних органів у термінових випадках. Важливо забезпечити пропорційність, запитуючи лише необхідну інформацію. Третій крок – забезпечення взаємності. ПФР повинні бути готові надавати інформацію у відповідь, оскільки взаємність є основою неформальної співпраці, що означає здатність та практику обміну подібною інформацією.

Четвертий крок – захист конфіденційності та безпеки даних. Необхідно дотримуватися "правила третьої сторони" (не розголошувати розвідувальну інформацію без попередньої згоди), забезпечувати безпечне поводження, зберігання та видалення обмінюваної інформації та використовувати технології, що підвищують конфіденційність (PET) для аналізу при мінімізації розкриття даних. П'ятий крок – надання зворотного зв'язку. Необхідно інформувати ПФР, яка надала інформацію, про її використання та потребу у додаткових даних, а також ділитися отриманими висновками для зміцнення співпраці.

Посібник закликає максимально використовувати технології, що підвищують конфіденційність, та штучний інтелект (AI) для сприяння безпечній та ефективній транскордонній співпраці. Це можуть бути гомоморфне шифрування, безпечні багатосторонні обчислення (MPC), мережевий аналіз на основі AI та блокчейн для безпечних аудиторських слідів. Для подолання бар'єрів у неформальному обміні, таких як правові та інституційні обмеження, мовні бар'єри, різниця в часових поясах та обмеженість ресурсів, ПФР повинні працювати в рамках Рекомендацій FATF 29 та 40, виступати за законодавчі зміни, де це необхідно, укладати MoU, використовувати стандартизовані шаблони, багатомовні можливості (включаючи ШІ для перекладу), цілодобові контактні пункти та регіональні партнерства.

Майбутнє неформальної співпраці ПФР включає ширше використання розслідувань, керованих AI (наприклад, для відстеження підозрілих транзакцій або автоматизованого оцінювання ризиків), розвідки цифрових та віртуальних активів, зміцнення регіональних груп та спільнот за інтересами, розширену співпрацю за межами ПФР (діагональна співпраця з ПО,

розвідслужбами, регуляторами, митницею, податковими органами, а також державно-приватні партнерства), обмін інформацією про загрози в реальному часі та правове й етичне управління AI в ПФР. Підсумовуючи, неформальна міжнародна співпраця є невід'ємною частиною ефективного збору фінансових розвідданих, що дозволяє ПФР посилити свою здатність боротися з фінансовою злочинністю, балансуючи швидкість, безпеку та відповідність.

Практичний посібник для правоохоронних органів (ПО) [4]

Ця брошура, також підготовлена Egmont Group, FATF, INTERPOL та UNODC. Вона має на меті надати керівництво щодо інструментів та механізмів міжнародної співпраці, зосередитися на виявленні, розслідуванні та судовому переслідуванні транснаціональних справ про ВК, посилити розуміння ролі ПО на кожному етапі процесу, заохотити покращену внутрішню координацію та сприяти діагональній співпраці та/або спільним розслідуванням між юрисдикціями.

ПО відіграють вирішальну та всеосяжну роль у досягненні успішних транскордонних результатів у боротьбі з ВК. Оскільки ВК пов'язане з більшістю предикатних злочинів, націлювання на його незаконні фінансові потоки є ключовим у боротьбі з транснаціональною злочинністю. Неформальна співпраця є критично важливою, оскільки вона забезпечує швидкість та гнучкість, дозволяючи швидкий обмін розвідувальною інформацією для виявлення транскордонних злочинних мереж, підтримки розслідувань та арештів. Вона сприяє цілеспрямованому збору розвідувальної інформації для виявлення незаконних фінансових потоків, ідентифікації злочинних активів, розкриття структури організованих злочинних груп та розробки спільних операційних планів. Крім того, неформальна співпраця сприяє та доповнює формальний процес співпраці, попереджаючи іноземних партнерів про потенційний запит ВПД та дозволяючи ранню оцінку запиту для забезпечення відповідності всім вимогам. Рекомендація FATF 40 закликає країни забезпечувати найширший спектр міжнародної співпраці.

ПО повинні прагнути залучатися до неформальної міжнародної співпраці якомога раніше, вже на етапі виявлення та розслідування. Вони можуть прямо або опосередковано звертатися до іноземних агентств (ПО, ПФР, митниці, податкових органів) для отримання інформації, що може підтвердити розслідування, наприклад, з реєстрів землі, компаній, митних перевірок, фінансових операцій, міжнародних поліцейських записів (таких як повідомлення INTERPOL) або відомостей про попередні судимості. Важливо використовувати визнані та безпечні комунікаційні мережі, такі як INTERPOL I-24/7, Egmont Secure Web або Europol SIENA. ПФР є ключовими партнерами, надаючи цінну, дієву розвідувальну інформацію, яка допомагає ПО виявляти та розслідувати транскордонні фінансові злочини.

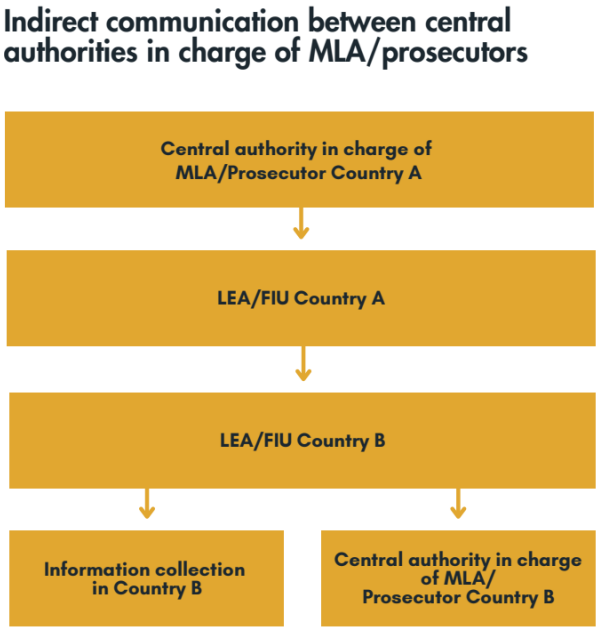
[4] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Informal%20Int%20Cooperation%20Brochure%20-%20For%20LEAs.pdf.coredownload.pdf

На етапі переходу від розслідування до судового переслідування критично важливим стає отримання доказів, придатних для суду, що часто вимагає формальних процедур (запитів ВПД). Неформальна співпраця може підтримувати ці процеси, наприклад, через спільні слідчі групи (JIT), які сприяють збору та обміну інформацією та доказами в реальному часі. ПО також можуть використовувати регіональні/міжнародні організації (INTERPOL, Europol) для координації масштабних розслідувань. Неформальні запити допомагають попередньо оцінити доступність та релевантність даних, необхідних для отримання інформації за допомогою примусових повноважень. Для арешту та екстрадиції злочинців або отримання свідчень свідків можуть бути використані повідомлення та циркуляри INTERPOL, такі як Red Notice та Blue Notice. Національні центральні бюро INTERPOL є ключовими контактними пунктами для обміну кримінальними даними та розвідувальною інформацією.

При надсиланні міжнародного запиту про співпрацю ПО повинні чітко визначити мету та обсяг, вказати кримінальний зв'язок з розслідуванням та юрисдикцією-одержувачем та надати мінімальні деталі справи (факти, транзакції, предикатний злочин, період, ідентифікатори). Важливо вказувати бажані терміни відповіді, обґрунтовуючи терміновість, писати простою, точною мовою та інформувати іноземного партнера про паралельні запити, щоб уникнути дублювання та забезпечити кращу координацію. При отриманні запиту ПО повинні надавати проміжну відповідь, якщо повна відповідь неможлива негайно, координувати з іншими вітчизняними органами, прагнути відповісти у розумні терміни (зазвичай 30 днів), надавати відповідь, навіть якщо інформація відсутня, та пропонувати альтернативні шляхи, якщо законодавство перешкоджає обміну.

Для побудови та підтримання довіри, яка є основою неформальної співпраці, ПО повинні регулярно брати участь у міжнародних/регіональних зустрічах, використовувати членство в організаціях, налагоджувати державно-приватні партнерства, розвивати можливості для спільних розслідувань/аналітичних груп та укладати MoU. Міцна внутрішня координація є важливою для ефективної міжнародної співпраці, вимагаючи тісного партнерства з усіма відповідними національними органами: ПФР, податковими, митними та судовими органами, а також приватним сектором.

Практичний посібник для центральних органів, відповідальних за взаємну правову допомогу (ВПД), включаючи прокурорів [5]



Ця брошура, створена Egmont Group, FATF, INTERPOL та UNODC, має на меті допомогти центральним органам, відповідальним за ВПД, включаючи прокурорів, використовувати неформальну міжнародну співпрацю для швидкого та ефективного обміну розвідувальною інформацією у справах про ВК/ФТ.

Важливо відзначити, що неформальна співпраця не замінює, а лише підтримує офіційний процес ВПД. Її мета – зробити розслідування швидшими, більш цілеспрямованими та ефективними шляхом збору своєчасної розвідувальної інформації, а не побудови доказової бази. Через внутрішні правові обмеження в деяких юрисдикціях

[5] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Informal%20Int%20Cooperation%20Brochure%20-%20For%20Prosecutors.pdf.coredownload.pdf

багато компетентних органів не можуть прямо взаємодіяти зі своїми іноземними колегами на неформальній основі; натомість співпраця зазвичай відбувається опосередковано через місцеві ПФР або ПО (діагональна співпраця). У цьому випадку вітчизняний посередник виступає сполучною ланкою між прокурорськими органами, забезпечуючи дотримання законодавства та сприяючи обміну розвідувальною інформацією.

Неформальна співпраця є важливою для прокурорів, оскільки вона забезпечує швидкість та гнучкість обміну розвідувальною інформацією, що допомагає виявляти транскордонні злочинні мережі до розпорошення активів. Вона зосереджується на отриманні стратегічних та оперативних даних, а не формальних доказів, підтримуючи загальний процес розслідування. Неформальна співпраця заповнює прогалини повільніших формальних процесів, пропонуючи механізм для швидкого доступу до розвідувальної інформації, яка згодом може скеровувати формальні запити. Вона також підтримує ризик-орієнтований підхід, швидко виявляючи нові загрози, тенденції та злочинні типології.

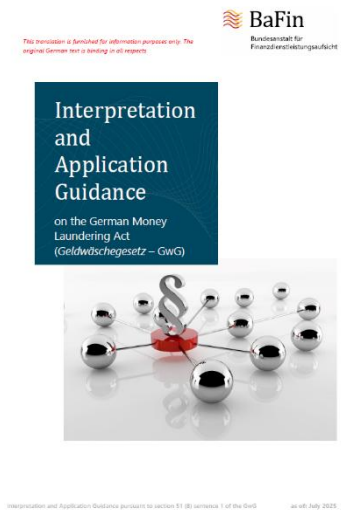
Побудова довіреної мережі для неформальної співпраці передбачає: регулярну участь у міжнародних форумах (наприклад, Міжнародна асоціація прокурорів – IAP), призначення спеціальних контактних осіб, розвиток двосторонніх/багатосторонніх каналів зв'язку, "Знай своїх партнерів" (KYP) для розуміння правових повноважень та процесів іноземних колег, а також навчання та підвищення кваліфікації через спільні тренінги. Обов'язковим є використання визнаних, зашифрованих комунікаційних платформ для обміну конфіденційною розвідувальною інформацією, таких як захищені веб-портали або зашифровані системи обміну повідомленнями.

Ефективний обмін інформацією відбувається у кілька кроків. Крок 1: Визначення мети та обсягу запиту, який має бути вузькоспрямованим, уникаючи широких запитів. Він також повинен включати ідентифікацію конкретного предикатного злочину та бути адаптованим до конкретної юрисдикції та потреб розслідування. Крок 2: Ініціювання запиту через внутрішніх посередників (місцеві ПО або ПФР), якщо існують вітчизняні правові обмеження для прямої співпраці. Запит повинен бути чітким, лаконічним, містити необхідні деталі (ідентифікатори суб'єктів, обґрунтування, терміновість) та запит на попередню згоду на розповсюдження. Крок 3: Сприяння діагональній співпраці, де вітчизняний посередник зв'язується з відповідним іноземним органом. Крок 4: Забезпечення зворотного зв'язку внутрішньому посереднику щодо використання інформації та подальших потреб, що зміцнює довіру та покращує майбутню співпрацю. Крок 5: Інтеграція зібраної розвідувальної інформації в офіційний процес ВПД, роблячи запити більш цілеспрямованими.

Посібник також розглядає використання передових технологій для безпечного обміну розвідувальною інформацією, таких як шифрування та безпечні канали, технології, що підвищують конфіденційність (гомоморфне шифрування, безпечні багатосторонні обчислення), а також AI та аналітику даних для виявлення закономірностей та оцінки ризиків. Для подолання бар'єрів прокурорам рекомендується розуміти вітчизняні правові рамки та працювати через призначених посередників (ПО/ПФР) для транскордонного обміну інформацією. Важливо також будувати інституційну довіру через протоколи, MoU та взаємність, а також забезпечувати конфіденційність, підтримуючи суворі стандарти безпеки даних та обмінюючись лише мінімально необхідною інформацією.

Неформальна міжнародна співпраця є незамінним інструментом для сучасних розслідувань у сфері ПВК/ФТ. Вона пропонує гнучкий та чуйний засіб для збору важливої розвідувальної інформації, яка може оптимізувати та покращити формальні розслідування. Прокурорам рекомендується впроваджувати ці найкращі практики у свою щоденну роботу, щоб обмін розвідувальною інформацією не тільки підтримував, а й зміцнював загальну структуру розслідувань у сфері протидії відмиванню коштів.

Від національних норм до європейської уніфікації: роз'яснення BaFin щодо GwG [6]



Документ є офіційним роз'ясненням Федерального органу фінансового нагляду Німеччини (BaFin) щодо практичного застосування норм Закону про відмивання коштів. Він має нормативно-методологічний характер і слугує центральним інструментом для уніфікованого тлумачення законодавства у сфері ПВК/ФТ усіма піднаглядними установами. Головна ідея документа полягає в тому, що ефективна протидія відмиванню коштів та фінансуванню тероризму неможлива без чіткого розуміння обов'язків, правильного впровадження внутрішніх процедур та належного функціонування системи ризик-менеджменту. У преамбулі наголошується на значенні довіри суспільства до фінансової системи та визначається роль фінансових інститутів, для яких підготовка якісних підозрілих повідомлень нерідко стає ключовим елементом у запуску кримінальних розслідувань. BaFin через дане керівництво реалізує свій мандат забезпечення належної імплементації та однакового застосування норм GwG, а також наближення німецької практики до нового європейського регуляторного середовища.

Документ чітко вбудовує національні вимоги у контекст нової законодавчої архітектури Європейського Союзу, яка сформувалася після ухвалення так званого «AML Package» у 2024 році. Він враховує появу нової наднаціональної установи AMLA з повноваженнями накладати санкції, обов'язковість виконання Регламенту ЄС 2024/1624 приватним сектором, транспозицію Директиви AMLD VI до 2027 року та безпосереднє застосування Регламенту TFR щодо прозорості транзакцій з коштами та криптоактивами. Особливий акцент зроблено на тому, що визначення політично значущих осіб (PEP) буде деталізовано, правила ідентифікації бенефіціарних власників зміняться, а також з'являться нові вимоги у випадках, коли бенефіціара неможливо визначити. Крім того, очікується запровадження обов'язку звітувати про готівкові платежі чи депозити понад 10 тисяч євро до ПФР.

Зміст документа охоплює практично всі ключові сфери діяльності піднаглядних установ. У частині, присвяченій адресатам, деталізуються категорії суб'єктів, які підпадають під дію GwG, зокрема банки, інвестиційні компанії, платіжні установи, страховики, управителі активами, а також постачальники криптоактивних послуг та емітенти певних токенів. Значна увага приділена ризик-менеджменту як основі всієї системи ПВК/ФТ. Розкрито вимоги до проведення повної оцінки ризиків: починаючи від аналізу клієнтської бази, продуктів, каналів розповсюдження і транзакцій до систематичного використання національних і наднаціональних оцінок ризиків, типологій FATF, аналітики ПФР та інших релевантних джерел. Ризики мають документуватися, оновлюватися щонайменше раз на рік і диференціюватися за рівнем значущості, що дає змогу формувати відповідні запобіжні заходи.

Другим фундаментальним блоком є внутрішні запобіжні заходи, які зобов'язані впроваджувати всі установи. До них належить розробка внутрішніх політик, процедур і контролів, призначення відповідального працівника з фінансового моніторингу та його заступника, забезпечення їхніх повноважень і незалежності, достатніх ресурсів та права видавати обов'язкові інструкції всередині організації. BaFin отримує право відкликати призначення відповідального працівника у разі виявлення браку кваліфікації чи ненадійності. Відповідальний працівник з фінансового

6 https://www.bafin.de/SharedDocs/Downloads/EN/Auslegungsentscheidung/dl_ae_auas_gw2025_en.pdf?__blob=publicationFile&v=1

моніторингу не може суміщати свою функцію з роллю внутрішнього аудитора чи офіцера із захисту даних, що спрямовано на усунення конфлікту інтересів. Важливим є і забезпечення навчання персоналу, наявність процедур для перевірки доброчесності працівників та захисту внутрішніх викривачів.

Розділ щодо належної перевірки клієнтів (CDD) описує усі тригери для ідентифікації — від відкриття бізнес-відносин до здійснення разових транзакцій або виникнення підозр у достовірності даних. Окремо пояснюються правила ідентифікації фізичних та юридичних осіб, верифікації наданої інформації, перевірки повноважень осіб, що діють від імені клієнта, а також порядок встановлення та підтвердження бенефіціарних власників. Документ поглиблено деталізує визначення КБВ, зокрема у багаторівневих структурах власності та у випадках фондів. Встановлюється обов'язок з'ясування мети і характеру ділових відносин, визначення статусу PEP, а також регулярного моніторингу відносин та оновлення клієнтських даних. У випадках високого ризику чи сумнівів щодо бенефіціара застосовується принцип відмови у встановленні відносин чи проведенні операцій.

Окрема увага приділена спрощеній та посиленій перевірці клієнтів. Спрощена допускається за наявності низькоризикових факторів, тоді як посилена обов'язкова щодо PEP, клієнтів з високоризикових юрисдикцій, у разі складних транзакцій, кореспондентських відносин чи операцій із криптовалютами, особливо з використанням некастодіальних гаманців. Це відображає сучасні тенденції, коли ризики цифрових активів виходять на перший план.

Важливою частиною документа є роз'яснення процедур повідомлення про підозрілі операції. Підкреслюється обов'язок негайного інформування ПФР незалежно від суми операції, встановлюється заборона на розголошення факту повідомлення клієнтові чи третім особам, уточнюється взаємозв'язок із повідомленням про розбіжності в даних КБВ. Також окреслюється необхідність організаційної структури для обробки STR, порядок документування, наслідки для клієнтів, зокрема можливість перегляду їхньої ризикової класифікації після подання повідомлення.

Висновки:

- **Ризик-орієнтований підхід є ядром системи ПВК/ФТ –** усі установи повинні щорічно проводити й документувати аналіз ризиків, враховуючи національні, наднаціональні оцінки та керівні настанови FATF, і відповідно оновлювати внутрішні процедури.
- **Посилюються вимоги до відповідального працівника з фінансового моніторингу –** він має бути незалежним, ресурсно забезпеченим, мати право видавати обов'язкові інструкції та відповідати за ефективність усієї системи ПВК/ФТ. BaFin може відкликати його призначення у разі неналежної кваліфікації чи надійності.
- **Криптоактиви та нові технології під особливим контролем –** вводяться специфічні зобов'язання щодо верифікації власників некастодіальних гаманців і передачі даних за Регламентом 2023/1113 (TFR), що вимагає інвестицій у технологічні рішення.
- **Посилений контроль за готівковими операціями та КБВ –** усі платежі/депозити понад 10 000 євро підлягають обов'язковому повідомленню до ПФР; водночас уточнюються правила визначення та верифікації бенефіціарних власників, що зменшує можливості для приховування реального контролю.

Групові обов'язки означають, що холдингові структури зобов'язані впроваджувати єдину систему управління ризиками, призначати групового відповідального працівника з фінансового моніторингу, забезпечувати обмін інформацією та водночас дотримуватися правил захисту даних. Водночас документ визнає можливість певних винятків, але тільки у вузьких випадках і за рішенням BaFin.

Загалом, документ формує цілісну методологію застосування GwG у практиці та готує фінансовий сектор до неминучих змін, які принесе повна імплементація AML Package. Він інтегрує вимоги FATF, Європейського банківського органу та майбутньої AMLA, робить акцент на ризик-орієнтованому підході, посилює вимоги до відповідальних працівників з фінансового моніторингу і внутрішніх процедур, ускладнює порядок роботи з криптовалютами та готівкою, а також поглиблює регуляторні вимоги до верифікації бенефіціарних власників. У такий спосіб документ закладає основу для переходу від нинішнього національного режиму до уніфікованого європейського режиму ПВК/ФТ, що має вступити в дію до 2027 року.

Зловживання на крипторинках: нові ризики та глобальні виклики регулювання [7]

Документ присвячений проблематиці ринкових зловживань у криптовалютних екосистемах, які з розвитком технологій та децентралізованих фінансів набули більшої складності, багатогранності та глобального масштабу. У центрі уваги перебуває аналіз ключових схем маніпуляцій, їх вплив на довіру інвесторів, цілісність ринку та регуляторні виклики, що постають перед органами нагляду. Документ підкреслює, що хоча деякі форми ринкових зловживань мають прямі аналоги у традиційних фінансових ринках, криптосередовище створює абсолютно нові можливості для недобросовісних дій, підсилені псевдонімністю учасників, відсутністю централізованих емітентів, розпорошеністю торгових майданчиків і швидким розвитком децентралізованих інструментів.

У тексті докладно описуються такі патерни, як імітаційна торгівля, яка використовується для штучного створення обсягів торгівлі та завищення позицій токенів у рейтингах, що вводить в оману інвесторів і підриває механізм ціноутворення. Розглядаються миттєві позики без забезпеченя, що дозволяють здійснювати складні атаки без застави, використовуючи маніпуляції з оракулами, міжбіржовими арбітражами або навіть атаками на управління децентралізованими автономними організаціями. Значна увага приділяється максимальній вилучуваній вартості (MEV), що виникає через можливість майнерів чи валідаторів впливати на послідовність транзакцій задля отримання прибутку, створюючи практики випереджувальної торгівлі, торгівлі з відстеженням та комбінованої атаки з двома транзакціями, які руйнують довіру до DeFi-протоколів. Окремо аналізуються схеми «накрутки і скидання», що поширюються завдяки соціальним мережам і залученню інфлюенсерів, які формують короткостроковий ажіотаж навколо маловартісних токенів, а також кросчейн-маніпуляції і штучне завищення показників загальної заблокованої вартості (TVL) у DeFi, що дає неправдиве уявлення про ліквідність та стійкість протоколів.

Підкреслюється, що технологічні інновації одночасно ускладнюють регуляторний нагляд і створюють нові ризики, наприклад, появу послуг Market Manipulation-as-a-Service (маніпуляція ринком як послуга), які пропонують штучне збільшення обсягів торгів для проходження лістингових вимог. Навіть при зростанні потужності блокчейн-аналітики подібні практики важко виявляти, оскільки вони маскуються у високочастотних і транскордонних транзакціях. На цьому тлі ключовим викликом стає питання того, як адаптувати традиційні регуляторні інструменти до

[7] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/market-abuse-in-crypto-markets_20250826.pdf?sc_lang=en&hash=22B47226C82B92999656707B8F56EBD7

децентралізованого середовища. Якщо у класичних фінансових ринках головним адресатом регуляцій є емітент, то у криптовалютах часто неможливо встановити такого суб'єкта, що зумовлює потребу у переорієнтації відповідальності на торговельні платформи та заявників, які ініціюють лістинг токенів.

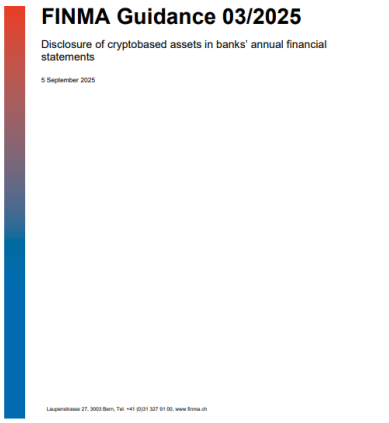
Автори підкреслюють, що існуючі міжнародні норми, зокрема положення MiCA, можуть стати базою для регулювання, проте цього недостатньо, оскільки реалії крипторинків вимагають більш гнучких та технологічно орієнтованих підходів. З огляду на глобальну природу ринків, критичною є координація між регуляторами різних країн та розробка спільних технічних стандартів, які дадуть змогу ефективніше ідентифікувати та зупиняти маніпулятивну поведінку. Для цього важливим є поєднання ончейн та офчейн даних, адже блокчейн дає величезний масив інформації, але часто без контексту, який у традиційних ринках забезпечують звітність емітентів та регуляторні вимоги. Водночас зазначається, що розвиток технологій reg-tech може стати ключовим інструментом: впровадження вбудованого нагляду безпосередньо у торговельну інфраструктуру, використання автоматизованих систем аналізу транзакцій у режимі реального часу та обмін результатами між платформами дозволять знизити витрати на дотримання норм і водночас посилити ефективність протидії.

Документ завершується акцентом на необхідності міжнародної співпраці та створення угод про обмін інформацією між регуляторами, що є єдиним шляхом до подолання ризику регуляторного арбітражу та формування рівних правил гри. Підкреслюється, що ринок криптоактивів є середовищем, яке постійно еволюціонує, і тому регуляторна відповідь має бути не статичною, а динамічною, здатною адаптуватися до нових викликів. У підсумку наголошується, що розробка спеціального режиму боротьби з ринковими зловживаннями у криптовалютах, який би базувався на поєднанні міжнародних стандартів, технологічних інновацій і тісної взаємодії між приватним та державним секторами, є першочерговим кроком для забезпечення довіри, прозорості та стійкості глобальної фінансової системи.

Висновки:

- **Необхідність створення спеціального режиму протидії зловживанням на крипторинках.** Традиційні норми (як у MiCA) дають базу, але повинні бути доповнені новими механізмами, адаптованими до децентралізованих ринків і ончейн-транзакцій.
- **Пріоритет поєднання технологій та регуляції.** Для ефективного нагляду слід розвивати інструменти ончейн-моніторингу, впроваджувати технології reg-tech (вбудований нагляд у платформи) та використовувати аналіз великих масивів даних у реальному часі.
- **Посилення вимог до бірж і платформ.** Саме вони повинні нести відповідальність за запобігання інсайдерським торгам, повідомлення про підозрілі дії, а також співпрацювати з регуляторами у сфері розкриття інформації та обміну даними.
- **Критична роль міжнародної координації.** Транскордонна природа крипторинків потребує нових форматів співпраці між регуляторами (обмін даними, спільні стандарти), щоб уникати регуляторного арбітражу та ефективно протидіяти маніпуляціям.

Роль Швейцарії у формуванні стандартів звітності для криптоактивів: аналіз нових вказівок FINMA [8]



Документ FINMA є детальним роз'ясненням Швейцарського органу фінансового нагляду щодо того, як банки повинні розкривати інформацію про токенізовані активи у своїх річних фінансових звітах після набрання чинності Законом про розподілені реєстри (DLT Act). Потреба у цьому роз'ясненні виникла через зміну термінології та правового статусу цифрових активів: якщо раніше у FINMA Accounting Ordinance 2019 та FINMA Circular 2020/1 використовувався термін «криптовалюти», то з ухваленням DLT Act у 2021 році з'явилося юридичне визначення поняття «токенізовані активи», що охоплює ширший спектр цифрових активів і змінює їхнє місце у системі бухгалтерського обліку та наглядової звітності. FINMA відзначає, що існуюча практика створила непослідовність: з одного боку, банки вже мали нормативні орієнтири щодо криптовалют як платіжних токенів, з іншого — новий закон надав токенізованим активам статус касодіальних активів відповідно до статті 16, пункт 1bis Закону про банки, що робить застарілим їхнє трактування як довірчі операції згідно зі статтею 16, пункт 2.

Щоб зрозуміти цей перехід, варто врахувати історію: ще у 2018 році FINMA опублікувала настанови щодо ICO, у яких розділила токени на три типи: платіжні, утилітарні та інвестиційні. Платіжні токени тоді фактично ототожнювалися з терміном «криптовалюти» і відображалися у звітності особливим чином: якщо банк утримував криптовалюти від імені клієнта, вони могли бути віднесені до довірчих інвестицій і розкривалися у примітках до фінансової звітності в межах пункту 214 FINMA Circular 20/1. Це вимагало, щоб у випадку банкрутства банк забезпечував сегрегацію активів клієнтів і діяв відповідно до директив Швейцарської банківської асоціації щодо довірчих інвестицій. У наглядовій звітності Швейцарського національного банку відповідні суми відображалися у формах AU201 чи AUH201 у спеціальному розділі 6.4. Таким чином, ще до ухвалення DLT Act банки мали обов'язок показувати криптовалюти або у балансі, або у примітках, але завжди з обов'язковим розкриттям інформації.

З ухваленням DLT Act підхід змінюється принципово. Тепер токенізовані активи визнаються кастодіальними активами, навіть якщо вони не є цінними паперами. Це означає, що старе правило розкриття через довірчі операції більше не застосовується, а отже, пункт 214 FINMA Circular 20/1 не може використовуватися для обліку таких активів. Водночас це не знімає із банків обов'язку забезпечувати прозорість: FINMA наголошує, що розкриття токенізованих активів має продовжуватися у примітках до фінансової звітності, адже йдеться про активи, що несуть специфічні технологічні ризики, пов'язані із зберіганням приватних ключів, кіберзагрозами, правовою невизначеністю чи швидкими змінами ринкової вартості. Тому, доки регулятор не введе окрему обов'язкову позицію у примітках до фінансової звітності, банки мають самостійно обрати місце для відображення токенізованих активів у розділі «касодіальні активи», дбаючи про те, щоб користувачі звітності могли легко порівняти дані з попередніми роками. Для цього FINMA рекомендує, наприклад, залишати у пункті 214 примітку з відсиланням на новий розділ, де буде наведена інформація про токенізовані активи, визначені

[8] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20250905-finma-aufsichtsmitteilung-03-2025.pdf?sc_lang=en&hash=1C6C67682A4C9170C45A185F2BE32482

як кастодіальні активи. Такий підхід покликаний уникнути інформаційних розривів у динаміці звітності та підтримати якість фінансової інформації.

Значні зміни стосуються і наглядової звітності. FINMA повідомляє, що банки більше не мають звітувати про криптовалюти у формах AU201, AUH201, AU301 чи AUH301 у відповідних розділах 6.4, які стосувалися довірчого зберігання. Замість цього інформація про токенізовані активи збиратиметься через нову окрему анкету — EHP-опитувальник «Токенізовані активи – банки та фондові компанії». Це дозволить регулятору мати точне уявлення про масштаби та динаміку токенізованих активів у банківському секторі, водночас знімаючи обов'язок дублювати дані у старих формах, які втратили актуальність. Важливо, що якщо токенізовані активи мають статус цінних паперів (наприклад, токенізовані облігації чи акції), вони, як і раніше, повинні відображатися у звітності як кастодіальні активи у розділі 5.1, який охоплює обсяг цінних паперів та дорогоцінних металів, що належать клієнтам. Таким чином, регулятор розмежовує: для нецінних паперів вводиться новий підхід через EHP-опитувальник, а для цінних паперів продовжує діяти чинна практика.

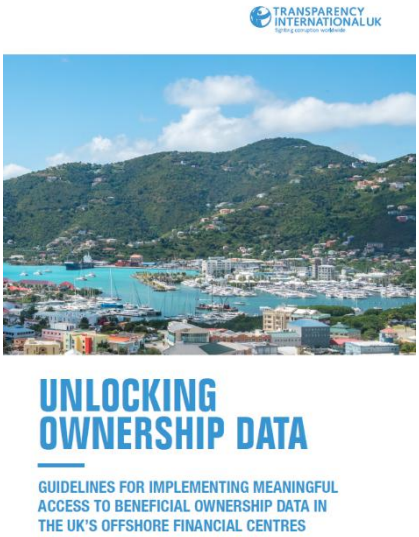
Важливим акцентом є те, що FINMA підкреслює технологічні ризики токенізованих активів, які відрізняють їх від традиційних фінансових інструментів і роблять необхідним особливий режим прозорості. Ці ризики стосуються як операційних аспектів (ризик втрати доступу до активів, кібератаки, збої у блокчейн-мережах), так і правових (відсутність уніфікованої міжнародної практики, проблеми із захистом прав власності, невизначеність у випадку неплатоспроможності провайдера послуг зберігання). Саме через це FINMA вважає неприйнятним залишати токенізовані активи поза увагою користувачів звітності, навіть попри те, що формальна вимога розкриття через довірчі операції скасована.

У підсумку Guidance 03/2025 формує місток між попередньою практикою і новою регуляторною реальністю. FINMA надає банкам гнучкість, дозволяючи самостійно визначати розділ для розкриття токенізованих активів, але водночас висуває ключову вимогу — прозорість і порівнянність із попередніми роками. Документ підтверджує, що токенізовані активи відтепер визнаються кастодіальні активи і що їхнє відображення у фінансовій звітності має відбуватися у спосіб, який гарантує інвесторам і регуляторам достатню інформацію про ризики та обсяги цих активів. Це фактично відображає еволюцію швейцарського підходу: від тимчасових компромісних механізмів, які дозволяли інтегрувати криптовалюти у традиційну систему обліку, до більш зрілого й системного регулювання, що враховує новий правовий статус токенізованих активів і прагне зробити фінансову звітність більш надійною, узгодженою та пристосованою до сучасних технологічних викликів.

Висновки:

- **Виключення старого підходу:** криптовалюти більше не можуть відображатися як довірчі операції (п.214 FINMA Circular 20/1).
- **Визнання нового статусу:** токенізовані активи, навіть якщо не є цінними паперами, тепер мають розкриватися як кастодіальні активи відповідно до ст.16(1bis) BA.
- **Обов'язок банків:** кожен банк самостійно визначає місце у примітках до річної звітності для розкриття таких активів, але має забезпечити прозорість і можливість порівняння з попереднім роком.
- **Оновлення у звітності:** дані більше не подаються у формах AU201/AUH201 у розділі «довірчі операції», натомість регулятор отримуватиме інформацію через нове опитування EHP-опитувальник щодо токенізованих активів.

Глобальні стандарти прозорості: як реєстри КБВ змінюють фінансову систему [9]



Документ є комплексним аналітичним і методологічним дослідженням Transparency International UK, що фокусується на проблемі корпоративної непрозорості та необхідності створення ефективних механізмів доступу до інформації про кінцевих бенефіціарних власників у британських офшорних фінансових центрах. Його поява зумовлена масштабними міжнародними викриттями, насамперед витоками «Панамських документів» у 2016 році, які показали, як офшорні юрисдикції, зокрема ті, що пов'язані з Великою Британією, стають головними каналами для відмивання коштів, ухилення від сплати податків і приховування активів, здобутих через корупцію, організовану злочинність чи державні зловживання. Автори наголошують, що Велика Британія, завдяки Лондонському Сіті та мережі заморських територій і коронних володінь, відіграє системоутворюючу роль у глобальній архітектурі тіньових фінансів, створюючи сприятливі умови для накопичення і перерозподілу непрозорого капіталу. Втрати світових бюджетів оцінюються у сотні мільярдів доларів щороку, а сам феномен призводить до поглиблення так званого «прокляття фінансів», коли надмірна концентрація фінансових потоків гальмує розвиток реального сектору, провокує економічні дисбаланси, соціальну нерівність і корупційні ризики.

Документ ґрунтовно описує історичні витоки формування офшорної системи, починаючи з 1950-х років, коли у Лондоні було створено євродоларовий ринок, що дозволив банкам обходити американські регуляції. Саме тоді британські заморські території в Карибському регіоні стали базовими майданчиками для фінансових потоків, а пізніше утвердилися як ключові центри глобального офшорного бізнесу. Автори підкреслюють, що цей процес активно підтримувався британськими урядовими структурами, які розглядали офшори як спосіб підвищення самодостатності територій і зменшення їхньої залежності від фінансової допомоги метрополії. Водночас наводяться численні приклади, як така політика призвела до системної корупції та політичного захоплення влади в цих юрисдикціях, зокрема у Туркс і Кайкос, на Британських Віргінських островах і в Гібралтарі, де відбувалися гучні скандали та розслідування.

Особливий акцент зроблено на тому, що корпоративна непрозорість британських офшорів сприяє масштабним глобальним зловживанням, серед яких корупційні мегасправи на кшталт скандалу 1MDB у Малайзії, обходження санкцій російськими олігархами, діяльність міжнародних наркокартелів, використання примусової праці в риболовецькій індустрії та незаконне знищення тропічних лісів. Таким чином, хоч офшори і приносять певні доходи територіям, їхня діяльність створює непропорційно високу ціну для світової економіки, довкілля і суспільств у різних країнах.

На цьому тлі документ аналізує еволюцію підходів до прозорості власності у Великій Британії та її територіях. Якщо у 2020 році всі заморські території та коронні володіння добровільно погодилися створити публічні реєстри бенефіціарних власників (PARBOs), то після рішення Суду ЄС у 2022 році, яке визнало, що повна відкритість для боротьби лише з відмиванням коштів є непропорційним втручанням у право на приватність, процес загальмувався. У 2024 році було вироблено компроміс у вигляді запровадження реєстрів з доступом на основі легітимного інтересу (LIARBOs), які забезпечують широкі права доступу для державних органів, фінансової розвідки, наглядових інституцій, підзвітних суб'єктів фінансового моніторингу, а також для журналістів і громадських організацій, що працюють у сфері протидії відмиванню коштів і

[9] https://www.transparency.org.uk/sites/default/files/2025-09/Unlocking%20Ownership%20Data.pdf

корупції. Документ пропонує конкретні правові й технічні стандарти для реалізації LIARBOs як проміжного кроку до повноцінних публічних реєстрів.

Окремий розділ присвячений методології, яка спирається на стандарти FATF, законодавство ЄС (зокрема шосту Директиву з протидії відмиванню коштів) та практику Великої Британії. Автори систематизують ключові стандарти у вигляді законодавчого «блакпринту», що охоплює визначення бенефіціарного власника, обов'язки юридичних осіб і самих КБВ щодо декларування та оновлення інформації, вимоги до реєстраторів стосовно перевірки, зберігання та цифрової доступності даних, механізми санкцій за невиконання обов'язків, а також різні моделі доступу для державних органів, зобов'язаних суб'єктів і громадськості. Визначення КБВ має бути уніфікованим, із порогом не вище 25% володіння чи контролю, охоплювати прямі й непрямі права, вплив на управління та трастові структури, а також містити заборону інструментів, які унеможливлюють перевірку (наприклад, акцій на пред'явника). Реєстр повинен бути централізованим, цифровим, доступним у режимі 24/7, із можливістю машинного зчитування, API та масового завантаження, а інформація має оновлюватися у максимально короткі строки. Значна увага приділяється перевірці достовірності, включаючи звірку з іншими джерелами, перевірку на санкційні списки та усунення розбіжностей. Передбачені ефективні санкції — як адміністративні, так і кримінальні — для юридичних осіб, керівників і бенефіціарів у разі неподання, несвоєчасного або неправдивого подання інформації.

Окремо розглядається баланс між прозорістю і захистом персональних даних. Автори визнають право на приватність, але наголошують, що воно має бути обмежене там, де йдеться про запобігання злочинам, національну безпеку, економічний добробут та захист прав інших осіб. Тому запропоновані обмежені винятки для захисту від переслідувань чи насильства, з чітко прописаними процедурами й обов'язком реєстраторів публікувати статистику про кількість і підстави таких винятків. Підкреслюється, що кінцевою метою має стати повноцінний перехід до публічних реєстрів (PARBOs), які, як показує досвід Великої Британії та Companies House, створюють реальний економічний ефект, полегшують розслідування, зміцнюють доброчесність бізнесу і приносять вигоду державі, бізнесу та суспільству в цілому.

Висновки:

- **Впровадження єдиного чіткого визначення КБВ** відповідно до стандартів FATF та ЄС (низькі пороги, охоплення всіх форм контролю, заборона «іменних акцій») є обов'язковою умовою для дієвих реєстрів.
- **Реєстри КБВ повинні бути цифровими, централізованими й такими, що перевіряються,** із обов'язковим внесенням змін протягом 14 днів і санкціями за недостовірні дані.
- **Доступ за законним інтересом (LIARBOs) має стати проміжним кроком до повної відкритості (PARBOs),** включаючи доступ для журналістів, НУО, підзвітних суб'єктів і міжнародних партнерів.
- **Кінцева мета – відкриті публічні реєстри КБВ (PARBOs),** що забезпечать максимальну прозорість, зменшать ризики ВК/ФТ та підвищать довіру до фінансових систем.

Загалом документ є не лише технічним керівництвом, а й політичним закликом: Велика Британія та її території мають усвідомити, що подальше збереження режимів секретності сприяє глобальній шкоді, тоді як рух до прозорості у сфері бенефіціарної власності здатен посилити міжнародну боротьбу з відмиванням коштів, зменшити масштаби корупції, запобігти санкційним обходам та водночас стимулювати економічний розвиток і зміцнення довіри до фінансових систем.

Організована злочинність як виклик демократії: економічний вплив, корупція та шляхи протидії [10]

Документ підготовлений Аналітично-дослідницькою групою Ради ЄС (ART) у липні 2025 року і являє собою ґрунтовний аналіз того, як організована злочинність перетворюється з проблеми кримінального характеру на масштабну загрозу демократичним суспільствам. Автори показують, що сьогодні організовані кримінальні мережі охоплюють десятки тисяч осіб з понад сотні країн світу, а їхня діяльність вже не обмежується класичними «чорними» сферами на кшталт наркотрафіку, торгівлі людьми чи нелегальної зброї. Вони активно проникають у фінансові та політичні інституції, підриваючи легальну економіку і формуючи власні паралельні системи впливу. Це проявляється у корупції, маніпуляції публічними закупівлями, тиску на місцеву владу, проникненні в бізнес для відмивання коштів і створенні таких умов, коли громадяни починають сприймати злочинні структури як більш ефективні чи доступні «альтернативні» механізми вирішення своїх потреб. У результаті знижується довіра до демократичних інституцій, слабшає правова держава, а вплив організованих мереж поширюється на ключові суспільні сфери.

Особливу увагу в документі приділено тому, як сучасні технології та глобальні процеси відкрили для злочинців нові можливості. Використання штучного інтелекту, криптовалют, зашифрованих каналів зв'язку, а також посилення геополітичної нестабільності зробили діяльність мереж більш гнучкою, мобільною та важкодоступною для традиційних інструментів розслідування. Держави і міжнародні структури часто не встигають адаптуватися, оскільки регуляторні та правоохоронні механізми діють повільніше, ніж динаміка технологічних інновацій. Водночас відсутність уніфікованого підходу до боротьби з організованою злочинністю, різний рівень ресурсів у країнах ЄС, обмежене міжнародне співробітництво й корумпованість окремих державних структур створюють додаткові лазівки, якими злочинні угруповання користуються для зміцнення свого становища.

Великий блок документа присвячено економічному виміру цієї проблеми. Обсяги торгівлі контрафактними товарами вже сягають понад трьох відсотків світової торгівлі, що еквівалентно приблизно одному трильйону доларів у 2023 році, і ця цифра може зрости до майже двох трильйонів до 2030 року. Вартість відмивання грошей оцінюється у 2-5 відсотків глобального ВВП, що показує масштаби інтеграції злочинних фінансових потоків у світову економіку. Окремо згадано роботу Європейської прокуратури (EPPO), яка нині веде понад дві з половиною тисячі справ, пов'язаних із шахрайством із бюджетними коштами, що оцінюється майже у двадцять п'ять мільярдів євро. Ці дані свідчать, що організована злочинність завдає збитків не лише приватним особам чи бізнесу, а й безпосередньо підриває фінансову стабільність державних і наддержавних інституцій.

Ще одна загрозлива тенденція полягає у вербуванні нових поколінь злочинців. Через соціальні мережі та онлайн-ігри підлітків і молодих людей залучають до діяльності злочинних груп під виглядом «швидкого заробітку», винагород чи підвищення статусу. Це створює довгострокову проблему: кримінальні мережі фактично формують власний кадровий резерв, що ще більше ускладнює подолання проблеми у майбутньому. Такий процес не лише розширює масштаби злочинної діяльності, а й руйнує соціальні та моральні норми у громадах.

[10] https://www.consilium.europa.eu/media/3cpejugj/2025_683_art_organisedcrime_web_july-2025.pdf

Документ наголошує, що відповіді на ці виклики не можуть бути фрагментарними чи виключно силовими. Потрібен підхід «усім суспільством», який поєднує роботу правоохоронців, органів влади, міжнародних структур, бізнесу, освітніх закладів і громадських організацій. Превенція повинна включати просвітницькі кампанії, зміцнення соціальної стійкості, захист молоді, створення альтернативних можливостей для заробітку й розвитку, які роблять кримінальні пропозиції менш привабливими. Водночас ключовим елементом є посилення фінансового контролю й ефективне вилучення активів у злочинних угруповань. Саме конфіскація незаконно отриманих коштів і повернення їх у легальний обіг може істотно послабити економічну основу організованих мереж, адже саме завдяки накопиченню й легалізації капіталу вони зміцнюють свою владу і вплив.

Таким чином, організована злочинність у сучасному світі постає не просто як сукупність кримінальних практик, а як складне явище, що інтегрується у політичні, економічні та соціальні системи, підриваючи демократію зсередини. Європейським країнам і міжнародним структурам доведеться розглядати її не лише як кримінальний виклик, а як стратегічну загрозу для безпеки й розвитку суспільств. Від того, наскільки комплексно буде вибудувана система протидії — від правових механізмів і технологічних інновацій до освітніх програм і мобілізації громадян — залежить, чи вдасться зупинити процес перетворення злочинних мереж на паралельні «тіньові держави» з власними правилами і системами влади.

Висновки:

- **Організована злочинність перетворилась із кримінального на системний виклик**, що руйнує демократичні інституції через корупцію, підрив довіри, залякування та вплив на державні процеси.
- **Новітні технології та геополітична нестабільність** розширили можливості злочинних мереж, що вимагає швидкого оснащення правоохоронців сучасними технічними і аналітичними інструментами.
- **Необхідний комплексний підхід «всім суспільством»**, де крім правоохоронців задіяні громади, освітяни, бізнес, медіа — для попередження злочинної експансії й відновлення соціальної стійкості.
- **Системи конфіскації активів** і боротьба з фінансовими потоками мають стати пріоритетом, інакше відмиті доходи вкладаються в інституції й дозволяють мережам зміцнюватися.

Звіти окремих інституцій та експертів

Нова хвиля регулювання боротьби з відмиванням коштів для стимулювання стратегічних інновацій. Роль AMLA [11]

Документ є ґрунтовним дослідженням, яке присвячене створенню Європейського органу з питань боротьби з відмиванням коштів (AMLA) та його впливу на фінансовий сектор ЄС. Автори аналізують причини появи AMLA, очікування стейкхолдерів, практичні виклики для підзвітних установ, а також можливості для створення інноваційної екосистеми боротьби з фінансовими злочинами у Франкфурті.

У вступі наголошується, що AMLA створюється у відповідь на зростання масштабів фінансових злочинів, технологічні виклики та недостатню ефективність фрагментованої національної системи регулювання. У 2024 році було ухвалено новий пакет законодавства — AMLR, AMLA

[11] https://www.ey.com/content/dam/ey-unified-site/ey-com/en-nl/industries/banking-capital-markets/documents/fco/ey-fc-navigating-the-next-wave-of-aml-regulation.pdf

Regulation та 6AMLD, які формують єдиний «AML/CFT Single Rulebook». Його мета — гармонізувати правила, підвищити прозорість, зменшити ризики регуляторного арбітражу та зміцнити координацію між національними підрозділами фінансової розвідки (ПФР).

AMLA отримає широкі повноваження: прямий нагляд за приблизно 40 найбільшими високоризиковими фінансовими установами з транскордонною діяльністю; розробка технічних стандартів і методологій; створення єдиної бази даних кінцевих бенефіціарних власників; координація роботи національних ПФР та впровадження інноваційних технологій для моніторингу транзакцій. Важливим завданням є розширення нагляду і на нефінансові сектори — ринок нерухомості, юридичні професії, торгівлю високовартісними товарами.

Дослідження EY на основі інтерв'ю з близько 50 керівниками банків, фінтехів, страховиків, регуляторів і академічних установ у 10 юрисдикціях окреслило як очікувані переваги, так і ризики створення AMLA. Серед позитивних аспектів респонденти назвали: спрощення процесів комплаєнсу завдяки уніфікації правил, підвищення ефективності управління ризиками, більш прозору систему КБВ, активне використання технологій (AI/ML), зміцнення співпраці між фінансовими установами, регуляторами і правоохоронними органами. Разом з тим, були визначені і виклики: невизначеність майбутніх вимог і стандартів, ризик дублювання зобов'язань із національними регуляторами, висока вартість адаптації внутрішніх систем і процесів, проблеми ресурсного забезпечення та потреба у висококваліфікованих кадрах. Особливо складним є завдання для малих установ і постачальників послуг з віртуальними активами, які змушені інвестувати у складні системи моніторингу транзакцій та процедури CDD.

Важливим акцентом документа є приклади кращих практик з Нью-Йорка, Лондона та Тель-Авіва, де розвиток інноваційних AML-рішень відбувається завдяки активному партнерству між приватним і державним секторами та використанню технологій. Для Франкфурта рекомендовано створення регуляторних «пісочниць», проведення щорічних AML/RegTech-самітів, залучення міжнародних експертів через спрощені міграційні процедури, а також активну співпрацю з університетами у сфері навчання та сертифікації фахівців.

У висновках підкреслюється, що AMLA має потенціал стати одним з трьох найважливіших глобальних регуляторних органів у сфері ПВК/ФТ/ФР, формуючи міжнародні стандарти та підвищуючи стійкість фінансової системи ЄС. Водночас його ефективність залежатиме від прозорості мандату, якості персоналу,

Висновки:

- **Гармонізація правил і зменшення регуляторного арбітражу** — AMLA створює єдиний підхід до нагляду в ЄС, закриваючи прогалини, які дозволяли відмивачам коштів використовувати різні режими у різних країнах.
- **Фокус на технологіях і даних** — впровадження AI/ML, централізованих баз даних КБВ і транскордонного моніторингу транзакцій стане основним інструментом AMLA для підвищення ефективності нагляду.
- **Високі вимоги для підзвітних суб'єктів** — банки, фінтехи і VASP стикаються з необхідністю значних інвестицій у системи контролю, ризик втрат через санкції та потребу у кваліфікованих кадрах.
- **Необхідність партнерства і навчання** — успіх AMLA залежатиме від ефективного PPP, активного діалогу з індустрією та розвитку спеціалізованих освітніх програм для формування професійного AML-ринку.

балансу між регулюванням і підтримкою інновацій, а також рівня співпраці з приватним сектором.

Тіньовий флот: як нелегальні перевезення нафти перетворюють моряків на жертв торгівлі людьми [12]

Стаття опублікована на платформі Context висвітлює масштабну та небезпечну проблему, яка постала на тлі міжнародних санкцій проти Ірану та росії. Її основна ідея полягає в тому, що заходи, покликані обмежити доходи авторитарних режимів, фактично сприяли створенню й розвитку так званого тіньового флоту — суден, які перевозять санкційну нафту поза системою міжнародного нагляду, часто без страхування, з непрозорими власниками та за відсутності будь-якої відповідальності. Цей «dark fleet» за останній рік зріс майже на половину, що стало прямим наслідком санкційної політики. Для прикриття своїх операцій ці судна застосовують маніпуляції із системою відстеження AIS, проводять небезпечні ship-to-ship перевалки та постійно змінюють прапори реєстрації, що ускладнює контроль.

Наслідки цього явища виходять далеко за межі економіки чи політики: на перший план виходять людські трагедії. Сотні моряків, переважно з Індії та країн із низьким рівнем доходів, стають жертвами шахрайських схем і фактично потрапляють у систему трудового рабства. Рекрутингові агентства заманюють їх привабливими обіцянками роботи в міжнародному судноплавстві, але вимагають попередньої плати за працевлаштування, інколи в розмірі кількох сотень доларів. Потім ці моряки опиняються на суднах, які перевозять контрабандну нафту, позбавлені зарплати, харчування, можливості зв'язку з рідними та навіть особистих документів. Багатьох відправляють у табори в Ірані, де вони перебувають під охороною в умовах, що можна кваліфікувати як торгівлю людьми й примусову працю.

Висновки:

- **Запроваджені проти росії та Ірану санкції** стимулювали формування й швидке зростання тіньового флоту, який уникає нагляду, страхування та прозорих реєстрацій, забезпечуючи нелегальні поставки нафти.
- **Тисячі моряків із країн Південної Азії**, зокрема Індії, потрапляють у пастку фальшивих рекрутингових схем, сплачуючи великі суми за «працевлаштування» і зрештою опиняючись у ситуаціях примусової праці та торгівлі людьми.
- **Старі, технічно несправні та незастраховані танкери** тіньового флоту становлять величезну загрозу, адже їхні аварії призводять до людських жертв, вибухів і значного забруднення морського середовища.
- **Допомогу морякам** у таких ситуаціях часто можуть надати лише міжнародні організації на кшталт ISWAN, однак їхні можливості обмежені й вимагають значного посилення підтримки та фінансування.

Одним із прикладів є історія молодого індійця Шубхама Сінгха. Він заплатив значну суму, щоб отримати обіцяну роботу, але натомість виявив себе на старому судні, яке займалося нелегальним перевезенням дизелю. У Перській затоці він ледве уникнув

[12] https://www.context.news/money-power-people/long-read/cost-of-sanctions-dark-shipping-fleet-fuels-human-trafficking

затримання місцевою береговою охороною, а протягом кількох місяців постійно жив із відчуттям небезпеки. Лише завдяки допомозі міжнародної організації ISWAN йому вдалося повернутися додому. Його досвід ілюструє, наскільки вразливими є моряки перед шахрайством і як легко вони стають заручниками глобальних санкційних ігор.

Крім того, використання старих, часто аварійних суден створює екологічні й безпекові ризики. Відомі випадки вибухів і пожеж, які призводили до загибелі членів екіпажу та значного забруднення моря, але ніхто не ніс відповідальності, оскільки власність на такі танкери зазвичай прихована через мережу офшорних компаній і фіктивних реєстрацій. Це перетворює тіньовий флот на загрозу не лише для окремих працівників, а й для глобальної безпеки та екології.

Таким чином, стаття робить висновок, що санкції, не підкріплені комплексними заходами контролю й захисту, породили новий кримінальний сектор із власними правилами й масштабною експлуатацією людей. Розширення тіньового флоту стало прямим результатом санкційної політики, а його існування створило умови для торгівлі людьми, трудового рабства та екологічних катастроф. Єдиним порятунком для моряків залишаються міжнародні мережі допомоги, які мають обмежені ресурси. Проте очевидно, що проблему можна вирішити лише комплексно: посилюючи контроль над судноплавством, запроваджуючи суворіші вимоги до страхування й технічного стану суден, регулюючи діяльність рекрутингових агентств у країнах-донорах робочої сили та підтримуючи системи міжнародної допомоги. Інакше наслідки «тіньової економіки на морі» й надалі залишатимуться невидимими, але смертельно небезпечними для тих, хто стає її жертвами.

Глобальний альянс проти злочинних мереж: нова міжнародна стратегія боротьби з організованою злочинністю [13]

Документ, підготовлений Tony Blair Institute for Global Change спільно з Crest Advisory, представляє стратегічне бачення того, як світ має переосмислити підходи до протидії серйозній та організованій злочинності (SOC). На думку авторів, SOC вже не можна розглядати виключно як питання внутрішньої безпеки окремих держав. Це комплексна глобальна проблема, що підриває демократії, руйнує економічні системи, створює соціальну нестабільність і користується перевагами сучасних технологій та глобалізованої економіки.

Організована злочинність стала феноменом, який легко адаптується до будь-яких умов. Якщо ще два десятиліття тому основні виклики обмежувались наркоторгівлею, нелегальними перевезеннями чи торгівлею людьми, то сьогоднішні злочинні мережі діють у сфері фінансових технологій, кіберпростору, криптовалют, логістики, офшорних юрисдикцій, навіть у легальних ланцюгах постачання. SOC транснаціональна за природою, часто побудована як «павутина», де відсутній єдиний центр, а автономні осередки можуть самостійно генерувати прибутки й одночасно підпорядковуватися загальній мережевій логіці. Злочинці користуються шифрованими месенджерами, штучним інтелектом, системами анонімних платежів, що робить традиційні поліцейські методи фактично безсилими.

[13] http://institute.global/insights/public-services/a-new-international-approach-to-beating-serious-and-organised-crime

Проблема полягає в тому, що уряди та міжнародні організації досі відповідають на SOC інструментами минулого. Існують численні конвенції, угоди, міждержавні робочі групи, але їхня реакція майже завжди запізнюється. Поки правоохоронні органи узгоджують спільні кроки, злочинні мережі вже адаптуються до нових умов. Відсутність єдиного глобального органу координації створює прогалини, які злочинці миттєво використовують. Наприклад, різні підходи до регулювання криптовалют у різних країнах дозволяють їм «перемикати» фінансові потоки між юрисдикціями.

Автори документа стверджують, що потрібна не еволюція існуючих методів, а радикальна трансформація міжнародної відповіді. Саме для цього запропоновано створити Міжнародний альянс із боротьби з організованою злочинністю (International Alliance on Serious and Organised Crime). Його ключова ідея — вийти за межі бюрократичних форматів і зробити структуру максимально мобільною, зосередженою на конкретних діях. Це не має бути «ще одна міжнародна організація», що генерує резолюції й аналітику, але мало впливає на практику. Альянс має стати оперативним майданчиком, здатним діяти на випередження.

Документ наголошує на трьох базових принципах Альянсу. Перше — оперативність: здатність координувати міждержавні дії швидко, проводити синхронні «удари» по злочинних мережах, включаючи замороження активів, арешти ключових осіб, блокування ланцюгів постачання. Друге — технологічна перевага: створення платформи обміну аналітичними даними, використання штучного інтелекту, систем раннього попередження, спільних цифрових інструментів для відстеження транскордонних операцій. Третє — суспільне партнерство: обов'язкове залучення приватного сектору (фінансових інституцій, технологічних компаній, логістичних операторів) та громадянського суспільства. Це визнає очевидну реальність: значна частина інфраструктури, якою користуються злочинці, перебуває поза прямим контролем держави, тому лише співпраця з цими секторами може забезпечити реальний ефект.

Прикладом для такого альянсу наводиться досвід Five Eyes — союзу спецслужб Великої Британії, США, Канади, Австралії та Нової Зеландії, що відзначається високим рівнем довіри й практично безперервним обміном даними. Подібний рівень співпраці у сфері боротьби з організованою злочинністю дозволив би ефективно діяти проти глобальних мереж, які нині користуються фрагментарністю міжнародних зусиль.

Автори підкреслюють особливу роль Великої Британії. Вона має не лише досвід і ресурси, а й політичне зобов'язання виступити лідером у створенні такого Альянсу. Національні реформи у сфері безпеки показали певний прогрес, але їхні результати обмежені рамками країни. Організована злочинність не знає кордонів, і без глобальної ініціативи всі навіть найсучасніші внутрішні інструменти приречені на часткову ефективність.

Важливим є і те, що в документі піднімається питання про превентивний характер боротьби. SOC не можна сприймати як щось, на що слід реагувати постфактум. Альянс має працювати за логікою

Висновки:

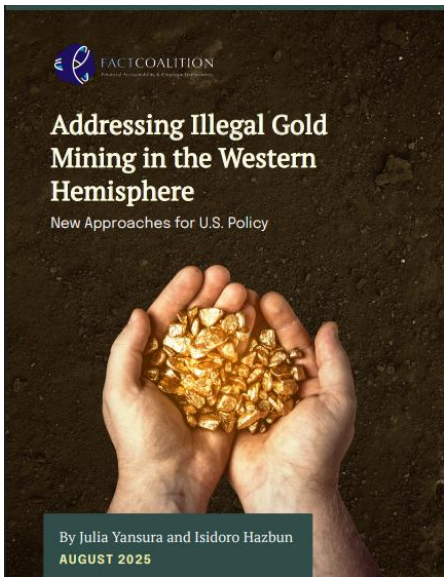
- **Необхідність переосмислення глобальної відповіді на організовану злочинність:** кримінальні мережі працюють швидко, технологічно, глобально — традиційні механізми правосуддя за ними не встигають.
- **Створення Міжнародного Альянсу (Альянс SOC)** — критично необхідний крок для оперативного, координаційного тиску: санкції, технології, перехоплення ланцюгів постачання.
- **Технічна співпраця — ключ до ефективності:** високошвидкісна аналітика, обмін даними, спільні «удари» в режимі реального часу.
- **Публічно-приватне партнерство як фундамент:** бізнес і громадськість — не лише потужні інструменти протидії, а й частина інфраструктури, яка може як допомогти, так і бути вразливою.

«превентивної агресії»: діяти на етапі зародження кримінальних схем, коли вони ще не набули глобального масштабу. Це означає систематичне виявлення нових каналів відмивання грошей, раннє блокування криптовалютних гаманців, що пов'язані з незаконною діяльністю, контроль за транспортними потоками, які використовуються для контрабанди.

Ще один ключовий акцент — роль інновацій. Технологічна база злочинних мереж нині часто випереджає можливості держав. Використання децентралізованих платформ, штучного інтелекту, deepfake-технологій для шахрайства чи вербування робить традиційні правоохоронні інструменти безсилими. Альянс має інвестувати в розробку спільних інноваційних систем, які дозволять «грати на випередження» — від автоматизованого аналізу транзакцій до виявлення підозрілих патернів у глобальній торгівлі.

Таким чином, документ формує чіткий меседж: серйозна та організована злочинність сьогодні є однією з найбільших глобальних стратегічних загроз, порівнянною за масштабом із тероризмом чи гібридною війною. Традиційні методи, побудовані на індивідуальних зусиллях держав, вже не працюють. Потрібен новий міжнародний механізм, що поєднає держави, бізнес і суспільство в єдину мережу швидкого реагування. Лише тоді можна буде говорити про реальний захист демократій і економік від руйнівного впливу SOC.

Як США планують протидіяти незаконному видобутку золота в Західній півкулі [14]



Документ, підготовлений FACT Coalition, представляє собою ґрунтовне дослідження та політичний маніфест щодо одного з найнебезпечніших і водночас найбільш недооцінених викликів у західній півкулі — незаконного видобутку золота. Автори наголошують, що ця діяльність давно вийшла за межі локальної кримінальної проблеми: вона перетворилася на системну кризу, яка водночас є екологічною катастрофою, загрозою правам людини, механізмом фінансування організованої злочинності та серйозним викликом для міжнародної фінансової безпеки.

На прикладах із країн Латинської Америки — насамперед Колумбії, Перу, Еквадору та Венесуели — показано, як швидко розростається нелегальний золотодобувний сектор. У Колумбії прибутки від незаконного золота вже перевищили доходи від торгівлі наркотиками, що є безпрецедентним сигналом про масштаби цієї тіньової економіки. У регіоні створено складні багаторівневі схеми, які поєднують рекрутинг місцевих громад, часто з використанням насильства, корумпування урядових структур, фальсифікацію сертифікатів походження золота та створення цілої індустрії «відмивання» через офшорні компанії та фіктивні структури. Золото, видобуте підпільними шахтами, швидко інтегрується в легальні глобальні ринки, зокрема у фінансову систему США, що робить американську економіку не лише споживачем, але й невільним «партнером» цього злочинного бізнесу.

Водночас документ демонструє багатовимірність шкоди. Екологічний аспект полягає у масштабному руйнуванні лісів Амазонії, отруєнні ртуттю річкових систем, які забезпечують мільйони людей питною водою, а також у довготривалому забрудненні ґрунтів. Соціальний вимір проявляється у зростанні масштабів трудової експлуатації та торгівлі людьми: місцевих мешканців змушують працювати у небезпечних умовах, а прибутки спрямовуються на

[14] https://thefactcoalition.org/wp-content/uploads/2025/08/Gold-Mining-Policy-Report-FACT-ENG-V3.pdf

фінансування збройних груп і кримінальних картелів. Усе це створює замкнене коло бідності, насильства та безправ'я, яке важко розірвати без рішучих зовнішніх і внутрішніх втручань.

Особливо важливою є роль США. Америка є одним із найбільших ринків збуту золота у світі й водночас одним із ключових «транзитних вузлів» для фінансових потоків, пов'язаних із золотодобувним бізнесом. Через відсутність жорстких правил контролю за походженням золота, низький рівень прозорості компаній і прогалини в митному законодавстві величезні обсяги нелегально видобутого металу щороку опиняються в американській економіці. Це означає, що боротьба з кризою неможлива без активної та системної політики США.

У документі пропонується цілий комплекс законодавчих і виконавчих заходів. На законодавчому рівні ключовим кроком має стати ухвалення «United States Legal Gold and Mining Partnership Act», який передбачатиме створення довгострокової рамкової стратегії для співпраці з країнами регіону з метою зменшення екологічних і соціальних наслідків незаконного видобутку. Важливим кроком також є внесення незаконного видобутку золота до переліку предикатних злочинів для звинувачень у відмиванні грошей. Це дозволить прокуратурі переслідувати компанії та фізичних осіб, які легалізують золото сумнівного походження. Ще одна пропозиція — змінити правила фінансової звітності при перетині кордону: так само, як зараз потрібно декларувати готівку понад 10 тисяч доларів, має бути обов'язковою декларація щодо золота, що дозволить відслідковувати та блокувати канали дрібних нелегальних перевезень через кур'єрів.

На рівні виконавчої влади наголошується на важливості повного впровадження Corporate Transparency Act (CTA). Саме цей інструмент може ліквідувати механізм фіктивних компаній, які сьогодні слугують головним способом маскування нелегального походження золота. Крім того, у документі пропонується створити санкційну програму, спеціально спрямовану проти екологічних злочинів, у тому числі незаконного видобутку золота. Такі санкції мають накладатися не лише на фізичних осіб і компанії, безпосередньо причетних до незаконних шахт, а й на фінансових посередників та логістичні структури, які обслуговують цей бізнес. Автори закликають також до розширення інструментів Департаменту юстиції, Міністерства внутрішньої безпеки (HSI) та інших структур для проведення спільних операцій, що дозволять ефективніше виявляти і переслідувати учасників міжнародних злочинних мереж.

Висновки:

- **Включення незаконного видобутку золота до предикатних злочинів**, що дають підставу для обвинувачення у відмиванні грошей, створює реальний правовий механізм для кримінального переслідування і руйнування схем легалізації.
- **Запровадження обов'язкової декларації золота при перетині кордону** на рівні $10 000 — дозволить перекрити ключовий канал нелегальної логістики й зменшити масштаби дрібної контрабанди.
- **Повне впровадження Corporate Transparency Act** — позбавить злочинців можливості користуватися фіктивними компаніями для легалізації золота.
- **Створення спеціальної санкційної програми для екологічних злочинів** — забезпечить точковий тиск на учасників тіньових схем і зробить нелегальний видобуток економічно менш привабливим.

Окремий розділ документа присвячено необхідності міжнародного співробітництва. США мають відновити фінансування програм допомоги країнам Латинської Америки, спрямованих на боротьбу з нелегальним видобутком. Йдеться як про фінансову підтримку екологічних та правозахисних проєктів, так і про технічну допомогу правоохоронним органам. Автори зазначають, що скорочення такої допомоги в минулі роки стало серйозною помилкою, адже країни

походження нелегального золота залишилися сам-на-сам із проблемою, яка має глобальний характер.

Таким чином, документ підводить до висновку: незаконний видобуток золота — це багаторівнева загроза, що вимагає комплексної відповіді. Йдеться не лише про злочинність і відмивання грошей, а й про екологічну катастрофу в Амазонії, підрив легітимності держав, фінансування кримінальних і терористичних груп. США, як глобальний фінансовий і торговельний центр, не можуть залишатися осторонь. Їхня роль має полягати у створенні нової стратегії, яка поєднає законодавчі реформи, виконавчі дії та міжнародне співробітництво, щоб зламати економічну модель незаконного золотого ринку й зупинити руйнівну діяльність, що сьогодні підриває демократію, екологію та права людини.

Рекомендовані та навчальні матеріали

Переоцінка фінансування тероризму у 2025 році [15]

Це своєчасний та глибокий аналітичний матеріал, який чітко окреслює фундаментальні зсуви у ландшафті фінансових загроз. Автори слушно наголошують, що ми стоїмо на порозі нової ери, де традиційні підходи до протидії фінансуванню тероризму (ПФТ) виявляються все менш ефективними перед лицем стрімкої технологічної еволюції та зміни самої природи терористичних загроз. Стаття є не просто оглядом поточних тенденцій, а стратегічним прогнозом, що вимагає негайної реакції як від регуляторів, так і від приватного сектору.

Ключова теза, що проходить червоною ниткою крізь увесь документ, полягає в тому, що терористичні організації активно диверсифікують свої фінансові потоки, створюючи складну, гібридну модель, яка поєднує новітні цифрові інструменти з перевіреними часом традиційними методами. Особливу тривогу викликає майстерне використання віртуальних активів. Мова йде не лише про загальновідомі криптовалюти, такі як Bitcoin чи Ethereum, а й про анонімні монети (Monero) та стейблкоїни (Tether), що дозволяє терористам не тільки ефективно збирати кошти в глобальному масштабі, але й швидко переміщувати їх, минаючи класичну фінансову систему. Це створює серйозний виклик для підрозділів фінансової розвідки та працівників з комплаєнсу, оскільки відстеження транзакцій у блокчейні вимагає специфічних навичок та інструментарію, а використання міксерів та децентралізованих бірж може повністю розірвати ланцюг походження коштів.

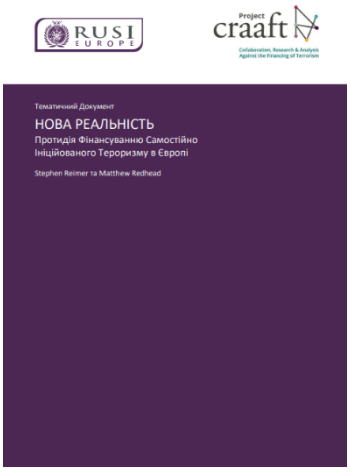
Водночас стаття акцентує увагу на тому, що фінансування тероризму все частіше стає елементом ширших гібридних загроз. Це означає розмиття меж між тероризмом, організованою злочинністю, кібератаками та операціями підривної діяльності, що можуть спонсоруватися певними державами. Фінансові потоки в таких умовах стають значно складнішими для ідентифікації, адже кошти, зібрані нібито на злочинну діяльність, можуть бути легко перенаправлені на фінансування терористичного акту. Це вимагає переходу від вузькоспеціалізованого погляду на ПФТ до комплексного, інтегрованого підходу, що враховує увесь спектр фінансових злочинів та загроз національній безпеці.

[15] https://www.rusi.org/explore-our-research/publications/insights-papers/reassessing-financing-terrorism-2025

Важливо, що автори не ігнорують і традиційні канали, які залишаються актуальними. Готівка, неформальні системи переказу коштів на кшталт "гавали" та зловживання статусом неприбуткових організацій (НПО) нікуди не зникли. Навпаки, вони часто використовуються для переведення віртуальних активів у готівку або для фінансування осередків на місцях, де цифровий слід є небажаним. Це підкреслює необхідність збереження та посилення контролю за цими, здавалося б, "застарілими" векторами загроз.

Аналізуючи причини недостатньої ефективності існуючих систем ПФТ, стаття вказує на критичне відставання регуляторних рамок та правозастосовної практики від швидкості технологічних змін. Багато юрисдикцій досі не мають адекватної правової бази для регулювання ринку віртуальних активів, а фінансовий сектор, особливо у сфері FinTech, не завжди володіє достатньою зрілістю та ресурсами для побудови ефективних систем ризик-менеджменту без чітких вказівок з боку держави. Фундаментальною проблемою залишається ідентифікація фінансування тероризму, яке, на відміну від відмивання коштів, часто походить із легальних джерел і може включати невеликі суми, що не викликають підозр у стандартних системах моніторингу.

У якості шляху вперед, автори наполягають на необхідності побудови нової, проактивної та адаптивної архітектури ПФТ. Центральним елементом цієї архітектури має стати поглиблена співпраця між державним та приватним секторами. Це не повинно обмежуватися формальним обміном інформацією, а має перерости у справжнє партнерство, де фінансові установи отримують від розвідувальних та правоохоронних органів актуальні дані про загрози, типології та індикатори, а натомість надають якісні та своєчасні повідомлення про підозрілі операції. Лише такий інтегрований, заснований на розвідувальних даних підхід, що поєднує фінансовий аналіз, оперативно-розшукову діяльність та міжнародну кооперацію, дозволить нам ефективно протистояти фінансовим загрозам майбутнього, які вже сьогодні стають нашою реальністю.



Дана аналітична записка була створена в рамках проєкту Craaft який покликаний забезпечити співпрацю та проведення аналітичних досліджень в контексті ПФТ. В рамках цього проєкту було випущено три звіти, які розглядали різні аспекти фінансування тероризму. На офіційному сайті Міністерства фінансів України доступні переклади цих документів: Фінансування тероризму за допомогою злочинної діяльності у Європі [16] , Вплив нових технологій на ризики фінансування тероризму [17] , Протидія фінансуванню самостійно ініційованого тероризму в Європі[18].

Інші новини

Джерсі розслідує справу Романа Абрамовича за підозрою у відмиванні коштів [19]

Влада Джерсі проводить розслідування щодо російського мільярдера Романа Абрамовича за підозрою у відмиванні коштів, при цьому судові записи свідчать про рух сотень мільйонів доларів через швейцарські банківські рахунки. Це розслідування бере свій початок з платежів, які Абрамович здійснив у 1990-х роках для збереження контролю над російською нафтовою компанією. Деталі поточного розслідування стали відомі завдяки серії судових рішень, виданих

[16] http://bit.ly/3ImUXZK
[17] http://bit.ly/4n3G7Xd
[18] http://bit.ly/41RAtPn
[19] https://www.occrp.org/en/news/jersey-probes-roman-abramovich-over-suspected-money-laundering

у травні швейцарським судом і отриманих OCCRP, які також вказують на підозри влади Джерсі щодо порушення економічних санкцій компаніями "під [його] контролем". Ці судові рішення дали швейцарській владі дозвіл на надання банківської інформації Джерсі. Швейцарські судові рішення обговорюють бізнесмена, якого згадують лише як "G", але містять довідкову інформацію, включаючи ділові операції, що дозволило репортерам остаточно ідентифікувати його як Абрамовича. Прокурори Джерсі підозрюють, що "G" здійснював "корупційні платежі" у 1990-х роках для збереження контролю над російською компанією, а доходи від подальшого продажу цієї компанії за 13 мільярдів доларів були депоновані на банківські рахунки пов'язаних з ним компаній. Ці деталі збігаються з добре відомим продажем російської нафтової компанії Sibneft Абрамовичем у 2005 році за 13 мільярдів доларів, причому виручені кошти були перераховані на рахунки компаній, контрольованих двома організаціями, зареєстрованими на Джерсі, згідно зі швейцарськими рішеннями.

Окремо, суддя Високого суду Англії у 2012 році постановив, що Абрамович здійснив "значні грошові виплати" у 1990-х роках для отримання необхідного політичного заступництва та впливу, що дозволило йому зберегти контроль над Sibneft. Юристи Абрамовича заявили OCCRP, що англійське рішення "не містить висновків про те, що наш клієнт порушив будь-який закон щодо своїх ділових операцій, і в захисті нашого клієнта не було припущень, що його придбання відповідної юридичної особи було досягнуто через корупцію. Будь-яке протилежне припущення є оманливим, неправдивим та наклепницьким".

Крім того, влада Джерсі підозрює, що "компанії, опосередковано під контролем G", порушили законодавство Джерсі, здійснюючи операції та надаючи фінансові послуги після того, як Абрамович був включений до санкційних списків 10 березня 2022 року. Джерсі, разом з іншими юрисдикціями, такими як Велика Британія та Європейський Союз, наклала санкції на Абрамовича через його зв'язки з Кремлем після повномасштабного вторгнення Росії в Україну у лютому 2022 року.

Запитуючи допомогу у швейцарської влади, прокурори Джерсі заявили, що вони підозрюють порушення. Офіс генерального прокурора Джерсі відмовився коментувати поточні розслідування, тоді як офіс генерального прокурора Швейцарії підтвердив виконання запиту про взаємну правову допомогу від Джерсі, але відмовився надавати подальшу інформацію. Швейцарські рішення показують, як федеральні прокурори у 2023 та 2024 роках зобов'язали швейцарський банк надати записи, що стосуються трьох компаній, зареєстрованих на Кіпрі, Британських Віргінських Островах та Джерсі. Кожна компанія оскаржила це розпорядження, але у травні швейцарський кримінальний суд відхилив їхні апеляції. Подальші апеляції цих трьох компаній до Верховного суду Швейцарії були визнані неприйнятними. Юридична фірма MME, яка представляє ці три неназвані компанії, що оскаржували розкриття інформації про банківські рахунки, не відповіла на запит про коментар.

Окремо кіпрські посадовці повідомили репортерам, що вони передали інформацію про компанії, пов'язані з розслідуванням, на запит влади Джерсі. Прес-служба поліції Кіпру підтвердила надання інформації, але додала, що "подальша інформація наразі не може бути розкрита, оскільки розслідування триває". Посадовець правоохоронних органів Кіпру, який побажав залишитися анонімним, описав запити Джерсі як "великі" і заявив, що було надано "багато матеріалу". Джерсі отримала інформацію про "відкриття банківських рахунків, записи компаній з реєстру та записи для трастів від Комісії з цінних паперів та бірж Кіпру".

Юридична фірма Kobre & Kim, яка представляє Абрамовича, заявила, що її клієнту не було пред'явлено жодних звинувачень на Джерсі і він "заперечує будь-які звинувачення у неправомірних діях". Фірма відмовилася відповідати на питання щодо змісту швейцарських рішень, зазначивши, що "наш клієнт не був стороною цих проваджень, і жодних подань від його імені не робилося. З цієї причини він не в змозі відповісти".

Ця стаття OCCRP також згадує попередні розслідування, такі як те, що Credit Suisse кредитував сотні мільйонів доларів офшорним компаніям Абрамовича, які використовували акції США як заставу, а також секретне партнерство Абрамовича з Кремлем у великій лісовій компанії.

Криптомати під прицілом: як США відповідають на хвилю шахрайств і вводять масові обмеження [20]

Стаття, опублікована Cointelegraph, аналізує нову хвилю законодавчих та адміністративних рішень у США, спрямованих проти криптоматів (crypto ATMs, або «крипто-банкоматів»). Ці пристрої, які колись символізували поширення та демократизацію криптовалют, поступово перетворилися на об’єкт серйозної критики. Спочатку вони приваблювали користувачів швидким і відносно простим доступом до цифрових активів, зокрема можливістю анонімно купувати чи конвертувати криптовалюту без банківських рахунків і складних процедур перевірки особи. Однак саме ця анонімність і відсутність жорстких вимог до ідентифікації зробили криптомати одним із головних інструментів шахрайства, фінансових злочинів і навіть міжнародних кримінальних схем.

Федеральне бюро розслідувань повідомило, що у 2024 році зафіксувало близько 11 тисяч скарг, пов’язаних із шахрайством через криптомати, на загальну суму понад 246 мільйонів доларів. При цьому переважна більшість постраждалих — це люди похилого віку, старші за 60 років. Саме ця група населення стала улюбленою мішенню шахраїв: жертвам телефонують або пишуть, створюючи відчуття терміновості чи небезпеки, а потім вмовляють внести готівку через криптомат для «вирішення проблеми». Схема працює практично миттєво: як тільки гроші вносяться, вони відразу надсилаються на анонімні криптогаманці за кордон, і шансів повернути їх практично немає. Ці випадки не поодинокі, а формують системну тенденцію, яку дедалі важче ігнорувати правоохоронцям і місцевій владі.

У відповідь окремі міста ухвалили радикальні рішення. Так, у місті Stillwater (штат Міннесота) запровадили повну заборону на криптомати після випадку з літньою мешканкою, яка втратила понад 5 тисяч доларів. Поліція міста повідомила, що з 2023 року зафіксувала 31 випадок шахрайства, пов’язаного з криптоматами, включно з історією іншої жертви, яка втратила 29 тисяч доларів. З огляду на те, що Stillwater має лише 20 тисяч мешканців, масштаби втрат виглядають особливо загрозливими. Аналогічно, у червні 2025 року місто Spokane у штаті Вашингтон заборонило як нові, так і існуючі криптомати, пояснивши, що ці машини стали «улюбленим інструментом шахраїв».

Деякі громади діють наперед, навіть не маючи криптоматів на своїй території. Grosse Pointe Farms у Мічигані, невелике містечко неподалік від Детройта, ввело попереджувальні обмеження — ліміт у 1 000 доларів на день і 5 000 доларів за 14 днів. Місцева влада прямо визнала, що криптомати становлять підвищений ризик шахрайства, який може поставити під загрозу добробут мешканців, якщо не вжити заходів заздалегідь.

[20] https://cointelegraph.com/news/crypto-atm-limits-bans-sweep-across-us

На рівні штатів картина ще масштабніша. Арізона ухвалила закон, який дозволяє новим користувачам витрачати не більше 2 000 доларів на день, а постійним — до 10 500 доларів. У випадку шахрайства оператори зобов'язані повертати кошти протягом 30 днів. Арканзас прийняв власний закон після того, як офіс Генерального прокурора отримав скарги на шахрайські операції на суму понад 400 тисяч доларів за рік. Колорадо додав спеціальні вимоги: оператори мусять не лише відшкодовувати кошти, а й дзвонити літнім клієнтам перед їхньою першою транзакцією для підтвердження намірів.

Особливо показовим є приклад Айови, де влада не обмежилася законодавчими рамками. Генеральна прокурорка Бренна Берд подала позови проти двох найбільших операторів — Bitcoin Depot і CoinFlip — звинувачуючи їх у співучасті у шахрайських схемах, оскільки компанії отримують комісійні від транзакцій, що здійснюються шахраями. Берд наголосила, що такі дії не просто аморальні, а й незаконні. Це означає перехід від регуляторних заходів до прямих юридичних процесів проти ключових гравців ринку.

Схожі закони ухвалили й інші штати: Меріленд, Міннесота, Небраска, Північна Дакота, Оклахома, Род-Айленд, Вермонт, Вісконсин. У них містяться суворі ліміти на транзакції (від 1 000 до 2 000 доларів на день), обов'язкове ліцензування операторів, вимога реєструватися як платіжні організації, суворі процедури ідентифікації користувачів (KYC), а також встановлені обмеження на комісії (зазвичай не більше 15–18 % від суми). Деякі штати прописали обов'язкове відшкодування для нових користувачів у разі шахрайства протягом 14–90 днів, а також спеціальні правила для захисту літніх людей.

У статті підкреслюється, що ця хвиля обмежень набуває загальнонаціонального характеру. У Вашингтоні розглядається федеральний законопроєкт, який передбачає поширення подібних правил на всі штати. У разі ухвалення це фактично поставить під сумнів економічну доцільність бізнесу криптоматів: нові вимоги до ліцензій, комісій та KYC-процедур різко зменшують їхню прибутковість. Уже зараз експерти попереджають, що цей бізнес може стати нерентабельним або витіснитися в «сіру зону».

Таким чином, криптомати у США пройшли трансформацію від символу технологічної інновації та популяризації криптовалют до явища, яке асоціюється з шахрайством, втратою заощаджень та соціальними ризиками. Вони стали прикладом того, як фінансова інновація без достатнього регуляторного супроводу може створити масштабну проблему для суспільства. Нині їхнє майбутнє виглядає невизначеним: або суворе регулювання виведе їх у легальну та контрольовану площину, або посилення вимог остаточно позбавить цей сектор економічного сенсу.

Аеропорти на передовій: як навчання персоналу допомагає виявляти та рятувати жертв торгівлі людьми[21]

Управління ООН з наркотиків і злочинності (UNODC) опублікувало матеріал, в якому зосередило увагу на аеропортах як на критично важливих точках у боротьбі з торгівлею людьми. Саме авіаційні хаби дедалі частіше стають каналами переміщення жертв — жінок, чоловіків і дітей — адже через авіасполучення можна швидко переправити людину на великі відстані, маскуючи операцію під звичайну подорож. Торгівці

[21] https://www.unodc.org/unodc/frontpage/2025/August/equipping-airports-to-identify-and-assist-human-trafficking-victims.html

людьми використовують аеропорти як своєрідні «сірі зони», де пасажиропотоки величезні, а ризик виявлення залишається мінімальним, якщо персонал не знає, на що звертати увагу. Саме тому UNODC підкреслює: аеропорти повинні бути не лише транспортними вузлами, а й першою лінією ідентифікації та допомоги жертвам.

Публікація докладно описує ініціативу, запроваджену у співпраці з аеропортом Лас Américas у Санто-Домінго (Домініканська Республіка). Тут за підтримки UNODC проводяться комплексні тренінги для широкого кола авіаційного персоналу — від працівників безпеки та прикордонників до співробітників служб підтримки пасажирів і поліцейських підрозділів. Головна мета — навчити цих людей розпізнавати ознаки того, що пасажир може бути жертвою торгівлі людьми. Йдеться про поєднання поведінкових сигналів (страх, уникнення розмов, суперечливі пояснення щодо маршруту), фізичного стану (сліди виснаження, хвороб, насильства) та контекстуальних маркерів (квитки, придбані іншою особою, відсутність документів чи багажу, супровід особи, яка контролює відповіді жертви).

Особливий акцент робиться не лише на виявленні, а й на правильному реагуванні. У статті наголошується: недостатньо ідентифікувати потенційну жертву, потрібно також створити для неї безпечний простір, де вона зможе висловитися без ризику помсти від торгівця. Працівники аеропорту мають знати чіткі алгоритми — кого викликати, як діяти, як забезпечити конфіденційність, як уникнути повторної травматизації людини. Для цього в навчальних програмах UNODC використовуються як теоретичні заняття, так і практичні вправи з моделюванням реальних сценаріїв у терміналах. Такий підхід дозволяє закріпити знання та перевірити, як персонал поводиться в умовах максимально наближених до реальності.

UNODC розглядає Домініканську Республіку як пілотний майданчик, але водночас підкреслює, що ця практика має стати моделлю для масштабування у світі. У статті пояснюється: саме аеропорти часто є останнім шансом урятувати людину до того, як вона потрапить у ситуацію примусової праці, сексуальної експлуатації чи інших форм сучасного рабства. Якщо персонал не готовий і не навчається регулярно, цей шанс буде втрачено. Водночас там, де впроваджені подібні тренінги, вже спостерігаються успішні випадки виявлення жертв і надання їм допомоги. Це свідчить, що інвестиції в підготовку персоналу є ефективним і практично досяжним засобом боротьби з глобальною проблемою.

Матеріал також підкреслює, що боротьба з торгівлею людьми в аеропортах вимагає широкої міжсекторальної співпраці. Йдеться не лише про персонал аеропорту чи прикордонників, а й про авіакомпанії, які мають бути залучені у процес підвищення пильності та обізнаності. Пілоти, бортпровідники, працівники реєстрації також можуть відігравати важливу роль, адже вони часто бачать пасажирів у різних ситуаціях і здатні помічати нетипові деталі поведінки. UNODC закликає до створення єдиних протоколів взаємодії, де кожна ланка авіаційної системи розумітиме свої завдання і знала б, як передати сигнал тривоги у випадку підозри.

Таким чином, стаття позиціонує аеропорти як стратегічний фронт у глобальній боротьбі з торгівлею людьми. Вона демонструє, що навіть у переповнених і стресових середовищах можна створити умови для виявлення жертв, якщо персонал підготовлений, мотивований і забезпечений інструментами для швидкого реагування. Пілотна ініціатива в Санто-Домінго є лише початком, але вона чітко показує напрямок: боротьба з торгівлею людьми має виходити за межі абстрактних кампаній і втілюватися в конкретних точках, де жертви мають шанс бути поміченими та врятованими.

Для загального розвитку

Майбутнє прозорості трастів: міжнародні стандарти, регіональні виклики та шляхи до ефективного розкриття бенефіціарів [22]

Документ узагальнює ключові результати та дискусії міжнародного круглого столу, організованого в травні 2025 року EU AML/CFT Global Facility спільно з CFATF та GAFILAT, який був присвячений питанням прозорості кінцевих бенефіціарних власників у сфері трастів та інших правових утворень. У заході взяли участь понад 950 представників із 104 країн, що відображає глобальну зацікавленість та усвідомлення нагальності проблеми. Серед учасників були представники міжнародних організацій (FATF, Єврокомісія, APGML, MENAFATF, Moneyval, Global Forum), державних органів з Австралії, Чехії, Еквадору, Мальти та Намібії, приватного сектору (трастові юристи, банки, адміністратори), а також журналісти-розслідувачі, науковці та представники громадянського суспільства (Transparency International, Basel Institute, Open Ownership).

У центрі уваги дискусій було подвійне значення трастів як інструментів управління майном: з одного боку, вони можуть служити легітимним механізмом захисту активів чи податкового планування, а з іншого — становлять серйозний ризик для прозорості фінансових потоків, ефективності фінансового моніторингу та повернення активів. Наголошувалося, що трасти створюють особливі виклики через відсутність обов'язкової реєстрації, складність багаторівневих структур і можливість використання так званих «дискреційних трастів», які формують правовий вакуум, де жодна зі сторін не визнається власником активів, що ускладнює арешт та конфіскацію. Ці проблеми були ілюстровані прикладами міжнародних журналістських розслідувань («Panama Papers», «Paradise Papers», «Pandora Papers»), які показали зростання ролі трастів у схемах ухилення від оподаткування, відмивання коштів та приховування активів політиків, олігархів та осіб, пов'язаних із корупцією.

Окремо розглядалися міжнародні стандарти. FATF презентувала оновлені вимоги у Рекомендаціях 24 і 25 та відповідні настанови 2023–2024 років, які акцентують на необхідності своєчасного, повного та достовірного доступу компетентних органів до інформації про бенефіціарів як юридичних осіб, так і правових утворень, включаючи іноземні трасти, що мають «суттєвий зв'язок» із юрисдикцією. Європейська комісія наголосила на новому AML Package, який набуде чинності з 2027 року та передбачає широке визначення КБВ для трастів (усі засновники, усі бенефіціари, контролери та об'єкти повноважень) і впровадження диференційованих рівнів доступу до реєстрів: від повного для органів влади до обмеженого для журналістів, громадськості та суб'єктів фінансового моніторингу. Global Forum розкрив значення трастів у сфері оподаткування, адже вони можуть генерувати дохід, що підлягає різним видам податків, та водночас створюють труднощі через відокремлення юридичної власності від фактичного контролю, багатоюрисдикційність і відсутність повного обліку. Для подолання цих викликів пропонується комбінований підхід, який поєднує податкові, реєстрові механізми та механізми ПВК/ФТ.

Важливу частину документа складає аналіз регіонального досвіду. У країнах Азії та Тихоокеанського регіону більшість юрисдикцій залишаються частково або повністю несумісними з Рекомендацією 25 FATF, а рівень ефективності оцінюється як низький. У країнах

[22] https://www.global-amlcft.eu/wp-content/uploads/2025/08/EUGF-CFATF-GAFILAT_Trust-webinar_Report_Final.pdf

Близького Сходу та Північної Африки додатковим викликом є специфічна форма правових утворень — Waqf, яка частково співвідноситься з трастами, але має суперечливу класифікацію. У Карибському басейні, де трастові послуги мають міжнародне значення, лише окремі юрисдикції досягли прийнятного рівня відповідності, тоді як більшість стикається з проблемою неформальних і непрофесійних трастів, відсутністю централізованих реєстрів та слабкою верифікацією. У Латинській Америці зафіксовано низький рівень правового врегулювання та відсутність доступу до актуальних даних, що робить трасти вразливими до зловживань. У Європі більшість країн формально виконують вимоги FATF і ЄС, однак ефективність оцінюється як помірна, оскільки на практиці реєстри ще не повністю заповнені, контроль за непрофесійними трастами залишається слабким, а значна частина активів утримується за межами юрисдикцій.

Особливе місце приділено практичним прикладам. Чехія, Намібія, Еквадор і Австралія поділилися досвідом впровадження реєстрів КБВ трастів. У Чехії створено реєстр, який передбачає автоматичне припинення діяльності трастів без реєстрації, тоді як у Намібії запроваджено сучасну онлайн-систему з регулярним оновленням даних та механізмами контролю за добросовісністю користувачів. Австралія та Еквадор показали власні підходи до врегулювання, які відображають поєднання податкового, корпоративного аспектів, та аспекту у сфері ПВК.

Водночас документ висвітлює позиції практиків: трастові юристи та банкіри підкреслюють, що трасти використовуються не лише для ухилення, а й для легітимного планування (наприклад, спадкування, захист вразливих бенефіціарів, сімейний бізнес). Проте навіть у таких випадках вони створюють високі ризики для прозорості, особливо коли засновники впливають на управління неофіційно або коли трастові структури приховують реальний економічний інтерес. Малтійський досвід продемонстрував комплексний підхід: поєднання реєстрів, нагляду за трастовими адміністраторами, банківськими перевірками та координації з органами фінансової розвідки.

Завершальна частина документа акцентує на необхідності поєднувати формальну відповідність стандартам із реальною ефективністю. Країни мають зміцнювати національні оцінки ризиків, активно залучати академічні інституції, журналістів та громадянське суспільство до виявлення зловживань, посилювати регулювання непрофесійних трастів та суб'єктів, що надають відповідні послуги, створювати й підтримувати ефективні реєстри КБВ і забезпечувати міжнародну співпрацю для обміну інформацією. Загальний висновок полягає у тому, що хоча технічна база багатьох країн поступово вдосконалюється, ефективність залишається низькою, і без системних змін у нагляді, верифікації, обміні даними та регіональній координації трасти й надалі залишатимуться одним із найскладніших інструментів для протидії відмиванню коштів і приховуванню активів.

Висновки:

- **Необхідність комплексних національних оцінок ризиків трастів.** Країни мають інтегрувати дані академії, журналістів і НУО для виявлення зловживань та прогалин у контролі.
- **Посилення регуляції та нагляду за трастовими провайдерами і непрофесійними трастами.** Особливо важливо для ВНУП (адвокати, нотаріуси, трастові адміністратори), які часто залишаються поза увагою.
- **Запровадження ефективних реєстрів КБВ трастів.** Реєстри повинні бути повними, оновлюваними, з верифікацією і механізмами повідомлення про розбіжності, забезпечуючи доступ органів, банків і суспільства.
- **Міжнародна співпраця та прозорість як умова успіху.** Без швидкого обміну даними, визнання іноземних рішень і гармонізації стандартів (FATF, ЄС, Global Forum) ризики зловживань залишатимуться високими.

Ваша думка важлива!

1. З огляду на заклик до посилення неформальної співпраці, які, на вашу думку, є головними практичними перешкодами для налагодження ефективної "діагональної" взаємодії (наприклад, між прокуратурою однієї країни та ПФР іншої) і як можна збудувати необхідний рівень довіри, що випереджатиме формальні процедури ВПД?
2. Що, на ваш погляд, є найбільш критичним елементом для забезпечення реальної ефективності реєстрів бенефіціарних власників?
3. Де, на вашу думку, проходить межа між необхідним регулюванням криптосектору для запобігання фінансовим злочинам та надмірним тиском, який може пригнічувати технологічні інновації та фінансову інклюзію?
4. Який баланс між стимулюванням розвитку криптоіндустрії та запобіганням фінансовим злочинам слід вибудувати Україні, щоб уникнути ситуації, коли інновація перетворюється на загрозу?
5. Як можна забезпечити баланс між інноваціями у сфері токенізованих активів та захистом інвесторів і вкладників, враховуючи специфічні технологічні ризики, які підкреслює FINMA?
6. Чи здатні традиційні регуляторні моделі (як-от MiCA чи закони про ринки капіталу) ефективно протидіяти унікальним схемам зловживань у децентралізованих крипторинках, та чи потрібно Україні розробити власний спеціалізований підхід і чому?
7. Як запобігти вербуванню молоді в злочинні структури в умовах війни, економічної нестабільності та високого рівня соціальної вразливості?
8. Які технологічні рішення та партнерства з приватним сектором Україна може використати вже сьогодні, щоб блокувати фінансові й логістичні потоки організованих злочинних мереж, особливо тих, що пов’язані з війною та контрабандою?

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-2025-37

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].