

“Маленька дія часто спричиняє великий поштовх”

Ноа Скалін

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.

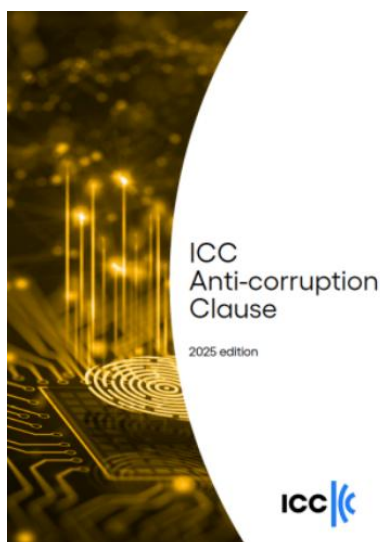
Для регуляторів та правоохоронних органів є інструментом для розробки ефективних стратегій боротьби з ВК, включаючи навчання та координацію дій між різними установами для забезпечення належної співпраці та обміну інформацією.

Звіти міжнародних організацій та окремих юрисдикцій

Як захистити бізнес від корупційних ризиків: нові положення ICC у сфері комплаєнсу¹



[АУДІОПЕРЕКАЗ](#)



Документ є оновленою редакцією модельної антикорупційної клаузули, розробленої Міжнародною торговою палатою (ICC) з метою сприяння запобіганню та протидії корупції в договірних зобов'язаннях між підзвітними суб'єктами. Він має практичне прикладне значення для широкого кола учасників міжнародної торгівлі, постачальників, інвесторів, державних органів, юридичних радників та комплаєнс-офіцерів, які прагнуть забезпечити прозорість і доброчесність ділових відносин.

Клаузула 2025 року структурується навколо трьох альтернативних механізмів її включення до комерційних контрактів. Перший варіант (Option I) пропонує включити до договору загальне посилання на ICC Rules on Combating Corruption (2023) без потреби інтегрувати повний текст правил. Цей варіант підходить у ситуаціях, коли сторони бажають зберегти стислий формат

¹ <https://iccwbo.org/wp-content/uploads/sites/3/2025/07/2025-ICC-Anti-corruption-Clause-2025-edition.pdf>

контракту, але водночас підтвердити прихильність до міжнародних стандартів доброчесності. Другий варіант (Option II) дозволяє включити повний текст ICC Rules 2023 до контракту, забезпечуючи таким чином пряму правову дію правил і мінімізуючи можливі суперечності у тлумаченні. Третій варіант (Option III) базується на включенні положення про обов'язкове дотримання власної корпоративної програми антикорупційного комплаєнсу, яка має відповідати вимогам статті 11 Правил 2023 року. Такий підхід особливо релевантний для великих компаній, які вже мають комплексно розроблені внутрішні політики та процедури комплаєнсу.

У документі подано детальні коментарі до кожної з опцій, у яких розглядаються правові наслідки застосування клаузули, її взаємодія з іншими положеннями контракту, а також ризики, пов'язані з недотриманням або формальним підходом до імплементації. Особливу увагу приділено питанню відповідальності сторін, визначенню фактів порушення та можливості розірвання договору в разі встановлення фактів корупційної поведінки. Усі три варіанти дозволяють сторонам адаптувати механізми контролю за дотриманням антикорупційних зобов'язань відповідно до юрисдикційних особливостей, характеру правовідносин і ступеня ризику, який сторони готові взяти на себе.

Другу половину документа займає текст ICC Rules on Combating Corruption (2023), який є основоположним джерелом для формування змісту антикорупційної клаузули. Ці Правила мають чітку структуру і поділяються на обов'язкові правила, керівні настанови, елементи ефективної програми корпоративного комплаєнсу та глосарій термінів. Правила містять зобов'язання щодо недопущення активного і пасивного хабарництва, уникнення конфлікту інтересів, сприяння прозорості, а також передбачають заходи щодо запобігання реталіації проти викривачів. Керівні настанови розроблені як практичні рекомендації для компаній, що не мають усталених практик боротьби з корупцією, та слугують дорожньою картою для імплементації ефективних заходів на всіх рівнях. Окремо описано, як має функціонувати внутрішня комплаєнс-система: визначення відповідальної особи, навчання персоналу, внутрішній аудит, канали повідомлень про порушення та механізми внутрішніх розслідувань. Визначення термінів у глосарії (наприклад, «корупція», «комерційне хабарництво», «викривач», «посередник» тощо) забезпечують уніфікованість розуміння положень та сприяють гармонізації з національним і міжнародним правом.

Ключовою особливістю документа є його гнучкість і універсальність. Він може бути інтегрований як у великі транснаціональні договори, так і в стандартні контракти малого та середнього бізнесу, забезпечуючи прозорість у ділових відносинах. ICC наголошує, що запропонована клаузула не замінює вимоги національного законодавства щодо боротьби з корупцією, але може бути використана як доказ доброчесної поведінки сторони в досудових або судових процесах, а також у перевітках з боку наглядових і фінансових органів. У підсумку, ICC Anti-corruption Clause 2025 року слугує ефективним

Висновки:

- **Універсальність і гнучкість формулювання:** Три опції антикорупційної клаузули дають змогу адаптувати документ до потреб сторін — від стандартного посилання до глибокої інтеграції механізмів комплаєнсу.
- **Підвищення юридичної безпеки:** ICC Clause знижує ризики недобросовісної поведінки та покращує можливості захисту інтересів у разі порушення антикорупційних зобов'язань.
- **Сумісність із внутрішніми політиками:** Третій варіант дозволяє прив'язати клаузулу до власної програми комплаєнсу компанії, що особливо корисно для великих корпоративних структур.
- **Практична цінність ICC Rules 2023 як методології:** Включені правила і глосарій можуть використовуватись як базис для розробки локальних політик у сфері протидії корупції в компаніях.

інструментом для інтеграції міжнародних антикорупційних стандартів у договірну практику та корпоративне управління, сприяючи зниженню ризиків, підвищенню довіри між контрагентами та дотриманню принципів належного управління.

Загрози в серці фінансової системи ЄС: підсумки моніторингу ЕВА щодо відмивання коштів та фінансування тероризму ²

Документ є п'ятим регулярним бієнале-висновком Європейського банківського органу (ЕВА), який містить системну оцінку ризиків відмивання коштів та фінансування тероризму (ВК/ФТ) у фінансовому секторі Європейського Союзу за період 2022–2024 років. Висновок підготовлено на основі узагальнення інформації від 52 компетентних органів 29 країн-членів ЄС/ЕЕА, аналітики з платформи EuReCA, а також нагляду в межах механізмів колегіального моніторингу у сфері ПВК/ФТ. ЕВА аналізує не лише актуальні ризики та вразливості, але й те, як фінансові установи та регулятори впроваджують ризик-орієнтований підхід, застосовують технологічні рішення та реагують на нові виклики у сфері ПВК/ФТ.



У звіті зафіксовано, що фінансовий сектор ЄС залишається під впливом дедалі складніших і технологічно просунутих форм зловживань. Найбільш уразливими визначено сектори FinTech та криптоактивів, де відзначено різке зростання кількості учасників, зокрема постачальників послуг у сфері криптовалют (CASPs), і водночас – відсутність належних механізмів перевірки клієнтів (CDD), слабкість внутрішніх контролів, небажання або нездатність дотримуватися вимог реєстрації. У FinTech ЕВА відзначає переважання бізнес-моделей, орієнтованих на швидкий ріст, які часто нехтують належним управлінням ризиками, комплаєнсом і моніторингом транзакцій. Особливо занепокоєння викликають схеми надання послуг під чужим брендом (white-label), агентські структури, використання віртуальних IBAN та інших конструкцій, які ускладнюють ідентифікацію реального надавача послуг.

Важливе місце у висновку посідає аналіз використання технологій – з одного боку, ЕВА спостерігає повільне та недостатньо якісне впровадження RegTech-рішень і штучного інтелекту фінансовими установами, з іншого – виявляє зростаюче застосування AI злочинцями, зокрема для створення підроблених документів, ідентифікації за допомогою дипфейків, маскування походження активів і обходу контролів. Більшість фінансових установ покладається на типові RegTech-продукти, які не налаштовуються з урахуванням особливостей бізнесу, не тестуються перед впровадженням, а процеси управління ризиками делегуються зовнішнім провайдерам без належного аудиту.

Ще одним критичним аспектом є санкційний комплаєнс. Звіт вказує на високі ризики пов'язані з обходом санкцій, особливо через SEPA Instant і карткові платформи, які мають прогалини в обміні інформацією та скринінгу контрагентів. Деякі установи не забезпечують достатньо ефективний механізм виявлення санкційних осіб або транзакцій у реальному часі, що створює вразливість у загальній системі захисту ЄС від фінансування тероризму, а також від схем, пов'язаних із обходом санкцій щодо держав, що ведуть агресивну політику або розробляють ЗМЗ.

ЕВА також висвітлює проблематику недостатнього управління ризиками щодо політично значущих осіб (PER), транскордонних корпоративних структур, використання трастів і офшорних юрисдикцій. Зокрема, відзначається, що FinTech та криптовалютні сервіси дедалі частіше

² <https://www.eba.europa.eu/sites/default/files/2025-07/13ae2f94-dc04-4a50-9f24-af2808e78944/Opinion%20and%20Report%20on%20ML%20TF%20risks.pdf>

використовуються для переміщення незаконних коштів, пов'язаних із корупцією або непрозорими потоками капіталу.

Окрему увагу приділено загрозам, пов'язаним із використанням стейблкоїнів у схемах фінансування тероризму. Хоча загальний рівень ризику ФТ в ЄС оцінюється як стабільний, платформи, які дозволяють анонімні перекази за допомогою стейблкоїнів, створюють серйозну загрозу для безпеки. Особливо небезпечними є випадки P2P обміну без KYC, де платформи не володіють інформацією про відправника чи отримувача коштів.

У висновках також зазначено позитивні тенденції, зокрема зниження рівня необґрунтованого відмовлення у наданні послуг, покращення управління ризиками у секторі страхування життя та

Висновки:

- **Криптовалютний сектор та FinTech мають стати пріоритетними напрямками регуляторної уваги.** ЕВА рекомендує впроваджувати нагляд заздалегідь, посилювати вимоги до корпоративного управління, CDD та внутрішнього контролю, проводити глибші перевірки нових CASPs.
- **Регулятори мають надавати орієнтири щодо безпечного впровадження RegTech і AI.** Необхідна методологія для тестування RegTech-рішень, реєстри надійних провайдерів, інструменти оцінки ризиків при автоматизації функцій ПВК.
- **Потрібна гармонізація санкційного комплаєнсу в інфраструктурах платежів.** Особливо у SEPA Instant та карткових мережах — через ризики обходу санкцій з боку держав, які підтримують війну чи ядерні програми.
- **Боротьба з використанням анонімних юридичних осіб потребує активного міжвідомчого обміну.** Посилення вимог до бенефіціарної прозорості, зобов'язання верифікувати інформацію в реєстрах компаній, особливо в межах «платформи довіри».

інвестиційних фондів, а також більш глибоке включення податкових злочинів до національних оцінок ризиків. Проте ці успіхи залишаються частковими та не компенсують зростання нових і складних ризиків, які потребують системного та проактивного реагування з боку фінансових установ і регуляторів.

Загалом, висновок ЕВА 2025 року є попередженням щодо необхідності трансформації регуляторного підходу: від реагування на відомі загрози — до передбачення нових векторів ризику, від фрагментарного впровадження комплаєнс-рішень — до комплексного управління ризиками ПВК/ФТ, включаючи санкційний та кіберкомпонент. Документ закликає фінансові установи, наглядові органи та уряди країн ЄС активізувати співпрацю, гармонізувати

станданти, удосконалювати технології контролю та адаптувати національні політики до стрімко змінюваного ландшафту фінансових злочинів.

Пакт доброчесності як інструмент колективної дії: нова модель прозорих публічних закупівель³

Документ підготовлений Transparency International є ґрунтовним аналітичним керівництвом щодо концепції, цілей, структури та практичної реалізації Пакту доброчесності — багатостороннього інструменту колективної дії для забезпечення прозорості, підзвітності та доброчесності у сфері публічних закупівель. У вступі підкреслюється, що публічні закупівлі є критичним елементом управління державними фінансами і стратегічним інструментом досягнення цілей сталого розвитку, однак вони залишаються вразливими до корупції,

³ <https://baselgovernance.org/sites/default/files/2025-02/Global%20Integrity%20Pacts%20Publication%20Dec%2018%202024.pdf>



зловживань та управлінських помилок. Корупційні практики на етапах планування, тендерного оголошення, присудження контрактів та їх реалізації призводять до значних втрат бюджетних коштів (до 30% вартості контрактів) і підривають довіру до державних інститутів. Для усунення цих ризиків, Transparency International просуває ідею колективної дії, що базується на тристоронній взаємодії державних органів, приватного сектору та громадянського суспільства.

Пакт доброчесності, як флагманський інструмент такої взаємодії, є публічним зобов'язанням між державним замовником і потенційними постачальниками щодо утримання від корупції, надання повної прозорості процедур та забезпечення зовнішнього громадського моніторингу. Документ визначає Пакт доброчесності як гнучкий, але структурований підхід, що включає не лише декларативну

частину, а й низку практичних компонентів: публічну обіцянку доброчесності з боку замовника, корпоративне зобов'язання постачальника, згода з громадським контролем, механізми вирішення спорів, санкції та стимули. Важливим акцентом є надання громадській організації права на доступ до всієї інформації щодо тендеру, участь у контролі процедур, фіксацію та повідомлення про порушення, а також — активну комунікацію з громадськістю і залученими спільнотами.

Документ детально описує етапи реалізації Пакту доброчесності: ініціювання (визначення проєктів, обґрунтування ризиків, бюджетування), підготовка та підписання (розробка зобов'язань, правові механізми, інструменти забезпечення виконання), а також виконання (моніторинг, технічна допомога, комунікації, оцінка впливу). Окрему увагу приділено критеріям вибору закупівель, до яких застосовується Пакт доброчесності: стратегічна значущість, висока вартість, значущість для громадськості, підвищений ризик корупції, недостатність існуючих механізмів контролю. Запропоновано три моделі впровадження Пакту доброчесності: одноразова — для пілотних проєктів; системна — для секторальних або програмних підходів; міждержавна — для програм міжнародних фінансових інституцій або донорів. У документі наведено приклади успішних Пактів доброчесності з Мексики, Індії, Італії, Колумбії, Південної Кореї, Румунії, Іспанії, Угорщини, Руанди та інших

Висновки:

- **Пакт доброчесності — ефективний інструмент колективної дії у закупівлях**, що поєднує державу, бізнес і громадянське суспільство навколо спільних антикорупційних цілей. Його сила — в зовнішньому громадському моніторингу та добровільних зобов'язаннях сторін.
- **Пакт доброчесності має найбільшу ефективність у сферах високої стратегічної, фінансової та соціальної значущості**, де існує підвищений ризик корупції або неефективного управління. Важливо застосовувати Пакт доброчесності як частину загальної стратегії управління ризиками в закупівлях.
- **Успішна реалізація Пакту доброчесності залежить від наявності незалежного та професійного громадського моніторингу, політичної волі та належного фінансування**. Забезпечення прозорості фінансування — ключ до довіри та ефективності ініціативи.
- **Пакт доброчесності потребує правового визнання та інституціоналізації для системного ефекту**. Країни, які законодавчо передбачили механізми впровадження Пакту доброчесності (Мексика, Італія, Індія, Пакистан), продемонстрували вищий рівень стійкості антикорупційних результатів.

країн, що демонструють гнучкість механізму та його адаптацію до різних політичних і регуляторних середовищ.

Автори підкреслюють, що Пакт доброчесності не має замінювати законодавство чи дублювати наглядові функції, але повинен посилювати дію правових норм, створювати додатковий захисний шар і підвищувати якість реалізації проєктів через прозорість і участь громадськості. З огляду на значний досвід реалізації Пакту доброчесності, у документі запропоновано оновлену методологію — своєрідний «блакитний план» (blueprint) — що узагальнює уроки, виклики та кращі практики, водночас забезпечуючи достатню гнучкість для адаптації до місцевого контексту. Зокрема, підкреслено, що Пакт доброчесності ефективно працює за умов: наявності політичної волі, спроможності громадянського суспільства, прозорого фінансування, згоди замовника на незалежний моніторинг, а також технічної підтримки з боку міжнародних партнерів або донорів.

У підсумку, Пакт доброчесності позиціонується як універсальний механізм підвищення якості публічних закупівель, який дозволяє не лише мінімізувати корупцію, але й покращити ринкову конкуренцію, підвищити підзвітність державних установ, сформувати нову культуру корпоративної доброчесності та забезпечити реальне залучення громадськості до процесів, що безпосередньо впливають на якість життя людей.

Золото і найманці: Як росія через ПВК "Вагнер" посилює вплив в Африці ⁴

Документ, підготовлений Transparency International, є всебічним дослідженням діяльності приватної військової компанії (ПВК) "Вагнер" у трьох африканських країнах — Центральноафриканській Республіці (ЦАР), Судані та Малі — з акцентом на їхню роль у видобутку природних ресурсів, таких як золото, алмази та деревина, а також на зв'язки з місцевими елітами, корупційні схеми та обхід міжнародних санкцій. Після смерті Євгена Пригожина у серпні 2023 року активи "Вагнера" в Африці перейшли під контроль Міністерства оборони росії та Головного розвідувального управління (ГРУ), а сама організація була реорганізована у так званий "Африканський корпус". Звіт також детально аналізує роль Об'єднаних Арабських Еміратів (ОАЕ) як ключового хабу для торгівлі золотом, видобутим під контролем російських структур, і коротко описує невдачу спробу росії вплинути на внутрішню політику Мадагаскару через політичні та медійні маніпуляції.



Дослідження базується на англо- та франкомовних публікаціях, інтерв'ю з експертами (анонімними з міркувань безпеки), а також відкритих даних, таких як торговельні записи та реєстри компаній. Звіт підкреслює систематичне використання насильства, корупції та політичного маніпулювання для забезпечення економічних інтересів росії в Африці, а також висвітлює, як золото стало ключовим інструментом для обходу санкцій через його легкість у приховуванні від міжнародних регуляторів.

У Центральноафриканській Республіці "Вагнер" досяг найбільшого успіху в реалізації російської стратегії "захист режимів в обмін на ресурси". З 2017 року, після відходу французьких військ, найманці надають військову підтримку режиму президента Фостена-Аркажа Туадери,

⁴ <https://ti-russia.org/en/wp-content/uploads/sites/2/2025/06/gold-and-crossbows-%E2%80%93-ti-russias-report-on-wagner.pdf>

спочатку виступаючи як інструктори, а до 2021 року ставши ключовою силою у боротьбі з повстанцями, зокрема Коаліцією патріотів за зміни (CPC). Вони контролюють значну частину армії ЦАР, допомагаючи відновити контроль над територіями, охопленими громадянською війною з 2012 року.

В обмін на військову підтримку "Вагнер" отримав доступ до золотих і алмазних родовищ, зокрема шахти Ндассіма, яка генерує близько 209 мільйонів доларів США щорічно та має запаси золота вартістю понад 1 мільярд доларів. Компанії, пов'язані з Пригожиним, такі як Midas Resources SARLU, Lobaye Invest SARLU і Diamville SAU, контролюють видобуток і експорт золота та алмазів, часто застосовуючи насильство для захоплення дрібних копалень. Логістичні ланцюги включають порт Дуала в Камеруні, через який експортуються ресурси, а також імпортується обладнання.

Звіт фіксує численні воєнні злочини, включаючи вбивства понад 900 цивільних осіб з грудня 2020 по березень 2024 року, сексуальне насильство та пограбування, зокрема задокументовано масові розправи над мігрантами-фермерами та напади на шахтарів. Після смерті Пригожина контроль над активами "Вагнера" перейшов до російських державних структур, а ключові особи, такі як Дмитро Ситий, продовжують керувати операціями, включаючи медіа-кампанії та культурний вплив через "російський дім" у Бангі, який організовує театральні вистави, кіносеанси та освітні програми для зміцнення іміджу росії як захисника.

У Судані "Вагнер" демонструє гнучкість, адаптуючись до політичної нестабільності. росія почала співпрацю з Суданом за правління Омара аль-Башира, постачаючи зброю в обхід ембарго ООН, зокрема гелікоптери Мі-24 і літаки Су-30, які використовувалися у конфлікті в Дарфурі. Після повалення аль-Башира у 2019 році найманці встановили зв'язки як з урядовими силами, так і з Силами швидкого реагування (RSF) під командуванням Мохамеда Хамдана Дагало ("Хемедті"), які контролюють значну частину золотовидобутку.

Компанія Meroe Gold Co. Ltd., пов'язана з Пригожиним, отримала контроль над золотими копальнями, зокрема поблизу міста Ель-Обейд, і стала одним із головних гравців на суданському ринку золота, експортуючи ресурси вартістю близько 1 мільярда доларів у 2021 році. російські найманці забезпечують логістику та постачання зброї для RSF в обмін на доступ до золота, одночасно підтримуючи офіційний уряд Судану через пропозиції гуманітарної допомоги та переговори про створення військової бази на Червоному морі. Така двоїста політика дозволяє росії зберігати вплив незалежно від результатів громадянської війни, демонструючи прагматичний підхід до конфлікту.

У Малі "Вагнер" зіткнувся з обмеженим успіхом через опір місцевих сил. Після відходу французьких військ у 2021 році найманці стали головним військовим партнером військової хунти, яка захопила владу. Вони намагалися отримати доступ до найбільшого золотого родовища, раніше контролюваного канадською компанією B2Gold, але уряд Малі чинить опір прямому доступу росіян до ресурсів, прагнучи зберегти суверенітет. Незважаючи на це, "Вагнер" домогся контролю над кількома родовищами на півдні країни та сприяв зміні гірничого кодексу, що збільшив частку держави в нових проєктах до 35%. Після смерті Пригожина насильство за участю російських найманців зросло на 81%, зокрема в північних регіонах, багатих на золото, де вони зазнали значних втрат (до 84 осіб) у сутичках із повстанцями поблизу алжирського кордону в липні 2024 року. росія також лобіює націоналізацію золотовидобувних підприємств, таких як родовища біля Лулу-Гунуту, які контролює канадська Barrick Gold, що виробила 19,4 тонни золота у 2022 році.

ОАЕ, зокрема Дубай, відіграють центральну роль у торгівлі золотом, видобутим під контролем російських структур у ЦАР, Судані та Малі. У 2022–2023 роках значна частина золота (41–49% з ЦАР) експортувалася нелегально через посередницькі країни, такі як Камерун і Чад. Згідно з даними FATF, у 2022 році 66,5% африканського золота, імпортованого до ОАЕ (405 тонн), було

контрабандним, що становить 115,3 мільярда доларів США за середньою ціною золота за останні 11 років. Незважаючи на вихід ОАЕ з "сірого списку" FATF у 2024 році, країна залишається вразливою до схем ухилення від санкцій, що дозволяє Росії фінансувати свої операції, включаючи війну в Україні.

Висновки:

- **Посилення міжнародного моніторингу торгівлі золотом через ОАЕ:** ОАЕ залишаються головним хабом для контрабанди африканського золота, що дозволяє Росії обходити санкції. Міжнародним організаціям, зокрема FATF, слід посилити контроль за фінансовими потоками в Дубаї, запровадивши жорсткіші перевірки походження золота та санкції проти компаній, пов'язаних із російськими структурами.
- **Підтримка місцевих інституцій у ЦАР, Судані та Малі:** Для протидії впливу російських найманців необхідно зміцнювати громадянські інституції в цих країнах. Міжнародні донори повинні надавати підтримку антикорупційним ініціативам, прозорості видобутку ресурсів і захисту прав людини, щоб зменшити залежність місцевих урядів від російської військової допомоги.
- **Санкції проти ключових фігур і компаній:** Слід розширити санкції на осіб, таких як Дмитро Ситий і компанії, як-от Midas Resources, Lobaye Invest і Meroe Gold, які контролюють видобуток і експорт ресурсів. Це обмежить фінансові потоки, що підтримують російські операції в Африці та війну в Україні.
- **Міжнародний тиск на режими, залежні від Росії:** Міжнародна спільнота має чинити тиск на уряди ЦАР і Малі, щоб зменшити їхню залежність від російських найманців. Це може включати пропозиції альтернативної військової та економічної підтримки, а також програми для захисту місцевих громад від насильства з боку найманців.

Звіт також зазначає, що ЦАР експортує до ОАЕ не лише золото, а й алмази високої якості, хоча їхній експорт був заборонений до 2024 року відповідно до Кімберлійського процесу через тривалий збройний конфлікт.

На Мадагаскарі "Вагнер" використовував політичних стратегів і медіа-ресурси замість військової присутності. У 2018 році російські консультанти підтримували президентські кампанії, спочатку Хері Раджаонарімампіаніні, а потім Андрі Раджоеліні, який переміг. Росія намагалася отримати доступ до видобутку хромі через компанію Ferrum Mining, але проєкт зазнав невдачі через страйки працівників і борги державної компанії Kraoma. На відміну від ЦАР, Судану та Малі, у Мадагаскарі не було внутрішніх збройних конфліктів, а присутність найманців обмежувалася захистом російських геологів і стратегів.

Загалом звіт підкреслює, що російські найманці є невід'ємною частиною стратегії Росії для зміцнення впливу в Африці, діючи за моделлю "захист режимів в обмін на ресурси". Найбільш успішно ця модель реалізована в ЦАР, де Росія поєднує військовий, економічний і культурний вплив. У Судані Росія демонструє гнучкість, підтримуючи

різні сторони конфлікту, тоді як у Малі стикається з опором місцевих сил. Після смерті Пригожина контроль над "Вагнером" перейшов до російської держави, що свідчить про інституціоналізацію впливу Росії в Африці, а золото залишається ключовим інструментом для обходу санкцій через торгівлю з ОАЕ.

Регулювання

Підвищення суми порогових операцій у Сполученому Королівстві⁵



legislation.gov.uk

Указ про доходи від злочинної діяльності (відмивання грошей) (порогова сума) (поправка) 2025 року, прийнятий 10 липня 2025 року та введений в дію 31 липня

2025 року, вносить значні зміни до Закону про доходи від злочинної діяльності 2002 року (РОСА). Цей документ поширюється на Англію та Уельс, Шотландію та Північну Ірландію. Основна мета Указу – збільшити фінансові порогові суми з 1 000 фунтів стерлінгів до 3 000 фунтів стерлінгів для двох винятків, які стосуються основних злочинів з відмивання коштів, визначених у розділах 327-329 Закону РОСА. Ці зміни спрямовані на перерозподіл обмежених ресурсів від низьковартісних операцій до розслідувань більшої вартості та підвищення ефективності режиму звітування про підозрілу діяльність. Проект цього інструменту був поданий до Парламенту та схвалений резолюцією кожної палати Парламенту.

Перший виняток, який зазнає змін, стосується порогової суми, зазначеної у розділі 339A(2) РОСА. Він застосовується до діяльності, пов'язаної з операціями по рахунку, таких як оплата витрат, які здійснюються установами, що приймають депозити (по суті, банки та будівельні товариства), а також установами електронних грошей та платіжними установами. Згідно з новими правилами, ці фінансові установи можуть проводити транзакції нижче 3 000 фунтів стерлінгів для клієнта, без вчинення злочинів з відмивання коштів, передбачених розділами 327-329 РОСА. Тобто, якщо ці кошти (сумою до 3 000 фунтів стерлінгів) були злочинного походження, а установа не подала SAR/STR, то по відношенню до установи це не буде вважатися злочином ВК. Раніше цей поріг був підвищений з 250 до 1 000 фунтів стерлінгів Указом про доходи від злочинної діяльності (відмивання грошей) (порогова сума) 2022 року.

Другий виняток стосується порогової суми у розділі 339A(6A) РОСА. Він застосовується до випадків, коли суб'єкт господарювання, що здійснює діяльність у регульованому секторі (як визначено у Частині 1 Додатку 9 до РОСА), припиняє ділові відносини з клієнтом та повертає гроші чи інше майно клієнту. Новий поріг у 3 000 фунтів стерлінгів означає, що для транзакцій нижче цієї суми суб'єктам господарювання у секторі, що регулюється, не потрібно подавати SAR щодо захисту від відмивання коштів (DAML SARs).

Ці зміни відображають стратегічне рішення переорієнтувати ресурси правоохоронних органів на розслідування більш значних випадків відмивання коштів, тим самим підвищуючи загальну ефективність системи боротьби з фінансовими злочинами у Сполученому Королівстві.

Звіти окремих інституцій та експертів

Наскільки добре працює система контролю за відмиванням коштів?⁶

Дослідження Мірка Наззарі та Пітера Ройтера, опубліковане в журналі Чиказького Університету, критично оцінює ефективність глобального режиму протидії відмиванню коштів та фінансуванню тероризму. Автори стверджують, що, попри зростаючу складність і вартість цієї системи, немає жодних доказів зменшення обсягів відмивання коштів, або ж того, що цей процес став значно складнішим чи дорожчим. Незважаючи на загальне визнання неефективності системи, майже відсутня дискусія щодо суттєвих реформ.

⁵ <https://www.legislation.gov.uk/ukxi/2025/877/made/data.pdf>

⁶ <https://www.journals.uchicago.edu/doi/full/10.1086/735665>

Mirko Nazzari and Peter Reuter

How Well Does the Money Laundering Control System Work?

ABSTRACT

The continued globalization of finances has generated an ever-larger array of methods for making criminal earnings appear legitimate. The global regime to control money laundering has become more sophisticated and comprehensive, (i.e., expensive and intrusive). There is no evidence that money laundering is declining or becoming more difficult or expensive. The system's failure has many sources. Nations which pushed for its creation and development have been unwilling to implement critical elements. Major banks have repeatedly failed to meet their obligations, suggesting either insufficient commitment or a lack of the necessary skills and systems to comply. Regulatory oversight has been inadequate. There is, however, evidence that the system's self-enforcement of laws against criminal enterprises. Despite the consensus that the system works poorly, there is almost no discussion of substantial reforms.

Money laundering is the process aimed at disguising the origin of the proceeds of serious crimes, typically referred to as predicate offenses.¹ It is a

Mirko Nazzari is a postdoctoral research fellow in Political Science at University College London, UCL, and a Visiting Professor at the School of Public Policy and Government, University of Maryland. We thank Martin Schumacher, Mike Lee, Jason Shannon, and Mark Turkington for helpful comments on an early draft.

¹ Predicate offenses typically encompass all serious crimes defined by a country's national laws. These offenses are generally those punishable by a minimum penalty exceeding one year of imprisonment, in legal systems with a minimum threshold for penalties.

Internationally published July 1, 2005.

Crime and Justice, volume 19, 2005.

© 2005 The Authors. Journal compilation © 2005 Blackwell Publishing Ltd. This article is a U.S. Government work and, as such, is in the public domain in the United States of America.

DOI: 10.1002/cj.10000

000

Документ починається з визначення відмивання коштів як процесу маскування походження доходів від серйозних злочинів, відомих як "предикатні злочини". Зазначається, що ПВК-режим є ключовим прикладом "безпекового врядування", що здійснюється як державними, так і приватними суб'єктами. На відміну від традиційного правоохоронного підходу, цей режим перекладає значну частину функцій виявлення та розслідування на приватний сектор, зокрема на "підзвітні суб'єкти", такі як банки та страхові компанії. Однак, така делегація створює конфлікт інтересів, оскільки ці суб'єкти повинні одночасно захищати свої прибутки та виконувати роль у сфері громадської безпеки.

Незважаючи на високу стурбованість щодо відмивання коштів, яка мотивувала широку законодавчу та регуляторну реакцію,

дослідження показує відсутність консенсусу щодо ефективності системи ПВК. Багато заяв про "успіх" з боку міжнародних та національних органів не підтверджуються емпіричними даними і часто суперечать численним скандалам у фінансовому секторі, як, наприклад, неспроможність TD Bank відстежити транзакції на суму 18,3 трильйона доларів протягом десяти років. В цілому, дослідники вказують на обмежену ефективність глобального режиму в запобіганні серйозним злочинам, його потенційні ненавмисні наслідки та значні витрати, які він накладає на підзвітні суб'єкти та приватних осіб.

Серед ключових висновків дослідження: великі західні банки часто сплачують значні штрафи за порушення ПВК, але керівники банків рідко притягуються до кримінальної відповідальності. Відмивання коштів сьогодні не є складнішим чи дорожчим, ніж у 1989 році, коли була заснована FATF. Емпіричні дослідження послідовно показують, що більшість схем відмивання коштів є напрочуд простими. Рамки ПВК непропорційно вигідні багатшим країнам, які, ймовірно, містять більшість відмитих активів. Ініціативи ПВК надають цінну розвідувальну інформацію для розслідувань правоохоронних органів. Проте ці зусилля також несуть ризики, включаючи "деризкінг" (відмову банків від обслуговування певних категорій клієнтів, які вважаються занадто ризикованими) та потенційне неправомірне використання фінансових даних. Витрати на систему ПВК рідко обговорюються урядами або іншими зацікавленими сторонами.

Система ПВК передбачає трьохрівневу ієрархію: підзвітні суб'єкти (банки, страхові компанії), підрозділи фінансової розвідки (ПФР) та правоохоронні органи. Підзвітні суб'єкти відіграють центральну роль як "гейткіпери" фінансової системи, зобов'язані здійснювати належну перевірку клієнтів (KYC/CDD) та подавати повідомлення про підозрілу діяльність (SAR) до національних ПФР.

Одним з ключових елементів системи FATF є Звіти про взаємну оцінку (MER), які оцінюють технічну відповідність країн рекомендаціям FATF та ефективність національних систем ПВК. Однак MER критикуються за формалізм, зосередженість на процесах, а не на результатах, та ігнорування негативних наслідків ПВК, таких як прямі чи непрямі витрати. Скандали, подібні до справи Danske Bank або Commonwealth Bank of Australia, не були належним чином відображені в MER. Також наголошується на значних відмінностях в оцінках ефективності між розвиненими та країнами, що розвиваються, при цьому останні часто демонструють низьку ефективність за всіма показниками.

Оцінка ефективності політики ПВК є складною через неоднозначність цілей та відсутність якісних даних. Хоча первинна мета ПВК полягала в використанні незаконних грошових потоків для виявлення або запобігання серйозним злочинам, інституційні заяви FATF та МВФ переважно наголошують на захисті цілісності фінансової системи, а не на зменшенні

злочинності як такої. Незважаючи на теоретичні припущення, що посилення заходів ПВК має зробити відмивання коштів дорожчим і складнішим, а також позбавити злочинців капіталу, емпіричні дані про це відсутні.

Аналіз SAR та вироків за відмивання коштів у США показує значне зростання кількості SAR (з понад 50 000 у 1996 році до майже 4 мільйонів у 2023 році), але кількість вироків за відмивання коштів залишалася відносно стабільною, а співвідношення вироків до SAR зменшилося. Це вказує на те, що система стає менш ефективною за цим показником. Висока кількість SAR пояснюється їх багатоцільовим використанням (включаючи шахрайство, кіберзлочинність, інсайдерську торгівлю) та "захисним поданням", коли фінансові установи подають якомога більше звітів, щоб уникнути штрафів за невиявлення. Це призводить до перевантаження ПФР та ускладнює ефективне розслідування.

Однак, SAR виявляються цінними для правоохоронних органів як джерело розвідувальної інформації, що допомагає розширювати поточні розслідування та будувати сильніші справи проти злочинців, навіть якщо вони рідко є початковим тригером розслідувань. Наприклад, дані FinCEN у 2023 фінансовому році були безпосередньо пов'язані з 15,4% активних розслідувань ФБР та 88% розслідувань, відкритих відділом кримінальних розслідувань Служби внутрішніх доходів.

Щодо конфіскації доходів від злочинності, дослідження показує, що її рівень залишається низьким. Оцінки варіюються, але свідчать про конфіскацію менш ніж 2% щорічних доходів від

організованої злочинності. У США, незважаючи на деякі коливання, загальна вартість вилучених активів, пов'язаних з відмиванням коштів, за період 2018-2022 років зменшилася. Основними перешкодами для конфіскації є використання складних інструментів для приховування власності, потреба в широкій міжнародній співпраці та труднощі з прив'язкою активів до підозрюваних.

Висновки:

- **Необхідність переосмислення цілей ПВК/ФТ/ФР:** Система має перейти від переважної концентрації на "цілісності фінансової системи" до чіткішого фокусу на прямому зменшенні предикатних злочинів та ефективній конфіскації незаконних доходів, оскільки поточні показники свідчать про обмежений вплив на зниження злочинності.
- **Реформування структури "підзвітних суб'єктів":** Слід переглянути нинішню модель, що перекладає основний тягар ПВК на фінансові установи, оскільки це призводить до неефективності, "захисних" дій (надмірне подання SAR) та непропорційних витрат. Можливе перенесення деяких функцій, таких як KYC, на централізовані державні органи або впровадження сильніших стимулів для банків, що перевищують просто штрафи.
- **Вирішення проблеми "де-ризикінгу" та забезпечення фінансової інклюзії:** Збільшення витрат та суворість правил ПВК призводять до де-ризикінгу та виключення певних категорій клієнтів, що витісняє фінансові потоки у нерегульовані канали та завдає шкоди вразливим спільнотам. Реформи повинні передбачати диференційований підхід до ризиків та враховувати можливості країн, що розвиваються, а також забезпечувати доступ до базових фінансових послуг.
- **Покращення оцінки ефективності та прозорості даних:** Необхідно розробити надійніші методології оцінки реального впливу заходів з ПВК, що виходять за рамки формальної відповідності. Це включає збір якісних даних про обсяги відмивання коштів, ціни на послуги з відмивання коштів та фактичні результати розслідувань, а також підвищення прозорості використання SAR та інших розвідувальних даних, щоб уникнути їх зловживання.

Система ПВК також стикається з проблемами через неспроможність національних урядів повністю дотримуватися правил FATF. Навіть провідні країни, такі як США, мали значні прогалини у розкритті інформації про бенефіціарних власників. Для країн, що розвиваються, проблема посилюється браком кваліфікованих фахівців та тим, що стандарти FATF розроблені для заможніших націй. Це призводить до непропорційно високих витрат на дотримання вимог та "де-ризкінгу", що створює бар'єри для фінансової інклюзії та може витіснити незаконну діяльність у нерегульовані канали.

Дослідження також розглядає невиконання фінансовими установами вимог ПВК. Багато великих банків сплатили мільярдні штрафи за порушення, але це рідко призводило до кримінального переслідування керівників. Це свідчить про "цинічне" ставлення банків, які розглядають штрафи як прийнятну ціну за бізнес. Відсутність значних змін у поведінці банків після штрафів вказує на те, що ці заходи не є достатньо ефективними для забезпечення довгострокової відповідності.

Витрати системи ПВК величезні, оцінюючись у сотні мільярдів доларів у всьому світі, але серйозних оцінок цих витрат немає. Ці витрати перекладаються на клієнтів через банківські комісії та "де-ризкінг", що непропорційно впливає на маргіналізовані спільноти. Крім того, надмірна залежність від приватних баз даних для перевірки клієнтів викликає занепокоєння щодо їх точності, надійності та безпеки, що може призвести до помилкових ідентифікацій та значних наслідків для фізичних осіб. Також відзначається потенційне неправомірне використання інформації ПВК для цілей спостереження та придушення політичного інакомислення урядами.

Загалом, система ПВК/ФТ/ФР авторами вважається неефективною у скороченні предикатних злочинів або обсягів відмивання коштів, а відсутність широкої дискусії про фундаментальні реформи пояснюється "народною теорією" про переваги для впливових груп (наприклад, бар'єри для нових конкурентів у банківському секторі, інструменти для США проти ворожих країн) та "сакральним" характером боротьби з тероризмом.

Елітна молодь - нова хвиля російських відмивачів ^{7 8 9}

Представлені матеріали висвітлюють кардинальну зміну профілю суб'єктів, задіяних у відмиванні російських грошей та обході санкцій, акцентуючи увагу на "золотій молоді" — високоосвічених, багатомовних, технічно підкованих представників поколінь Z та міленіалів, які є елітою



та відіграють роль посередників в нелегальних фінансових операціях. Ці особи, часто виховані за межами росії та володіючи численним громадянством та паспортами, використовують свою глобальну мобільність та привілеї для дискретного переміщення значних обсягів капіталів. Вони комфортно функціонують у сферах криптовалют, елітної нерухомості та глобальних мереж, що суттєво змінює ландшафт сучасної протидії відмиванню коштів та ухиленню від санкцій. Мотивація цих осіб може виходити не лише з фінансової вигоди, але й з бажання кинути виклик

⁷ <https://www.compliancecorylated.com/news/golden-youth-the-new-face-of-russian-money-laundering-and-sanctions-evasion/>

⁸ <https://www.compliancecorylated.com/news/the-privileged-privately-educated-russian-who-ran-a-cash-to-crypto-mlaas-for-other-wealthy-russians-and-drug-traffickers/>

⁹ <https://www.compliancecorylated.com/news/wealthy-gen-z-russian-laundered-money-in-luxury-properties-claimed-adhd-caused-offending/>

системі. Це нове явище є прямою відповіддю на санкції проти російських банків, демонструючи адаптивність кримінальних мереж у пошуку та використанні "лазівок" для переміщення грошових потоків. Їхні зв'язки з високопоставленими родичами в росії надають їм відчуття безкарності та доступ до значних коштів.

Документи наводять кілька яскравих прикладів таких осіб та мереж. Семен Куксов, син російського нафтового керівника, здобув освіту у Сполученому Королівстві та був засуджений за організацію схеми відмивання готівки через криптовалюту, використовуючи розкішні об'єкти нерухомості в Лондоні як місця для обробки та перерахунку готівки в рамках схеми ВК. Він відігравав керуючу роль у багатомільярдній мережі, пов'язаній з наркоторговцями, хакерськими угрупованнями, шпигунами та організованою злочинною групою Кінахана. Його молодший брат, Олександр Куксов, також був підозрюваним у цій схемі. Операція Семена Кукова, що тривала трохи більше року з липня 2022 по вересень 2023, була відповіддю на санкції, що унеможливили звичні банківські перекази. Андрій Дзекца був ключовим помічником та кур'єром у цій операції. Іншим помітним гравцем є Артем Усс, син підсанкційного колишнього російського губернатора, який розшукується США за ухилення від санкцій, контрабанду нафти

та відмивання десятків мільйонів доларів для російських олігархів, використовуючи криптовалюту, мережу фіктивних компаній та шахраїв. Він навіть зумів втекти з-під домашнього арешту в Італії за допомогою боснійської організованої злочинної групи.

Серед ключових мереж відзначені Smart Group та TGR Group, які були "розкриті" в рамках операції NCA "Destabilise". Катерина Жданова (39 років) очолювала Smart Group і була під санкціями OFAC за допомогу російським олігархам у переміщенні понад 100 мільйонів доларів США до ОАЕ та сприяння в отриманні податкового резидентства, банківських рахунків та ідентифікаційних карт ОАЕ. Микита Краснов був одним з основних операторів Smart Group, співпрацюючи з Куковим у відмиванні коштів. Ці мережі не тільки допомагали обходити санкції, але й, згідно з NCA, фінансували російські шпигунські операції та сприяли незаконним інвестиціям у Сполученому Королівстві.

Методи відмивання коштів, які використовує ця золота молодь, включають широке використання криптовалют як основного

Висновки:

- **Адаптація програм з ПВК/ФТ:** Необхідно терміново оновити підходи до протидії відмиванню коштів, щоб врахувати новий профіль правопорушників – молодих, високоосвічених, глобально мобільних та крипто-орієнтованих осіб. Програми повинні зосередитися на виявленні непрямих зв'язків з елітами та використання цифрових активів.
- **Посилення перевірок росіян:** Для фінансових установ і контролюючих органів критично важливо проводити посилену належну перевірку щодо осіб з росії, які мають декілька громадянств, навчалися за кордоном та/або мають привілейоване походження, для виявлення прихованих зв'язків з підсанкційними суб'єктами або злочинними мережами.
- **Інвестиції в крипто-аналітику та відстеження активів:** З огляду на повсюдне використання криптовалют, розкішної нерухомості та "системи токенів" для відмивання коштів, вкрай необхідно інвестувати в передові інструменти крипто-аналітики та розвивати спроможності з відстеження активів у складних міжнародних структурах, включаючи офшорні компанії та цифрові гаманці.
- **Розширення міжнародної співпраці:** Ефективна боротьба з цими транснаціональними мережами потребує постійного поглиблення міжнародної співпраці між правоохоронними органами та фінансовими розвідками для обміну інформацією, проведення спільних операцій та закриття "лазівок", що виникають внаслідок санкційного тиску.

інструменту переказу. Вони застосовують систему "токенів" для вуличних передач готівки, що миттєво супроводжуються переказом криптовалюти тієї ж вартості, що нагадує хавалу. Також виявлено використання сід-фраз для доступу до крипто рахунків. Для приховування джерел походження коштів та їх переміщення залучаються фіктивні компанії та мережі шахраїв. Розкішна нерухомість слугує не лише місцем проживання, але й місцями для обробки готівки. Значна частина комунікації та координації здійснюється через зашифровані чати в Telegram та WhatsApp, де використовуються кодові імена, що дає правоохоронним органам важливі докази міжнародного масштабу цих операцій.

Розслідування, зокрема "Destabilise" від NCA, демонструють активні дії правоохоронних органів у відповідь на ці загрози. В рамках операції здійснено 84 арешти та вилучено понад 20 мільйонів фунтів стерлінгів готівкою та в криптовалюті. Однак ідентифікація таких осіб є складною через неочевидні зв'язки із підсанкційними елітами. Документи також висвітлюють спроби Семена Куксова використати сімейні статки та медичні висновки (щодо СДУГ, аутизму, пухлини мозку) для пом'якшення вироку, хоча суддя відхилив аргумент про "злочинний ген" СДУГ. Триває процес застосування наказів про запобігання серйозним злочинам (SCPO) щодо таких осіб, що може обмежувати їхню мобільність, спілкування та фінансові операції.

Стейблкоїни як новий стандарт глобальних розрахунків: як токенизовані гроші змінюють фінансову екосистему¹⁰

McKinsey
& Company

Financial Services Practice

The stable door opens: How tokenized cash enables next-gen payments

Stablecoins are transforming payments globally, and tailwinds may cause a material shift across the payments industry in 2025 for which incumbents and disruptors alike must make urgent preparations.

by Merrin Higginson
with Gary Sparrow



July 2025

У липневому звіті McKinsey & Company за 2025 рік під назвою детально розглянуто перспективи, ризики та стратегічні орієнтири для фінансових установ у зв'язку зі зростанням ролі стейблкоїнів у глобальній платіжній екосистемі. Документ фіксує, що 2025 рік може стати переломним моментом для впровадження токенизованих грошових коштів на основі блокчейн-технологій, що здатні радикально змінити традиційні підходи до обробки фінансових транзакцій. Стейблкоїни, як цифрова форма готівки, емітована приватними компаніями, мають низку суттєвих переваг над існуючими платіжними рішеннями: миттєвість, низька вартість транзакцій, прозорість, постійна доступність (24/7/365) та можливість програмування платежів через смарт-контракти. Це дозволяє вирішувати хронічні проблеми традиційної інфраструктури — затримки, високі витрати, обмежену доступність, недостатню фінансову інклюзію та непрозорість процедур.

У звіті проведено порівняльний аналіз між трьома типами токенизованих грошових інструментів: стейблкоїнами, цифровими валютами центральних банків (CBDC) та токенизованими депозитами банків. Хоча всі вони покликані забезпечити швидкі та захищені перекази, саме стейблкоїни наразі демонструють найбільший динамізм з огляду на приватний характер ініціатив, масштаби інновацій, а також швидкість зростання обсягів обігу. Згідно з даними, на кінець I кварталу 2025 року в обігу перебуває близько \$250 млрд стейблкоїнів, і прогнозується, що до 2028 року цей обсяг може перевищити \$2 трлн. Значну частку поточного обігу становлять USDT (Tether) і USDC (Circle), які використовуються як базова ліквідність для торгівлі криптоактивами, розрахунків у капітальних ринках і трансграничних платежів. Водночас частка

¹⁰ <https://www.mckinsey.com/industries/financial-services/our-insights/the-stable-door-opens-how-tokenized-cash-enables-next-gen-payments#/>

стейблкоїн-транзакцій у загальному обсязі глобальних грошових переказів наразі становить менше 1%, однак темпи зростання дозволяють очікувати суттєве розширення впродовж найближчих років.

У звіті окремо підкреслюється, що розширення функціоналу та популярності стейблкоїнів відбувається не лише завдяки технічним перевагам, а й через сукупність економічних, нормативних та геополітичних чинників. Наприклад, нестабільність національних валют у країнах, що розвиваються, стимулює населення до використання доларозалежних цифрових активів як засобу збереження вартості. Крім того, оновлена нормативна база у США (зокрема ухвалення закону GENIUS), Європейському Союзі (регламент MiCA), Сполученому Королівстві та ряді азійських країн створює підґрунтя для легалізації та стандартизації емісії та обігу стейблкоїнів. Розвиток технологій — зокрема багатоступеневих систем захисту ключів, інституційної кастодії, інфраструктури on-chain-аналітики та масштабованих блокчейнів (Solana, Ethereum L2) — також сприяє масовому впровадженню.

Автори документу особливу увагу приділяють загрозам для традиційної банківської моделі. У випадку масового переходу клієнтів на стейблкоїни банки можуть втратити обсяги депозитного фінансування, що підриває класичну модель прибутковості, засновану на кредитуванні та інвестуванні. Водночас стейблкоїни, емітовані приватними компаніями, не забезпечують прав власників на активи у разі банкрутства емітента, а також не мають гарантійного механізму на кшталт державного страхування вкладів, що створює додаткові юридичні ризики. Окремо наголошується на вразливості користувачів до втрати приватних ключів або доступу до гаманців, що може мати незворотні наслідки.

З огляду на динаміку змін, McKinsey закликає фінансові установи вже зараз визначити свою роль у новій парадигмі: створення власного стейблкоїну, участь у консорціумах, використання інфраструктури глобальних емітентів або технологічне партнерство з Web3-компаніями. Запропоновано набір практичних дій: формування команд з цифрових активів, розвиток технічних потужностей, навчання керівного складу, взаємодія з регуляторами та тестування продуктів на ринку. Автори підкреслюють, що очікування клієнтів щодо миттєвих глобальних переказів зростають, а отже фінансові інституції, які не адаптуються до нової екосистеми, можуть втратити конкурентні переваги. Як ознаки зрілості ринку зазначаються: законодавча визначеність, зростання обсягів транзакцій, розвиток інфраструктури зберігання й

Висновки:

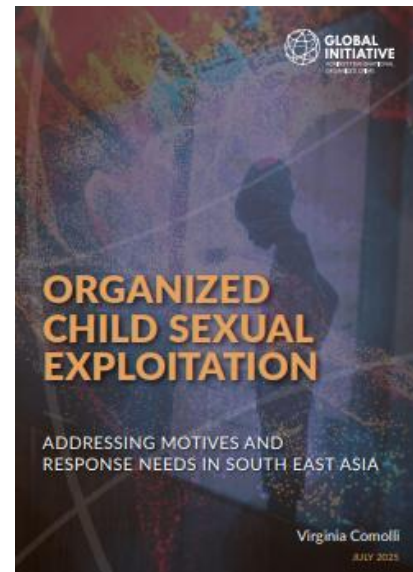
- **2025 рік — критичний момент для фінансових інституцій:** темпи зростання ринку токенизованих грошових коштів вимагають від банків терміново визначити свою стратегію участі — від емісії стейблкоїнів до партнерства з технологічними провайдерами.
- **Стейблкоїни пропонують значну перевагу над традиційними платежами:** майже миттєві розрахунки, низька вартість, автоматичне дотримання регуляторних вимог та відсутність часових/географічних обмежень роблять їх привабливими для широкого спектра користувачів.
- **Використання стейблкоїнів може підірвати традиційну модель банківського депозитного фінансування:** якщо кошти акумулюватимуться в токенах, а не на банківських рахунках, банки втратять джерело ліквідності й прибутковості (кредитування, інвестування в ринки).
- **Нормативна ясність та технологічна зрілість створюють умови для масштабування:** ухвалення законів (наприклад, GENIUS Act у США, MiCA в ЄС) та технологічні досягнення у сфері блокчейнів і кастодіальних рішень роблять інфраструктуру більш надійною й привабливою для загального вжитку.

обміну, поява нових фінансових продуктів на основі токенизованих активів та масштабні інвестиції.

У цілому, звіт аргументовано демонструє, що стейблкоїни з інструментів для нішевого використання у крипторгівлі перетворюються на універсальні засоби цифрової грошової комунікації, що мають потенціал змінити глобальну модель руху вартості, зокрема в транскордонних розрахунках, B2B-платежах, управлінні ліквідністю, державних переказах і програмованих транзакціях. Це створює безпрецедентне вікно можливостей — але також і ризиків — для учасників фінансового ринку.

Організована експлуатація дітей у Південно-Східній Азії: еволюція злочинів, мотиви та стратегії протидії¹¹

Документ підготовлений Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC), є глибоким і всебічним аналізом проблеми сексуальної експлуатації та насильства над дітьми (CSEA) та її онлайн-форми (OCSEA) у Південно-Східній Азії. Цей документ детально розглядає трансформацію цих злочинів від індивідуальних актів до складних організованих злочинних мереж, аналізує сучасні підходи до їхнього запобігання та протидії, а також пропонує низку практичних рекомендацій для посилення боротьби з цими злочинами. Основна увага приділяється регіону Південно-Східної Азії, зокрема таким країнам, як Філіппіни, Камбоджа, Таїланд і Сінгапур, які через економічну вразливість, слабкі правові системи та швидкий розвиток цифрових технологій стали гарячими точками для CSEA та OCSEA.



Документ розпочинається з окреслення масштабів проблеми.

Сексуальна експлуатація та насильство над дітьми охоплюють широкий спектр злочинів, включаючи фізичне насильство, сексуальну експлуатацію в контексті туризму, виробництво та поширення матеріалів із сексуальним насильством над дітьми (CSAM), а також сексторшн — шантаж із використанням компрометуючих матеріалів. Ці злочини спрямовані проти дітей різного віку та соціального походження, а їхні виконавці можуть діяти як самостійно, так і в складі міжнародних мереж. Особлива увага приділяється тому, як Південно-Східна Азія стала центром таких злочинів через поєднання бідності, зростання доступу до інтернету та попиту з боку іноземних клієнтів. Наприклад, Філіппіни відомі як міжнародний центр для прямих трансляцій сексуального насильства над дітьми, де зловмисники з-за кордону платять за організацію та перегляд таких актів у реальному часі.

Одним із ключових аспектів документа є аналіз еволюції мотивів і методів CSEA/OCSEA. Починаючи з початку 2000-х років, ці злочини зазнали значних змін завдяки технологічному прогресу. Розвиток зашифрованих комунікацій, анонімних платіжних систем і криптовалют дозволив злочинцям діяти більш організовано та масштабно. Якщо раніше CSEA переважно мотивувалася сексуальною насолодою окремих осіб, таких як педофіли, які обмінювалися CSAM, то нині дедалі частіше ці злочини здійснюються заради фінансової вигоди. Організовані злочинні групи, які можуть не мати прямого інтересу до сексуального насильства, використовують дітей для створення та продажу CSAM, організації прямих трансляцій або сексторшну. Наприклад, документ наводить випадок у Філіппінах, де п'ятьох дітей змушували

¹¹ <https://globalinitiative.net/wp-content/uploads/2025/07/Virginia-Comolli-Organized-child-sexual-exploitation-Addressing-motives-and-response-needs-in-South-East-Asia-GI-TOC-July-2025.pdf>

знімати порнографічні відео для продажу через онлайн-платформи, а також випадки сексторшну, спрямовані переважно проти підлітків-хлопців.

Документ аргументує, що CSEA/OCSEA усе частіше набуває рис організованої злочинності. Це проявляється у високому рівні координації, використанні складних технологій, таких як темна мережа (darknet), шифрування та криптовалюти, а також у транснаціональному характері злочинних мереж. Наприклад, операція INTERPOL у 2022 році в Сінгапурі та Гонконзі викрила сексторшн-синдикат, який використовував мобільні додатки для збору інтимних матеріалів і шантажу жертв на десятки тисяч доларів. Інший приклад — операція Endeavour, проведена правоохоронними органами Австралії, Сполученого Королівства та США, яка виявила групу на Філіппінах, що транслювала відео сексуального насильства над дітьми. Крім того, з'явилися нові методи, такі як пірамідоподібні сайти-запрошення (ICAP), які використовують вірусні маркетингові схеми для поширення CSAM, залучаючи користувачів до злочинних мереж через стимули, такі як доступ до більш «серйозного» контенту.

Сучасні підходи до протидії CSEA/OCSEA у Південно-Східній Азії включають законодавчі, правоохоронні та суспільні ініціативи. Усі країни регіону криміналізували виробництво, поширення та зберігання CSAM, а деякі, як-от Філіппіни та Малайзія, оновили закони для охоплення онлайну та прямих трансляцій. Наприклад, Малайзія прийняла Закон про сексуальні злочини проти дітей 2017 року, а Філіппіни використовують закони 2009 і 2012 років для боротьби з онлайн-злочинами. Спеціалізовані підрозділи поліції, такі як Антикіберзлочинна група на Філіппінах або Підрозділ із боротьби з технологічними злочинами у Таїланді, співпрацюють із міжнародними організаціями, такими як INTERPOL і UNICEF, для розслідування цих злочинів. Фінансові регулятори, зокрема Азійсько-Тихоокеанська група з протидії відмиванню грошей, почали включати OCSEA до рекомендацій щодо боротьби з відмиванням грошей, а банки та криптобіржі відстежують підозрілі транзакції. Технологічні компанії, такі як Google і Microsoft, надають інструменти, наприклад PhotoDNA, для виявлення CSAM, а соціальні мережі беруть участь у глобальних ініціативах із захисту дітей.

Висновки:

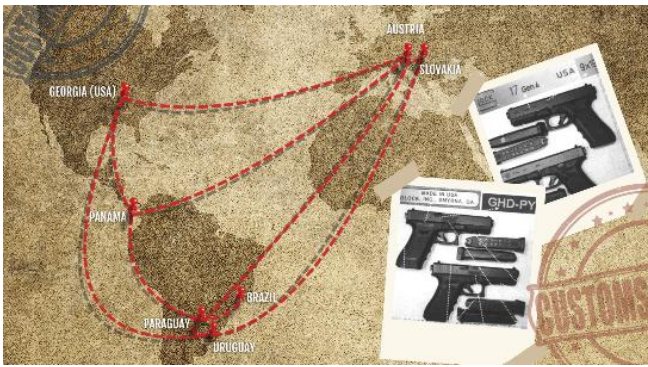
- **Переорієнтація на ідентифікацію злочинців:** Змінити акцент із виявлення жертв на розкриття та ліквідацію злочинних мереж, використовуючи аналіз фінансових транзакцій і цифрових слідів для ідентифікації організаторів.
- **Посилення законодавства та регуляцій:** Уряди країн АСЕАН, зокрема Лаосу, Індонезії та В'єтнаму, повинні запровадити чіткі визначення CSAM і зобов'язати інтернет-провайдерів повідомляти про підозрілий контент.
- **Розвиток публічно-приватного партнерства:** Технологічні компанії та фінансові установи мають створювати формалізовані протоколи співпраці з правоохоронними органами для швидкого реагування на CSAM та пов'язані транзакції.
- **Адаптація фінансових інструментів:** Впровадити локалізовані індикатори відмивання грошей, подібні до тих, що використовуються в Перу, для відстеження фінансових потоків, пов'язаних із CSEA/OCSEA, у країнах Південно-Східної Азії.

Проте документ підкреслює низку викликів. Більшість зусиль зосереджені на ідентифікації жертв, а не на розкритті злочинців і їхніх мереж, що дозволяє останнім продовжувати діяльність. Законодавство в регіоні має прогалини: лише дві з десяти країн АСЕАН вимагають від інтернет-провайдерів повідомляти про підозрілий CSAM, а в Лаосі, Індонезії та В'єтнамі бракує чітких визначень CSAM. Крім того, швидкий розвиток технологій, зокрема штучного інтелекту для створення глибоких фейків,

випереджає можливості правоохоронних органів. Прокуратура часто залежить від свідчень жертв, що ускладнюється через психологічні бар'єри та страх дітей не бути почутими.

Документ пропонує низку рекомендацій для вдосконалення протидії. По-перше, необхідно змістити фокус із ідентифікації жертв на виявлення та ліквідацію злочинних мереж, використовуючи аналіз фінансових транзакцій і цифрових слідів. По-друге, потрібне посилення співпраці між урядами, технологічними компаніями та фінансовими установами для відстеження транзакцій і припинення діяльності мереж. По-третє, документ наголошує на важливості адаптації фінансових інструментів, таких як індикатори відмивання грошей, до місцевих умов, як це було реалізовано в Перу. Нарешті, країни Південно-Східної Азії можуть ділитися своїм досвідом із іншими регіонами, зокрема тихоокеанськими країнами, для запобігання поширенню OCSEA.

Контрабанда зброї, злочинність і вбивство журналіста: кримінальна драма на кордоні Парагваю та Бразилії¹²



Стаття від Forbidden Stories є глибоким розслідуванням, що розкриває складну мережу організованої злочинності, контрабанди зброї та смертельних ризиків, з якими стикаються журналісти, які досліджують ці проблеми в прикордонному регіоні Парагваю та Бразилії, зокрема в місті Педро-Хуан-Кабальєро. Цей регіон, відомий своєю високою злочинністю через географічну близькість до кордону, став

епіцентром діяльності потужних злочинних організацій, таких як Primeiro Comando da Capital (PCC), а також ареною трагічних подій, пов'язаних із убивствами журналістів, які намагалися висвітлити ці незаконні операції.

У центрі розповіді — історія журналіста на ім'я Верса, який працював у Педро-Хуан-Кабальєро та був відомий завдяки своєму блогу Porta de Fuego та співпраці з медіа-платформою Zoot News. Його репортажі вирізнялися сміливістю, сарказмом і безкомпромісним підходом до висвітлення діяльності злочинних угруповань, зокрема торгівлі наркотиками та зброєю. Верса часто першим прибував на місця злочинів, отримував інформацію від джерел і ділився нею з іншими репортерами, що зробило його помітною та впливовою постаттю в регіоні. Проте ця діяльність коштувала йому життя: 12 лютого 2010 року Версу було вбито в його будинку групою найманих убивць, які випустили в нього 12 куль. Згідно з поліцейським звітом, отриманим Forbidden Stories, після вбивства на обличчя журналіста поклали закривавлену тканину — символічний жест, спрямований на залякування інших журналістів і примушення їх до мовчання. Розслідування вказує на причетність до цього вбивства Primeiro Comando da Capital, бразильської злочинної організації, яка має значний вплив у регіоні та зв'язки з місцевими політичними діячами, що забезпечують їй захист і безкарність.

Стаття детально описує механізми контрабанди зброї через кордон між Парагваем і Бразилією, підкреслюючи, як легальні канали імпорту використовуються для постачання зброї злочинним угрупованням. Особлива увага приділяється компанії Global Hawk Defense (GHD), яка з 2016 року почала імпортувати вогнепальну зброю до Парагваю. Зброя, зокрема пістолети Glock, надходила з кількох джерел: США, Австрії, де розташована штаб-квартира Glock, та Словаччини, де компанія має виробничі потужності. До 2013 року, коли Парагвай запровадив заборону на

¹² <https://forbiddenstories.org/guns-smugglers-journalist-murder/>

імпорт вогнепальної зброї, значна частина поставок GHD походила з Європи. Ця заборона, введена Управлінням військових матеріалів Парагваю (Dimabel), мала на меті обмежити незаконний обіг зброї, але виявилася неефективною через системну корупцію та слабкий контроль за виконанням законодавства. Звіт бразильської федеральної поліції за 2017 рік, отриманий Forbidden Stories, вказує на те, що GHD та пов'язана з нею компанія Seguridad Inteligencia y Tecnología Paraguay (SIT Paraguay) могли бути причетними до масштабної торгівлі контрабандною зброєю, яка згодом потрапляла до рук злочинних угруповань, зокрема РСС, у Бразилії.

Ключову роль у цих операціях відіграє Дан Кармі, колишній ізраїльський військовий, який є представником GHD і директором двох інших компаній, що займаються імпортом зброї: SIT Paraguay і DSR. Ці компанії отримали урядові контракти на мільйони доларів, що викликає підозри щодо можливих корупційних схем, які дозволяють легально імпортувати зброю, що згодом потрапляє на чорний ринок. Документ підкреслює, що вплив Кармі та його компаній у регіоні значною мірою зумовлений слабким регулюванням і недостатнім наглядом з боку державних органів, що створює сприятливі умови для незаконної діяльності.

Окрім контрабанди зброї, документ звертає увагу на надзвичайну небезпеку, з якою стикаються журналісти в Педро-Хуан-Кабальєро. З 2010 року в цьому місті було вбито сім журналістів, що робить його одним із найнебезпечніших місць для представників медіа. Робота Верси та його колеги Фігерєдо була пов'язана з постійним ризиком, оскільки вони регулярно отримували погрози через свої розслідування діяльності РСС і контрабанди. Звіт 2017 року, на який посилається Forbidden Stories, підкреслює систематичний характер цих загроз, вказуючи на те, що журналісти, які розкривають злочини організованих угруповань, стають мішенями для залякування та фізичного знищення.

Ще одним важливим аспектом, висвітленим у документі, є неефективність спроб мілітаризації кордону між Парагваем і Бразилією. Посилення військової присутності, спрямоване на боротьбу з контрабандою зброї та наркотиків, не дало очікуваних результатів. Документ зазначає, що глибоко вкорінені системні проблеми, такі як корупція, слабе правозастосування та політичні зв'язки злочинних організацій, перешкоджають ефективній боротьбі зі злочинністю. Замість зменшення контрабандної діяльності мілітаризація лише

Висновки:

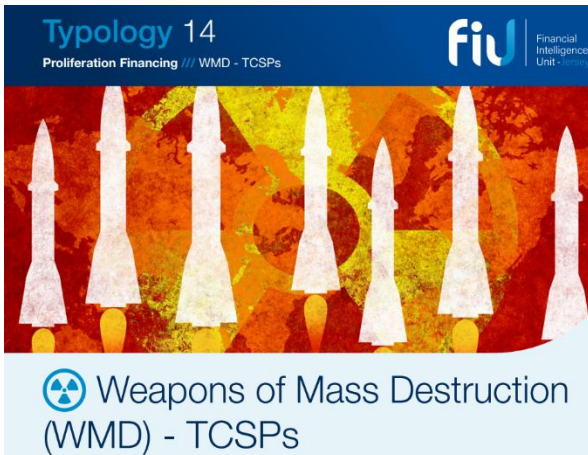
- **Захист журналістів:** Необхідно розробити та впровадити міжнародні програми захисту журналістів, які працюють у небезпечних регіонах. Це може включати створення анонімних каналів для звітування, забезпечення фізичної безпеки та продовження розслідувань загиблих репортерів.
- **Контроль за імпортом зброї:** Уряди Парагваю та Бразилії повинні посилити нагляд за імпортом зброї через компанії на кшталт GHD і SIT Paraguay. Рекомендується провести незалежний аудит урядових контрактів і запровадити суворіші санкції за порушення правил імпорту.
- **Реформа правоохоронних органів:** Для ефективної боротьби з організованою злочинністю, такою як діяльність РСС, необхідно реформувати правоохоронну систему, усунувши корупцію та підвищивши ефективність розслідувань. Міжнародна співпраця з Інтерполом може сприяти відстеженню контрабандних каналів.
- **Перегляд стратегії мілітаризації:** Замість посилення військової присутності слід зосередитися на розвитку розвідувальних мереж і прикордонної співпраці для виявлення контрабандних каналів. Антикорупційні заходи та економічні ініціативи для місцевих громад можуть зменшити залежність від злочинної діяльності.

посилила напруженість у регіоні, не вирішуючи основних причин проблеми.

Forbidden Stories також звертає увагу на ширший контекст, згадуючи інші розслідування, пов'язані з діяльністю злочинних організацій у різних регіонах світу, наприклад, боротьбу з кримінальними мережами на кордоні між Еквадором і Колумбією чи компанії в Киргизстані, які допомагають обходити санкції проти росії. Це підкреслює глобальний характер проблеми організованої злочинності та необхідність міжнародної співпраці для її подолання.

ВНУП

Відсутні зв'язки: фінансування тероризму в Європі, через злочинну діяльність¹³



ПФР Джерсі опублікувало типологію, яка деталізує схему фінансування розповсюдження зброї масового знищення (ЗМЗ) за участю компаній, що надають трастові послуги (ТСРП). Справа стосується Клієнта Х, який народився в Ірані, країні з високим ризиком, пов'язаною з фінансуванням тероризму (ФТ) та фінансуванням розповсюдження (ФР), і проживає в іншій близькосхідній юрисдикції з високим ризиком, пов'язаною з ризиками ФТ. Клієнт Х звернувся до ТСРП на Джерсі для створення дискреційного трасту з метою планування спадщини та відкриття

особистих банківських рахунків у різних валютах для передбачуваних закордонних інвестицій. Клієнт Х мав бізнес-інтереси на Близькому Сході, володіючи Компанією А в Лівані та Компанією В в Об'єднаних Арабських Еміратах (ОАЕ). Обидві компанії займалися торгівлею, включаючи імпорт, експорт та реекспорт товарів, що є сектором, який часто використовується організованими злочинними групами, професійними відмивачами грошей та мережами ФТ/ФР. Компанії А та В продавали дорогі шовкові килими, а також електронне та механічне обладнання. Після відкриття рахунків, банк виявив аномальну діяльність, коли на рахунок Джерсі було переведено 2,5 мільйона доларів США з Лівану (Компанія А) та 3,2 мільйона доларів США з ОАЕ (Компанія В). Транзакції містили посилання на "вартість доставки", "купівлю килимів" та "електронні товари". Банк також виявив численні банківські перекази в Туреччину та Гонконг з подібними посиланнями, часто на одну й ту ж суму в один день, а також придбання дорогих автомобілів на Близькому Сході та платежі третім особам у цих юрисдикціях. Відкриті джерела інформації вказали на зв'язок Клієнта Х із підсанкціонованою особою, Суб'єктом Z, яка була пов'язана з Корпусом вартових ісламської революції Ірану (КВІР) та непрямо причетна до розробки та виробництва ЗМЗ для Ірану.

Показники ризику включали: Клієнт Х є подвійним громадянином Лівану та Ірану (обидві юрисдикції з високим ризиком ФР); транзакції, що стосувалися осіб або організацій у країнах з проблемами розповсюдження; розпливчасті описи товарів та відсутність повної інформації про бенефіціарну власність компаній; відсутність інтернет-присутності компаній; нещодавнє створення компаній під керівництвом директорів в ОАЕ та Лівані. Підозріла діяльність включала: відсутність інформації або посилань щодо переказів, невідповідності та рукописні рахунки-фактури; великі, парні суми банківських переказів з швидким незрозумілим рухом коштів; незвичайна ділова активність, така як транзакції типу "pass-through" в один і той же день; та

¹³ [https://cdn.prod.website-files.com/6464df252c82010a0d5f893f/68668eb9b3eb1c738ca5f9e5_20250521_1081_V1%20Typology14%20-%20PF%20-%20Weapons%20of%20Mass%20Destruction\(x\).pdf](https://cdn.prod.website-files.com/6464df252c82010a0d5f893f/68668eb9b3eb1c738ca5f9e5_20250521_1081_V1%20Typology14%20-%20PF%20-%20Weapons%20of%20Mass%20Destruction(x).pdf)

транзакції, що залучали осіб або компанії в країнах зі слабкими законами або низьким рівнем дотримання експортного контролю.

ПФР Джерсі пріоритетно розглядає випадки, пов'язані з ФР та юрисдикціями з високим ризиком, залучаючи вітчизняні та міжнародні компетентні органи, включаючи інші ПФР та спеціалізовані підрозділи боротьби з тероризмом/ФР, для обміну розвідувальною інформацією та отримання додаткових відомостей. Вони проводять додаткові дослідження за допомогою розвідки з відкритих джерел (OSINT) для перевірки інформації, що підтверджує або спростовує звинувачення, та оцінюють ризики, пов'язані з ФР, виявляючи потенційні порушення, нереалізацію або ухилення від цільових фінансових санкцій.

Наслідки справи включали відмову в наданні згоди на вихід коштів через поточне розслідування. Інформація про транзакції підтвердила повідомлення ЗМІ про зв'язки Клієнта X із підсанкційним Суб'єктом Z, який непрямо причетний до діяльності з розповсюдження від імені Ірану. Виявлені показники надали контекст для транзакцій, проведених Клієнтом X та пов'язаними компаніями та особами, що мали на меті отримання незаконних коштів та їх легалізацію через Джерсі. Фінансовою установою було накладено арешт на рахунки.

ПФР Джерсі наголошує на важливості розрізнення ризиків ФР, ВК та ФТ, незважаючи на схожість показників, щоб чітко ідентифікувати інформацію, пов'язану з ФР, та допомагати підприємствам розуміти їхні вразливості. Установам слід перевіряти особистість та походження клієнтів, розуміти передбачуване використання придбаних/проданих товарів та відстежувати підозрілу активність або невідповідності. Також важливо використовувати індикатори "червоних прапорців" та довідкові матеріали для перевірки товарів подвійного призначення, що може вказувати на потенційне ухилення від експортного контролю та санкцій. Державно-приватні партнерства підтримують ефективні канали зв'язку та обмін розвідувальною інформацією, допомагаючи розуміти та виявляти тенденції та типології, що сприяє підходу, заснованому на ризиках, до відносин з клієнтами. ПФР Джерсі підтримує постійну взаємодію між державним та приватним секторами, включаючи місцеву фінансову розвідувальну мережу Джерсі (JFIN) та участь у тематичних робочих групах, таких як Європейське фінансове розвідувальне державно-приватне партнерство (EFIPPP) під керівництвом Європолу. Мережі ФР є стійкими та адаптованими до тиску санкцій, і після ідентифікації та застосування санкцій компанії можуть зникати та діяти під іншими псевдонімами. Близьке географічне розташування між ОАЕ та Іраном полегшує переміщення товарів, людей та грошей, що може бути використано для незаконної діяльності. Крім того, ОАЕ є значним торговим та транзитним центром, що дозволяє поширювачам приховувати кінцеве

Висновки:

- Необхідно посилити перевірку клієнтів з високоризикових юрисдикцій, особливо тих, що мають ділові інтереси у секторах, схильних до використання для фінансування розповсюдження.
- Фінансові установи повинні активно моніторити транзакції на наявність "червоних прапорців", таких як нечіткі описи товарів, невідповідності в документації, незвичайна швидкість або обсяг транзакцій, та перекази до країн зі слабким експортним контролем, оскільки це може вказувати на спроби ухилення від санкцій та експортного контролю, особливо щодо товарів подвійного призначення.
- Ефективна боротьба з фінансуванням розповсюдження потребує безперервного обміну розвідувальною інформацією та співпраці між державним та приватним секторами на національному та міжнародному рівнях, щоб адаптуватися до постійних та стійких мереж фінансування розповсюдження, які можуть змінювати ідентифікаційні дані для уникнення санкцій.

ідентифікації та застосування санкцій компанії можуть зникати та діяти під іншими псевдонімами. Близьке географічне розташування між ОАЕ та Іраном полегшує переміщення товарів, людей та грошей, що може бути використано для незаконної діяльності. Крім того, ОАЕ є значним торговим та транзитним центром, що дозволяє поширювачам приховувати кінцеве

призначення товарів, які можуть бути використані для незаконних цілей, включаючи предмети, що використовуються в програмах ЗМЗ. КВІР та Міністерство оборони та логістики збройних сил (MODAFI) Ірану, разом з їхніми пов'язаними структурами, перебувають у консолідованих санкційних списках через їхню участь у дослідженнях, розробці та виробництві, включаючи підтримку ракетних та ядерних програм Ірану.

Рекомендовані матеріали

10 ключових принципів для ефективних внутрішніх розслідувань¹⁴



FCPA Compliance and Ethics Report

THE PODCAST ON ALL THINGS COMPLIANCE RELATED

Даний подкаст є епізодом серії FCPA Compliance Report, що публікується на платформі Corporate Compliance Insights — одній із провідних медіа-ініціатив, орієнтованих на фахівців у сфері дотримання комплаєнсу, боротьби з корупцією та корпоративного управління. Це найтриваліший у

світі подкаст із питань комплаєнсу, створений Томом Фоксом, одним із найвідоміших експертів у сфері FCPA та корпоративної етики.

У цьому випуску Фокс проводить глибоке інтерв'ю з адвокаткою Мішель Пірс, співголовою практики white collar crime та урядових розслідувань у юридичній фірмі Hinckley Allen. Основним фокусом обговорення є нещодавно опублікована нею стаття “10 ключових принципів внутрішніх розслідувань”, яка має прикладне значення для будь-якого внутрішнього розслідування — кримінального, цивільного, регуляторного чи корпоративного.

Мішель Пірс окреслює низку критично важливих моментів, які стосуються як змістовного, так і процесуального боку розслідувань. Один із фундаментальних — необхідність чіткого усвідомлення мети розслідування та його потенційної аудиторії. Юристи повинні розуміти, чи це розслідування ініційоване відповідно до закону чи для самозахисту компанії перед регулятором або інвесторами. Це визначає як формат результату (усний брифінг чи письмовий звіт), так і ступінь юридичного захисту розслідування через адвокатську таємницю.

Особливу увагу приділено питанню збереження конфіденційності та захищеності результатів внутрішніх розслідувань. Частою помилкою, яку відзначає Пірс, є надмірна самовпевненість щодо того, що долучення юриста автоматично робить розслідування привілейованим. Вона наголошує на необхідності чітко прописати в листі про залучення (engagement letter), що адвокат надає саме юридичну допомогу, а не просто “збирає факти”. У противному разі в судовому процесі це може бути трактовано як позбавлення привілею конфіденційності.

Також обговорюється дилема між письмовим і усним викладом результатів розслідування. Письмовий звіт може стати незаперечним доказом професіоналізму та прозорості, але водночас потенційним джерелом юридичної вразливості в разі подальших процесів. Пірс радить виходити з цілей: якщо результат має бути переданий широкому колу осіб (регуляторам, громадськості, акціонерам), без письмового документу не обійтися; натомість у внутрішніх ситуаціях із прогнозованими юридичними ризиками доречніше обрати усну форму.

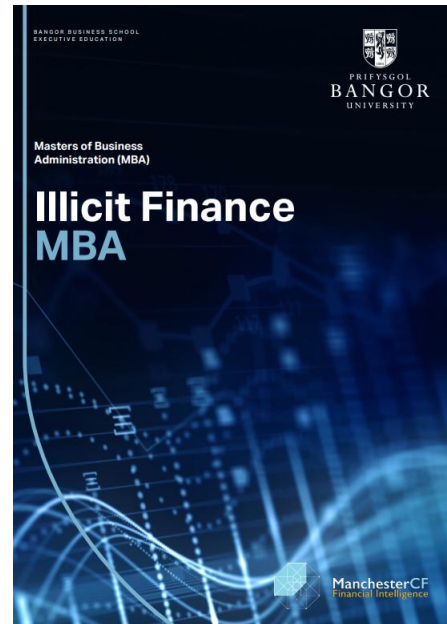
¹⁴ <https://www.corporatecomplianceinsights.com/fcpa-compliance-report/>

Інше суттєве питання — розподіл звіту та ризик втрати адвокатської таємниці. Навіть у межах компанії надмірне або несанкціоноване поширення документа може бути розцінене як відмова від привілею. Пірс радить завжди чітко визначати, хто є клієнтом (наприклад, вся компанія чи тільки комітет аудиту), та забезпечувати, щоб звіт не потрапив до сторонніх осіб без юридичних підстав.

У загальному контексті обговорення особливої ваги набуває тиск із боку регуляторів, особливо Мін'юсту США (DoJ), на швидке розкриття порушень і добровільне повідомлення (self-disclosure). Це ставить внутрішніх слідчих, як Пірс, перед викликом: діяти швидко, але з дотриманням стандартів об'єктивності, належної правової оцінки та формального захисту результатів розслідування. Авторка вказує, що хоча політика DoJ останніми роками заохочує добровільне повідомлення і навіть надає пільги для таких компаній, реальні юридичні наслідки таких кроків усе ще складно передбачити.

Illicit Finance MBA: інноваційна модель підготовки фахівців з фінансової розвідки та безпеки у глобальному контексті¹⁵

Програма Illicit Finance MBA (IFMBA), розроблена Бізнес-школою Бангорського університету у співпраці з ManchesterCF, є спеціалізованою магістерською програмою, яка поєднує академічну підготовку в галузі менеджменту з глибокими знаннями у сфері національної безпеки, фінансової розвідки, протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Ця програма унікальна тим, що випускник отримує не лише ступінь MBA, але й професійне визнання у формі звання фахівця з фінансової розвідки (FIS), що підтверджує його здатність працювати з комплексними фінансовими ризиками на перетині безпеки, права та економіки. IFMBA розроблена для професіоналів, які вже працюють або прагнуть працювати в галузях оборони, безпеки, державного управління, фінансової розвідки чи аналітичних центрів, і орієнтована насамперед на представників країн-партнерів безпекових союзів (зокрема, Five Eyes, Nine Eyes, Fourteen Eyes).



Програма реалізується у форматі дистанційного навчання на неповну зайнятість протягом 24 місяців із використанням платформи Blackboard та навчальних матеріалів ManchesterCF. Такий підхід дозволяє студентам поєднувати професійну діяльність із навчанням, зберігаючи при цьому високу якість освіти. Структура програми включає вісім модулів: чотири спеціалізовані (по 30 академічних кредитів) і чотири управлінські (по 15 кредитів). Фахові модулі охоплюють ключові теми: вступ до фінансових злочинів та комплаєнсу, національні безпекові аспекти фінансових злочинів, людський вимір глобальної фінансової злочинності, а також інституційний підхід до протидії злочинним схемам, включаючи санкції, злочини, пов'язані з довір'ям, торгівлею, корупцією та криптовалютами. Значна увага приділяється фінансуванню тероризму та розповсюдження зброї масового знищення з використанням новітніх фінансових технологій, включно з криптоактивами, а також відкритим джерелам розвідки (OSINT) як інструменту виявлення загроз.

¹⁵ https://www.manchestercf.com/wp-content/uploads/2025/02/20250206-Illicit-Finance-MBA_final-opti.pdf

Менеджерські модулі покликані сформувати в студентів стратегічне мислення, навички управління змінами, ресурсами та людським капіталом, що дозволяє їм діяти ефективно в умовах глобальної невизначеності. Всі модулі передбачають поєднання теоретичної підготовки з практичними завданнями, письмовими роботами (до 5500 слів), онлайн-презентаціями та кейс-аналізами. Оцінювання є комплексним і охоплює як академічний, так і прикладний рівень. Освітня модель також передбачає активну взаємодію студентів і викладачів через форуми, живі та записані лекції, доступ до електронної бібліотеки Bangor та навчального контенту ManchesterCF.

Програма має чітко виражену міждисциплінарну спрямованість та практичну орієнтацію. Вона формує розуміння ролі державних і недержавних інституцій у забезпеченні фінансової безпеки, взаємодії між ними, етичних і правових аспектів діяльності на перетині фінансового сектору та оборонно-безпекової сфери. IFMBA не лише поглиблює знання про методи і механізми протидії злочинному використанню фінансових систем, а й готує слухачів до практичної реалізації стратегій у реальних організаційних контекстах. У такий спосіб програма надає не тільки академічний ступінь, а й підсилює професійну мобільність, готовність до високих посад у державному та приватному секторах і адаптивність до нових безпекових викликів XXI століття.

Інші новини

Санкції як інструмент: Нова мета та старі методи у боротьбі з торгівлею людьми та контрабандою¹⁶



Стаття, опублікована Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC), представляє детальний аналіз ролі санкцій як інструменту для протидії торгівлі людьми та контрабанді мігрантів, з особливим акцентом на недавні ініціативи G7. У

документі зазначається, що ці види злочинів займають центральне місце у політичних дискусіях і багатосторонніх переговорах, спонукаючи світових лідерів шукати нові підходи та стратегії для їхнього вирішення.

У червні 2025 року, під час зустрічі в Кананаскісі, Канада, G7 офіційно підтримала використання санкцій як засобу боротьби з організаторами контрабанди та торгівлі людьми, наголосивши на важливості цільових фінансових і мобільних обмежень для зменшення їхньої діяльності. Цей крок узгоджується з ширшою глобальною тенденцією, започаткованою Сполученим Королівством в січні 2025 року, коли країна оголосила про створення спеціального санкційного режиму, спрямованого на боротьбу з цими злочинами, і закликала інші юрисдикції до аналогічних дій.

Незважаючи на зростаючу підтримку цієї стратегії, автор підкреслює, що реальні випадки застосування санкцій проти контрабандистів і торговців людьми залишаються відносно рідкісними порівняно з їхнім використанням у боротьбі з такими злочинами, як наркоторгівля, корупція чи кіберзлочинність. Наприклад, Сполучені Штати застосували санкції проти 13581 особи, пов'язаної з транснаціональною злочинністю, включаючи громадян Мексики, Гватемали, Пакистану та М'янми. ООН, у свою чергу, ввела обмеження проти зловживань контрабандистами та пов'язаних із ними охоронних структур у Лівії та Малі, тоді як Сполучене Королівство зосередило зусилля на торговцях людьми, пов'язаних із центрами шахрайства в Південно-Східній Азії. Однак брак емпіричних даних ускладнює точну оцінку ефективності таких

¹⁶ <https://globalinitiative.net/analysis/g7-sanctions-migrant-smugglers-human-traffickers/>

заходів, хоча є певні ознаки їхнього впливу на злочинні екосистеми, зокрема в Лівії, де санкції сприяли зменшенню соціальної прийнятності найбільш жорстоких форм контрабанди.

Дослідження GI-TOC пропонує переосмислити традиційні цілі санкцій, стверджуючи, що замість прагнення до повного припинення злочинної діяльності варто зосередитися на стратегічному зриві формування злочинних екосистем. Це передбачає регулярне оновлення списків санкцій для обмеження можливостей організаторів, вплив на оцінку витрат і вигод, а також розкриття прихованих аспектів злочинних ринків, таких як корупційні схеми чи ролі приватного сектору. Автори наголошують, що санкції не є універсальним рішенням і повинні інтегруватися з іншими інструментами, такими як розвиток місцевих правоохоронних структур, підвищення правової спроможності громад і міжнародна координація. Особлива увага приділяється необхідності враховувати всю екосистему злочинів, включаючи приватні компанії, урядових посадовців і соціальні фактори, які сприяють існуванню цих явищ.

Стаття також підкреслює важливість довгострокового підходу до застосування санкцій, визнаючи, що вони не є швидким рішенням, а радше частиною ширшої стратегії, яка потребує часу для реалізації. G7 прогнозує значне зростання використання санкцій у найближчі роки, що вимагає перегляду цілей, стратегій і способів комунікації з урахуванням специфіки кожної країни та її правоохоронних реалій. Нарешті, автори наголошують на критичній ролі прозорої комунікації з громадськістю та політиками, підкреслюючи, що успіх залежить від реальних результатів і правильного управління публічними очікуваннями, що потребує чіткого інформування про довгострокові цілі та досягнення стратегії.

Наркокартелі проти природи: Знищення екосистем в Мексиці¹⁷

Стаття, автором якої є Ендрю-Джеймс Ентоні, студент курсу екологічних досліджень Відкритого університету Великої Британії, висвітлює критичну проблему впливу діяльності наркокартелів на біорізноманіття



Мексика, зокрема на товстодзьобого папу (Rhynchopsitta pachyrhyncha), ендемічний вид, що перебуває під загрозою зникнення. Стаття опублікована на платформі Mongabay, яка спеціалізується на новинах про охорону природи, і зосереджується на екологічних злочинах, таких як незаконна вирубка лісів, спричинена організованою злочинністю, та її наслідках для середовища існування цього виду папуг у регіоні Сьєрра-Мадре-Оксиденталь.

Основна ідея полягає в тому, що діяльність наркокартелів у західній Мексиці, зокрема незаконна вирубка лісів для створення плантацій наркотичних культур, таких як мак чи марихуана, та відмивання грошей через лісозаготівельні операції, призводить до катастрофічної втрати старих соснових лісів, які є єдиним середовищем існування товстодзьобого папу. Цей вид залежить від цих лісів для гніздування та харчування, але масова вирубка лісів, підкріплена пасивністю уряду та слабким правозастосуванням, загрожує його виживанню. Автор посилається на дослідження Гарсія-Хіменеса та Варгаса-Родрігеса (2020), яке підкреслює зв'язок між бездіяльністю уряду, організованою злочинністю та масовою деградацією лісів, що посилює екологічну кризу в регіоні.

Автор також звертає увагу на зусилля зі збереження виду, зокрема на проєкт Джеймса Шеппарда, який використовував супутникові знімки для відстеження міграційних маршрутів папуг. Цей проєкт мав на меті зібрати дані про переміщення виду, щоб краще зрозуміти його потреби у збереженні, але стикався з труднощами через небезпеку роботи в регіонах,

¹⁷ <https://news.mongabay.com/2025/07/how-cartels-destroy-the-last-habitat-of-mexicos-thick-billed-parrot-commentary/>

контрольованих наркокартелями. Дослідники та природоохоронці, які працюють у таких зонах, наражаються на значні ризики, що обмежує можливості для польових досліджень і природоохоронних ініціатив. Крім того, документ підкреслює ширший контекст екологічних злочинів, таких як відмивання грошей через незаконні лісозаготівлі, що ускладнює відстеження та припинення такої діяльності.

Соціально-політичний аспект проблеми полягає в тому, що слабке державне управління та корупція дозволяють наркокартелям діяти безкарно, знищуючи природні ресурси. Це не лише загрожує біорізноманіттю, але й створює бар'єри для місцевих громад і природоохоронців, які намагаються захистити екосистеми.

Загалом, стаття є закликом до дії, спрямована на привернення уваги до взаємозв'язку між організованою злочинністю, екологічною деградацією та втратою біорізноманіття. Автор наголошує на необхідності міжнародної співпраці, посилення правозастосування та залучення місцевих громад до природоохоронних ініціатив, щоб зупинити знищення середовища існування товстодзьобого папуги та інших видів, які страждають від діяльності наркокартелів.

Ваша думка важлива!

1. З огляду на зростаюче використання AI злочинцями та виклики в секторах FinTech та криптоактивів, які конкретні кроки повинні зробити регулятори та фінансові установи для ефективної протидії ВК/ФТ?
2. Розглядаючи питання обмеженої ефективності поточної глобальної системи ПВК/ФТ, які кардинальні реформи є найбільш необхідними для підвищення її ефективності у боротьбі зі злочинністю?
3. Які механізми міжнародної співпраці та обміну розвідувальною інформацією слід посилити, щоб ефективно протидіяти адаптивним мережам з фінансування та розповсюдження ЗМЗ?
4. Яким чином країни, що прагнуть інтегруватися до платіжного простору ЄС (зокрема Україна), повинні адаптувати регулювання у сфері криптоактивів та FinTech, аби забезпечити баланс між інноваціями і контролем у сфері ПВК/ФТ?
5. Які механізми співпраці між правоохоронними органами, технологічними компаніями та фінансовими установами можна запровадити для ефективного відстеження та ліквідації злочинних мереж, що займаються виробництвом і поширенням матеріалів із сексуальним насильством над дітьми?
6. Яким чином пасивність державних інституцій в Україні сприяє екологічним злочинам, таким як незаконна вирубка лісів, і які конкретні кроки можна зробити для посилення правозастосування та захисту природи у небезпечних регіонах?
7. Як Україна може співпрацювати з міжнародними інституціями, для посилення санкцій проти російських структур, що використовуються для контрабанди африканського золота, з метою послаблення економічної бази росії?

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-2025-31

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