Методологічний бюлетень

Серійний номер: МінФін-AML-2026-25

Червень 2026

“Той, хто пересуває гори, починає з того, що відносить маленькі камінці!”

давньокитайська мудрість

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

Деконструкція ончейн-активності стейблкоїнів [1]

Публікація Банку міжнародних розрахунків пропонує концептуальний та емпіричний інструментарій, що змінює спосіб інтерпретації ончейн-активності стейблкоїнів для цілей фінансового моніторингу, макропруденційного нагляду та емпіричних досліджень. Центральна теза дослідження полягає у формальному розмежуванні двох понять, які традиційно ототожнювалися в аналітичній практиці: «транзакція» – як атомарно виконуваний пакет операцій, що може об’єднувати платежі, обмін активів, коригування забезпечення та інші фінансові дії в одну невід’ємну послідовність, – та «трансфер» – як окремий запис у журналі подій смарт-контракту стейблкоїна, що фіксує лише факт зміни володіння токеном. Автори демонструють, що ігнорування цієї структурної відмінності спричиняє системне викривлення оцінки масштабу, характеру та економічної функції платіжної активності у блокчейн-мережах.

Методологічна конструкція дослідження заслуговує окремої уваги з огляду на її верифікованість та відтворюваність – якості, що мають принципове значення для застосування у нагляді за дотриманням вимог ПВК/ФТ. На відміну від переважної більшості попередніх емпіричних робіт, що спираються на пропрієтарні, неперевірювані атрибуції адрес кінцевих користувачів від комерційних постачальників блокчейн-аналітики (Chainalysis, Iknaio, Allium

[1] https://www.bis.org/publ/work1359.pdf

Labs), автори формують класифікацію виключно на основі публічно перевірюваних вхідних даних: стандартизованих криптографічних підписів подій (event signatures) з реєстру 4byte.directory та членства протокольних контрактів, що визначається безпосередньо через запити до ончейн фабрики (onchain factory) контрактів автоматизованих маркет-мейкерів і кредитних протоколів. Дослідницький масив охоплює понад 593 мільйони записів подій, отриманих з 141,3 мільйона транзакцій Ethereum за повний 2025 календарний рік для трьох доларових стейблкоїнів – USDT (Tether), USDC (Circle) та PYUSD (PayPal/Paxos), що забезпечує безпрецедентну за обсягом та повнотою емпіричну базу.

Перший ключовий результат має пряме методологічне значення для аналітиків фінансового моніторингу, які традиційно працюють із даними на рівні трансферів. Авторами встановлено, що на рівні транзакцій 68,4% операцій кваліфікуються як «прості трансфери» (Simple Transfer) – тобто містять рівно один трансферний запис без додаткових подій, тоді як 31,6% транзакцій є структурно складними, поєднуючи в одній атомарній дії від кількох до понад 2000 подій. Однак асиметрія стає критичною на рівні трансферів: оскільки складні транзакції генерують у середньому значно більше трансферних подій кожна, саме на них припадає 59,96% усіх трансферних спостережень у вибірці. Це означає, що аналітик, який випадковим чином вибирає трансферну подію з типового масиву ончейн-да них, із вірогідністю майже 60% отримує спостереження, що походить із композитної фінансової операції, а не зі стандартного двостороннього платежу – інтерпретація кожного трансферу як самостійного платежу системно завищує вимірювані обсяги активності та спотворює оцінки концентрації потоків.

Для деталізації структури складних операцій автори розробляють шестикатегоріальну таксономію економічних дій (Simple Transfer, Multi Transfer, Exchange, Lending, Complex Financial, Other), що формується через зіставлення подій із реєстром із 555 176 верифікованих адрес контрактів протоколу. Обчислювальне навантаження кожної категорії вимірюється через споживання комісії (gas) – стандартизовану, протокольно зумовлену метрику, що, на відміну від кількості подій, не залежить від довільних рішень розробника смарт-контракту. Встановлено монотонне зростання витрат комісії від простих трансферів (медіана 62 248) до композитних фінансових операцій (медіана близько одного мільйона).

Другий ключовий висновок дослідження – відсутність взаємозамінності між трьома проаналізованими стейблкоїнами – має суттєве значення для розробки диференційованих ризик-індикаторів у типологіях ВК/ФТ. USDC і USDT виявляють глибоку структурну вбудованість у децентралізовану фінансову інфраструктуру (з домінуванням Wrapped Ether як активу, який використовується разом з ними, що відображає операції депонування/виведення забезпечення), тяжіння до робочих годин європейського та, у меншій мірі, північноамериканського ринку, а також відносно високу частку складних операцій. PYUSD, навпаки, демонструє виразно периферійну позицію у мережах спів-використання токенів обох інших стейблкоїнів, концентрацію активності в межах робочих годин американського континенту (коефіцієнт Пуассонівської регресії, що відповідає приблизно 110-відсотковому перевищенню інтенсивності платежів у американський робочий час порівняно з європейським) та домінування простих платіжних трансферів. Авторами емпірично доведено, що ці відмінності пояснюються не випадковою варіацією, а інституційними характеристиками емітентів – статусом регульованої довірчої компанії під наглядом Office of the Comptroller of the Currency для PYUSD, багатоюрисдикційним ліцензуванням Circle для USDC та офшорною структурою Tether International (Сальвадор) для USDT.

Аналіз терміновості виконання операцій, проведений через регресійне моделювання плати за пріоритетне виконання (priority fee) у поєднанні з чотирма взаємодоповнюваними специфікаціями (OLS у рівнях, вінзоризовані рівні, логарифмічна специфікація для додатної priority fee та Пуассонівська псевдомаксимальна правдоподібність), демонструє, що операції обміну на децентралізованих біржах супроводжуються найвищою премією за терміновість (приблизно 253% за оцінкою PPML відносно простого трансферу), тоді як композитні фінансові операції характеризуються суперечливою картиною – високе середнє значення за

рахунок «хвоста» розподілу при від'ємному ефекті для типової транзакції, що методологічно ілюструє ризики інтерпретації середніх показників без урахування форми розподілу.

Регуляторна релевантність дослідження прямо артикульована авторами через посилання на Принципи для інфраструктур фінансового ринку (PFMI), розроблені CPMI-IOSCO у 2012 році, та керівництво 2022 року щодо застосування PFMI до стейблкоїнів. Значна частка композитних транзакцій, виявлених у дослідженні, за своєю функцією наближається до поняття «грошового розрахунку» (money settlement) у розумінні Принципу 9 PFMI – категорії операцій із системними властивостями, що традиційно підлягають підвищеним вимогам управління ризиками в інфраструктурах фінансового ринку. Це створює прямий аналітичний місток між емпіричним вимірюванням складності ончейн-транзакцій та чинною пруденційною регуляторною архітектурою для системно значущих розрахункових механізмів.

З погляду суб'єктів первинного фінансового моніторингу, які здійснюють операції з віртуальними активами або обслуговують постачальників послуг, пов'язаних із віртуальними активами (VASP/CASP), методологічні висновки дослідження мають безпосереднє практичне застосування. Системи транзакційного моніторингу, які збирають і аналізують лише дані на рівні окремих переказів, можуть не бачити повної картини. Це характерно для багатьох комерційних рішень блокчейн-аналітики, що використовуються для стандартного скринінгу клієнтів і виявлення підозрілих операцій. У результаті такі системи часто недооцінюють або неправильно трактують операції, які насправді є лише частиною складніших фінансових схем. Це створює подвійний ризик: з одного боку, можливість маскування розшарування незаконних доходів усередині атомарно виконуваних багатокрокових операцій обміну, маршрутизації ліквідності та переказу між протоколами, які при поверхневому аналізі трансферного рівня виглядають як окремі, економічно незалежні події; з іншого боку – штучне завищення вимірюваних обсягів та частоти операцій клієнта, що спотворює калібрування порогових значень ризик-орієнтованого моніторингу та може провокувати як надмірну кількість хибно-позитивних сповіщень, так і пропуск істотних

Висновки:

- **Перехід від трансфер-орієнтованого до транзакційно-орієнтованого моніторингу:** СПФМ, що обслуговують VASP/CASP або самостійно проводять операції з віртуальними активами, мають переглянути архітектуру систем транзакційного моніторингу так, щоб аналізувати повний журнал подій атомарної транзакції, а не лише трансферні записи окремого стейблкоїна, оскільки майже 60% усіх трансферів виникають у межах композитних операцій, здатних маскувати справжню економічну причину руху коштів.
- **Диференціація типологій ризику за емітентами стейблкоїнів:** розробка індикаторів підозрілості має враховувати документально підтверджену структурну гетерогенність USDC/USDT проти PYUSD, оскільки уніфіковані порогові значення ризику для «стейблкоїнів» як єдиної категорії не відображають реальних відмінностей у профілі використання.
- **Інтеграція верифікованої методології до інструментарію нагляду:** підрозділи фінансового моніторингу та органи нагляду можуть розглядати запропоновану відтворювану класифікацію як доповнення або альтернативу пропрієтарним рішенням блокчейн-аналітики для незалежної верифікації оцінок обсягів підозрілої діяльності.
- **Врахування показника терміновості виконання операцій (priority fee):** статистично значуща премія за терміновість для операцій обміну на децентралізованих біржах може слугувати додатковим індикатором підвищеного ризику швидкого виведення активів і потребує окремого опрацювання в межах систем виявлення підозрілих операцій із віртуальними активами.

транзакційних аномалій. Запропонована авторами відтворювана, незалежна від постачальника методологія класифікації (на основі верифікованих підписів подій та членства в реєстрі протокольних контрактів) пропонує підрозділам фінансового моніторингу та регуляторам аудитопридатну альтернативу пропрієтарним рішенням комерційних постачальників блокчейн-аналітики, що частково усуває давню проблему непрозорості методологій, які лежать в основі ризик-скорингу віртуальних активів.

Типологія фінансових злочинів, пов'язаних із торгівлею людьми та сучасним рабством [2]

Публікація ПФР Острова Мен оновлює та замінює документ з індикаторів 2020 року, прямо позиціонуючи себе в межах обов'язку острова за Рекомендацією 29 FATF, яка вимагає від підрозділів фінансової розвідки розробляти та поширювати аналітичні матеріали щодо загроз. Доказова база ґрунтується на аналізі звітів про підозрілі операції (SAR), відкритих джерелах (OSINT) та безпосередньому внеску сектору; ілюстративні кейси анонімізовані або художньо адаптовані, проте відображають реальні розвідувальні моделі, виявлені як на острові, так і на міжнародному рівні.

Документ визначає торгівлю людьми та сучасне рабство (HT/MDS) у межах визначення Палермського протоколу – вербування, перевезення, переховування або одержання осіб шляхом примусу чи обману з метою експлуатації, – та наводить глобальні оцінки приблизно 50 мільйонів осіб, що перебувають у сучасному рабстві, та близько 500 мільярдів доларів США річного незаконного доходу, окреслюючи HT/MDS як один з найприбутковіших і водночас найменш успішно переслідуваних видів транснаціональної злочинності. Статус Острова Мен як міжнародного фінансового центру прямо визначається джерелом подвійної вразливості: як потенційної транзитної юрисдикції для розміщення, розшарування чи інтеграції доходів від HT/MDS, так і як локації, де може відбуватися саме діяння експлуатації; національна оцінка ризиків 2026 року фіксує тенденцію до зростання ризику HT для юрисдикції.

Статистика SAR за період 2021–2025 років виявляє аналітично значущу секторальну концентрацію: із 42 поданих SAR, де підозрювана злочинна діяльність стосувалася HT або MDS, 26 виникли на підставі тригерів з відкритих джерел, а не безпосередньої взаємодії з клієнтом, причому сектор онлайн-/е-гемблінгу забезпечив 65,79% (25 SAR) усіх подань – проти 23,68% з боку банківського сектору та лише 10,53% від TCSP.

Таксономія індикаторів ризику структурована за трьома взаємодоповнюваними вимірами – поведінкові індикатори, що спостерігаються під час прямої взаємодії з клієнтом, висновки належної перевірки клієнта (зокрема, негативні згадки у відкритих джерелах, спільні контактні дані для кількох непов'язаних заявок на відкриття рахунку, адреси, пов'язані з комерційною сексуальною діяльністю) та транзакційні індикатори (платежі постачальникам інструментів анонімності чи обладнання для приховованого запису, кілька готельних номерів в одну ніч, негайне переведення майже всієї отриманої заробітної плати непов'язаній третій стороні). ПФР прямо застерігає від надмірної довіри окремому індикатору, наголошуючи, що підозра найнадійніше формується через сукупне поєднання кількох індикаторів, особливо коли вони збігаються з зайнятістю у галузі підвищеного ризику або зв'язком із юрисдикцією підвищеного ризику.

Перелік галузей підвищеного ризику зберігає традиційні готівково-інтенсивні, низькокваліфіковані сектори (будівництво, сільське господарство, рибальство, текстильне виробництво, комерційний клінінг), водночас суттєво розширюючись для охоплення кібершахрайської інфраструктури. Документ виокремлює контр-інтуїтивний профіль жертв у цій типологічній галузі: жертви, що утримуються в шахрайських центрах, як правило, мають вищу освіту, що відображає схильність торговців людьми до використання технологічно

[2] https://www.fiu.im/media/1268/human-trafficking-and-modern-slavery-typology-2026.pdf

грамотних виконавців, здатних проводити правдоподібні інвестиційні та романтичні шахрайські схеми, – висновок із прямим наслідком для калібрування поведінкових індикаторів, оскільки традиційне уявлення про жертву торгівлі людьми як про вразливу, низькокваліфіковану особу не застосовується до цієї категорії.

Документ розвиває чотири типологічні кластери з ілюстративними кейсами. Трудова експлуатація (примусова праця, боргова кабала, домашнє рабство) ілюструється виявленням агентом з нерухомості факту проживання персоналу в комерційному приміщенні з вилученими роботодавцем паспортами, а також виявленням банком системного переведення заробітної плати з коментарями «житло», «їжа» та «борг» на рахунок непов'язаної третьої сторони. Сексуальна експлуатація – включно з виробництвом, поширенням та придбанням матеріалів сексуального насильства над дітьми (CSAM) – ілюструється виявленням TCSP орендованої нерухомості, пов'язаної з сайтами дорослих послуг, та виявленням банком здійснення контролю над рахунком третьою стороною в поєднанні з платіжними моделями, характерними для комерційної сексуальної діяльності; документ окреслює CSAM, згенерований штучним інтелектом, як новий доказовий виклик з огляду на зростаючу складність розрізнення синтетичного та справжнього матеріалу. Примусова кримінальна діяльність охоплює як діяльність «грошових мулів» (молода клієнтка, що швидко перенаправляє великі необґрунтовані готівкові депозити особі з попередніми судимостями за наркотрафік), так і фінансування шахрайських центрів (кейс перевірки заявки на бридж-кредит, де сфабриковані рахунки-фактури, неправдоподібна траєкторія накопичення багатства та повторне використання контактних даних, раніше пов'язаних із клієнтом, виключеним за підозрою у MDS, спільно зумовили подання SAR та відмову від обслуговування). Множинне проживання – типологія, розроблена спільно з Банківською операційною групою, – ілюструється одночасними заявками на відкриття рахунків в один день від непов'язаних іноземних громадян, які зазначають спільну адресу проживання, структурно нездатну розмістити заявлену кількість мешканців, та супроводжуються одним і тим самим перекладачем у різний час доби.

Висновки:

- **Перекалібрування систем виявлення в банківському та TCSP секторах:** впровадження сценаріїв виявлення множинного проживання (кілька непов'язаних клієнтів, одна адреса, той самий перекладач/посередник) та боргової кабали (системні платежі третій стороні з референсами «житло/їжа/борг») як пріоритетних індикаторів, з огляду на низьку частку звітності TCSP-сектору порівняно з його структурною вразливістю.
- **Адаптація типологій під сектор онлайн-гемблінгу:** з огляду на домінуючу частку SAR з цього сектору (65,79%) та задокументований зв'язок шахрайських центрів із підставними структурами з сектору азартних ігор, СПФМ у сфері е-гемблінгу мають впровадити цільові індикатори для виявлення фінансування примусової злочинної діяльності, прихованого за легітимними платіжними потоками.
- **Перегляд поведінкових індикаторів для жертв шахрайських центрів:** традиційний профіль «вразливої, низькокваліфікованої жертви» не застосовується до операторів інвестиційного або романтичного шахрайства, що утримуються в центрах; необхідні окремі індикатори для високоосвічених, технологічно грамотних осіб, що діють під примусом.

Торгівля органами розглядається як окрема аналітична категорія з посиланням на оцінку Всесвітньої організації охорони здоров'я (2007 р.), згідно з якою 5–10% усіх трансплантацій у світі використовували органи з чорного ринку, та оцінку Управління ООН з наркотиків і злочинності у понад 1 мільярда доларів США річного незаконного доходу від цього виду злочинної діяльності. Засудження у Великій Британії в травні 2023 року нігерійського політика, його дружини та медичного працівника за змову щодо вилучення нирки в жертви – перше засудження такого роду у Великій Британії – наведено для ілюстрації як ключового

фінансового індикатора (платежі з референсами на медичні процедури, спрямовані поза визнаними клінічними каналами), так і незмінно низького рівня виявлення та притягнення до відповідальності за цим видом НТ.

Архітектура звітності спрямовує розкриття інформації на рівні підозри через систему Themis, водночас прямо зберігаючи канал звітності нижчого за підозру рівня за статтею 24 Закону про ПФР 2016 року для діяльності, що ще не сформувала формальної підозри. Паралельні канали правоохоронних органів (екстрений та неекстрений контакт з поліцією, Crimestoppers та мобільний застосунок «STOP», що його оперує благодійна організація Stop the Traffik) розміщені поруч із каналом ФР, що узгоджується з участю острова в рамковій структурі групи «Egmont» для транскордонної співпраці фінансової розвідки.

Порівняно з попередником 2020 року, типологічний документ 2026 року демонструє суттєву еволюцію за трьома напрямами: пряме врахування CSAM, згенерованого штучним інтелектом, як типологічного й доказового ускладнення; інтеграцію фінансування шахрайських центрів як окремого вектора підвищеного ризику, пов'язаного з підставними структурами сектору азартних ігор; та формальну, спільно розроблену з сектором типологію множинного проживання – що разом сигналізує про методологічний перехід до технологічно актуального, спільно розробленого керівництва.

Відповідальне впровадження штучного інтелекту у фінансовому секторі: міжнародні практики управління ризиками та забезпечення фінансової стабільності [3]

Документ, підготовлений Радою з фінансової стабільності (FSB), присвячений формуванню міжнародного підходу до відповідального впровадження штучного інтелекту (AI) у фінансовому секторі та фактично є спробою створити комплексну систему принципів, яка дозволить фінансовим установам отримувати переваги від використання AI без створення надмірних ризиків для власної діяльності, споживачів фінансових послуг та фінансової стабільності загалом. Документ виходить із того, що фінансовий сектор вступає у новий етап цифрової трансформації, де штучний інтелект перестає бути окремим технологічним інструментом і поступово стає базовим елементом бізнес-моделей фінансових установ. Особлива увага приділяється швидкому розвитку генеративного штучного інтелекту (GenAI), великих мовних моделей (LLM) та агентного штучного інтелекту (Agentic AI), які здатні не лише аналізувати інформацію, а й автономно планувати та виконувати складні завдання без постійного втручання людини.

У документі детально аналізуються основні напрями використання AI у фінансовій системі. Зазначається, що банки, страхові компанії, інвестиційні фонди, платіжні установи та фінансові ринкові інфраструктури вже активно використовують AI для кредитного скорингу, оцінки кредитоспроможності, управління ризиками, виявлення шахрайства, проведення процедур KYC та ПВК, кіберзахисту, моніторингу ринкових зловживань, управління портфелями активів, прогнозування ринкових тенденцій, обслуговування клієнтів та автоматизації внутрішніх процесів. На думку FSB, масштаб впровадження AI продовжуватиме швидко зростати завдяки розвитку хмарних технологій, збільшенню доступності обчислювальних ресурсів, появі фундаментальних моделей та постійному збільшенню обсягів даних, які можуть використовуватися для навчання алгоритмів. Одночасно попит на AI стимулюється прагненням фінансових установ підвищити ефективність діяльності, скоротити витрати, посилити конкурентоспроможність та покращити управління ризиками.

Особливо детально у звіті розглядаються практичні кейси застосування AI. У сфері кредитування AI використовується для побудови складних моделей кредитного скорингу, які дозволяють враховувати значно ширший набір параметрів порівняно з традиційними

[3] https://www.fsb.org/uploads/P100626.pdf

моделями оцінки ризику. Завдяки використанню альтернативних даних банки можуть більш точно оцінювати кредитоспроможність клієнтів, розширювати доступ до фінансових послуг для окремих категорій населення та зменшувати рівень дефолтів. Наводяться приклади банків, які за допомогою машинного навчання виявляли понад 95% потенційно проблемних кредитів за декілька місяців до фактичного погіршення фінансового стану позичальників. Також розглядаються приклади використання GenAI для автоматичного аналізу фінансової звітності та підготовки кредитних висновків, що дозволяло скоротити час підготовки кредитних пропозицій із декількох днів до кількох хвилин.

У сфері управління активами та торгівлі фінансовими інструментами AI використовується для аналізу ринкових даних, прогнозування волатильності, аналізу новинних потоків, оцінки настроїв ринку, побудови торговельних стратегій та оптимізації інвестиційних портфелів. Документ підкреслює, що сучасні AI-системи здатні аналізувати великі масиви альтернативних даних та знаходити закономірності, які залишаються непомітними для традиційних методів аналізу. Хоча повністю автономна торгівля на основі GenAI поки не набула широкого поширення, фінансові установи вже експериментують із використанням агентного AI для автоматизації окремих етапів інвестиційного процесу, включаючи аналіз новин, підготовку торговельних сигналів та формування пропозицій щодо укладання угод.

Значний розділ документа присвячений використанню AI у сфері запобігання та протидії відмиванню коштів, фінансуванню тероризму та боротьбі з шахрайством. FSB відзначає, що AI здатний суттєво підвищити ефективність моніторингу транзакцій, виявлення аномальної поведінки клієнтів та встановлення складних зв'язків між фінансовими операціями. Алгоритми машинного навчання дозволяють скорочувати кількість хибнопозитивних спрацювань, швидше виявляти підозрілі схеми та покращувати якість фінансових розслідувань. У документі наведено приклади банків, які використовують агентний AI для автоматичного виявлення нових шахрайських схем та генерації правил моніторингу, що дозволило скоротити збитки від шахрайства більш ніж на 20%. Окремо розглядаються інструменти виявлення та протидії використанню технологій діпфейку, фальсифікованих цифрових особистостей і рахунків підставних осіб, які застосовуються для шахрайства, відмивання коштів та інших фінансових злочинів.

Окремий блок присвячений впливу AI на клієнтський сервіс та внутрішню продуктивність фінансових установ. Документ демонструє, що AI стає інструментом масової автоматизації бізнес-процесів, дозволяючи автоматично обробляти документи, готувати аналітичні матеріали, генерувати програмний код, підтримувати прийняття управлінських рішень та оптимізувати роботу персоналу. Наведені приклади свідчать про можливість скорочення сотень тисяч ручних операцій на рік та істотного зменшення витрат часу на виконання рутинних завдань. Особлива роль відводиться використанню генеративного AI у розробці програмного забезпечення, де автоматизовані інструменти здатні генерувати мільйони рядків коду, виконувати перевірку програмного забезпечення та прискорювати розробку нових цифрових продуктів.

Разом із перевагами FSB детально аналізує ризики, пов'язані з використанням AI. Найбільшу увагу приділено ризикам для фінансової стабільності. До них віднесено залежність фінансових установ від невеликої кількості великих постачальників хмарної інфраструктури та AI-моделей, концентрацію технологічних ресурсів, можливість одночасного використання однакових моделей багатьма фінансовими установами та формування схожих ринкових рішень. Такі явища можуть посилювати проциклічність, сприяти формуванню ринкових перекосів та створювати системні ризики під час кризових періодів. Окремо розглядаються ризики, пов'язані з недостатньою якістю даних, помилками навчання моделей, упередженістю алгоритмів та складністю пояснення логіки прийняття рішень складними AI-системами.

Особливе занепокоєння авторів викликають питання пояснюваності та прозорості AI. Документ підкреслює, що фінансові установи повинні розуміти причини, за якими AI-моделі формують ті чи інші результати. Недостатня пояснюваність може ускладнювати виконання

нормативних вимог, проведення незалежної валідації моделей, оцінку коректності результатів, виявлення дискримінаційних ефектів та забезпечення належного захисту прав клієнтів. При цьому FSB визнає, що певні типи сучасних AI-моделей за своєю природою мають обмежену пояснюваність, тому в таких випадках рекомендується застосовувати додаткові компенсуючі заходи контролю.

Важливий розділ присвячений кіберризикам. Автори наголошують, що AI здатний одночасно посилювати захист фінансових установ і створювати нові можливості для зловмисників. Документ детально описує такі загрози, як компрометація навчальних даних шляхом внесення шкідливих даних, впровадження шкідливих інструкцій до запитів користувача, обхід вбудованих обмежень та механізмів захисту моделі штучного інтелекту, атаки, спрямовані на вилучення даних або параметрів моделі, шахрайство із використанням технологій діпфейку, автоматизоване створення шкідливого програмного забезпечення та використання AI для пошуку вразливостей у цифрових системах. На думку FSB, фінансові установи повинні інтегрувати AI-сценарії до програм кіберстійкості, регулярно проводити тестування, обмінюватися інформацією про загрози та адаптувати системи захисту до нових типів атак.

Ключовою частиною документа є система із 12 належних практик (sound practices), які охоплюють усі аспекти управління AI. У центрі цієї системи перебуває роль ради директорів та вищого керівництва, які повинні визначати стратегію впровадження AI, встановлювати допустимий рівень ризику, забезпечувати належний рівень контролю та розподіл відповідальності. Документ рекомендує створювати комплексні системи корпоративного управління AI, інтегрувати AI-ризики до загальної системи управління ризиками, формувати централізовані реєстри AI-рішень, документувати всі етапи життєвого циклу моделей, проводити регулярне тестування та моніторинг їх ефективності. Особлива увага приділяється необхідності пропорційного підходу, коли рівень контролю залежить від критичності конкретного AI-рішення для діяльності установи.

Висновки:

- **FSB фактично формує міжнародну рамку відповідального впровадження AI у фінансовому секторі, яка базується на 12 практиках управління AI та охоплює весь життєвий цикл AI-рішень** – від стратегічного планування до постійного моніторингу та контролю ризиків.
- **Найбільшими системними ризиками AI для фінансової стабільності визначено** концентрацію постачальників AI-послуг, залежність від третіх сторін, кіберризики, проблеми якості даних та можливість формування однакових моделей поведінки фінансових установ через використання спільних AI-рішень.
- **Фінансовим установам рекомендується** створювати централізовані реєстри AI-рішень, впроваджувати ризик-орієнтовану класифікацію AI-випадків використання, проводити регулярне тестування моделей та забезпечувати безперервний людський контроль над критичними рішеннями.
- **Розвиток генеративного та агентного AI потребує посилення вимог до управління ризиками,** оскільки автономність таких систем створює нові загрози для операційної стійкості, захисту даних, кібербезпеки та належного корпоративного управління фінансових установ.

Завершуючи, FSB формує концепцію відповідального впровадження AI як безперервного процесу, який потребує поєднання технологічних інновацій із належним корпоративним управлінням, управлінням ризиками та людським контролем. Документ виходить із того, що майбутнє фінансового сектору буде нерозривно пов’язане зі штучним інтелектом, однак довгострокові переваги від його використання можуть бути реалізовані лише за умови побудови ефективних механізмів управління, прозорості, підзвітності та стійкості до нових технологічних ризиків. Для фінансових установ це означає необхідність переходу від експериментального

використання AI до формування повноцінної системи управління штучним інтелектом як одним із ключових елементів сучасної фінансової інфраструктури.

Нова ера міжнародної боротьби з транснаціональною корупцією [4]

Документ OECD є одним із найбільш комплексних досліджень сучасної практики міжнародного правозастосування у сфері боротьби з підкупом іноземних посадових осіб та транснаціональною корупцією. Його головна мета полягає у дослідженні того, як багатоюрисдикційні врегулювання (MJR) трансформують глобальну систему притягнення до відповідальності за корупційні правопорушення, які охоплюють декілька держав одночасно. Документ базується на масштабному емпіричному аналізі 31 міжнародної справи, що охоплюють 114 окремих рішень, ухвалених між 2008 та 2026 роками, та демонструє еволюцію міжнародної антикорупційної співпраці від традиційної моделі окремих національних розслідувань до складних механізмів координованого правозастосування за участю декількох держав.

У центрі дослідження перебуває концепція багатоюрисдикційного врегулювання, під якою OECD розуміє координовані дії двох або більше держав щодо застосування санкцій до юридичної особи за участь у єдиній транснаціональній корупційній схемі. Такі механізми можуть реалізовуватися як через одночасні оголошення рішень кількома юрисдикціями, так і через послідовне укладення домовленостей у різний час, але за умови їх попередньої координації між правоохоронними органами. Дослідження показує, що відправною точкою формування сучасної практики MJR стала справа Siemens у 2008 році, коли Німеччина та Сполучені Штати вперше узгоджено застосували санкції до компанії в межах однієї міжнародної корупційної справи. Саме цей кейс започаткував нову модель боротьби з міжнародною корупцією, в якій держави не діють ізольовано, а об'єднують свої зусилля для досягнення спільної мети – забезпечення невідворотності відповідальності незалежно від кількості залучених юрисдикцій.

Автори наголошують, що така модель безпосередньо випливає з положень Конвенції ОЕСР про боротьбу з підкупом іноземних посадових осіб у міжнародних комерційних операціях та Рекомендації ОЕСР 2021 року щодо подальшої боротьби з підкупом іноземних посадових осіб. Зокрема, стаття 9 Конвенції передбачає обов'язок держав забезпечувати швидку та ефективну міжнародну правову допомогу, а стаття 4.3 вимагає проведення консультацій між державами для визначення найбільш доцільної юрисдикції у випадках, коли декілька країн мають право переслідувати одне й те саме правопорушення. Таким чином, багатоюрисдикційні врегулювання фактично стали практичним механізмом реалізації цих міжнародних стандартів.

Одним із ключових висновків дослідження є те, що сучасна боротьба з транснаціональною корупцією майже повністю спирається на механізми позасудового врегулювання (NTR). Із 114 проаналізованих рішень 113 були реалізовані саме через такі інструменти, тоді як лише одне завершилося повноцінним судовим розглядом. OECD підкреслює, що домінування NTR не є випадковим. Складність міжнародних корупційних схем, велика кількість зацікавлених держав, різниця між правовими системами та необхідність швидкого досягнення результату роблять традиційний судовий процес надзвичайно складним інструментом міжнародної координації. Натомість механізми позасудового врегулювання забезпечують необхідну гнучкість, дозволяють погодити санкції між декількома державами, визначити порядок їх виконання та уникнути багаторічних процесуальних спорів.

У документі детально аналізуються різні моделі таких врегулювань. Серед них особливу роль відіграють угоди про нездійснення кримінального переслідування (NPA) та угоди про

[4] https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/05/sanctioning-foreign-bribery-through-multijurisdictional-resolutions_565ff93f/48ff398e-en.pdf

відкладене кримінальне переслідування (DPA), угоди про визнання вини, адміністративні та цивільні врегулювання. OECD зазначає, що різні країни використовують різні правові конструкції, проте для успішної участі у багатоюрисдикційних справах державі не обов'язково мати конкретну модель американського чи британського зразка. Важливим є саме існування законодавчого механізму, який дозволяє врегулювати справу без повного судового розгляду. Особливо ефективними виявилися інструменти, що не передбачають обов'язкового обвинувального вироку, оскільки вони дозволяють швидше координувати дії між кількома юрисдикціями та досягати глобального врегулювання справи.

Значна частина дослідження присвячена аналізу міжнародної співпраці між правоохоронними органами. OECD наголошує, що сучасні корупційні схеми можуть охоплювати п'ять і більше юрисдикцій одночасно. Компанія може бути зареєстрована в одній країні, здійснювати діяльність через дочірню структуру в іншій державі, використовувати фінансову систему третьої країни та надавати хабар посадовій особі у четвертій державі. У таких умовах жоден правоохоронний орган не має можливості самостійно отримати повну картину злочинної діяльності. Саме тому міжнародний обмін інформацією, взаємна правова допомога, створення спільних або паралельних слідчих груп і координація розслідувань стають критично важливими елементами успішного правозастосування.

Дослідження також демонструє безпрецедентне розширення кола держав, які беруть участь у таких механізмах. Якщо протягом багатьох років після справи Siemens фактично існували лише дві активні юрисдикції – США та Німеччина, то станом на 2026 рік у MJR вже брали участь 12 держав. Найактивнішим учасником залишаються США, які були стороною всіх проаналізованих справ і уклали майже 58 % усіх рішень. Водночас дедалі вагомішу роль відіграють Бразилія, Велика Британія, Швейцарія, Франція, Нідерланди та Південна Африка. Окремої уваги заслуговує поступове залучення юрисдикцій, які не є сторонами Конвенції ОЕСР про боротьбу з підкупом іноземних посадових осіб, зокрема Сінгапуру, Малайзії та Гонконгу, що свідчить про глобальне поширення практики багатоюрисдикційних врегулювань далеко за межі системи ОЕСР.

Однією з найважливіших тенденцій, зафіксованих у дослідженні, є поступовий перехід від моделі, за якої санкції застосовуються переважно державами, що переслідують юридичних осіб за підкуп іноземних посадових осіб, до моделі, у якій дедалі активнішу роль відіграють держави, посадові особи яких стали об'єктами корупційного впливу. Якщо на початковому етапі розвитку багатоюрисдикційних врегулювань домінували держави, які забезпечували переслідування підкупу іноземних посадових осіб, то після 2019 року спостерігається суттєве зростання ролі держав, які безпосередньо постраждали від корупційних схем та на території яких відбувалися відповідні корупційні діяння. Такий розвиток подій свідчить про посилення ролі держав, які постраждали від корупції у міжнародному правозастосуванні та про поступове вирівнювання балансу між інтересами держав, які переслідують хабародавців, і держав, які зазнали шкоди від корупційних дій.

Особливо цінним є аналіз фінансових результатів багатоюрисдикційних врегулювань. OECD оцінює, що сукупний обсяг санкцій, штрафів та конфіскацій у межах проаналізованих справ перевищив 33,7 млрд доларів США. Водночас одним із найбільш інноваційних інструментів сучасної практики стали механізми взаємного зарахування штрафів, які дозволяють уникати дублювання фінансової відповідальності шляхом врахування санкцій, уже сплачених компанією в іншій юрисдикції. Завдяки цьому забезпечується баланс між ефективним покаранням та принципом пропорційності, а також мінімізується ризик дублювання санкцій. Документ наголошує, що саме ці механізми стали одним із ключових факторів успіху багатоюрисдикційних врегулювань та дозволили уникнути надмірного дублювання санкцій між юрисдикціями, забезпечуючи ефективність, пропорційність і стримувальний характер фінансових стягнень.

Висновки:

- **Багатоюрисдикційні врегулювання стали новим глобальним стандартом боротьби з транснаціональною корупцією.** Із 114 проаналізованих рішень 113 були реалізовані через механізми позасудового врегулювання, що свідчить про їхню практичну ефективність та домінування у сучасному правозастосуванні.
- **Наявність принаймні одного механізму позасудового врегулювання є необхідною умовою для повноцінної міжнародної співпраці у сфері розслідування та санкціонування випадків підкупу іноземних посадових осіб.** Держави, які не мають законодавчих інструментів позасудового врегулювання, фактично обмежені у можливості брати участь у багатоюрисдикційних антикорупційних розслідуваннях.
- **Координовані міжнародні розслідування забезпечують суттєво вищий фінансовий результат.** Сукупний обсяг санкцій у проаналізованих справах перевищив 33,7 млрд доларів США, а механізми реституції та компенсації дозволили державам-жертвам корупції претендувати на близько 12,6 млрд доларів США.
- **Зростає роль держав, на території яких безпосередньо відбувалися корупційні правопорушення.** Сучасна практика багатоюрисдикційних врегулювань дедалі частіше передбачає участь таких держав у розслідуванні та врегулюванні справ, а також створює можливості для отримання ними частини штрафів, конфіскацій і компенсацій.

Важливим аспектом дослідження є також питання компенсації завданої шкоди та повернення коштів. OECD встановлює, що у 68 % проаналізованих справ були передбачені механізми реституції або компенсації. Це дозволяло спрямовувати частину конфіскованих коштів до державних бюджетів або державних підприємств, які постраждали від корупційних схем. За оцінками авторів, держави на стороні «попиту» потенційно могли отримати близько 12,6 млрд доларів США у вигляді штрафів, конфіскацій та інших платежів. Таким чином, багатоюрисдикційні врегулювання дедалі більше виконують не лише каральну, а й відновлювальну функцію, сприяючи компенсації економічних наслідків корупції.

Загалом OECD доходить висновку, що багатоюрисдикційні врегулювання стали одним із найважливіших інструментів сучасної міжнародної антикорупційної політики. Вони дозволяють поєднувати ресурси правоохоронних органів різних держав, забезпечувати більш справедливий розподіл стягнутих коштів, уникати дублювання покарання, підвищувати ефективність розслідувань та створювати додаткові стимули для добровільного співробітництва компаній з органами влади. Водночас документ наголошує, що подальший розвиток цієї системи потребує удосконалення національних правових механізмів позасудового врегулювання, розширення можливостей міжнародної співпраці та зміцнення спроможності держав, особливо країн, які є безпосередніми жертвами транснаціональної корупції, брати повноцінну участь у таких багатосторонніх механізмах правозастосування.

Посилена перевірка клієнтів у системі ПВК/ФТ: практичні механізми виявлення високоризикових відносин [5]

Документ, підготовлений Міністерством внутрішніх справ Нової Зеландії, є комплексним методичним керівництвом щодо застосування посиленої перевірки клієнтів (EDD) у межах

[5] https://www.dia.govt.nz/diawebsite.nsf/Files/AML-CFT-2026/$file/AMLCFT-Enhanced-Customer-Due-Diligence-Guidance-2026.pdf

сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення та роз'яснює механізми застосування посиленої перевірки клієнтів на основі ризик-орієнтованого підходу. Документ спрямований на забезпечення єдиного підходу до виконання вимог законодавства Нової Зеландії у сфері ПВК/ФТ та роз'яснює, яким чином суб'єкти фінансового моніторингу повинні оцінювати ризики клієнтів, визначати випадки застосування посиленої перевірки клієнтів та документувати результати відповідних заходів.

Основною концепцією документа є ризик-орієнтований підхід, відповідно до якого посилена перевірка розглядається не як формальна додаткова процедура, а як інструмент управління ризиками відмивання коштів та фінансування тероризму. Автори підкреслюють, що рівень перевірки має відповідати рівню ризику конкретного клієнта, його діяльності, структурі власності, характеру операцій та географічним факторам. Водночас наголошується, що наявність підвищеного ризику не означає автоматичної відмови від встановлення ділових відносин. Навпаки, підзвітні суб'єкти повинні забезпечити належне розуміння ризиків і впровадити адекватні механізми їх контролю та мінімізації. Документ прямо зазначає, що концепція «нульового ризику» не існує, а ефективність системи ПВК/ФТ визначається здатністю організації виявляти, оцінювати та управляти ризиками на практиці.

Значна увага приділяється розмежуванню стандартної та посиленої перевірки клієнта. Документ пояснює, що саме стандартна перевірка створює базу для визначення необхідності застосування EDD. Під час первинного встановлення ділових відносин підзвітний суб'єкт повинен отримати достатню інформацію про клієнта, характер і мету його діяльності, очікувані фінансові потоки, типові операції та структуру власності. Лише після формування первинного ризикового профілю стає можливим прийняття рішення щодо необхідності посиленої перевірки. Таким чином, EDD розглядається як продовження та поглиблення стандартних процедур ідентифікації та верифікації.

Документ детально описує обставини, за яких застосування EDD є обов'язковим. До них належать трасти та інші механізми володіння приватними активами, нерезиденти з юрисдикцій із недостатніми заходами ПВК/ФТ, компанії з номінальними акціонерами або акціями на пред'явника, політично значущі особи, компанії з номінальними директорами, партнерства з номінальними генеральними партнерами, клієнти, які використовують нові технології або продукти, що можуть сприяти анонімності, а також особи, які здійснюють складні, незвично великі або економічно необґрунтовані операції. Окремо підкреслюється, що перелік законодавчо визначених випадків не є вичерпним. Організація повинна самостійно визначати інші високоризикові ситуації, виходячи з власної оцінки ризиків, особливостей бізнес-моделі, клієнтської бази та географії діяльності.

Однією з центральних тем документа є встановлення та перевірка кінцевих бенефіціарних власників. Регулятор наголошує, що складні корпоративні структури часто використовуються для приховування фактичного контролю над активами або для маскування злочинного походження коштів. Тому підзвітні суб'єкти повинні не лише встановити формальну структуру власності, а й зрозуміти кожен її рівень, включаючи фізичних осіб, які здійснюють остаточний контроль. Особлива увага приділяється ситуаціям, коли структура власності є надмірно складною або позбавленою очевидної економічної логіки. У таких випадках сама структура може виступати індикатором ризику та вимагати додаткових перевірочних заходів. Документ також наголошує на необхідності ідентифікації та верифікації осіб, які діють від імені клієнта, а також перевірки їхніх повноважень.

Важливий блок керівництва присвячений трастам, які розглядаються як одна з найбільш вразливих категорій клієнтів з точки зору ризиків відмивання коштів. Документ визнає, що трасти можуть використовуватися для приховування реальних власників активів або джерел їх походження. Водночас застосовується диференційований підхід. Для внутрішніх сімейних трастів із простою структурою передбачається менш інтенсивна перевірка, тоді як міжнародні трасти, трасти з іноземними засновниками або бенефіціарами, а також трасти, пов'язані з

юрисдикціями підвищеного ризику, вимагають суттєво більш глибокого аналізу. Окремо регламентуються вимоги щодо встановлення бенефіціарів трасту, засновників, джерел фінансування, регулярних надходжень та активів, що перебувають під управлінням трасту.

Суттєве місце у документі займає концепція джерела статків та джерела коштів. Автори приділяють особливу увагу правильному розумінню відмінностей між цими поняттями. Джерело статків описує походження сукупного багатства особи та дозволяє зрозуміти, яким чином клієнт накопичив свої активи протягом тривалого часу. Джерело коштів має значно вужчий характер і стосується конкретних коштів, які використовуються в межах певної операції або ділових відносин. Документ наголошує, що підзвітні суб'єкти повинні самостійно визначати, коли достатньо аналізу лише джерела коштів, коли необхідний аналіз джерела статків, а коли потрібне комплексне дослідження обох елементів одночасно. Вибір має ґрунтуватися на ефективності управління ризиками, а не на простоті виконання вимог.

Документ надає детальні рекомендації щодо збору та перевірки інформації про джерела статків і джерела коштів. Передбачається використання широкого спектра незалежних та надійних джерел інформації, включаючи банківські виписки, податкові документи, аудовану фінансову звітність, договори купівлі-продажу, спадкові документи, інформацію державних реєстрів, документи щодо комерційної діяльності та інші підтверджувальні матеріали. Водночас підкреслюється, що перевірка не повинна охоплювати абсолютно всі активи клієнта. Головною метою є формування обґрунтованого розуміння того, чи відповідають масштаби та характер статків клієнта відомій інформації про нього. Для високоризикових клієнтів очікується значно більший обсяг доказів, використання оригіналів або належним чином засвідчених копій документів, а також залучення додаткових незалежних джерел перевірки.

Висновки:

- **Посилена перевірка повинна базуватися на ризик-орієнтованому підході, а не на формальному виконанні процедур.** Організації мають самостійно визначати високоризикові ситуації та застосовувати пропорційні заходи контролю залежно від рівня ризику клієнта.
- **Аналіз джерела статків та джерела коштів є центральним елементом EDD.** Високоризикові клієнти повинні підтверджувати походження активів та коштів незалежними й надійними документами, причому глибина перевірки має зростати пропорційно рівню ризику.
- **Складні структури власності, номінальні акціонери, номінальні директори та трасти залишаються одними з ключових індикаторів підвищеного ризику ВК/ФТ.** Для таких клієнтів необхідно забезпечувати детальне встановлення фактичних бенефіціарних власників та джерел походження активів.
- **Посилена перевірка має бути безперервним процесом протягом усього періоду ділових відносин.** Будь-яка суттєва зміна поведінки клієнта, географії діяльності, структури власності або характеру операцій повинна автоматично запускати повторну оцінку ризиків та, за потреби, новий цикл EDD.

Окремий розділ документа присвячений оцінці країнового ризику як одному з ключових елементів ризик-орієнтованого підходу у сфері ПВК/ФТ. Автори наголошують, що аналіз ризиків, пов'язаних із конкретними юрисдикціями, не повинен обмежуватися виключно оцінкою ефективності національних систем ПВК/ФТ. До уваги також мають братися рівень корупції, масштаби діяльності організованої злочинності, ризики фінансування тероризму, наявність збройних конфліктів, участь країни у транзиті або виробництві наркотиків та інші фактори, що можуть впливати на ризик легалізації злочинних доходів. Для проведення такої оцінки рекомендується використовувати широкий спектр міжнародних джерел, зокрема матеріали FATF, результати взаємних оцінок, Basel AML Index, Індекс сприйняття корупції

Transparency International, аналітичні матеріали ООН та інші незалежні джерела інформації. Особливо підкреслюється, що юрисдикції, щодо яких FATF оприлюднила заклик до застосування посилених заходів або контрзаходів, повинні автоматично розглядатися як країни з високим рівнем ризику у сфері ПВК/ФТ.

Важливим елементом документа є взаємозв'язок між посиленою перевіркою клієнта та поданням повідомлень про підозрілу діяльність. Регулятор виходить із того, що якісно проведена EDD значно підвищує цінність інформації, яка надходить до підрозділу фінансової розвідки. Тому в разі виникнення підозри, підзвітним суб'єктам рекомендується, наскільки це можливо, провести додатковий аналіз джерел коштів, структури власності та характеру операцій до моменту подання SAR. Водночас неможливість завершити посилену перевірку, відмова клієнта надати необхідну інформацію або надання недостовірних документів можуть самі по собі розглядатися як обставини, що потребують оцінки на предмет подання повідомлення про підозрілу діяльність.

Окремо розглядаються питання безперервного моніторингу клієнтів. Документ підкреслює, що EDD не є одноразовою процедурою під час встановлення ділових відносин. Будь-які суттєві зміни у діяльності клієнта, структурі власності, географії операцій, обсягах транзакцій або бізнес-моделі повинні розглядатися як потенційна підстава для повторного проведення посиленої перевірки. Регулятор наводить приклади ситуацій, коли клієнт починає працювати з високоризиковими юрисдикціями, суттєво збільшує обсяги операцій або переходить до використання нових фінансових інструментів. У таких випадках ризиковий профіль клієнта підлягає перегляду, а система моніторингу повинна забезпечувати своєчасне виявлення таких змін.

У підсумку документ формує цілісну сучасну модель посиленої перевірки клієнтів, засновану на міжнародних стандартах FATF та принципі пропорційності. Керівництво розглядає EDD як ключовий інструмент управління ризиками ПВК/ФТ, який поєднує глибоке розуміння клієнта, аналіз структури власності, встановлення походження статків і коштів, оцінку країнових ризиків, постійний моніторинг ділових відносин та активну взаємодію із системою фінансової розвідки. Такий підхід спрямований не лише на виконання регуляторних вимог, а й на підвищення здатності фінансових установ і нефінансового сектору виявляти складні схеми відмивання коштів, приховування бенефіціарної власності та фінансування тероризму.

Фінансування тероризму у глобальній фінансовій системі: нові схеми та механізми протидії [6]

Документ, підготовлений Підрозділом фінансової розвідки Острова Мен, є комплексним практичним дослідженням сучасних механізмів фінансування тероризму, секторних вразливостей та індикаторів ризику, які можуть використовуватися суб'єктами фінансового моніторингу для своєчасного виявлення та припинення відповідної діяльності. Документ розроблений на основі Національної оцінки ризиків фінансування тероризму Острова Мен 2025 року, матеріалів FATF щодо нових ризиків фінансування тероризму, аналізу повідомлень про підозрілу діяльність, відкритих джерел інформації, міжнародних кейсів та консультацій із представниками фінансового сектору, правоохоронних органів і регуляторів. Його основною метою є демонстрація того, як сучасні терористичні мережі використовують легальні фінансові інструменти, міжнародні фінансові центри та цифрові технології для приховування, переміщення та використання коштів на підтримку терористичної діяльності.

У документі підкреслюється, що Острів Мен не стикається з істотною внутрішньою терористичною загрозою, однак його роль як міжнародного фінансового центру формує специфічний профіль ризику. Завдяки розвиненій банківській системі, сектору трастових і корпоративних послуг, страховому ринку, сфері онлайн-гемблінгу та операціям із

[6] https://www.fiu.im/media/1266/terrorist-financing-typology-2026.pdf

віртуальними активами юрисдикція залишається потенційно привабливою для осіб, які прагнуть використовувати фінансову інфраструктуру для транскордонного переміщення коштів на користь терористичних організацій. Особливі ризики пов'язані з використанням неприбуткових організацій, складних корпоративних структур, транзакцій із високоризиковими юрисдикціями, схем обходу санкцій, приховування кінцевих бенефіціарних власників та застосуванням новітніх фінансових технологій для маскування джерел і призначення коштів. Автори наголошують, що навіть за відсутності безпосереднього зв'язку з терористичною діяльністю всередині країни фінансові потоки, які проходять через юрисдикцію, можуть бути частиною міжнародних мереж фінансування тероризму.

Значна увага приділяється поясненню природи фінансування тероризму та його відмінностей від відмивання коштів. На відміну від відмивання доходів, де злочинні кошти інтегруються в легальну економіку, фінансування тероризму може здійснюватися як за рахунок незаконних, так і цілком легальних джерел. У документі запропоновано шестиетапну модель фінансування тероризму, яка охоплює збір коштів, їх переміщення, зберігання, управління, приховування та кінцеве використання. Джерелами фінансування можуть виступати благодійні внески, діяльність неприбуткових організацій, прибутки від бізнесу, шахрайство, контрабанда, торгівля наркотиками, краудфандингові платформи та інші механізми. Для переміщення коштів використовуються банківські перекази, грошові перекази через платіжні сервіси, міжнародна торгівля, криптоактиви, готівка, кур'єри та неформальні системи переказу коштів на кшталт Hawala. Окремо підкреслюється роль посередників, підставних осіб, підконтрольних компаній та складних фінансових структур у приховуванні походження і кінцевого призначення коштів.

Документ визначає низку нових та найбільш актуальних методів фінансування тероризму. До них належать дроблення платежів на незначні суми для уникнення автоматизованого моніторингу, використання соціальних мереж, платформ онлайн-гемблінгу та краудфандингу для збору коштів, застосування криптоактивів, включаючи анонімні монети, криптоміксери та децентралізовані біржі, використання юрисдикцій-посередників для маскування кінцевого місця призначення коштів, створення багаторівневих структур власності для приховування бенефіціарів, переміщення готівки через міжнародні транспортні маршрути та інвестування коштів у бізнес чи нерухомість для їх інтеграції у легальну економіку. Автори наголошують, що сучасні терористичні мережі дедалі частіше використовують фінансові інструменти, які зовні виглядають законними та не викликають автоматичних підозр у фінансових установ.

Окремий розділ присвячено взаємодії між санкційними режимами та протидією фінансуванню тероризму. Документ детально описує роль списків заборонених терористичних організацій Великої Британії, санкційних списків ООН та інших міжнародних механізмів фінансових санкцій. Особливий акцент зроблено на тому, що ефективна перевірка клієнтів не може обмежуватися лише прямим порівнянням імен із санкційними списками. Значна частина сучасних схем обходу санкцій реалізується через членів сім'ї, довірених осіб, бізнес-партнерів та складні корпоративні структури. Саме тому установам рекомендується використовувати аналіз зв'язків, мережевий аналіз, перевірку історичних ділових відносин, моніторинг спільних адрес, контактних даних та інших непрямих ознак фактичного контролю над активами.

Особливо цікавим є блок, присвячений фінансовим аспектам праворадикального екстремізму. Документ розглядає широкий спектр символіки, яку використовують екстремістські рухи, включаючи історичну нацистську символіку, адаптовані релігійні символи, цифрові коди, рунічні знаки та сучасні інтернет-меми. Автори наголошують, що сама по собі наявність таких символів не може розглядатися як доказ фінансування тероризму, однак у поєднанні з поведінковими, транзакційними та мережевими ознаками вона може виступати додатковим фактором ризику. Документ демонструє, що сучасні праворадикальні рухи дедалі активніше використовують онлайн-магазини, продаж брендованої продукції, краудфандингові кампанії, платні конференції, музичні заходи та криптовалютні пожертви як джерела фінансування своєї діяльності. У зв'язку з цим фінансовим установам рекомендується посилювати аналіз

відкритих джерел інформації, враховувати поведінкові особливості клієнтів та інтегрувати мережевий аналіз у процедури оцінки ризиків.

Документ також містить огляд ризиків, пов'язаних із терористичною діяльністю у контексті Північної Ірландії, яка хоча й має значно менші масштаби порівняно з ісламістським тероризмом, однак продовжує розглядатися як потенційне джерело загроз через історичні зв'язки, географічну близькість та відносну свободу пересування в межах Спільної туристичної зони. Крім того, наведено перелік високоризикових юрисдикцій, які враховуються під час проведення оцінки ризиків та належної перевірки клієнтів. Особливу увагу приділено цільовим фінансовим санкціям ООН, які розглядаються як один із центральних міжнародних інструментів боротьби з фінансуванням тероризму. Документ наголошує, що суб'єкти фінансового моніторингу повинні аналізувати не лише формальні права власності, а й фактичний контроль над активами через довірених осіб, підконтрольні компанії та інші непрямі механізми впливу.

Найбільшу практичну цінність документа становить детальний опис п'ятнадцяти типологій фінансування тероризму, адаптованих до особливостей міжнародного фінансового центру. Серед них розглядаються схеми обходу санкцій через використання бізнес-партнерів та членів сім'ї, використання благодійних організацій для переказу коштів до зон конфлікту, ризики, пов'язані з родичами політично значущих осіб, складні ланцюги фінансування через мережі неприбуткових організацій, використання пожертв для придбання нерухомості, приховування контролю над компаніями після накладення санкцій, приховування географічного походження коштів через сусідні юрисдикції, використання онлайн-покеру для передачі коштів між учасниками терористичних мереж, придбання нерухомості через осіб, пов'язаних із терористичними організаціями, використання юридичних та бухгалтерських посередників для створення складних багаторівневих структур, рахунки осіб, які перебувають під слідством щодо фінансування тероризму, використання рахунків онлайн-гемблінгу особами із санкційних списків, застосування мереж Hawala для транскордонного переміщення коштів, фінансування через транзакції, пов'язані з турецько-сирійським маршрутом, а також фінансування поїздок до зон бойових дій з метою участі у збройних формуваннях або проходження військової підготовки. Для кожної типології наведено конкретні індикатори ризику, які можуть бути інтегровані в системи фінансового моніторингу, включаючи нетипову поведінку клієнтів, підозрілі

Висновки:

- **Перевірка лише санкційних списків уже є недостатньою.** Необхідно впроваджувати аналіз пов'язаних осіб, членів сім'ї, довірених представників, корпоративних зв'язків та фактичного контролю активів для виявлення схем обходу санкцій через підставних осіб.
- **Неприбутковий сектор залишається одним із ключових каналів ризику фінансування тероризму.** Особливу увагу слід приділяти готівковим пожертвам, багаторівневим схемам грантового фінансування, використанню особистих рахунків посередників та транзакціям до зон конфліктів.
- **Онлайн-гемблінг, криптоактиви та неофіційні системи переказів створюють нові можливості для прихованого переміщення коштів.** Суб'єктам фінансового моніторингу доцільно розвивати спеціалізовані сценарії моніторингу для виявлення нетипової ігрової поведінки, криптовалютних переказів та ознак використання мереж Hawala.
- **Ефективне виявлення фінансування тероризму потребує поєднання фінансового моніторингу, OSINT, аналізу поведінкових ознак та міжнародного обміну інформацією.** Багато наведених кейсів були ідентифіковані лише після зіставлення транзакційних даних із розвідувальною інформацією, санкційними даними та відкритими джерелами.

транзакційні моделі, невідповідність джерел доходів, використання високоризикових юрисдикцій, наявність зв'язків із санкційними особами та ознаки фактичного контролю над активами.

Загальний висновок документа полягає у тому, що сучасне фінансування тероризму дедалі більше спирається на використання легальних фінансових інструментів, цифрових платформ, міжнародних фінансових послуг та складних мереж посередників. Тому ефективна протидія таким загрозам потребує не лише формального виконання процедур належної перевірки клієнтів, а й активного використання ризик-орієнтованого підходу, аналізу відкритих джерел інформації, санкційного скринінгу, мережевого аналізу, міжнародного обміну інформацією та постійної взаємодії між фінансовим сектором, фінансовою розвідкою і правоохоронними органами. Документ фактично демонструє сучасне бачення фінансування тероризму як складного багатовимірного явища, для виявлення якого необхідно аналізувати не лише окремі фінансові операції, а й ширший контекст поведінки клієнтів, їхніх зв'язків, корпоративних структур та міжнародних фінансових потоків.

Регулювання

Інформаційний бюлетень FinCEN щодо зміни Розділу 314(b) Закону PATRIOT [7]

Оновлення нормативної бази у сфері протидії фінансовим злочинам сигналізує про перехід американського регулятора до значно агресивнішої та технологічнішої стратегії. Мережа боротьби з фінансовими злочинами США (FinCEN) оприлюднила оновлений інформаційний бюлетень (Fact Sheet), який регулює Розділ 314(b) Закону США PATRIOT (USA PATRIOT Act). Цей документ повністю замінює попередню редакцію від грудня 2020 року, яка роками змушувала відповідальних працівників балансувати між ризиком пропустити відмивання коштів та страхом отримати судовий позов за розголошення банківської таємниці.

Головне завдання обох документів – регулювання механізму «безпечної гавані» (safe harbor). Це правовий імунітет, який звільняє фінансові установи від цивільної відповідальності за порушення конфіденційності, якщо вони добровільно діляться даними про клієнтів для виявлення фінансових злочинів.

Однак, якщо версія 2020 року залишала занадто багато «сірих зон», змушуючи банки діяти надмірно обережно, то редакція 2026 року ліквідує колишні двозначності та суттєво розширює межі дозволеного обміну.

Критерій порівняння	Редакція 2020 року	Нова редакція 2026 року
Головний фокус (злочини)	Відмивання коштів та фінансування тероризму	Офіційно включено всі види шахрайства
Швидкість взаємодії	Обмежена класичними паперовими та електронними запитами	Дозволено оперативний обмін у реальному часі

[7] https://www.fincen.gov/system/files/2026-06/314bfactsheet-12-2020.pdf

Критерій порівняння	Редакція 2020 року	Нова редакція 2026 року
Клієнтські відносини	Обмін переважно в межах наявних спільних клієнтів	Дозволено обмін за відсутності ділових відносин
Спектр дозволених даних	Лише класична транзакційна та фінансова інформація	Розширено на кібердані, геолокацію та ідентифікатори пристроїв

Включення шахрайства до переліку підстав для взаємодії стало головним рушієм змін. Раніше банки часто вагалися, чи мають вони право сигналізувати колегам про підозрілі операції, якщо йшлося про звичайне електронне або поштове шахрайство, а не про класичне відмивання кримінальних доходів. Тепер FinCEN знімає ці сумніви: для активації захисту безпечної гавані достатньо мати лише обґрунтовану підозру на шахрайські дії.

Паралельно регулятор зняв часові та технічні бар'єри, дозволивши фінансовим установам обмінюватися даними в реальному часі за допомогою будь-яких зручних каналів зв'язку – від захищених месенджерів до усних телефонних дзвінків безпосередньо під час проведення транзакції. Ба більше, банки отримали право передавати інформацію про фігурантів навіть тим установам, які не мають із цими особами жодних ділових відносин. Це дозволяє фінансовому сектору діяти превентивно, наприклад, на етапі відкриття рахунків новим потенційним клієнтам.

Еволюціонував і сам характер інформації. Сучасна боротьба з правопорушеннями вимагає цифрових доказів, тому FinCEN офіційно дозволив ділитися IP-адресами, ідентифікаторами пристроїв (Device ID), геолокаційними мітками та навіть відеозаписами з камер спостереження. Закон про банківську таємницю (BSA) більше не обмежує передачу персональних даних (PII) у межах цієї програми.

Попри значну лібералізацію процедур, регулятор зберіг ключові запобіжники для уникнення зловживань та витоку інформації:

- **Таємниця звітів SAR:** Фінансовим установам досі суворо заборонено обмінюватися безпосередньо Звітами про підозрілу діяльність (SARs) або розкривати факт їхнього існування, за винятком випадків підготовки спільних звітів (Joint SAR).
- **Юрисдикція імунітету:** Банки можуть передавати інформацію своїм іноземними філіям для внутрішнього аналізу ризиків, проте юридичний захист «безпечної гавані» від FinCEN не поширюється на іноземні юридичні особи поза межами США.

Оновлений інформаційний бюлетень свідчить про намір регулятора остаточно зруйнувати інформаційні бар'єри всередині фінансової системи. Нові правила трансформують Розділ 314(b) з пасивного інструменту аналізу минулих подій на динамічну зброю проти кіберзлочинності, яка дозволяє блокувати виведення коштів безпосередньо в момент атаки.

Звіти окремих інституцій та експертів

Нова архітектура цифрової довіри: 101 реальний кейс застосування блокчейну у світовій економіці [8]

Посібник, підготовлений Глобальною радою бізнесу у сфері блокчейну (GBBC), є одним із найбільш комплексних міжнародних оглядів сучасного практичного застосування технологій блокчейну та розподілених реєстрів у реальній економіці. Документ об'єднує 101 приклад використання блокчейну, реалізований державними органами, міжнародними організаціями, фінансовими установами, технологічними компаніями, науковими центрами та громадськими організаціями у різних юрисдикціях світу. Основною метою посібника є демонстрація того, що блокчейн у 2026 році вже не є виключно технологією криптовалют чи спекулятивних цифрових активів, а поступово перетворюється на фундаментальну інфраструктуру цифрової довіри, яка використовується для підтвердження даних, управління активами, забезпечення прозорості, автоматизації процесів та координації взаємодії між великою кількістю незалежних учасників.

Документ показує, що розвиток блокчейн-екосистеми відбувається одночасно у декількох стратегічних напрямах. Перший із них пов'язаний із токенізацією реальних активів, яка розглядається як один із головних драйверів розвитку цифрової економіки. Автори демонструють численні приклади, коли фізичні активи або економічні права перетворюються на цифрові токени, які можуть вільно передаватися, обліковуватися та використовуватися в глобальній фінансовій інфраструктурі. Особливу увагу привертають рішення у сфері дорогоцінних металів. Зокрема, NatGold пропонує нову концепцію цифрового представлення вартості золота без його фізичного видобутку. У межах цієї моделі підтверджені запаси золота залишаються в надрах, тоді як їхня економічна вартість відображається через токени, випущені на блокчейні Ethereum. Такий підхід покликаний одночасно забезпечити інвесторам доступ до золота як до інвестиційного активу та мінімізувати екологічні наслідки традиційного гірничого виробництва. Паралельно представлений кейс Tether Gold демонструє інший підхід до токенізації, за якого кожен цифровий токен забезпечений конкретним злитком фізичного золота, що зберігається у сховищі та може бути ідентифікований за серійним номером. Таким чином блокчейн використовується для створення нового покоління фінансових інструментів, які поєднують традиційні активи з перевагами цифрової інфраструктури.

Одним із найбільш розвинених напрямів застосування блокчейну, представлених у посібнику, є енергетика. Автори демонструють трансформацію традиційної моделі централізованого виробництва та розподілу електроенергії у бік децентралізованих енергетичних спільнот. Приклад енергетичного кооперативу на острові Ameland у Нідерландах показує, як токенізація може використовуватися для колективного володіння сонячними електростанціями та організації взаємного обміну електроенергією між учасниками спільноти. Блокчейн забезпечує облік прав власності, розрахунок виробленої енергії та автоматизоване виконання правил розподілу через смарт-контракти. Водночас модель управління реалізована через децентралізовану автономну організацію (DAO), що дозволяє учасникам безпосередньо брати участь у прийнятті рішень. Подібні рішення доповнюються кейсами OpenGrid та Blockchain for Energy, які демонструють створення спільних цифрових платформ для енергетичних компаній, управління даними про викиди, верифікації енергетичних операцій та організації ринків обміну енергією між виробниками і споживачами.

8 https://assets.ctfassets.net/so75yocayyva/6zZVoaxLnwsCAgbOyRp5tu/b4ae4dea7553aea4781dab18310357bd/Handbook__2026__digital.pdf

Важливий блок кейсів присвячений сільському господарству та ланцюгам постачання. У цих прикладах блокчейн використовується як інструмент забезпечення наскрізної простежуваності продукції від первинного виробника до кінцевого споживача. Особливу увагу приділено проблемі фрагментованості інформації та відсутності довіри до походження продукції. Рішення CattleProof Verified формує для кожної тварини унікальний цифровий запис, який містить перевірену інформацію про її походження, переміщення та інформацію протягом усього життєвого циклу. Такий підхід сприяє запобіганню шахрайству, підвищенню прозорості операцій на ринку тваринництва, спрощує контроль за дотриманням ветеринарно-санітарних вимог і створює передумови для розвитку цифрових ринків сільськогосподарських тварин. Водночас система AgroTrack забезпечує наскрізну простежуваність молочної продукції – від збору даних про ферму, ідентифікації тварин, проведення вакцинації та моніторингу стану здоров'я до етапів транспортування, переробки молока та виробництва кінцевої продукції. Фіксація інформації на кожному етапі в блокчейні гарантує її незмінність, достовірність і можливість незалежної перевірки з боку регуляторних органів, учасників ринку та кінцевих споживачів. Загалом такі рішення демонструють значний потенціал блокчейн-технологій для підвищення прозорості, підзвітності та довіри у глобальних продовольчих ланцюгах постачання.

Висновки:

- **Токенізація реальних активів переходить до стадії практичного впровадження.** Блокчейн дедалі активніше використовується для цифрового представлення золота, енергетичних активів, вуглецевих кредитів, сільськогосподарської продукції та інших реальних активів, формуючи нові ринки реальних активів (RWA) з вищою ліквідністю та прозорістю.
- **Блокчейн стає базовою інфраструктурою для простежуваності та верифікації даних.** Найбільший практичний ефект спостерігається у сферах ланцюгів постачання, аграрного виробництва, звітності зі сталого розвитку, вуглецевих ринків та екологічних проєктів, де ключове значення мають прозорість інформації, можливість її перевірки та захист від несанкціонованих змін.
- **Інтеграція AI та блокчейну формує нове покоління комплаєнс-рішень.** Кейси Elliptic та NVNM Chain свідчать про формування нового покоління технологічних рішень, які поєднують можливості штучного інтелекту та блокчейну для автоматизації процедур комплаєнсу, управління ризиками, виявлення підозрілих операцій та забезпечення прозорості рішень автономних систем, що відкриває нові можливості для підвищення ефективності механізмів ПВК/ФТ і діяльності органів нагляду.
- **Для державних органів та регуляторів ключовою цінністю блокчейну стає не криптовалюта, а цифрова довіра.** Практичні кейси показують, що найбільший ефект досягається через використання блокчейну як інструменту забезпечення прозорості, підзвітності, автоматизованого контролю та міжвідомчого обміну перевіреними даними.

Значну частину посібника займають кейси, присвячені кліматичним ініціативам, ринкам вуглецевих кредитів та фінансуванню екологічних проєктів. Автори підкреслюють, що однією з головних проблем сучасних екологічних ринків є відсутність довіри до даних про екологічний ефект, ризики подвійного обліку та складність перевірки заявлених результатів. Саме тому блокчейн дедалі активніше використовується як інструмент створення перевірюваних екологічних реєстрів. У цьому контексті розглядаються проєкти Carbonmark, EcoRegistry та Klima Protocol, які створюють інфраструктуру для токенізації, торгівлі, погашення та оцінки вуглецевих кредитів. Особливий акцент робиться на інтеграції якісних

характеристик екологічних активів безпосередньо в структуру цифрових токенів, що дозволяє інвесторам та покупцям оцінювати не лише кількість скорочених викидів, але й додаткові екологічні та соціальні ефекти проєктів.

Показовими є також приклади використання блокчейну для підтримки біорізноманіття та захисту природних екосистем. Проєкт Biocultural Jaguar Credit демонструє модель, у якій блокчейн поєднує екологічні ринки із традиційними знаннями корінних народів Амазонії. Через цифрові екологічні кредити створюється механізм фінансування захисту середовища існування ягуарів та підтримки громад, які історично займаються охороною цих територій. Інший приклад – Biodiversity Blocks від Seatrees – демонструє застосування блокчейну для формування ринку кредитів біорізноманіття, кошти від реалізації яких спрямовуються на фінансування проєктів із захисту, відновлення та довгострокового моніторингу морських екосистем. Блокчейн у цьому випадку забезпечує повний цикл реєстрації, моніторингу та підтвердження екологічних результатів, а також створює механізми прозорого звітування для донорів та інвесторів.

Окремий блок документу присвячений взаємодії блокчейну та штучного інтелекту. Автори зазначають, що поширення генеративного AI створює нові виклики щодо прозорості, підзвітності та довіри до автоматизованих рішень. Саме тому блокчейн дедалі частіше використовується як незалежний механізм фіксації дій штучного інтелекту. Одним із найяскравіших прикладів є NVNM Chain, який створює криптографічно підтверджений журнал дій автономних агентів через механізми Proof of Origin, Proof of Process та Proof of State. Це дозволяє відстежувати походження даних, алгоритми їх обробки та контекст прийняття рішень без необхідності розкривати самі дані. Така модель розглядається як потенційна основа для майбутнього регулювання штучного інтелекту, фінансових сервісів та цифрових ринків.

Для сфери ПВК/ФТ особливий інтерес становить кейс Elliptic Copilot, який демонструє практичну інтеграцію штучного інтелекту у процеси аналізу ризиків криптоактивів. Система автоматично аналізує результати блокчейн-аналітики, визначає джерела ризиків, формує пояснення щодо ризикових транзакцій, відображає зв'язки між суб'єктами та допомагає готувати матеріали для подання повідомлень про підозрілу діяльність. Використання такого підходу дозволяє суттєво скоротити навантаження на аналітиків та підвищити ефективність процедур комплаєнсу, що особливо актуально в умовах стрімкого зростання обсягів цифрових активів та кількості транзакцій.

Загалом посібник формує цілісне уявлення про те, що блокчейн поступово перетворюється на універсальний інфраструктурний рівень цифрової економіки. Практично всі представлені кейси демонструють однакову закономірність: головна цінність блокчейну полягає не у створенні нових форм цифрових активів як таких, а у можливості забезпечити незмінність даних, прозорість взаємодії між незалежними учасниками, автоматизацію виконання правил через смарт-контракти та створення середовища цифрової довіри. Саме ці властивості дозволяють використовувати блокчейн для модернізації фінансових ринків, енергетики, державного управління, екологічних програм, міжнародної торгівлі, систем комплаєнсу та механізмів верифікації інформації, що робить його одним із ключових технологічних інструментів цифрової трансформації наступного десятиліття.

Військовий терор як інструмент утримання влади [9]

Документ, підготовлений організацією Defiende Venezuela у співпраці з InSight Crime, є ґрунтовним розслідуванням військової операції венесуельського уряду під кодовою назвою «Zaraza 2024». Цей матеріал не просто фіксує окремі випадки насильства, а викриває глибоку

[9] https://insightcrime.org/wp-content/uploads/2026/06/Human-Rights-Violations-During-Operation-Zaraza-2024.pdf

системну кризу, в якій державні інституції, замість захисту населення, виступають інструментом терору та репресій.

Операція, розпочата як відповідь на інцидент із бойовиками угруповання «Tren del Llano», швидко перетворилася на масштабну каральну акцію проти цивільного населення, що мешкає у сільських районах штатів Гуаріко, Міранда та Апуре. Хоча формальною метою було послаблення контролю злочинної групи, фактичні дії урядових сил засвідчують намір залякати та підкорити цілі громади, використовуючи методи, які за своєю жорстокістю нагадують воєнні злочини.

Особливе занепокоєння викликає те, що операція «Zaraza» не є ізольованим випадком. Автори доповіді проводять паралель із попередньою операцією «Грім» (Operación Trueno), що проходила у 2022-2023 роках в Альтаграсія-де-Орутуко, де також були задокументовані незаконні обшуки, тортури, сексуальне насильство та примусові зникнення. Це свідчить про усталену практику та своєрідний «прецедент», коли військові та спецслужби діють поза правовим полем, а будь-який спротив або навіть просто проживання на «небезпечній» території стає підставою для репресій. Така спадкоємність порушень вказує на те, що ми маємо справу не з ексцесами окремих виконавців, а з частиною державної політики, спрямованої на утримання влади через страх та насильство.

Хронологія подій, описана у звіті, вражає своєю цинічністю та зухвалістю. Поштовхом до початку широкомасштабних дій став епізод у Сан-Франсіско-де-Макайра, де члени «Tren del Llano» оточили та роззброїли військовослужбовців на виборчій дільниці. Цей інцидент, що стався після спірних президентських виборів у липні 2024 року, був використаний як привід для демонстрації сили. Уряд не обрав шлях поліцейської операції чи переговорів, а натомість розгорнув понад 6000 військових, авіацію та важку техніку. Така непропорційна відповідь – класична ознака того, що влада розглядає будь-який виклик своєму авторитету, навіть з боку злочинних угруповань, як загрозу власному існуванню, що потребує найжорсткішого придушення.

Кульмінацією цієї ескалації став авіаудар 13 серпня 2024 року по сільських громадах Бока-де-Марія, Бока-де-Парія та Ель-Хобіто у муніципалітеті Асеведо штату Міранда. Використання винищувачів Су-30 для бомбардування цивільних об’єктів – ферм, невеликих будинків і городів – є актом відвертої агресії проти мирного населення. Попередні обльоти розвідувальної авіації, а згодом і саме бомбардування, завдали шкоди не лише фізичному здоров’ю людей, а й їхній психіці. Поранення семи осіб, включно з 15-річним підлітком – це лише вершина айсберга. Свідки розповідають про жах та паніку, що охопили мешканців, які опинилися під бомбами без жодного попередження чи можливості евакуюватися. Це не просто порушення права на життя та особисту недоторканність, це акт тероризму в цілому регіоні, покликаний змусити людей втікати з власних домівок.

Подальші наземні операції, які розпочалися після авіаударів, були не менш жорстокими та системними. Документ фіксує цілий спектр порушень, які перетворили життя сільських громад на пекло. Несанкціоновані обшуки, які проводилися переважно вночі, стали засобом залякування та деморалізації населення. Арешти здійснювалися без ордерів та без доказів скоєння злочину, що вказує на їхню політичну та залякуючу природу. Особливо кричущим є використання тортур, зокрема електрошокерів та жорстоких побиттів, із метою вибити зізнання у неіснуючих злочинах. Це повертає нас до темних практик тоталітарних режимів, де судова система перетворюється на інструмент розправи, а зізнання, отримане під тортурами, стає єдиним доказом.

Право на здоров’я було грубо порушено через свідому відмову влади надавати медичну допомогу постраждалим. Люди, поранені внаслідок бомбардувань, залишалися без допомоги, а доступ до медичних послуг був ускладнений або заблокований. Така поведінка влади є не просто недбалістю, а частиною стратегії, спрямованої на те, щоб залишити жертв без будь-якої підтримки та змусити їх залишити свої домівки. Факти примусового переміщення, коли цілі сім’ї покидали все майно через страх репресій та регулярні військові блокпости, свідчать

про навмисне створення атмосфери терору, яка робить неможливим нормальне життя в цих регіонах. Знищення врожаїв, худоби та завдана шкода навколишньому середовищу додатково підривають економічну базу цих громад, фактично прирікаючи їх на вимирання.

Одним із найтривожніших аспектів цього розслідування є повна бездіяльність судової системи Венесуели. Генеральна прокуратура, яка мала б розслідувати скарги та притягати винних до відповідальності, не вжила жодних заходів. Відсутність незалежних, неупереджених та ретельних розслідувань, незважаючи на серйозність задокументованих злочинів, створює ситуацію повної безкарності. Судді, своєю чергою, стали співучасниками репресій, ухвалюючи вироки на підставі сфабрикованих доказів та позбавляючи затриманих права на захист. Таке зрощення виконавчої та судової влади перетворює державу на структуру, яка діє поза законом, що є прямою загрозою основам правової держави.

Відповідальність за ці злочини, як зазначається у звіті, лежить не лише на безпосередніх виконавцях, а й на вищому командуванні. Стратегічне оперативне командування Збройних сил (CEOFANB), яке планувало, координувало та публічно підтримувало військові дії, несе пряму відповідальність як організатор системних порушень. Військова авіація (AMB), підрозділи швидкого реагування (URRA), розвідка (SEBIN) та регіональні командування (REDI та ZODI) – кожен відіграв свою роль у механізмі насильства. Той факт, що після нещодавніх кадрових змін у вищих військових колах більшість безпосередніх винуватців залишаються на своїх посадах, свідчить про те, що влада не має наміру змінювати свою політику і розглядає ці репресії як ефективний інструмент контролю.

Висновки:

- **Венесуельська держава застосувала військову авіацію** та важке озброєння для бомбардування цивільних громад, що є актом непропорційного застосування сили та може кваліфікуватися як воєнний злочин.
- **Систематичне застосування тортур**, електрошоків, незаконних арештів та зникнень свідчить про усталену практику репресій, спрямовану на залякування всього населення, а не на боротьбу зі злочинністю.
- **Судова система Венесуели повністю провалила свої функції**, відмовившись розслідувати скарги жертв, і фактично легітимізувала безкарність військових та спецслужб, які продовжують свої операції без жодних наслідків.
- **Міжнародна спільнота залишається чи не єдиним механізмом стримування**, оскільки національні інституції не здатні або не бажають притягати винних до відповідальності.

Рекомендації, запропоновані Defiende Venezuela, є не просто технічним переліком побажань, а дорожньою картою для відновлення мінімального правопорядку та справедливості. Вони вимагають незалежного розслідування всіх подій, притягнення до відповідальності командирів, негайного припинення насильства та повноцінної компенсації жертвам.

Особливої уваги заслуговує вимога переглянути кримінальні справи заарештованих та виключити докази, отримані під тортурами. Це ключовий пункт, оскільки він безпосередньо впливає на долю людей, які вже відбувають тривалі терміни за сфабрикованими звинуваченнями. Крім того, рекомендації спрямовані на реформування самих операційних протоколів для запобігання подібним злочинам у майбутньому, що передбачає встановлення дієвого цивільного та судового контролю над збройними силами.

На завершення, цей аналітичний документ є вагомим доказом того, що венесуельська держава системно порушує права людини, використовуючи військову силу проти власного населення. Операція «Zaraza 2024» постає не як боротьба зі злочинністю, а як широкомасштабна акція залякування, що супроводжується воєнними злочинами та злочинами проти людяності. Безкарність виконавців та їхніх командирів, підтримана мовчанкою судової системи, створює небезпечний прецедент, який може призвести до ще більш масштабних трагедій у

майбутньому. Міжнародна спільнота, включаючи механізми захисту прав людини та окремі держави, має продовжувати моніторинг ситуації, тиснути на владу Венесуели з метою проведення прозорих розслідувань та сприяти процесам встановлення істини, справедливості та виплати репарацій. Без цього тиску та міжнародної солідарності з жертвами режим і надалі зможе з нехтуванням ставитися до найелементарніших прав своїх громадян, перетворюючи окремі регіони країни на зони беззаконня та постійного терору.

Чому глобальна співпраця у боротьбі з організованою злочинністю не виправдала очікувань [10]

Світ, у якому ми живемо, зазнає фундаментальних змін, що переосмислюють природу та масштаби організованої злочинності, а також ефективність міжнародних механізмів протидії їй. Звіт Глобальної ініціативи проти транснаціональної організованої злочинності (GI-TOC), пропонує глибокий аналіз сучасного стану боротьби з організованою злочинністю в умовах безпрецедентних геополітичних зрушень. Цей документ не просто констатує наявні проблеми, але й пропонує концептуальне переосмислення стратегій, необхідних для ефективного протистояння злочинності, яка стала невід'ємною частиною повсякденного життя мільярдів людей.

Протягом останніх трьох десятиліть міжнародна спільнота створила доволі комплексну нормативну базу для боротьби з організованою злочинністю. Конвенція ООН проти транснаціональної організованої злочинності (UNTOC), ухвалена в 2000 році, стала кульмінацією багаторічних зусиль із гармонізації національних законодавств, посилення уваги до відмивання грошей та інших механізмів функціонування злочинних угруповань. Однак, як слушно зазначається в доповіді, цей нормативний базис не був підкріплений єдиною стратегічною реалізацією. Натомість організована злочинність, незаконні ринки та геополітичне середовище змінилися до невпізнання, створивши принципово нову реальність, яка вимагає адекватних відповідей.

Ключова теза доповіді полягає в тому, що організована злочинність більше не обмежується темними кутками вулиць чи діяльністю класичних мафіозних структур, які домінували в дискурсі 1990-х років. Сьогодні злочинність пронизує всі аспекти нашого життя: від смартфонів у наших кишенях, які стали потенційними порталами у світ наркотиків, шахрайства та торгівлі людьми, до глобальних ланцюгів постачання, корумпованих систем управління та викривлених правових систем. Це явище набуло характеру системної загрози, яка потребує не менш системної відповіді.

Особливо показовим є те, що найвпливовішими суб'єктами в сучасній злочинній екосистемі є не класичні мафіозні угруповання, а державні інституції та їхні представники – міністри, бюрократи, місцеві політики, працівники правоохоронних органів. Цей факт фактично перевертає основну концепцію UNTOC 2000 року, яка була зосереджена на протидії злочинним угрупованням як автономним структурам, а не на системній корупції в самих державних інституціях. Такий зсув має серйозні наслідки для фундаментальних понять верховенства права та належного врядування, адже коли сама держава стає частиною злочинної екосистеми, традиційні механізми протидії втрачають свою ефективність.

Багатовекторна система, яка теоретично має забезпечувати комплексну протидію організованій злочинності, переживає глибоку кризу. У доповіді виокремлюються три основні причини цього: нездатність адаптуватися до швидких змін, недостатня ефективність та внутрішня дисфункціональність. Установи, створені для боротьби зі злочинністю минулого століття, виявилися неготовими до викликів сучасності. Наприклад, UNTOC була створена для протидії мафіозним структурам, а не тому багатошаровому злочинному світу, який ми

[10] https://globalinitiative.net/wp-content/uploads/2026/06/Prisoners-dilemma-Responding-to-organized-crime-in-a-new-world-GI-TOC-June-2026.pdf

спостерігаємо сьогодні. Світова митна організація вже ледь справлялася з обсягом контейнерних перевезень, а тепер стикається з новим викликом у вигляді використання кур'єрських служб та поштових систем для переміщення наркотиків, об’єктів дикої природи та зброї.

Водночас FATF (Група з розробки фінансових заходів боротьби з відмиванням грошей) стикається з критикою щодо неефективності своїх стандартів, адже відмивання грошей продовжує процвітати, незважаючи на зростаючий тягар комплаєнс-вимог. Криптовалюти та система «хавала» ускладнили традиційні зусилля з протидії відмиванню грошей, а регулювання технологій часто відстає від реального розвитку подій. Система ООН стала повільною, внутрішньо фрагментованою та недофінансованою, а консенсусу держав-членів стає дедалі важче досягти. Показовим є приклад сесій Комісії ООН з наркотичних засобів у березні 2026 року, де жодна резолюція не досягла консенсусу, що свідчить про зростаючі політичні розбіжності.

У відповідь на цю кризу з'являються нові форми співпраці – так звані «гнучкі» коаліції, які пропонують більш сфокусовані підходи до конкретних проблем. Прикладом може слугувати партнерство ЄС із країнами Асоціації держав Південно-Східної Азії для протидії скам-центрам, оголошене у квітні 2026 року. Однак такі підходи несуть ризик політизації відповідей на злочинність, перетворення правоохоронних органів на інструмент проекції сили, геополітичного суперництва та економічної вигоди. Попри всі недоліки, глобальні норми та глобальний форум залишаються критично необхідними, а UNTOC, незважаючи на всі компроміси, залишається маяком консенсусу щодо нагальної потреби боротьби зі злочинністю.

Однією з найбільш тривожних тенденцій останніх років є перехід багатьох держав до жорстких, часто мілітаризованих заходів протидії злочинності, що супроводжується недостатньою увагою до першопричин та системних факторів. Президент США Дональд Трамп значно збільшив ресурси Імміграційної та митної поліції (ICE) – з менш ніж 6 мільярдів доларів у 2016 році до 85 мільярдів у 2026 році, що перевищує сукупний бюджет усіх інших федеральних правоохоронних органів. Жорсткі прикордонні заходи набувають популярності в Латинській Америці, зокрема новообраний президент Чилі Хосе Антоніо Каст пообіцяв депортувати понад 330 000 нерегулярних мігрантів і побудувати прикордонний бар'єр у трьох північних регіонах країни.

Особливо показовим є випадок Сальвадору, де президент Наїб Букеле запровадив надзвичайно жорсткі заходи проти банд. Хоча цей підхід мав певний успіх у зниженні рівня насильства, його конституційна легітимність викликає серйозні сумніви. Майже 1,7% населення країни перебуває у в'язницях – найвищий показник у світі, а довгі терміни ув'язнення, які отримують члени банд, означають, що багато хто ніколи не повернеться на свободу, що створює колосальне навантаження на пенітенціарну систему. Досвід інших країн, які застосовували політику «mano dura» (твердої руки), таких як Мексика, Гондурас та Бразилія, свідчить про те, що організована злочинність зазвичай відновлює свої позиції після періоду загострення. Крім того, такі підходи часто супроводжуються порушеннями прав людини, а відсутність громадянського нагляду створює ризик безконтрольного зростання державних зловживань.

Водночас зусилля, спрямовані на усунення першопричин організованої злочинності – широке соціально-економічне зростання, боротьба зі зміною клімату, соціальна згуртованість, врегулювання конфліктів та протидія корупції – зазнають скорочення через кризу вартості життя та переорієнтацію політичної уваги на безпекові питання. Автори доповіді наголошують на необхідності змінити спосіб комунікації: замість технократичних пояснень причин та тенденцій, потрібно надавати чіткі дані та повідомлення, які резонують із поточними настроями суспільства. Необхідно довести, що стратегічна боротьба з організованою злочинністю у співпраці з міжнародними партнерами принесе кращі результати, ніж будівництво стін або погоня за легкою статистикою.

Одним із найбільш тривалих викликів у боротьбі з організованою злочинністю залишаються системні вразливості правових та регуляторних систем, які дозволяють злочинцям діяти безкарно. Глобальна фінансова система з її податковими гаванями, офшорними трастами, компаніями-оболонками та іншими інструментами десятиліттями використовується для переміщення та приховування брудних грошей. Особливі економічні зони в деяких випадках перетворилися на беззаконні простори, де процвітають кіберзлочинність, скам-центри, торгівля людьми, ухилення від оподаткування, фінансове шахрайство, контрабанда та виробництво контрафактних товарів. «Зручні прапори», які використовуються як прикриття для всього – від незаконного рибальства та торгівлі людьми до контрабанди наркотиків, зброї, готівки та санкційних товарів, – залишаються проблемою, про яку говорять щонайменше з 1948 року, а тепер ще й дали початок так званому «тіньовому флоту», який є ключовим інструментом для обходу санкцій.

У сфері технологій зростає занепокоєння щодо ролі технологічних гігантів та їхніх платформ як посередників у злочинній діяльності. Незважаючи на величезну кількість незаконного контенту, який можна знайти на таких платформах, як Meta, YouTube, TikTok та Telegram, зусилля щодо підвищення їхньої підзвітності довго зустрічали опір. У США компанії соціальних медіа не несуть відповідальності за контент, який вони розміщують, згідно з сумнозвісним Розділом 230. Telegram, який часто називають «темною мережею у вашій кишені», став особливо відомим через розміщення незаконного контенту та відмову від саморегулювання. Однак нещодавні судові рішення проти Meta та Google, засновані на дизайні платформ, а не на контенті, можуть стати моделлю для протидії злочинній діяльності на платформах соціальних медіа.

Однією з найбільш тривожних тенденцій, описаних у доповіді, є зростаюче використання злочинних методів деякими державами, як правило, під час важких санкцій та політичного та економічного тиску. Північна Корея десятиліттями лідирує в такій діяльності через державний Офіс 39, який відповідає за збір іноземної валюти різноманітними засобами, включаючи браконьєрство, хакерство та виробництво метамфетаміну. Іран використовує різноманітні злочинні засоби для ухилення від санкцій і постачання своїх проксі-мереж на Близькому Сході, включаючи торгівлю наркотиками, контрабанду зброї, кіберзлочинність та відмивання грошей. Російська федерація, через Wagner Group та інші структури, використовує злочинні методи для проектування впливу в Африці та Сирії, а після повномасштабного вторгнення в Україну також здійснює кампанії саботажу та замахів у Європі.

Автори доповіді використовують термін «геокримінальність» для позначення цього явища, коли злочинність стає визнаним важелем державної влади – нарівні з дипломатією, розвідкою, економікою та інформаційними операціями. Включення держав у злочинну діяльність може мати серйозні структурні наслідки для функціонування як організованої злочинності, так і самої держави. Відповідь на це явище надзвичайно складна, не в останню чергу через зростаючу складність міжнародної співпраці. Багатополярність світу відроджує ідею сфер впливу, де сильні держави можуть просувати власні цінності понад глобальні норми управління. Важливим є питання, де розмістити відповіді на геокримінальність у структурі держави – між питаннями внутрішньої правоохоронної діяльності та державними загрозами виникає плутанина щодо правильної відповіді. У майбутньому може статися так, що розмежування між правоохоронними органами та розвідкою по суті зникне, оскільки злочинні практики стають все більш інтегрованими в інструментарій держав.

Одним із найпотужніших інструментів проти організованої злочинності є викриття. Поки злочинність процвітає в таємниці, мовчанні та страху, публічне обговорення виводить ці дії на світло, посилює розуміння та створює політичний тиск. Журналісти-розслідувачі часто прокладають шлях у розкритті внутрішньої роботи організованої злочинності, незважаючи на зростаючу загрозу судових переслідувань та часто складне фінансування, яке скорочує штат і іноді закриває новинні видання. Журналістика та громадянське суспільство в цілому стикаються з посиленням державного нагляду, репресій та використанням правових інструментів (таких як закони про «іноземних агентів»), до такої міри, що незалежні

дослідження та дії проти організованої злочинності в деяких країнах стають практично неможливими.

Водночас з'являються інноваційні підходи до подолання цих обмежень. Bellingcat, наприклад, використовує розвідку на основі відкритих джерел (OSINT) для відстеження злочинців та їхньої діяльності, частково надихнувши «золоте століття OSINT». Громадянська документалістика, яка набула розвитку під час невдалої Зеленої революції в Ірані в 2009 році, постійно зростає, забезпечуючи дослідників потоком даних у реальному часі. Штучний інтелект також стає ключовим інструментом для роботи з дедалі більшими обсягами даних та складністю, доступними для активістів з боротьби з корупцією. Однак екосистема журналістики переживає екзистенційну кризу – новини, орієнтовані на особистість, стають дедалі поширенішими, а зростаюча частка громадян отримує інформацію з соціальних медіа, де домінують наративи дезінформації.

Кіберзлочинність еволюціонувала з блискавичною швидкістю, оскільки штучний інтелект знизив технічні бар'єри входу: тепер можна створювати складні кібератаки без знання кодування. За даними CrowdStrike, атаки з використанням штучного інтелекту зросли на 89% у 2025 році порівняно з 2024 роком, а середній час проникнення – період між початковою атакою та ширшою експлуатацією на інших машинах – скоротився до 29 хвилин у 2025 році, що на 65% швидше, ніж попереднього року.

Висновки:

- **Глобальна система протидії організованій злочинності, виявилася неспроможною адаптуватися до стрімких змін** – інституції стали повільними, політизованими та неефективними, що змушує держави шукати альтернативні форми співпраці.
- **Організована злочинність більше не є суто кримінальним явищем** – вона глибоко вплетена в державні інституції, глобальні ланцюги постачання, цифрові платформи та фінансові потоки, а найвпливовішими злочинцями стали не класичні мафіозні структури, а корумповані чиновники та державні службовці.
- **Держави дедалі частіше використовують злочинні методи як інструмент зовнішньої політики** – феномен «геокримінальності» став системною загрозою, яка розмиває межі між правоохоронною діяльністю та розвідкою.
- **Жорсткі, мілітаризовані заходи, які набувають популярності в багатьох країнах, дають лише короткостроковий ефект**, супроводжуються масовими порушеннями прав людини та не усувають першопричин організованої злочинності.

Звіт завершується закликом до колективної дії та стратегічного переосмислення підходів до боротьби з організованою злочинністю.

У концепції теорії ігор «дилема в'язня» – найбільші винагороди досягаються через співпрацю, навіть якщо окремі особи спокушаються діяти егоїстично через перспективу особистої вигоди. Реакції на глобальну організовану злочинність сьогодні стикаються з подібною дилемою: спокуса діяти в односторонньому порядку може здаватися найшвидшим шляхом до успіху, але зрештою це не принесе найкращого загального результату.

У підсумку, доповідь наголошує, що подолання організованої злочинності вимагає співпраці між громадянами, державами, приватним сектором та громадянським суспільством. Якщо цей шлях не буде обрано, організована злочинність та незаконні ринки просто адаптуються.

Світ показав, що може швидко реагувати на кризи. Сьогодні необхідно принести те саме відчуття терміновості, уяви та амбіцій до глобальної кризи організованої злочинності, визнаючи, що справжні зміни можуть вимагати радикальних змін, забезпечуючи при цьому, щоб верховенство права та права людини залишалися в центрі наших відповідей.

Як цифрові активи змінюють світову злочинність [11]

За останні п'ять років глобальна екосистема цифрових активів зазнала феєричної трансформації. Звіт GI-TOC фіксує історичний момент: криптовалюти перестали бути екзотичним інструментом для «технарів» або спекулянтів і стали повноцінною фінансовою артерією, якою циркулюють капітали наркокартелів, мереж торгівлі людьми, кібершахраїв та навіть держав. Цей зсув є настільки фундаментальним, що ставить під сумнів саму ефективність класичної парадигми правоохоронної діяльності, де «слідування за грошима» було наріжним каменем протягом десятиліть, адже тепер гроші можуть зникати в цифровому тумані децентралізованих реєстрів так само швидко, як світло в чорній дірі.

Криптовалюти пропонують не просто альтернативний платіжний канал, а створюють принципово нову операційну реальність для злочинців. Швидкість транзакцій, яка вимірюється секундами, поєднується з транскордонністю, що робить неможливим застосування традиційних механізмів блокування активів на основі юрисдикції. Псевдонімність, яку часто помилково називають анонімністю, дозволяє створювати складні ланцюги переказів, де реальний власник коштів захований за десятками гаманців та транзакцій, кожен шар яких вимагає окремого розслідування. А зростаюча ліквідність ринків – як централізованих, так і децентралізованих – забезпечує можливість миттєвої конвертації цифрових активів у стейблкоіни, а згодом і в реальну фіатну валюту через численні обмінники та позабіржових брокерів.

Однак найбільш показовою є еволюція ролі криптовалют у структурі організованої злочинності – від допоміжного інструменту до критичної інфраструктури, без якої сучасні мережі просто не можуть функціонувати. Звіт наводить численні приклади, зокрема використання зашифрованих комунікаційних платформ типу Sky ECC, де криптовалюта була інтегрована безпосередньо в координацію наркотрафіку, дозволяючи одночасно і планувати маршрути поставок, і здійснювати миттєві розрахунки між постачальниками в різних країнах. Це свідчить про те, що цифрові активи стали своєрідним нервом злочинних операцій, який пов'язує воєдино логістику, комунікацію та фінанси.

На рівні фінансових функцій криптовалюти повністю трансформували процес легалізації коштів, створивши багатошарову екосистему, яка використовує регуляторні арбітражі між різними юрисдикціями. Централізовані біржі, де комплаєнс часто поступається місцем конкурентній боротьбі за клієнтів, виступають воротами між криптосвітом та регульованою банківською системою. Водночас децентралізовані біржі, крос-чейн мости та міксери дозволяють дробити транзакції до такої міри, що відновити первісне джерело коштів стає майже неможливо без залучення суперкомп'ютерів та місяців ручної аналітики.

Окремо варто зупинитися на феномені стейблкоїнів, які, за оцінками FATF, у 2025 році забезпечили більшу частину всього обсягу незаконних криптовалютних транзакцій. Їхня привабливість для злочинних мереж є очевидною: вони поєднують усі переваги криптовалют – швидкість, глобальність, непідконтрольність окремим центробанкам – з відсутністю волатильності, що дозволяє зберігати вартість активів навіть під час різких ринкових коливань. Це зробило USDT основною валютою для розрахунків між російськими олігархами, які намагаються обійти міжнародні санкції, для китайських мереж відмивання грошей, пов'язаних із фентаніловим трафіком, та для мексиканських картелів, які розраховуються з постачальниками хімічних прекурсорів.

Розширення криптовалютних ринків спричинило небачений раніше бум специфічних видів злочинів, які раніше були обмежені географією або масштабами. У сфері кібершахрайства криптовалюти стали основою для персоналізованих схем, де використання штучного

[11] https://globalinitiative.net/wp-content/uploads/2026/06/John-Collins-The-currency-of-global-crime-How-crypto-is-reshaping-illicit-economies-GI-TOC-June-2026.pdf

інтелекту підвищило прибутковість шахрайства у 4,5 раза. Зокрема, зростання на 1400% шахрайств з імітацією особи між 2024 та 2025 роками свідчить про те, що злочинці блискавично адаптують нові технології для обману жертв, які втрачають не просто заощадження, а часто й усе своє майно, переказуючи його в криптовалюті під впливом витончених психологічних маніпуляцій. Але найбільш системною загрозою стали так звані «скам-центри» у Південно-Східній Азії, зокрема в М'янмі, Камбоджі та Лаосі, де на територіях зі слабким управлінням та корупцією діють цілі міста, що спеціалізуються на шахрайстві та фішингу.

Однак найбільш загрозливим виміром криптореволюції, який детально аналізується у звіті, є конвергенція організованої злочинності з державами. 2025 рік став переломним, оскільки обсяг незаконних транзакцій досяг рекордних 154 мільярдів доларів, і це зростання на 694% було забезпечено переважно діяльністю підсанкційних суб'єктів. Північна Корея продемонструвала «найуспішніший» рік, перевищивши позначку у 2 мільярди доларів, які були спрямовані на фінансування програм розробки зброї масового знищення. Викрадення 1,5 мільярда доларів з біржі Bybit, яке широко приписують північнокорейським хакерським угрупованням, стало найбільшою фінансовою крадіжкою в історії. Ці операції мають ознаки не просто кіберзлочинів, а ретельно спланованих розвідувальних місій, які передбачають тривале спостереження, зламування третіх сторін та блискавичне переміщення активів через десятки блокчейнів. Це стирає межу між криміналом, шпіонажем та міждержавним протистоянням, перетворюючи криптовалютний простір на поле битви новітньої холодної війни.

Росія, у свою чергу, демонструє приклад стратегічної державної толерантності та інтеграції криптовалют для обходу західних санкцій. Незважаючи на початково жорстку позицію Центрального банку, після вторгнення в Україну та запровадження безпрецедентних обмежень москва різко змінила курс. Від липня 2024 року було дозволено використання криптовалют для міжнародної торгівлі, а навесні 2025 року запропоновано трирічний експериментальний режим для інвестицій у цифрові активи. Російські банки, такі як Сбербанк, активно розширюють послуги з крипто-кредитування та зберігання цифрових активів, що сигналізує про поступову, але невідворотну інтеграцію криптоактивів у національну фінансову систему.

Особливо показовою є історія бірж Garantex та її наступниці Grinex. Незважаючи на санкції США, запроваджені у квітні 2022 року, Garantex продовжувала обробляти транзакції на суму понад 100 мільярдів доларів, з яких, за оцінками, 70–80% були пов'язані з підсанкційними суб'єктами. Коли у березні 2025 року вона була остаточно закрита, майже ідентична платформа Grinex з'явилася протягом кількох днів, зареєстрована в Киргизстані. Паралельно росія активно розробляє рублевий стейблкоїн A7A5, який за неповний рік обробив майже 93,3 мільярда доларів, створюючи альтернативну платіжну систему, здатну працювати в Африці та інших регіонах, повністю ігноруючи SWIFT.

На цьому тлі глобальний регуляторний ландшафт виглядає вкрай фрагментованим, що створює величезні можливості для арбітражу. Європейський Союз через впровадження регламенту MiCA рухається до посилення прозорості, ліцензування постачальників послуг віртуальних активів та захисту споживачів. Сполучене Королівство також розробляє схожі рамки, хоча й дещо повільніше. Однак Сполучені Штати за адміністрації Трампа обрали кардинально інший шлях, проголосивши завершення «війни з криптовалютами». Це створило ситуацію, де злочинні мережі можуть вільно переміщувати свої активи між юрисдикціями, обираючи ті ринки, де тиск регуляторів є найменшим. Розслідування, цитовані у звіті, показують, що рахунки, пов'язані з картелем Сіналоа, китайськими торговцями фентанілом та російськими мережами, що обслуговують північнокорейську збройову програму, вільно переміщували кошти через Binance, Coinbase, OKX та HTX, що свідчить про системну проблему, яку не можна вирішити точковими заходами проти однієї платформи.

Особливої уваги заслуговує аналіз «фінансової периферії» – зон, де регуляторний нагляд є слабким, суперечливим або цілеспрямовано послабленим. У Південно-Східній Азії це М'янма, Камбоджа та Лаос, де скам-центри процвітають у спеціальних економічних зонах. У Латинській Америці картина є більш складною та водночас більш показовою. Бразилія, яка має відносно розвинену нормативну базу, є прикладом того, як навіть сувора регуляція не витісняє злочинність, а змушує її мігрувати в більш складні гібридні схеми з використанням OTC-брокерів та неформальних мереж. Найбільший бразильський картель PCC активно використовує криптовалюту для прискорення транскордонних переказів, зменшуючи залежність від фізичного перевезення готівки.

Висновки:

- **Цифрові активи інтегровані в усі рівні організованої злочинності** – від логістики наркотрафіку до фінансування кібершахрайств, дозволяючи миттєво переміщувати капітали через кордони, уникаючи традиційних банківських систем та регуляторного нагляду.
- **Стейблкоїни (USDT) є основною валютою тіньової економіки.** Вони поєднують швидкість криптовалют зі стабільністю фіатних грошей, що зробило їх головним засобом для відмивання коштів.
- **Відбувається небезпечна конвергенція організованої злочинності та держав.** Такі країни, як росія, Північна Корея та Іран, використовують криптовалюту як стратегічний інструмент для фінансування воєнних програм, обходу міжнародних санкцій та ведення гібридних операцій.
- **Фрагментація глобального регулювання створює «фінансову периферію».** Різниця в підходах між Європою та США у поєднанні зі слабкими інституціями в країнах Південно-Східної Азії, Африки та Латинської Америки дозволяє злочинним мережам вільно мігрувати між юрисдикціями, обираючи найслабший рівень контролю.

Нарешті, звіт звертає увагу на новітні форми крипто-злочинності, пов'язані з децентралізованими фінансами та смарт-контрактами. Справа Forsage, яка стала першим кримінальним переслідуванням за DeFi-піраміду, показує, як технологія, що позиціонувала себе як інструмент фінансової свободи, може бути використана для створення глобальних шахрайських структур, які використовують прозорість коду для створення ілюзії легітимності, тоді як реальні вигодонабувачі контролюють ключові параметри та виводять мільйони.

Аналогічно, злам Resolv, де використання скомпрометованого приватного ключа дозволило зловмисникам створити 80 мільйонів фальшивих токенів та вивести 23 мільйони доларів, демонструє вразливість сучасних протоколів на стику хмарних сервісів та управління ключами. Ці випадки свідчать про те, що організована злочинність переходить на якісно новий технічний рівень, де успішна атака може бути проведена невеликою групою висококваліфікованих спеціалістів, які не просто зламують блокчейн, а використовують його архітектурні особливості для створення вартості з нічого та її миттєвого виведення.

У підсумку, перед світовою спільнотою постає виклик, який вимагає не точкових, а системних рішень. Реформи вже не встигають за швидкістю адаптації злочинних крипто-екосистем. Необхідно створювати спеціалізовані підрозділи з доступом до блокчейн-аналітики, розширювати механізми взаємної правової допомоги та спільних слідчих груп, що здатні працювати в реальному часі, а також гармонізувати процедури конфіскації цифрових активів на міжнародному рівні.

Водночас автори доповіді наголошують на необхідності зміни фокусу з переслідування окремих злочинців на системне руйнування інфраструктурних елементів: OTC-брокерів, тіньових банків, китайських систем відмивання та транснаціональних мереж. Без цього криптовалюта назавжди залишиться головним стратегічним активом, що дозволяє злочинцям

існувати та процвітати поза межами будь-якого правового поля, перетворюючи цифровий фінансовий простір на нову арену глобального беззаконння, де старі правила вже не діють, а нові ще не написані.

Як нелегальний ринок золота підриває глобальну фінансову архітектуру [12]

Нелегальне золото давно перестало бути другорядною проблемою, що обмежується кількома віддаленими регіонами, і перетворилося на системну загрозу, яка підриває міжнародну безпеку, фінансову архітектуру та екологічний баланс планети. Експерти наголошують, що ми стали свідками безпрецедентного зростання злочинного впливу, яке випереджає будь-які спроби міжнародного регулювання, а механізми контролю, створені ще на початку 2010-х років, виявилися безсилими перед новими викликами та адаптивними стратегіями кримінальних мереж.

Ключова теза звіту GI-TOC полягає у необхідності кардинального переосмислення самого феномену «нелегального золота». Традиційний підхід, який зосереджується виключно на кустарному видобутку (ASGM) або золоті з так званих «конфліктних та високоризикових зон» (CAHRAs), є небезпечно застарілим, оскільки він ігнорує справжній масштаб та різноманіття загроз, які пронизують усі етапи ланцюга постачання.

Одним з найтривожніших висновків звіту є констатація того, що міжнародні центри торгівлі золотом (IBCs), такі як Велика Британія, Об'єднані Арабські Емірати, Швейцарія та Китай, які обслуговують левову частку світового обороту цього дорогоцінного металу, залишаються критичною «сліпою зоною» для регуляторів. Через ці хаби, де щодня укладаються угоди на сотні мільярдів доларів, проходять величезні обсяги «брудного» золота, яке після переплавки та змішування з легальними зливками набуває абсолютно «чистого» походження.

Експерти GI-TOC наголошують, що фінансові інституції та банки, які працюють у цих хабах, часто не здійснюють належної перевірки (due diligence), покладаючись на сумнівні сертифікати або обмежуючись перевіркою безпосереднього контрагента, не заглиблюючись у походження металу. Це створює ситуацію, коли золото, видобуте в умовах рабської праці у Південній Африці або профінансоване терористичними угрупованнями в Сахелі, безперешкодно надходить на полиці ювелірних магазинів та в інвестиційні портфелі західних фондів. Особливу увагу дослідники приділяють ролі Об'єднаних Арабських Еміратів, зокрема Дубаю, який став магнітом для африканського золота, включаючи ресурси, що видобуваються в зонах активних бойових дій у Судані та Демократичній Республіці Конго. Звіт цитує випадки, коли логістичні коридори, що використовуються для контрабанди золота з Дарфуру через Лівію до ОАЕ, паралельно слугують маршрутами для постачання зброї протилежним сторонам конфлікту, що є класичним прикладом «геокримінальності», коли державні та приватні злочинні інтереси зливаються воєдино для досягнення політичних цілей.

Глибинною причиною такої вразливості є хронічна непрозорість, яка пронизує сектор на всіх рівнях. Автори звіту безпосередньо зазначають, що це не випадкова вада, а структурна риса ринку, який ніколи не вимагав справжньої відкритості. Прогалини у даних, коли країни-виробники публікують некоректну або відсутню статистику, а розбіжності між звітами про експорт та імпорт сягають мільярдів доларів, є живильним середовищем для шахрайства. Наприклад, золотодобувна промисловість Сомалі, про яку практично немає офіційних даних, насправді переживає бурхливий ріст у віддаленому регіоні Мілксо, де влада не контролює процес, а місцеві злочинці та терористичні угруповання, такі як Аль-Шабаб, активно експлуатують родовища, продаючи золото через Дубай. Так само вражаючими є приклади Руанди, яка, маючи власний видобуток менше 3 тонн на рік, експортує майже 20 тонн, завозячи золото з сусіднього Конго, часто пов'язаного з фінансуванням збройного угруповання

[12] https://globalinitiative.net/wp-content/uploads/2026/05/Marcena-Hunter-Sophia-Pickles-Commodity-currency-crime-How-illicit-gold-markets-are-outpacing-global-responses-GI-TOC-June-2026.pdf

M23. Це явище отримало назву «юрисдикційного арбітражу», коли трейдери використовують країни, що не вважаються «високоризиковими» згідно з класифікацією CAHRA, для легалізації металів, які насправді походять з епіцентрів конфліктів.

Висновки:

- **Організовані злочинні групи та корумповані еліти не просто займаються незаконним видобутком,** вони інвестують в промислове обладнання та створюють вертикально-інтегровані ланцюги постачання, що контролюють процес від копальні до фінансових ринків.
- **Міжнародні торговельні хаби (IBCs) та фінансові інституції є найбільшою "сліпою зоною" регуляторів.** Такі центри, через високу концентрацію торгів та відсутність належної перевірки, дозволяють "відмивати" золото з конфліктних регіонів, при цьому банки та інвестиційні фонди часто не проводять дослідження походження металу.
- **Існуючі міжнародні стандарти (OECD, LBMA) є застарілими, що унеможливлює боротьбу із сучасними викликами.** Фокус на "конфліктних територіях" (CAHRAs) та кустарному видобутку вже не відповідає реальності: злочинці використовують "юрисдикційний арбітраж", перетворюючи країни без офіційного статусу високоризикових на хаби для легалізації "брудного" золота.
- **Зростає роль "геокримінальності", де держави використовують злочинні золоті потоки як інструмент зовнішньої політики.** Золото стало інструментом обходу санкцій, фінансування проксі-сил, а також геополітичного впливу, що перетворює ринок на поле бою гібридної війни, де кримінальні мережі діють у партнерстві з державами.

Дослідження також детально аналізує механізми промислової експансії криміналітету, які докорінно змінили ландшафт видобутку за останнє десятиліття. Сучасні нелегальні операції – це не примітивна кустарна праця, це високомеханізовані підприємства, що використовують важкі екскаватори, бульдозери та складні хімічні процеси, що значно підвищує прибутковість. Ця трансформація стала можливою завдяки значному припливу іноземного капіталу, насамперед з боку китайських інвесторів та синдикатів, які не лише фінансують операції, але й постачають обладнання та технології, створюючи паралельну економіку обслуговування.

Розділ звіту, присвячений фінансовому сектору, викриває глибоку вразливість міжнародної банківської системи та ринків капіталу. У той час як увага громадськості часто прикута до фізичного золота, дослідники наголошують, що найбільші ризики ховаються у сфері похідних фінансових інструментів (деривативів), біржових інвестиційних фондів (ETF) та операціях на позабіржовому (OTC) ринку, де обертаються трильйони доларів без належного контролю за походженням активів. Як наслідок, банки, які укладають такі угоди, навіть не підозрюють, що обслуговують торгівлю злочинних груп, і, як правило, не застосовують до цих операцій ті ж стандарти перевірки клієнтів (KYC), що і до готівкових транзакцій.

Окремо підкреслюється ризик центральних банків, які, будучи основними гравцями на ринку та тримачами близько 5 трильйонів доларів у золоті, часто не підпадають під дію стандартів боротьби з відмиванням коштів. Згадується випадок з Монетним двором США, який, за свідченнями, роками не перевіряв походження металу, купуючи золото, пов'язане з колумбійськими наркокартелями. Це демонструє системний характер проблеми, яка торкнулася навіть тих інституцій, які вважаються найбільш надійними.

Розглядаючи перспективи вирішення проблеми, експерти GI-TOC наголошують, що ситуація не є безнадійною, однак вона вимагає переходу від добровільних до обов'язкових юридичних

механізмів, які б ліквідували прогалини в законодавстві, що дозволяють здійснювати «арбітраж».

Найбільш яскравим прикладом неефективності існуючої системи є справа проти Лондонської асоціації ринку дорогоцінних металів (LBMA), яка перебуває у судовому провадженні у Великій Британії через звинувачення в сертифікації золота з шахти в Танзанії, пов'язаної з систематичними порушеннями прав людини. Цей судовий прецедент ставить під сумнів саму природу сертифікації, яка сьогодні базується на перевірці формальних процедур аудиторами, а не на реальному розслідуванні фактів на місцях. Аудитори, як зізнаються самі учасники процесу, часто перебувають під тиском бюджетних обмежень, не володіють достатньою кваліфікацією у специфіці золотого ринку або просто зацікавлені у збереженні відносин з клієнтом, що робить незалежність таких перевірок фікцією.

Рекомендації, викладені у фінальній частині звіту, закликають до кардинальної реформи: зробити стандарти належної перевірки обов'язковими для всіх ланок ланцюга постачання, включаючи центри торгівлі, фінансові установи та центральні банки; вимагати повного розкриття бенефіціарних власників та деталізованих звітів про аудити; а також забезпечити реальну відповідальність за порушення. Крім того, дослідники наполягають на модернізації статистичних даних, зокрема запровадженні окремих митних кодів для золотого концентрату та підсиленні контролю на морських портах, які є основними воротами для цих потоків.

Водночас автори звіту попереджають, що будь-які жорсткі заходи мають супроводжуватися реальними програмами підтримки легального та відповідального видобутку, надаючи старателям доступ до фінансів та ринків, бо без цього тиск на сектор лише перемістить його ще глибше в тінь, посиливши вплив організованої злочинності та підірвавши і без того слабку довіру до державних інституцій у найвразливіших регіонах світу.

Інші новини

Викриття «банку-фантома» у Прато: мережа hawala як інструмент відмивання доходів від наркотрафіку та контрабанди товарів [13]

Розслідування Антимафіозної дирекції Флоренції (DDA) під керівництвом прокурора Рози Вольпе, проведене Центральною оперативною службою поліції та мобільним підрозділом Прато, призвело до застосування 41 запобіжного заходу (17 – позбавлення свободи, 16 – домашній арешт, 8 – обов’язок з’являтися до судової поліції) щодо 57 підозрюваних, переважно громадян Китаю, Італії та Албанії. Слідчий магістрат Антоніо Пеццуті ухвалив рішення про масштабне превентивне накладення арешту на активи на суму близько 60 мільйонів євро. Обвинувачення включають кримінальну організацію з обтяжуючою обставиною мафіозного характеру (сприяння кланам Sacra Corona Unita, ’Ndrangheta та Camorra), відмивання коштів, незаконну банківську діяльність, наркотрафік та сприяння незаконній імміграції.

Нелегальний «банк», здатний, за оцінками, переміщувати від 80 до 100 мільйонів євро на рік, використовував систему hawala – механізм передачі вартості, що базується на довірі між посередниками і не залишає сліду фізичного транскордонного переміщення готівки. Розрахунки структурувалися через готівкові потоки китайських компаній швидкої текстильної промисловості, що працюють у районі Прато (провідному текстильному центрі Європи), у зв’язці з виробничими центрами готового одягу на Піренейському півострові (Мадрид, Малага, Валенсія, Севілья), що дозволяло доходи від наркотрафіку змішувати зі – і маскувати під – звичайними торговельними розрахунками між текстильними фірмами, тоді як мережа

[13] https://en.ilsole24ore.com/art/phantom-bank-uncovered-in-prato-100-million-euros-in-drugs-and-goods-moved-AIAqwwgD

кур'єрів фізично переміщувала збирачів коштів між Італією, Іспанією, Францією та Португалією.

Організації також пред'явлено обвинувачення у сприянні незаконній імміграції, що ілюструється епізодом липня 2023 року за участю п'яти громадян Китаю, які заплатили по 9 500 євро кожен за транзит через Сербію (країну, що не входить до Шенгенської зони і не вимагає візи для громадян Китаю), через Белград, Угорщину та Словенію, з кінцевими пунктами призначення в Прато, Турині та Соммакампаньї – що демонструє операційне перетинання інфраструктури TBML та логістики контрабанди мігрантів у межах однієї злочинної мережі.

Справа ілюструє більш широку типологічну модель, що дедалі частіше документується в європейських юрисдикціях, – використання неформальних/альтернативних систем грошових переказів, вбудованих у комерційні мережі етнічної торговельної діаспори, як заміни (а не доповнення) регульованому кореспондентському банкінгу, зокрема для інтеграції доходів від кількох предикатних злочинів (наркотики, контрабанда мігрантів) через легітимні розрахунки B2B-торгівлі – типологія, що значною мірою уникає транзакційного моніторингу регульованими фінансовими установами саме тому, що базовий рух вартості ніколи не торкається формальної банківської системи.

Фінансові потоки та сумнівні операції за участі білоруського бізнесмена [14]

На основі витоку внутрішніх документів новозеландського фінансового посередника Worldclear, банку Pacific Private Bank (PPB) з Вануату та компаній, пов'язаних з білоруським підприємцем Олексієм Алексіним, вимальовується складна картина фінансових операцій, які викликають серйозні питання у експертів з протидії відмиванню коштів.

Ці матеріали, отримані у межах міжнародного розслідування за участі OCCRP та його партнерів, проливають світло на механізми руху коштів між енергетичними компаніями Алексіна, двома кіпрськими фірмами та його особистим банківським рахунком, які відбувалися в період з 2014 по 2020 рік – часи, коли вплив Алексіна в Білорусі стрімко зростав, а його ім'я ще не потрапило під міжнародні санкції.

Зростання статків та впливу Олексія Алексіна збіглося з періодом, коли старі білоруські олігархи зазнали європейських санкцій. Не зачеплений обмежувальними заходами 2012 року, спрямованими проти режиму Олександра Лукашенка, Алексін отримав низку указів від президента, починаючи з 2018 року, які надали йому майже повний контроль у певних галузях. Це відбувалося на тлі того, як Сполучені Штати намагалися підірвати те, що вони називали «корумпованим і жорстоким режимом» Лукашенка, цілеспрямовано впливаючи на ключових бізнесменів, або так званих «гаманців», які, за їхніми даними, підтримували правління президента та отримували від цього вигоду.

Центральним елементом розслідування стали операції між кіпрською компанією Wallitus та особистим рахунком Олексія Алексіна. Згідно з викритими документами, Wallitus, співвласником якої на той час був Віліус Каваляускас, котрий до 2018 року володів PPB, здійснила спроби переказати на рахунок бізнесмена суми, що загалом перевищували 3,4 мільйона доларів США, причому понад половина цих коштів пройшла через рахунки Worldclear. Кожен переказ було позначено як «погашення кредиту» згідно з угодою 2015 року, за якою Алексін надав Wallitus кредитну лінію у розмірі 13,1 мільйона доларів. Однак сам договір позики викликає подив через свою розмиту мету – фінансування поточних витрат позичальника – та початкову відсутність відсотків, що, на думку експерта з фінансової безпеки Мартіна Вудса, ставить під сумнів комерційну логіку такої угоди.

[14] https://www.occrp.org/en/project/the-worldclear-files/leaked-files-raise-questions-over-millions-flowing-to-belarusian-tycoon

Ще більше питань виникає при аналізі часу та структури цих «кредитних виплат». Викриті дані свідчать, що щоразу, коли Wallitus намагалася переказати гроші Алексіну, за кілька днів до цього вона отримувала майже ідентичну суму від іншої кіпрської компанії – Sumsteg International, яка мала прямі зв'язки з родиною Алексіна. Власником Sumsteg був Мехті Мехтієв, російський бізнесмен азербайджанського походження, близький друг сина Алексіна, Дмитра, що підтверджується спільними фотографіями та даними про польоти на приватному літаку. Ці перекази від Sumsteg до Wallitus, своєю чергою, маркувалися як погашення позик від Wallitus, наданих у 2015-2016 роках, створюючи замкнене коло фінансових зобов'язань.

Операції не завжди були успішними, що додає в історію ще більше запитань щодо належної перевірки з боку фінансових посередників. Документи фіксують кілька відхилених транзакцій. Наприклад, у січні 2018 року прямий переказ від РРВ на суму понад 629 тисяч доларів був відхилений банком-отримувачем. У лютому того ж року спробу переказати через Worldclear понад 565 тисяч євро було заблоковано без зазначення причини, а наступна пряма спроба знову провалилася, і цього разу в документах з'явилася примітка, що комплаєнс-служба банку-кореспондента «не дала схвалення». Лише після зміни схеми – розбиття суми на дві частини та направлення коштів на рахунок самої Wallitus у білоруському МТБанку, а не на особистий рахунок Алексіна – перекази було завершено успішно. Така наполегливість у реструктуризації транзакцій після відмов викликала критику з боку експертів, які зазначили, що система належної перевірки мала б ставити запитання, особливо після того, як банки відхилили частину переказів.

Роль Worldclear у цих схемах виглядає особливо значущою, оскільки компанія, не будучи банком, надавала послуги транзакційного банкінгу, зберігаючи кошти клієнтів на своїх рахунках у провідних банках і пересилаючи їх далі. Документи свідчать, що Worldclear знав про кінцевого клієнта Wallitus, але незрозуміло, яку перевірку він проводив. Звіт Департаменту внутрішніх справ Нової Зеландії, який критикував Worldclear за недостатні заходи протидії відмиванню коштів, зазначав, що компанія надто покладалася на перевірки, проведені її власними банківськими клієнтами. Засновник Worldclear Девід Хілларі рішуче заперечує будь-які звинувачення та стверджує, що ні він, ні компанія ніколи свідомо не сприяли кримінальним правопорушенням.

Ще один пласт розслідування стосується глибших зв'язків між компаніями Алексіна та Sumsteg, які підписали контракти на постачання нафтопродуктів на сотні мільйонів доларів. Попри значні суми, фінансова звітність Sumsteg визначала її основну діяльність як «надання фінансування, а не торгівля нафтою. Більше того, 17 з 18 проаналізованих контрактів згодом були скасовані, що експерт з нафтогазового ринку Михайло Крутіхін назвав «аномальним». Внутрішні документи компаній Алексіна свідчать про відстеження фінансових потоків між ними та Sumsteg, і в одному випадку Sumsteg повернула платіж за контрактом одній з енергетичних компаній. Це наводить на думку про те, що частина цих угод могла мати на меті не реальне постачання товарів, а рух коштів.

Подальший аналіз фінансової звітності Sumsteg за 2017-2020 роки виявив картину гігантського клірингового центру з десятками мільйонів євро на балансі, але з мізерними комерційними доходами. Основними статтями були позики, які вона надавала та отримувала, а також величезні обсяги торгової кредиторської та дебіторської заборгованості. Наприклад, у 2017 році Sumsteg надала позик на понад 94,5 мільйона євро та отримала погашень майже на 93,8 мільйона євро. Експерти, зокрема Росс Делстон, колишній банківський регулятор та експерт з AML, вбачають у цих операціях класичний приклад «розшарування» (layering), тобто використання багатьох банків та корпорацій для приховування походження коштів. Адвокати колишнього власника РРВ Віліуса Каваляускаса, однак, «рішуче заперечують будь-які звинувачення» у сприянні фінансовим злочинам, наголошуючи, що його ніколи не допитували відповідні органи.

Окрім зв'язків з Алексіним, розслідування виявило ще одну складну фінансову схему за участі РРВ, Каваляускаса та інших бізнесменів, зокрема литовського мільйонера Вітольда

Томашевського. Документи PPB свідчать, що компанія Томашевського Bestaniaco Corporation у 2017 році внесла заставу у розмірі 16,5 мільйона доларів для забезпечення серії кредитів від PPB компанії Invest Alliance, власником якої, ймовірно, був російський підприємець Максим Жуков. Мільйони доларів було переведено між різними компаніями, включаючи EE Airport Holding та Air Flying Ltd, у той час як Bestaniaco робила депозити в PPB, а банк надавав кредити Invest Alliance, які майже миттєво переказувалися на кіпрські рахунки в Promsvyazbank. Для виконання цих переказів також використовувався Worldclear.

Аудитор Вайда Качергієне та експерт Алекс Кобем висловили сумніви щодо економічної доцільності такої структури, зазначивши, що складні ланцюги транзакцій за участі фінансових установ Вануату, які не мають чіткої комерційної мети, можуть свідчити про спробу приховати справжнє джерело коштів та ускладнити ідентифікацію кінцевого бенефіціарного власника. Показово, що документи PPB містять «червоні прапорці», зокрема позначку «Compliance Did Not Give Approval», що чітко вказує на те, що певні транзакції викликали занепокоєння у банків-кореспондентів.

Незважаючи на це, кошти продовжували рухатися, а схеми – ускладнюватися, що ставить під сумнів ефективність комплаєнс-процедур як у PPB, так і в Worldclear, особливо в контексті використання юрисдикцій зі слабким регулюванням, таких як Вануату, та офшорних центрів, як Кіпр, які часто використовуються для подібних фінансових маніпуляцій.

Для загального розвитку

Комюніке CSSF щодо практик де-ризикінгу та управління ризиками ВК/ФТ [15]

Комюніке Комісії з фінансового нагляду Люксембургу (CSSF) від 16 червня 2026 року видане у відповідь на скарги фізичних та юридичних осіб щодо труднощів з відкриттям банківських рахунків у Люксембурзі, які кредитні установи нібито пояснювали обтяжливими вимогами ПВК/ФТ та власним (помилковим) розумінням очікувань CSSF щодо схильності до ризику піднаглядних суб'єктів. Центральне повідомлення документа полягає в тому, що CSSF очікує від піднаглядних суб'єктів управління ризиком ВК/ФТ, а не його уникнення.

Перший блок комюніке проводить розмежування між управлінням ризиком та його уникненням: документи з керівними принципами (із посиланням на лінію Циркулярів CSSF 21/782, посилену Циркулярами 23/842 та 25/878, що інтегрують настанови EBA щодо факторів ризику ВК/ФТ EBA/GL/2021/02 та EBA/GL/2024/01) не слід тлумачити як заборону на встановлення ділових відносин з підвищеним рівнем ризику, і вони не надають піднаглядним суб'єктам права на категоричне виключення цілих категорій клієнтів, продуктів чи послуг понад те, що прямо передбачено Законом від 12 листопада 2004 року про боротьбу з відмиванням коштів і фінансуванням тероризму та Регламентом CSSF № 12-02. Документ прямо підтримує Керівництво FATF щодо фінансової інклюзії та допустимість застосування спрощеної належної перевірки до груп клієнтів з низьким рівнем ризику як механізму балансування між інклюзією та управлінням ризиком.

Другий блок формулює інституційну позицію CSSF щодо невтручання в бізнес-моделі та комерційні рішення піднаглядних суб'єктів стосовно онбордингу клієнтів. Регулятор проводить принципове концептуальне розмежування між де-ризикінгом, що вводиться самим CSSF (виключний, вузько застосовуваний наглядовий захід, що використовується лише тоді, коли ризик ВК/ФТ вважається таким, що вже не піддається управлінню), та власною «стратегією виходу» установи, що реалізується з міркувань прибутковості, – останнє є легітимним стратегічним бізнес-рішенням, щодо якого CSSF не висловлює позиції, за умови що воно по суті не є замаскованою реакцією на висновки про невідповідність вимогам.

[15] https://www.cssf.lu/en/2026/06/de-risking-practices-and-ml-ft-risk-management/

Третій блок наголошує на взаємному обов'язку співпраці клієнта: труднощі з відкриттям рахунку, що виникають через неспроможність або відмову клієнта надати документацію щодо джерела коштів, прямо відмежовуються від де-ризикінгу, спричиненого регулятором. CSSF доручає фахівцям розглядати застосування альтернативних і пропорційних заходів, коли клієнт демонструє законні практичні труднощі, відповідно до оновлених настанов EBA/GL/2023/03 та Циркуляра CSSF 23/842.

Четвертий блок окреслює перспективну регуляторну архітектуру: стаття 21(4) Регламенту (ЄС) 2024/1624 (AMLR1) зобов'язує EBA та Орган ЄС з ПВК/ФТ (AMLA) видати до липня 2027 року спільні настанови, спрямовані саме на необґрунтований де-ризикінг та категорії ділових відносин, найбільш постраждалих від цієї практики, – розташовуючи це комюніке як проміжне пояснення в очікуванні більш структурованого інструменту на рівні ЄС.

Значення комюніке полягає не стільки у запровадженні нових зобов'язань, скільки у публічному перекалібруванні наглядового наративу навколо політично чутливої точки тертя (фінансової ексклюзії) без послаблення ризик-орієнтованої архітектури ПВК/ФТ. Документ функціонує як керівництво з управління регуляторними очікуваннями для кредитних установ, що орієнтуються в настановах EBA щодо факторів ризику, а не як принципово нова нормативна вимога, і сигналізує, що CSSF, ймовірно, посилить пильність щодо установ, які покликаються на «ризик ВК/ФТ» як на узагальнене обґрунтування широких категоричних виключень, не підкріплених індивідуалізованою оцінкою ризику.

Ваша думка важлива!

1. Як поєднання блокчейну та штучного інтелекту може вплинути на майбутнє фінансового моніторингу, комплаєнсу та управління ризиками, і чи готові регулятори до появи автономних систем, які самостійно прийматимуть фінансові рішення?
2. Які механізми співпраці між державними органами, фінансовими установами та неприбутковими організаціями можуть бути найбільш ефективними для запобігання використанню благодійного сектору у схемах фінансування тероризму?
3. Як Україні ефективно протидіяти «геокримінальній» діяльності росії, яка використовує злочинні мережі та «тіньові флоти» для обходу санкцій, контрабанди зброї та впливу на європейські країни?
4. Наскільки поширеною є практика де-ризикінгу серед українських банків – наприклад, щодо благодійних і неприбуткових організацій чи клієнтів із тимчасово окупованих та деокупованих територій? Які регуляторні або інституційні механізми, на вашу думку, дозволили б ефективно відрізняти обґрунтоване управління ризиком від його фактичного уникнення?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-25

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

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