Методологічний бюлетень

Серійний номер: МінФін-AML-2025-24

Червень 2025

“У житті немає нічого, чого варто було б боятися, є тільки те, що потрібно зрозуміти.”

Марія Склодовська-Кюрі

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

Емісія стейблкоїнів та зберігання криптоактивів [1]

Консультаційний документ FCA CP25/14 формує перший у Сполученому Королівстві комплексний регуляторний режим для емітентів фіат-орієнтованих стейблкоїнів та кастодіанів криптоактивів. У вступі регулятор пояснює, що після набрання чинності поправок до FSMA та майбутнього статутного інструмента Казначейства саме «qualifying stablecoins», тобто токени, які відносяться до однієї фіатної валюти й призначені для платежів британських споживачів, опиняються в центрі нового режиму. FCA концентрується на

[1] https://www.fca.org.uk/publications/consultation-papers/cp25-14-stablecoin-issuance-cryptoasset-custody

трьох стратегічних цілях — захисті клієнтів, цілісності ринку та конкуренції, одночасно підтримуючи міжнародну привабливість Лондона як криптохабу. Політичний контекст доповнено оглядом попередніх консультацій DP23/4 і дорожньої карти «Crypto-roadmap», що передбачає окремі папери щодо пруденційних вимог, поведінкових стандартів, торгових платформ та стейкінгу.

Основні правила для емітентів викладено у главі 3. Кожен випущений стейблкоїн має бути постійно забезпечений активами у співвідношенні 1:1, що зберігаються у статутному трасті на користь власників і розміщуються виключно в незалежного кастодіана, не пов'язаного з групою емітента. Базовий пул дозволених активів обмежено грошовими депозитами на вимогу та державними облігаціями строком до одного року; розширений перелік (довші держпапери, репо, публічні грошові фонди) доступний лише після окремого повідомлення FCA та підкріплюється динамічним коефіцієнтом складу резервів BACR[2], який раз на 14 днів враховує прогноз пікових викупів і історію помилок у ліквідності. Не менш ніж 5 % резерву мають бути депозитами «on demand» (ODDR) для миттєвого доступу до готівки. Емітенти зобов'язані затвердити політику управління ліквідністю, щороку тестувати план альтернативного фінансування та розподіляти активи між кількома кастодіанами, аби мінімізувати концентраційний ризик.

Право на викуп стейблкоїнів поширюється на всіх власників, незалежно від їх статусу чи юрисдикції: емітент мусить розмістити платіжне доручення за номіналом у тій самій валюті не пізніше ніж T+1 робочий день після отримання коректного запиту й інформації для AML/KYC-перевірок; відстрочка дозволена лише у разі правових заборон або за бажанням клієнта провести конвертацію валюти . Комісії за викуп мають відображати реальні операційні витрати й жодним чином не перекривати вартість токена або втрати від продажу резервних активів. Всі політики щодо резервів, викупу, комісій та участі третіх сторін публікуються у зрозумілій формі; раз на квартал емітент звітує про структуру резервів, а не рідше раз на рік незалежний аудитор підтверджує точність тверджень про співвідношення 1:1 . У разі спалення стейблкоїнів після викупу нерезидентні або «розморожені» токени мають бути або повністю повторно забезпечені, або знищені протягом 24 годин, щоб уникнути надемісії.

Документ вводить суворі вимоги до кастодіанів криптоактивів у главі 4,

Висновки:

- **Емітенти мають негайно реструктуризувати резерви під модель «статутний траст + BACR»**, тримати щонайменше 5% у депозитах на вимогу та налаштувати 14-денний цикл розрахунку BACR для уникнення примусових продажів у стресі.
- **Виконання вимоги T+1 щодо викупу потребує безперервного KYC/CDD-процесу** та інтеграції швидких платіжних рейок; компанії повинні протестувати операційну готовність до масових викупів і зафіксувати SLA з банківськими партнерами.
- **Кастодіани зобов'язані переоформити всі клієнтські відносини під трастове право й забезпечити технічну сегрегацію ключів**; без цього ліцензійний ризик і потенційна субординація активів клієнтів у процедурі банкрутства зростають критично.
- **Щорічний незалежний аудит резервів і квартальне розкриття їх структури стануть мінімальним стандартом прозорості**; бюджети на комплаєнс повинні включати оплату аудитора, публічні звіти й оновлення політик, оскільки відсутність перевіреного 1:1 покриття блокуватиме доступ на платіжний ринок.

[2] це запропонований FCA динамічний показник, який визначає, яку мінімальну частку резерву стейблкоїна (backing pool) емітент мусить тримати у core backing assets (кошти «на вимогу» + короткострокові держоблігації), якщо він вирішив інвестувати частину резерву в менш ліквідні expanded backing assets (облігації > 1 рік, репо, публічні MMF). Мета показника — гарантувати, що навіть із розширеним набором активів у пулі залишиться достатньо ліквідності для задоволення всіх запитів на викуп T+1 і мінімізувати вимушені продажі під час стресу.

переносячи принцип «same risk — same regulatory outcome» на цифрові активи. Усі клієнтські криптоактиви повинні зберігатися у довірчій власності (non-statutory trust) окремо від активів фірми; дозволено як індивідуальні, так і омнібус-гаманці, але записи мають безпомилково ідентифікувати бенефіціарів та кількість токенів. Кастодіан зобов'язаний вести щоденні та зовнішні звіряння, негайно повідомляти FCA про будь-які розбіжності у балансах, а також забезпечити, щоб у випадку неплатоспроможності клієнти отримали свої активи в найкоротші терміни. Особливу увагу приділено вертикальній інтеграції бірж і кастодіальних сервісів: FCA вимагає чітких меж між торгівлею, зберіганням і кредитуванням, щоб усунути конфлікти інтересів та забезпечити прозорість операцій.

У завершальній главі FCA встановлює дедлайн для коментарів — 31 липня 2025 р., після чого планує опублікувати підсумкові політичні заяви й рухатися до другої хвилі консультацій, що охопить пруденційні норми, стандарти поведінки та правила для торгових платформ і стейкінгу, з поступовими перехідними періодами для вже діючих компаній.

Консультаційний документ щодо запропонованих вимог з ПВК/ФТ для регульованої діяльності зі стейблкоїнами [3]

Консультаційний документ Грошово-кредитного управління Гонконґу (HKMA) від 26 травня 2025 р. окреслює проєкт вимог ПВК/ФТ до діяльності ліцензованих емітентів «специфікованих» стейблкоїнів – цифрових токенів, що прив'язані до офіційної валюти та використовуються як платіжний засіб. На підставі нещодавно ухваленого Stablecoins Ordinance (SO) емітенти, а також особи, які пропонують або викупають такі токени, повинні отримати ліцензію Грошового управління; при цьому емітентів планують внести до переліку «фінансових установ» Закону про ПВК/ФТ з принципу «однакова діяльність – однакові ризики – однакове регулювання». Документ резюмує міжнародний та місцевий контекст: стрімкий розвиток ринку віртуальних активів, запровадження режиму ліцензування криптобірж SFC у 2023 р. і високі вразливості стейблкоїнів до відмивання коштів через анонімні (unhosted) гаманці, що FATF прирівнює до «анонімних пред'явницьких інструментів».

Усі ліцензіати мають побудувати ризик-орієнтовану систему ПВК/ФТ, що охоплює інституційні оцінки ризику, корпоративне управління, тренінги, санкційний та ФР-контроль, підозрілі повідомлення й ведення записів. Спеціальні вимоги для емісії передбачають ідентифікацію одержувачів, підтвердження володіння гаманцем, обов'язкову перевірку постачальників кастодіальних гаманців і застосування порогового CDD від 8 000 HKD. Якщо токени надсилаються на unhosted-гаманець, емітер повинен посилити моніторинг, дозволяти переказ лише на «надійні» адреси за результатами аналітики блокчейну й, за потреби, встановлювати ліміти операцій . Перед викупом стейблкоїнів емітер повторно верифікує власника та джерело активу; правом викупу володіє будь-який тримач, а сам викуп має відповідати всім правовим та санкційним вимогам.

Для трансферів стейблкоїнів діє «Travel Rule» (ст. 13A Додатку 2 до AMLO): залежно від ролі учасника (ordering, intermediary чи beneficiary) ліцензіат зобов'язаний збирати та передавати ідентифікаційні дані відправника й одержувача, що узгоджується з підходом SFC до

[3] https://www.hkma.gov.hk/media/eng/regulatory-resources/consultations/20250526_Consultation_Paper_on_the_Proposed_AMLCFT_Req_for_Regulated_Stablecoin_Activities.pdf

Висновки:

- Потенційні емітенти вже зараз мають розгорнути блокчейн-аналітику й сформувати процедури CDD для гаманців клієнтів, інакше отримати ліцензію буде неможливо.
- Всі перекази на unhosted-адреси повинні проходити посилений контроль і можуть обмежуватися лімітами; без технологічного скринінгу такі операції розглядатимуться НКМА як неприйнятний ризик.
- Виконання Travel Rule вимагає інтеграції клієнтських даних у транзакційні повідомлення; провайдери повинні переобладнати свої IT-системи для підтримки стандарту до моменту запуску схеми ліцензування.
- Щоб мінімізувати вторинні ризики, емітенти мають укласти угоди лише з регульованими VASP та банками, вести «чорні списки» адрес і готуватися до розкриття політик моніторингу НКМА під час подання заяви на ліцензію.

криптовалютних платформ . Ліцензіат має впровадити технічні рішення для безперервного скринінгу всіх вихідних і вхідних транзакцій стейблкоїна, зокрема автоматизовані інструменти аналізу ланцюга, які відстежують історію токенів і маркують адреси, що належать санкційним чи підозрілим суб'єктам. У вторинному обігу емітер зобов'язаний ужити «адекватних і пропорційних» заходів: обмежувати первинний продаж і викуп тільки регульованими установами, застосовувати постійний блокчейн-моніторинг поза первинними майданчиками, підтримувати «чорні» й «білі» списки адрес та за можливості створювати закриті контури обігу для зниження ризиків, подібних до анонімних пред'явницьких інструментів. Окремий додаток до інструкції НКМА, що регулюватиме інші пов'язані цифрові активи (кастодіальні послуги, пропозиція токенів), буде винесено на консультацію пізніше у 2025 р., щоб забезпечити рівні правила для всіх фінансових установ. Зауваження до проєкту приймаються до 30 червня 2025 р., після чого НКМА опрацює відгуки та фіналізує керівництво.

Стратегія боротьби з економічною злочинністю [4]

Фінальний звіт про виконання Стратегії боротьби з економічною злочинністю до 2025 року, опублікований Королівською прокурорською службою Сполученого Королівства (CPS), підсумовує чотирирічні зусилля країни у протидії фінансовим злочинам, посиленні цифрових можливостей, захисті жертв та поверненні активів. У документі детально представлено досягнення CPS у співпраці з правоохоронними, регуляторними та судовими органами в рамках міжвідомчої системної відповіді на зростання економічної злочинності, зокрема шахрайства, відмивання коштів, корупції, зловживань у криптосфері та штучному інтелекті.

CPS демонструє високі показники результативності: з 2021 по 2024 роки було притягнуто до відповідальності 25 665 осіб у справах, де шахрайство або фальсифікація були основним злочином, із 21 717 обвинувальними вироками (рівень засудження 85.4 % у 2024/25 фінансовому році). Протягом останніх п'яти років судові органи за сприяння CPS вилучили понад 450 млн фунтів стерлінгів у вигляді конфіскацій, з яких 88 млн було повернуто жертвам у формі компенсацій. Крім того, CPS допомогла забезпечити надходження понад 1,2 млрд фунтів у межах цивільного й кримінального врегулювання — зокрема через перше в історії служби «відстрочене кримінальне переслідування» (DPA) на суму 615 млн фунтів.

[4] https://www.cps.gov.uk/publication/economic-crime-strategy-2025-final-progress-report-may-2025

Особливу увагу у звіті приділено впровадженню нового злочину — Failure to Prevent Fraud згідно з Законом про прозорість корпоративної економіки (ECCTA). CPS брала участь у розробці офіційного керівництва для бізнесу та готує оновлення настанов для прокурорів щодо взаємодії нових правових норм із реформою доктрини ідентифікації юридичних осіб. У 2024 році було також оновлено прокурорські інструкції з питань відмивання коштів із фокусом на діяльність money mules і запроваджено міжвідомчий план MMAP.

У сфері цифрових викликів значне місце займає боротьба з використанням криптоактивів для відмивання злочинних доходів. CPS розгорнула нові підрозділи, призначила спеціальних координаторів із питань криптоактивів, уклала меморандум з Національним агентством з протидії злочинності щодо навчання слідчих і прокурорів, а також створила національну базу даних криптосервісів. У межах гучної справи було забезпечено конфіскацію криптовалюти вартістю понад 2 млрд фунтів. У фокусі також — адаптація до штучного інтелекту: CPS ініціювала оцінку готовності до впровадження AI, розробила етичну рамку та планує інтеграцію AI у обробку цифрових доказів і управління справами, зберігаючи при цьому людське судження у прийнятті рішень.

CPS послідовно просуває цифрову трансформацію: від створення повністю цифрового обміну матеріалами між поліцією і прокуратурою до впровадження систем для обробки великих справ (off-CMS). У справі про шахрайство на суму 50 млн фунтів вдалося ефективно обробити 945 цифрових пристроїв завдяки ранньому узгодженню між слідством і захистом, уникнувши процесуальних затримок. Також було суттєво оновлено інфраструктуру роботи з аналітичними доказами, включаючи часові лінії подій, розшифровку даних з месенджерів та зображення.

У частині партнерства CPS зробила внесок у створення Національного підрозділу з протидії шахрайству (National Fraud Squad), запропонувала зміни до стратегії боротьби з корупцією та надала підтримку Уряду в реалізації рекомендацій щодо покращення режиму розкриття доказів. У міжнародному аспекті CPS брала участь у розбудові Міжнародного центру боротьби з транснаціональною злочинністю та Глобального хабу з повернення активів, зокрема через нові інструменти для обробки запитів про доказову допомогу та конфіскацію.

Особливу роль у звіті відіграє робота з потерпілими. CPS активно переглядає та вдосконалює керівництво щодо взаємодії з жертвами економічної злочинності, зокрема в рамках Програми трансформації прав потерпілих, приділяючи окрему увагу вразливим групам — людям з інвалідністю, літнім особам та молоді. У співпраці з такими організаціями, як Age UK і NSPCC, CPS впроваджує нові підходи до інформування жертв і адаптації процедури участі в судових процесах.

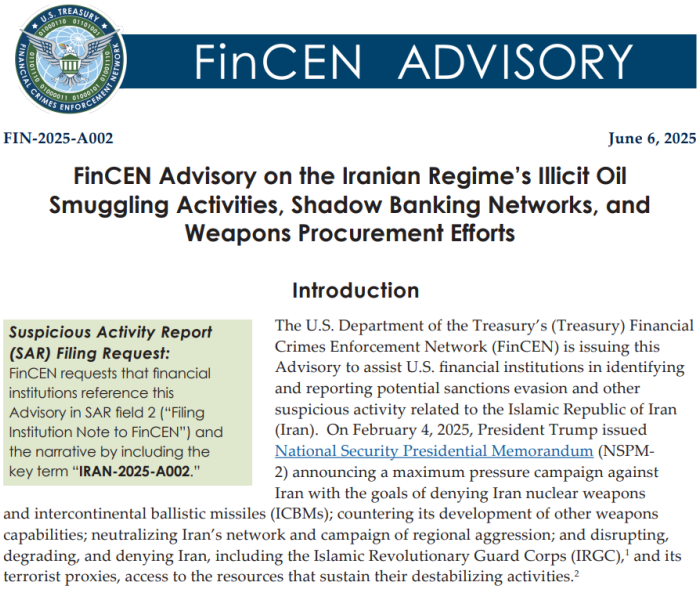
У підсумку, звіт підкреслює, що економічна злочинність — одна з

Висновки:

- **CPS продемонструвала ефективну модель співпраці з правоохоронцями** у справах щодо криптоактивів, забезпечивши успішне вилучення £2 млрд у BTC; регуляторам варто впровадити аналогічну модель взаємодії та кадрової спеціалізації.
- **Завдяки оновленню підходу до money mules, CPS створила правові передумови для диференційованого переслідування виконавців і організаторів схем**; іншим юрисдикціям доцільно адаптувати подібні керівництва.
- **Впровадження злочину «відсутності перешкоджанню шахрайству» та реформування доктрини ідентифікації підвищують ризики для корпоративних правопорушників** і вимагають від компаній швидкої побудови внутрішніх програм превенції.
- **Використання AI у цифровому доведенні, управлінні розкриттям і аналітиці кейсів має розгортатися поступово, з обов'язковим збереженням людської участі в ухваленні рішень**; створення етичної рамки — необхідна умова довіри.

наймасштабніших і найскладніших загроз у Сполученому Королівстві: станом на кінець 2024 року шахрайство становило 43 % усіх злочинів, із зростанням на 33 % за рік. Система реагування має залишатися гнучкою, підготовленою в цифровому вимірі, технологічно оснащеною та глибоко міжвідомчо інтегрованою. Нова стратегія CPS до 2030 року вже враховуватиме ризики, пов'язані з AI, криптовалютами, міжнародними корупційними схемами та кіберфінансовими злочинами.

Консультативний лист FinCEN щодо незаконної контрабанди нафти, тіньових банківських мереж та закупівель зброї іранським режимом [5]



FinCEN ADVISORY

FIN-2025-A002 June 6, 2025

FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts

Introduction

Suspicious Activity Report (SAR) Filing Request: FinCEN requests that financial institutions reference this Advisory in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative by including the key term "**IRAN-2025-A002**."

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist U.S. financial institutions in identifying and reporting potential sanctions evasion and other suspicious activity related to the Islamic Republic of Iran (Iran). On February 4, 2025, President Trump issued National Security Presidential Memorandum (NSPM-2) announcing a maximum pressure campaign against Iran with the goals of denying Iran nuclear weapons and intercontinental ballistic missiles (ICBMs); countering its development of other weapons capabilities; neutralizing Iran's network and campaign of regional aggression; and disrupting, degrading, and denying Iran, including the Islamic Revolutionary Guard Corps (IRGC),[1] and its terrorist proxies, access to the resources that sustain their destabilizing activities.[2]

Мережа з протидії фінансовим злочинам Міністерства фінансів США (FinCEN) випустила Консультативний лист, щоб допомогти американським фінансовим установам виявляти та повідомляти про можливі випадки ухилення від санкцій та іншу підозрілу діяльність, пов'язану з Ісламською Республікою Іран. Цей документ підтримує кампанію максимального тиску США проти Ірану, ініційовану Президентом Трампом 4 лютого 2025 року Національною безпековою президентською директивою (NSPM-2), яка має на меті відмовити Іран в ядерній зброї та міжконтинентальних балістичних ракетах (МБР), протидіяти розвитку інших видів озброєнь, нейтралізувати мережу регіональної агресії Ірану та перекрити Ірану, включаючи Корпус вартових Ісламської революції (КВІР) та його терористичних проксі, доступ до ресурсів, що підтримують їхню дестабілізуючу діяльність. Для реалізації NSPM-2, Управління з контролю за іноземними активами Міністерства фінансів (OFAC) здійснило кілька раундів санкцій, спрямованих проти експорту іранської нафти, що є значним джерелом доходу для режиму та його терористичних проксі. Цей консультативний лист оновлює "червоні прапорці" та інформацію про поточні тенденції та типології ухилення Ірану від санкцій та іншої незаконної діяльності, включаючи контрабанду нафти, мережі "тіньового банкінгу" та закупівлю зброї, і був виданий одночасно з санкційною акцією OFAC 6 червня, яка вперше після NSPM-2 була спрямована на іранську мережу "тіньового банкінгу".

Іран, що вважається провідним державним спонсором тероризму, становить дестабілізуючий вплив у регіоні та світі з моменту заснування ним фундаменталістської шиїтської ісламської республіки в 1979 році. Особливе занепокоєння викликають його ядерна програма, асиметричні військові можливості та підтримка мережі терористичних партнерів та проксі, таких як ХАМАС, ліванська Хезболла, Ансаралла (Хусити) та інші іранські ополчення в Іраку та Сирії, відомі як "Вісь опору". Іран несе відповідальність за різанину ХАМАС 7 жовтня 2023 року в Ізраїлі та прямі балістичні й крилаті ракетні атаки проти Ізраїлю з квітня 2024 року, надаючи фінансову та матеріальну підтримку. Для озброєння себе та своїх проксі Іран розробив потужну програму балістичних ракет та великий інвентар безпілотних літальних апаратів (БПЛА), які він постачав,

[5] https://www.fincen.gov/sites/default/files/advisory/2025-06-06/FinCEN-Advisory-Illicit-Oil-Smuggling-508.pdf

наприклад, Хуситам та росії. Економічно та військово Іран розвинув тісні зв'язки з росією та Китаєм, відображаючи стратегію "погляд на Схід".

Іран фінансує свою дестабілізуючу діяльність за рахунок доходів від продажу нафти. Щоб приховати свою участь у цих продажах та отримати доступ до міжнародної фінансової системи, режим використовує "тіньовий флот" — часто старі та погано обслуговувані судна, які переміщують нафту по всьому світу, та багатоюрисдикційну мережу "тіньового банкінгу", що включає обмінні пункти, торгові та підставні компанії для переміщення та розрахунку коштів, а також подальшої закупівлі зброї та інших можливостей. Нафта, переважно продана Національною Іранською Нафтовою Компанією (NIOC), є основним джерелом доходу для збройних сил Ірану та його терористичних партнерів. Значні обсяги нафти виділяються Міністерству оборони та логістики Збройних сил Ірану (MODAFL), Генеральному штабу збройних сил Ірану (AFGS) та Силам Кудс (IRGC-QF) для продажу на міжнародному ринку. До кінця 2025 року понад половина загальних доходів Ірану від нафти буде розподілена на його збройні сили. Іран пропонує нафту за цінами, нижчими за ринкові, здебільшого продаючи її невеликим незалежним нафтопереробним заводам у Китаї, відомим як "чайникові НПЗ". Щоб обійти повторно введені у 2018 році санкції США, режим створив масштабні глобальні мережі контрабанди нафти та відмивання грошей, використовуючи підставні компанії в третіх країнах, часто в зонах вільної торгівлі, для приховування іранської участі.

"Тіньовий флот" Ірану, що складається зі старих суден з непрозорою власністю, використовує тактики обфускації, що ускладнює їх ідентифікацію та відстеження. Ці судна часто належать і керуються операційними або судноплавними компаніями за межами Ірану (наприклад, ОАЕ та країни Південно-Східна Азія), які також сприяють продажу іранської нафти. Вони можуть бути незастрахованими або недострахованими, що створює ризики для портової інфраструктури, інших суден та довкілля. Режим використовує підставні компанії для оренди суден та оплати послуг, приховування зв'язків з Іраном через часті зміни назв, власників або прапорів, а також використання "фальшивих прапорів". Для маскування походження та кінцевого пункту призначення вантажу судна займаються оманливою судноплавною практикою, включаючи фальсифікацію документів, відключення або маніпулювання автоматичними ідентифікаційними системами (AIS), нерегулярності маршруту та перевалки "судно-судно". Іранська нафта також може змішуватися з нафтою з третіх країн або перемарковуватися як "малайзійська суміш" за допомогою підроблених документів.

"Тіньові банківські" мережі Ірану, що складаються з обмінних пунктів, торгових компаній та іноземних підставних компаній, дозволяють підсанкційним іранським організаціям, таким як MODAFL та KBIP, отримувати доступ до міжнародної фінансової системи, приховувати торгівлю та доходи. Ці мережі, підсилені постачальниками фінансових послуг (MSB), юридичними особами та постачальниками корпоративних та трастових послуг (TCSP), забезпечують ліквідність у багатьох юрисдикціях та підривають цілісність світової фінансової системи. Доходи від продажу нафти відмиваються через ці мережі, фінансуючи закупівлю компонентів зброї та підтримку проксі-груп, таких як хусити та росія. Обмінні пункти в Ірані часто керують підставними та торговими компаніями, зареєстрованими у таких юрисдикціях, як Гонконг або ОАЕ. Ці підставні компанії, часто нещодавно зареєстровані, з мінімальною присутністю в Інтернеті та великими транзакціями без чіткої ділової мети, створюють банківські рахунки за межами Ірану для отримання коштів та здійснення платежів. За даними BSA, гонконгські компанії, що співпрацюють з китайськими фінансовими установами через нерезидентні рахунки, та торгові компанії ОАЕ в зонах вільної торгівлі, часто використовуються іранськими суб'єктами як підставні компанії. Вони також використовуються для закупівлі компонентів зброї та інших матеріалів на міжнародному ринку. Використання таких рахунків за межами Ірану дозволяє підсанкційним суб'єктам здійснювати транзакції без репатріації коштів до Ірану. За даними BSA, ознаками контролю з боку Ірану можуть бути зв'язки з іранськими компаніями

(спільні контрагенти, адреси, схожі назви) або історія сприяння відправленням до та з Ірану. 6 червня 2025 року OFAC наклав санкції на мережу з понад 40 осіб та організацій, пов'язаних з братами Заррінґаламами, які відмили мільярди доларів через міжнародну фінансову систему, використовуючи іранські обмінні пункти та мережу підставних компаній в ОАЕ та Гонконзі.

Доходи від продажу нафти також використовуються для закупівлі компонентів зброї, товарів подвійного призначення та хімікатів на міжнародному ринку, головним чином для програм балістичних ракет та БПЛА. Іран уникає контролю за експортом через складні мережі агентів із закупівель, підставних компаній, посередників та постачальників, що діють у третіх країнах, включаючи Китай, Гонконг, Туреччину та Південно-Східну Азію. Ці мережі використовують такі методи, як шарування транзакцій, фальсифікація документації та транзит через треті країни, щоб приховати кінцевого користувача — Іран.

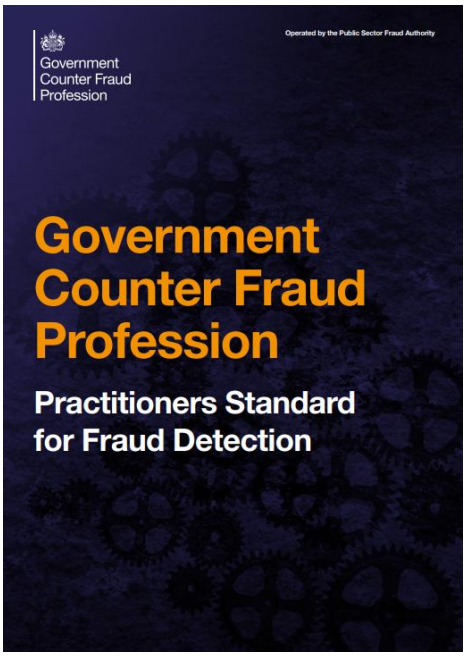
Висновки:

- **Посилена пильність та комплексна перевірка:** Фінансові установи зобов'язані посилити пильність і проводити ретельну належну перевірку щодо всіх транзакцій, клієнтів та контрагентів, особливо тих, хто має будь-який зв'язок з Іраном або діє в юрисдикціях високого ризику (наприклад, ОАЕ, Гонконг, Китай, країни Південно-Східної Азії, Туреччина). Це включає ретельний аналіз непрозорих структур власності, нещодавніх реєстрацій компаній, мінімальної присутності в Інтернеті та невідповідності заявленої ділової активності.
- **Активне виявлення оманливих практик та своєчасне інформування:** Необхідно активно шукати "червоні прапорці", пов'язані з незаконною контрабандою нафти (наприклад, судна "тіньового флоту", маніпуляції AIS, "малайзійська суміш" нафти, підроблені документи, часті зміни деталей суден) та "тіньовим банкінгом" (наприклад, використання множинних обмінних пунктів/підставних компаній, підроблені документи, нерепатріація коштів, нехарактерні великі платежі). Негайне повідомлення про таку діяльність через SAR є критично важливим.
- **Розуміння зв'язку з фінансуванням ЗМЗ:** Важливо усвідомлювати, що доходи від незаконних продажів нафти та "тіньового банкінгу" безпосередньо фінансують іранські програми озброєнь (балістичні ракети, БПЛА) та підтримують його терористичних проксі. Фінансові установи повинні бути пильними щодо транзакцій, що стосуються товарів подвійного призначення, електроніки або хімікатів, особливо якщо вони пов'язані з універсальними торговими компаніями або підозрюваними підставними компаніями у регіонах високого ризику.

FinCEN надає "червоні прапорці" для допомоги фінансовим установам у виявленні підозрілої діяльності, пов'язаної з Іраном. Вони включають: невідповідність документації з морськими базами даних, часті зміни назв або прапорів суден, посилання на "малайзійську суміш" нафти, використання підроблених документів для приховування зв'язку з Іраном. Для "тіньових банківських" мереж "червоні прапорці" включають: транзакції через численні обмінні пункти/торгові компанії зі значними необґрунтованими комісіями, використання підроблених документів обмінними пунктами поблизу Ірану, відсутність інформації про джерело коштів, використання компаній з непрозорою власністю в зонах вільної торгівлі, або гонконгські компанії з мінімальною присутністю в Інтернеті та великими незрозумілими платежами. Для мереж закупівлі зброї ознаками є: транзакції з підставними компаніями, невідповідність заявленої діяльності, платежі між непов'язаними бізнесами (наприклад, від товарних компаній до постачальників електроніки), а також кілька компаній з однаковими контрагентами, адресами, власниками, або схожими профілями транзакцій.

Фінансові установи повинні подавати Звіти про підозрілу діяльність (SARs) при виявленні такої діяльності, необхідно надавати всю доступну інформацію про рахунки, сторони та залучені фінансові установи. У випадках, що вимагають негайної уваги, таких як поточні схеми відмивання грошей або підозрювана терористична діяльність, слід негайно повідомляти правоохоронні органи, на додаток до подання SAR. Наголошується на важливості належної перевірки клієнтів (CDD) та поглибленої перевірки (EDD) для рахунків нерезидентів та політично значущих осіб (PEP), а також на заохоченні обміну інформацією між фінансовими установами.

Сучасні стандарти виявлення шахрайства у публічному секторі: Практичний путівник від Public Sector Fraud Authority [6]



Документ, розроблений Public Sector Fraud Authority Сполученого Королівства у травні 2025 року, є частиною ширшого стандарту Government Counter Fraud Profession (GCFP) і слугує практичним інструментом для формалізації вимог до виявлення шахрайства в публічному секторі. Його головна мета полягає у визначенні професійних стандартів і компетенцій, необхідних для фахівців, які займаються виявленням шахрайства, а також у наданні детальних рекомендацій щодо процесів, інструментів та організаційних практик, що дозволяють реалізовувати цю функцію ефективно й системно.

Документ започатковує чітку рамку компетенцій, яка складається з п’яти ключових компонентів: знання про шахрайство, хабарництво та корупцію; розуміння структури організації та її підходів до протидії шахрайству; знання методів виявлення шахрайства; навички оцінки результатів і здатність ефективно взаємодіяти з різними зацікавленими сторонами. Ці компоненти розділені на два рівні — базовий та практичний, що дозволяє організаціям та фахівцям будувати поступову траєкторію професійного зростання у сфері протидії шахрайству. Підкреслюється, що виявлення шахрайства є не лише технічним завданням, а й невіддільною частиною загального циклу управління шахрайством, який включає також запобігання, розслідування, навчання персоналу та вдосконалення внутрішніх контролів.

Центральне місце у підході займає Модель виявлення шахрайства, яка визначає п’ять основних етапів: встановлення контрольної точки, ідентифікація ризиків і вразливостей, застосування методів виявлення, оцінка результатів і формування подальших дій. Цей підхід інтегрується в модель безперервного вдосконалення, яка зосереджується на постійному зворотному зв’язку між результатами виявлення, аналітики, розслідувань і превентивних заходів. Окремо висвітлюється зв’язок між виявленням шахрайства і процесами управління ризиками, проведенням аудитів, збором розвідувальних даних, а також культуральними аспектами всередині організації, які підтримують або блокують ефективне виявлення зловживань.

Документ детально описує набір обов’язкових і рекомендованих продуктів, які має розробити організація для реалізації функції виявлення шахрайства. Зокрема, йдеться про стратегію виявлення шахрайства (як окрему, так і вбудовану в загальну антикорупційну стратегію), план дій, плани вправ, підсумкові звіти про виявлення, внутрішні маршрути повідомлення про

[6] https://assets.publishing.service.gov.uk/media/682c660160f66b9c23b00c7f/PSFA_Standards_-_Standard_for_Fraud_Detection_Practitioners.pdf

підозру, дашборди та чеклісти. Важливу увагу приділено використанню сучасних інструментів — аналітики даних, штучного інтелекту, машинного навчання, автоматизованих систем моніторингу — що мають стати ядром системного підходу до виявлення шахрайства в умовах цифрової трансформації. Зазначається, що цифрові методи не повинні замінювати людський фактор, оскільки верифікація результатів і розрізнення помилкових спрацьовувань, помилок та справжніх фактів шахрайства вимагають професійної інтерпретації.

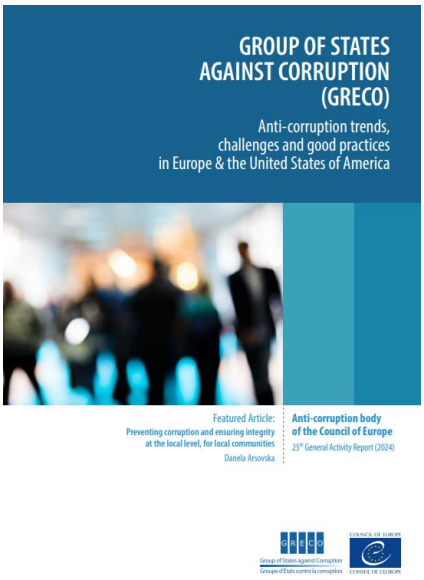
Ключовим аспектом є вимога забезпечити інституційний рівень готовності до виявлення шахрайства, що передбачає регулярну оцінку рівня шахрайства, горизонтальне сканування ризиків, залучення ресурсів (аудитори, аналітики), наявність каналів для конфіденційного інформування та безперервне навчання персоналу. Рекомендовано проводити регулярні тренінги, забезпечити культуру доброчесності та довіри, впровадити політики викривання і залучати працівників усіх рівнів до підтримки механізмів виявлення.

Таким чином, документ є комплексним довідником, який формує уніфікований підхід до професійної діяльності в галузі виявлення шахрайства, поєднуючи нормативну рамку, компетентний підхід, сучасні технологічні практики та стратегічні організаційні механізми. Його структура дозволяє застосовувати підхід як на індивідуальному рівні фахівця, так і на рівні всієї установи, формуючи цілісну, ризик-орієнтовану, інтегровану систему виявлення шахрайства у публічному секторі.

Висновки:

- **Впровадження моделі виявлення шахрайства (FDM) та системи безперервного вдосконалення є обов'язковими для ефективного циклу виявлення–оцінки–дії.:**
  Рекомендація: Інституціям слід створити внутрішні стандартизовані моделі виявлення на основі FDM із фокусом на вхідні ризики, аналітичні дані, контрольні точки та механізм зворотного зв'язку.
- **Формалізована стратегія виявлення шахрайства має бути частиною загальної антикорупційної політики організації, із чіткими цілями, ресурсами та відповідальними.**
  Рекомендація: Розробити окрему або інтегровану стратегію виявлення (із щорічним оновленням) та звітуванням про її виконання на рівні вищого керівництва.
- **Аналітика даних і цифрові інструменти повинні стати ядром підходу до виявлення — особливо в контексті великих масивів даних і нових форм шахрайства (цифрове шахрайство, діпфейки, тощо).**
- **Рекомендація:** Побудувати внутрішню або партнерську команду data science з доступом до інтегрованих джерел даних, з урахуванням вимог GDPR.
- **Роль культури й освіти — фундаментальна. Без участі всього персоналу (включно з контрактниками) неможливо побудувати ефективне середовище для виявлення та повідомлення про шахрайство.**
- **Рекомендація:** Регулярно проводити обов'язкове навчання, підсилювати політику захисту викривачів, і створити внутрішній канал для безпечного повідомлення з анонімністю.

GRECO 2024: Нові виклики та пріоритети антикорупційної політики в Європі та США[7]



Звіт GRECO за 2024 рік, який є двадцять п'ятим Загальним звітом про діяльність Групи держав проти корупції Ради Європи, охоплює глибокий огляд антикорупційної ситуації в державах-членах та у США, а також містить аналітичний огляд основних тенденцій, викликів і прикладів належної практики у боротьбі з корупцією на всіх рівнях влади. Звіт, прийнятий у березні 2025 року, охоплює досягнення попередніх оцінювальних раундів GRECO, зокрема 4-го і 5-го, а також задає напрямок нового — 6-го раунду, який уперше зосереджується на субнаціональному рівні управління.

Змістовним ядром звіту є констатація, що попри певний поступ у розбудові нормативно-правових рамок антикорупційної політики, держави-члени все ще стикаються з глибоко вкоріненими проблемами, такими як брак прозорості, політичний вплив на судову владу, неефективність механізмів виявлення конфлікту інтересів, а також системна слабкість в імплементації антикорупційних заходів у сфері топ-чиновників і правоохоронних органів. GRECO підкреслює, що стійкість демократичних інституцій нерозривно пов'язана з довірою громадськості, яку можна відновити лише за умови реального зміцнення доброчесності, підзвітності та незалежного нагляду за владою. Звіт наголошує, що попри святкування 25-річчя GRECO, реальний стан виконання його рекомендацій у багатьох країнах залишається незадовільним. Особливо це стосується виконання рекомендацій 5-го раунду, який охоплює топ-виконавчі функції (PTEFs) та правоохоронні органи. Усі оприлюднені у 2024 році звіти про виконання рекомендацій показали, що рівень дотримання стандартів у сфері топ-чиновників є критично низьким, що свідчить про структурну неготовність держав ефективно реагувати на ризики політичної корупції на найвищому рівні.

GRECO також фіксує фрагментарність і нерівномірність підходів до запобігання конфлікту інтересів, управління активами, прозорості взаємодії з лобістами та третім сектором, відсутності ефективних санкцій за порушення етичних норм. При цьому, держави-члени продовжують застосовувати добровільні тренінги з етики для PTEFs, але участь у них є низькою, а системи конфіденційного консультування з питань доброчесності — не розгорнуті належним чином. GRECO окремо наголошує на вразливості доступу до публічної інформації, що гальмує прозорість урядових рішень. Пропонується запровадження чітких строків відповіді, обов'язкових механізмів апеляції та посилення незалежних органів нагляду за дотриманням законодавства про доступ до інформації. У звіті також детально описано серйозні прогалини в запровадженні постслужбових обмежень для колишніх високопосадовців, де GRECO рекомендує принаймні дворічний перехідний період перед працевлаштуванням у приватному секторі.

Щодо правоохоронних органів GRECO позитивно оцінює поступ у формалізації кодексів етики, політик щодо подарунків, створення механізмів конфіденційного консультування та запровадження реєстрів подарунків, але наголошує, що без належного фінансування та незалежного нагляду ці заходи залишаються декларативними. Особливо підкреслено необхідність запровадження регулярних перевірок доброчесності, покращення прозорості у наймі й кар'єрному зростанні, а також захисту викривачів. GRECO застерігає, що в багатьох країнах працівники поліції не довіряють чинним механізмам захисту викривачів через

[7] https://rm.coe.int/general-activity-report-greco-2024-045825-gbr-web-final-1-/1680b631a0

відсутність конфіденційності та страх перед репресіями. Водночас позитивним прикладом є країни, що запровадили централізовані електронні системи для фіксації подарунків та доходів, а також приклади окремих країн, які запровадили процедури попереднього доброчесного скринінгу кандидатів на високі посади в поліції.

Значну частину звіту присвячено огляду ситуації з прозорістю політичного фінансування. GRECO звертає увагу на те, що попри законодавчі зрушення щодо розкриття джерел пожертв та витрат, залишаються значні прогалини у сфері фінансування з боку третіх осіб, а також загрози анонімних і закордонних внесків. Відтак рекомендується посилити незалежність контролюючих органів, знизити пороги для звітування, впровадити механізми попереднього аудиту і жорсткі санкції за порушення правил фінансування. GRECO зазначає, що чинна Рекомендація Rec(2003)4 вичерпала свою актуальність, і вимагає її перегляду з урахуванням сучасних політичних і технологічних реалій.

Звіт також вперше інтегрує гендерну перспективу в антикорупційні оцінки. Питання збалансованого представництва жінок і чоловіків, наявність гендерних статистик, механізмів рівного доступу до керівних посад розглядаються як засіб зниження ризиків корупції, уникнення «мислення групи» та зміцнення підзвітності в публічному управлінні. У 6-му раунді цей гендерний аспект буде включений у оцінювання на місцевому рівні.

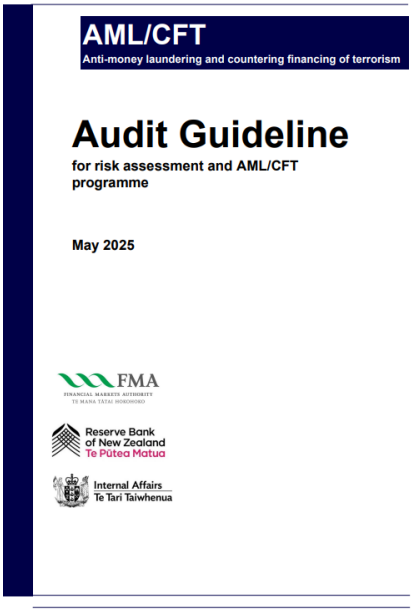
Особливе значення у звіті надано статті Данели Арсовської, яка підкреслює критичну роль субнаціонального рівня у формуванні культури доброчесності. Вона окреслює приклади інноваційних практик, таких як цифрові платформи для прозорості державних закупівель, участь громадськості у формуванні антикорупційної політики, а також навчання для місцевих чиновників. Конгрес місцевих і регіональних влад Ради Європи розробив кілька кодексів, хартій і звітів, що закладають підґрунтя для боротьби з корупцією на рівні муніципалітетів, включаючи регулювання конфліктів інтересів, прозорість бюджету, доступ до інформації, і недопущення зловживань у держзакупівлях. GRECO у 6-му раунді сподівається сформувати базу найкращих практик і посилити обмін досвідом між країнами-членами.

Висновки:

- **Недостатня реалізація рекомендацій у центральних урядах (PTEFs):** У 2024 році не було жодної держави, яка повністю виконала всі рекомендації 5-го раунду; особливо слабкою залишається сфера прозорості, конфлікту інтересів і притягнення до відповідальності топ-чиновників.
- **Правоохоронні органи потребують посилення внутрішнього контролю:** Незалежні механізми інспекцій та захист викривачів залишаються слабкими; GRECO закликає до структурних змін у політиці доброчесності.
- **Нерівномірна імплементація у сфері парламентського контролю та судової доброчесності:** Хоча впроваджено кодекси поведінки і публічні консультації, механізми перевірки декларацій та санкції залишаються неефективними.
- **Новий фокус на місцевому рівні (6-й раунд):** Вперше оцінювання охоплюватиме субнаціональні органи влади з акцентом на етику, прозорість, ґендерну рівність і цифрові інструменти прозорості — Україна має шанс адаптувати локальні антикорупційні політики до європейських стандартів.

Таким чином, звіт GRECO 2024 року не лише підсумовує існуючі антикорупційні прогалини, але й формує системний орієнтир для національних урядів, які прагнуть зміцнити державне управління, ґрунтуючись на доброчесності, верховенстві права та участі громадськості.

Незалежний аудит у системі ПВК/ФТ: практичний посібник для оцінки ризиків і ефективності програм відповідності [8]



Керівництво з аудиту оцінки ризиків та програми запобігання відмиванню коштів та фінансуванню тероризму (ПВК/ФТ), опубліковане у травні 2025 року, розроблено для підтримки суб'єктів фінансового моніторингу у розумінні та ефективному виконанні їхніх обов'язків щодо проведення незалежного аудиту відповідно до Закону Нової Зеландії про запобігання відмиванню коштів і фінансуванню тероризму 2009 року (AML/CFT Act 2009). Документ має прикладний характер і слугує як для самих суб'єктів, так і для осіб, які проводять аудити, щоб забезпечити уніфікований, послідовний та ефективний підхід до перевірок, які є обов'язковими в межах регуляторної системи. Основною метою цього керівництва є не лише нагадати про законодавчі вимоги, а й забезпечити глибше розуміння важливості аудиту як інструменту управління ризиками, посилення внутрішнього контролю, а також зменшення потенційних загроз відмивання коштів і фінансування тероризму.

Згідно з положеннями закону, кожен суб'єкт має забезпечити проведення незалежного аудиту щонайменше раз на три роки (або чотири – за згодою наглядового органу), а також зберігати усю документацію, пов'язану з аудитом, щонайменше протягом п'яти років. Аудит повинен охоплювати як відповідність оцінки ризиків вимогам статті 58(3) закону, так і аналіз програми ПВК/ФТ щодо її адекватності та ефективності в реальному функціонуванні. При цьому аудитор не може бути особою, яка брала участь у розробці або впровадженні оцінки ризиків чи програми ПВК/ФТ, що гарантує незалежність перевірки. Закон не визначає формат чи рівень впевненості, тож вибір залежить від потреб суб'єкта та складності його бізнесу. Документ підкреслює, що незалежний аудит має бути більше, ніж формальністю: це інструмент критичного аналізу того, наскільки ефективно програма працює в практиці, з виявленням не лише невідповідностей, а й можливостей для вдосконалення.

Керівництво надає практичні поради щодо вибору аудитора, з урахуванням критеріїв незалежності, професійної кваліфікації та досвіду у сфері ПВК/ФТ, а також аудиторської практики. Пропонується оцінювати як наявність знань про законодавство, так і обізнаність у специфіці діяльності суб'єкта. Зазначено, що аудит може проводитися як зовнішніми, так і внутрішніми аудиторами, якщо забезпечено незалежність та уникнуто конфлікту інтересів. Значну увагу приділено належній підготовці до аудиту: укладанню письмового договору, наданню необхідних документів, організації доступу до персоналу, клієнтських файлів та результатів внутрішнього моніторингу. Окремо підкреслюється, що інформація зі звітів про підозрілі операції (SARs) не повинна розкриватися аудитору, що відповідає вимогам статті 46 Закону.

Після завершення аудиту аудитор готує письмовий звіт, у якому оцінюється відповідність програм ПВК/ФТ законодавству, ефективність реалізації програм, а також надаються рекомендації щодо усунення виявлених недоліків. При цьому вказується, що навіть якщо запропоноване рішення має необов'язковий характер, сам факт виявлення невідповідності створює обов'язок суб'єкта вжити заходів з її усунення. Важливо, що відсутність реакції на

[8] https://www.dia.govt.nz/diawebsite.nsf/Files/AML-CFT-2025/$file/AMLCFT-Audit-Guideline-May-2025.pdf

виявлені порушення може призвести до регуляторного втручання. У щорічному звіті ПВК/ФТ суб'єкт повинен підтверджувати, що рекомендації були враховані і виправлення проведено.

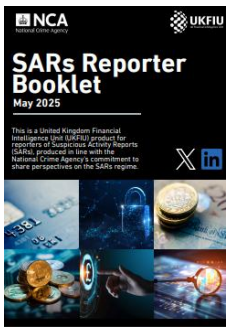
У додатку 1 наведено докладну структуру змісту аудиторського звіту, яку очікують наглядові органи, що включає загальну інформацію про суб'єкта, опис діяльності, кваліфікацію аудитора, межі аудиту, критерії, зобов'язання сторін, методологію перевірки, узагальнення результатів та аудиторський висновок із рекомендаціями. Також можливе включення таблиці спостережень і плану дій для усунення порушень, а також офіційного коментаря менеджменту до виявлених проблем. У додатку 2 деталізовано строки проведення першого та наступних аудитів, зокрема приклади дотримання та порушення термінів, з відповідними наслідками. Підкреслено, що кінцевою датою завершення аудиту вважається дата підписання остаточного звіту, а не дата завершення перевірки, а регулятор може вимагати повторного аудиту, якщо попередній був незадовільним.

Висновки:

- **Обов'язковість незалежного аудиту кожні 3 роки:** Всі суб'єкти фінмоніторингу зобов'язані забезпечити проведення аудиту незалежним і кваліфікованим фахівцем у чітко визначені строки. Недотримання строків тягне за собою можливе регуляторне втручання.
- **Аудит має виявляти не лише формальні порушення, а й оцінювати фактичну ефективність програми ПВК/ФТ:** Звіт повинен охоплювати як відповідність політик законодавству, так і їх практичне впровадження та результативність.
- **Результати аудиту повинні бути враховані у щорічному ПВК/ФТ-звіті:** Суб'єкт повинен документально підтверджувати виконання рекомендацій аудитора, навіть якщо рішення залишено на розсуд організації.
- **Обов'язкове документування обґрунтування вибору аудитора:** Потрібно зберігати пояснення незалежності аудитора та його кваліфікації для подальшої перевірки з боку наглядача.

Документ завершується застереженням, що керівництво має допоміжний, а не юридично зобов'язуючий характер, і не може бути використане як доказ відповідності вимогам закону. У разі неповного розуміння зобов'язань, рекомендується звертатися по юридичну консультацію або до наглядового органу. Загалом керівництво є комплексним і практикоорієнтованим інструментом, що стимулює не лише формальне дотримання вимог, а й розвиток культури управління ризиками, прозорості та належного врядування у сфері ПВК/ФТ.

SARs Reporter Booklet May 2025: Як фінансова розвідка Сполученого Королівства бореться зі злочинністю [9]



Reporter Booklet, підготовлений Національним агентством з боротьби зі злочинністю (NCA) Сполученого Королівства через підрозділ фінансової розвідки (UKFIU), є спеціалізованим виданням, призначеним для суб'єктів, які подають звіти про підозрілу діяльність (Suspicious Activity Reports, SARs).

Цей буклет має на меті інформувати учасників SAR-режиму, зокрема банки, фінансові установи, компанії та інші суб'єкти, про те, як правоохоронні органи використовують фінансову розвідку, отриману через SARs, для боротьби з серйозними злочинами. Він також спрямований на заохочення найкращих

[9] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/750-sars-reporter-booklet-may-2025/file

практик серед підзвітних суб'єктів, надання зворотного зв'язку щодо функціонування SAR-режиму та покращення взаємодії.

Документ містить детальний огляд діяльності UKFIU, яка несе національну відповідальність за прийом, аналіз і поширення фінансової розвідувальної інформації, а також включає знеособлені приклади реальних розслідувань, зібрані у жовтні 2024 року, що демонструють ефективність SARs у виявленні та припиненні таких злочинів, як торгівля наркотиками, шахрайство та відмивання грошей.

У передмові керівник UKFIU Вінс О'Браєн підкреслює, що SARs є критично важливим ресурсом для правоохоронних органів, оскільки надають детальну інформацію, таку як номери телефонів, адреси, дані про компанії, інвестиційну діяльність, банківські рахунки та інші активи. Ця інформація допомагає виявляти сексуальних злочинців, жертв шахрайства, підозрюваних у вбивствах, зниклих осіб, торговців людьми, утікачів і випадки фінансування тероризму.

Значна частина документа присвячена кейс-стаді, які ілюструють, як SARs сприяють розслідуванням. У сфері боротьби з наркотиками один суб'єкт подав SAR, підозрюючи, що бізнес-рахунок клієнта використовується для відмивання £270,000, отриманих від торгівлі наркотиками через готівкові вклади, сторонні перекази та платежі з карт. UKFIU відхилила запит і передала справу до правоохоронців, які вилучили готівку та цінні предмети на суму понад £800,000, а розслідування триває.

В іншому випадку раптовий сплеск активності на раніше неактивному бізнес-рахунку, пов'язаному з мережею фіктивних компаній, призвів до виявлення відмивання £250,000. Правоохоронці конфіскували £60,000 після того, як суб'єкт відмовився від коштів, а також отримали ордер на замороження рахунку (AFO).

У сфері шахрайства SARs допомогли розвинути розслідування щодо компанії, яка фальсифікувала звіти про хімічний склад продуктів, виявивши рух криптоактивів між низько- та високоризиковими рахунками та незаконний продаж хімічних речовин через соціальні мережі, при цьому розслідування триває. В іншому випадку підзвітний суб'єкт подав SAR після виявлення значного зростання готівкових надходжень на рахунок клієнта з судимостями за наркотики, і правоохоронці конфіскували £8,000, спростувавши твердження про виграші в азартних іграх.

Ще один кейс показав, як бізнес-рахунок, що отримав £400,000 від компаній, не пов'язаних із заявленою галуззю, використовувався для приховування злочинного походження коштів, що призвело до виявлення мережі фіктивних компаній, залучених до податкового шахрайства, і конфіскації £40,000.

У сфері відмивання грошей SAR виявив підозрілу діяльність на рахунку директора компанії з ознаками фіктивності, такими як некоректний вебсайт, невідповідність профілю та відсутність реальних операцій, що призвело до конфіскації £300,000 після встановлення, що це була операція з відмивання грошей.

Висновки:

- **Підзвітні суб'єкти повинні проводити ретельні перевірки клієнтів** і використовувати відкриті джерела для підвищення якості SARs, що сприяє успішним розслідуванням і конфіскації активів.
- **Оперативне подання SARs** до UKFIU дозволяє фінансовим установам уникнути юридичних ризиків і підтримати правоохоронні дії.
- **Особливу увагу слід приділяти ознакам фіктивних компаній**, які часто пов'язані з податковим шахрайством і відмиванням грошей.

Буклет наголошує, що ретельні перевірки клієнтів (due diligence) і використання відкритих джерел значно підвищують якість SARs, а оперативна передача інформації UKFIU сприяє швидкому реагуванню правоохоронців. Формат документа є

структурованим і доступним, з акцентом на практичну цінність для репортерів, а знеособлені кейси містять конкретні суми та результати, що підкреслюють ефективність SAR.

Санкції

Міністерство фінансів США запроваджує санкції проти іранської мережі, яка відмиває мільярди для режиму через схему тіньового банкінгу [10]

Міністерство фінансів США нещодавно здійснило рішучі кроки, запровадивши санкції проти розгалуженої іранської "тіньової банківської" мережі. Ця мережа, контрольована та керована братами Мансуром, Насером та Фазлолою Заррінґалам (Mansour, Nasser, and Fazlolah Zarringhalam), була викрита у відмиванні мільярдів доларів для іранського режиму, використовуючи міжнародну фінансову систему. Ця дія є частиною кампанії "максимального тиску" на Іран, спрямованої на перешкоджання його ядерній та ракетній програмам, а також підтримці терористичних проксі-угруповань.

"Тіньова банківська" система Ірану функціонує як паралельна фінансова структура, що дозволяє підсанкційним іранським особам та військовим організаціям отримувати доступ до міжнародної фінансової системи та сприяти іранському експорту. Розрахунки в цій системі здійснюються через іранські обмінні пункти, які використовують підставні компанії, переважно розташовані в Гонконзі та Об'єднаних Арабських Еміратах (ОАЕ), для здійснення або отримання платежів від імені підсанкційних осіб. Для обґрунтування платежів за підсанкційні товари, брокери "тіньового банкінгу" можуть генерувати фіктивні рахунки-фактури або деталі транзакцій. Ці підставні компанії створюються в юрисдикціях з нижчим рівнем регуляторного нагляду, що дозволяє їм уникати ретельного контролю за їхньою діловою практикою та структурою власності. Ця система не тільки фінансує дестабілізуючу діяльність режиму, але й

[10] https://home.treasury.gov/news/press-releases/sb0159

призводить до корупції та розкрадання коштів усередині Ірану, що негативно впливає на іранський народ.

Брати Заррінґалам, використовуючи мережу підставних компаній в ОАЕ та Гонконзі, допомагали підсанкційним чиновникам та пов'язаним з режимом бізнесменам отримувати платежі від продажу нафти, нафтопродуктів та інших товарів. Їхня мережа використовувалася основними іранськими експортерами нафти та нафтохімічної продукції, а також іранськими військовими, для ухилення від санкцій та переміщення коштів. Мансур Заррінґалам та Насер Заррінґалам оперують іранськими обмінними пунктами Mansour Zarrin Ghalam and Partners Company (також відомий як GCM Exchange) та Nasser Zarrin Ghalam and Partners Company (також відомий як Berelian Exchange) відповідно. Ці обмінні пункти контролюють величезну мережу підставних компаній, відкриваючи рахунки в різних валютах для сприяння платежам заблокованих іранських організацій, включаючи Корпус вартових ісламської революції – Сили "Кудс" (IRGC-QF), Фонд Астан Кудс, Національну іранську нафтову компанію (NIOC), Міністерство оборони та логістики Збройних сил Ірану (MODAFL), а також Persian Gulf Petrochemical Industry Company (PGPIC) та її маркетинговий підрозділ Persian Gulf Petrochemical Industry Commercial Co. (PGPICC). За оцінками, Мансур щорічно керував валютними операціями на мільярди доларів, пов'язаними з продажем нафтохімічної продукції PGPIC. Berelian Exchange також залучала співробітників як в Ірані, так і за кордоном, зокрема Фатеме Сарлак Кухі в Ірані та Ю Чжан у Китаї, для координації транзакцій. Третій брат, Фазлола Заррінґалам, керує обмінним пунктом Zarrin Ghalam and Partners Company (також відомий як Zarrin Ghalam Exchange), який допомагав Центральному банку Ірану обмінювати сотні мільйонів доларів і дозволяв Національній іранській танкерній компанії (NITC) розраховуватися з неіранськими компаніями.

Підставні компанії здійснювали операції на сотні мільйонів доларів у різних валютах, включаючи долари та євро. Окрім фінансового бізнесу, сім'я Заррінґаламів контролює інші компанії в різних секторах іранської економіки, зокрема інвестиційну компанію Zarrin Tehran Investment Company та компанію Kimia Sadr Pasargad Company, що працює в нафтогазовому та нафтохімічному секторах. Також були ідентифіковані та піддані санкціям інші члени родини та пов'язані особи, такі як Мітра Заррінґалам,

Висновки:

- **Постійний ризик "тіньового банкінгу" Ірану**: Іранський режим активно використовує складні тіньові банківські мережі та підставні компанії (особливо в Гонконзі та ОАЕ) для обходу санкцій, фінансування своїх ядерних, ракетних програм та терористичних угруповань, що вимагає постійної пильності та адаптації стратегій протидії.
- **Важливість посиленого контролю та звітності:** Фінансові установи повинні невідкладно оновлювати свої внутрішні системи моніторингу та програми з ПВК/ФТ, звертаючи особливу увагу на транзакції, пов'язані з Іраном, а також з Гонконгом та ОАЕ, та повідомляти про будь-яку підозрілу діяльність до відповідних органів, зокрема FinCEN, відповідно до оновлених вказівок.
- **Комплексний підхід до санкцій:** Уряд США використовує різноманітні виконавчі укази та інструменти для цілеспрямованого блокування не тільки основних фінансових посередників, а й їхніх розгалужених мереж, включаючи сімейні економічні інтереси, що підкреслює необхідність глибинного розуміння структури власності та контролю при оцінці ризиків.
- **Використання розвідданих та публічної інформації:** Інформація з відкритих джерел, зокрема з попередніх витоків, може містити цінні дані для виявлення незаконних фінансових схем, що свідчить про доцільність інтеграції розвідданих з різних джерел у процеси належної перевірки та аналізу фінансових ризиків.

Парвіс Солтанізаде, Хоссейн Шетабан, Фарахназ Мешкат та Пурія Заррінґалам, які обіймали керівні посади в цих компаніях.

Запроваджені санкції означають, що все майно та майнові інтереси цих осіб, які перебувають у США або під контролем осіб зі США, заблоковані та повинні бути повідомлені до Управління з контролю за іноземними активами (OFAC). Порушення санкцій США можуть призвести до цивільних або кримінальних покарань, а також до значних ризиків для фінансових установ, які взаємодіють із підсанкційними суб'єктами. Хоча метою санкцій є зміна поведінки, а не покарання, OFAC має право застосовувати суворі заходи. Паралельно, Мережа боротьби з фінансовими злочинами (FinCEN) Міністерства фінансів випустила оновлену консультацію, щоб допомогти фінансовим установам виявляти, запобігати та повідомляти про підозрілу діяльність, пов'язану з незаконною фінансовою активністю Ірану, включаючи контрабанду нафти, "тіньовий банкінг" та закупівлю зброї. Ці дії базуються на Виконавчих указах (E.O.) 13902 та 13846, які стосуються фінансового, нафтового та нафтохімічного секторів Ірану. Примітно, що подібні мережі вже викривалися раніше, а детальна інформація про діяльність мережі Мансура Заррінґалама, включаючи банківські рахунки та SWIFT-коди, була доступна у публічному домені через попередні витоки ще у 2022 році.

Звіти окремих інституцій та експертів

Майбутнє стейблкоїнів [11]

У документі автор переконливо доводить, що стрімка еволюція сектору стейблкоїнів наблизила його до критичної межі, за якої відсутність єдиного технічного та регуляторного каркаса перетворить ринок на «зоопарк» несумісних токенів, здатний лише частково виконувати платіжну функцію. Вступна частина пояснює, що саме узгоджений мінімалістичний стандарт ERC-20 колись увімкнув ефект мережевого вибуху для усієї DeFi-екосистеми, а отже галузі конче потрібна подібна «угода другого покоління» щодо стейблкоїнів, інакше розрізнені підходи до емісії, викупу та нагляду посилюватимуть операційні, системні й ПВК/ФТ ризики.

Центральну частину праці становить докладний розбір семи взаємопов’язаних вимірів, які, на думку автора, повинні лягти в основу глобального стандарту.

- Перший вимір — «баланс активів»: запропоновано доповнити класичну логіку mint/burn обов’язковими функціями deposit/withdraw і публічним on-chain показником totalCirculating, щоб в багатоланцюговому середовищі завжди було видно, скільки токенів реально в обігу та де саме вони перебувають; прозорість резервів забезпечують оракули Proof-of-Reserve, а їхній склад відкриває proof-of-composition-мапа, що розкриває конкретні активи до рівня ISIN.
- Другий вимір — «комплаєнс»: від елементарних чорних/білих списків еволюція йде до модульних rule-engine-блоків на кшталт ERC-3643, які через децентралізовані ідентифікатори (ONCHAINID, DID-графи) дозволяють динамічно застосовувати санкційні режими, правила travel rule, кількісні ліміти чи навіть ініціювати примусові трансфери у разі судових рішень, причому ядро токена лишається незмінним.

[11] https://www.kcl.ac.uk/business/assets/PDF/qcgbf-working-papers/taking-the-next-step-stablecoins.pdf

- Третій вимір — «інтероперабельність»: щоб ліквідність стейблкоїна не «розсипалася» по різних блокчейнах, усі мережі мають поводитися з ним однаково. Це означає: однакові правила для створення монет (mint) і їхнього знищення (burn) у кожному ланцюзі; відкритий список «locker»-адрес, куди міст упевнено «паркує» токени під час переказу; і докладні журнали подій смарт-контракту, які фіксують кожен крок монети. Тоді бридж-протоколи, наприклад Chainlink CCTP, можуть переносити той самий стейблкоїн між мережами так само легко, як надсилати електронний лист, а аудитори отримують машинно-читані підтвердження, що жодна монета не була створена двічі чи загублена.
- Четвертий вимір — «приватність»: нинішні підходи (міксери, зовнішні ZKP-сервіси, прототип Circle × Inco на базі FHE) ще зарано жорстко кодувати в стандарт, але потрібні розширювані інтерфейси, здатні підключати ZK-або FHE-шари без оновлення основного контракту, щоб одночасно зберегти регуляторну прозорість і захищати комерційну таємницю бізнес-користувачів.
- П’ятий вимір — «комісії та дохідність»: навіть якщо сьогодні більшість стейблкоїнів «нічого не заробляє» і не бере плати за переказ, у коді токена вже зараз треба передбачити гнучкі налаштування. По-перше, змогу легко змінювати розмір комісії (наприклад, зробити її символічною чи, навпаки, підняти для покриття витрат). По-друге, «роз’єм» ERC-4626 — це такий додатковий модуль, який дозволить під’єднати токен до джерел прибутку (наприклад, короткострокові державні облігації чи депозити) і виплачувати власникам відсотки, коли регулятори дадуть на це зелене світло.
- Шостий вимір — «ролі та події»: у смарт-контракті стейблкоїна не має бути одного всесильного «господаря». Замість цього вводяться окремі ролі з чіткими повноваженнями: хтось створює нові монети (mint), хтось їх спалює (burn), хтось веде список дозволених адрес (list-admin), хтось може тимчасово зупинити роботу контракту (pause), а ще інший — оновлювати код (upgrade). Для кожної ролі контракт публікує зрозумілу довідку (getRoleInfo) й автоматично записує події, коли права передаються або змінюються. Завдяки цим подіям зовнішні системи одразу бачать, хто саме та на яких умовах отримав доступ, що особливо важливо для контролю ПВК/ФТ і перевірок аудиторів.
- Сьомий вимір — «гнучка послідовність»: фінальний стандарт має бути достатньо строгим, аби гарантувати взаємозамінність і довіру до резервів, але водночас відкритим для майбутніх модулів приватності, токенізованого прибутку чи навіть інтеграції з CBDC-

Висновки:

- Емітенти, які прагнуть регуляторної легітимності, уже сьогодні мають запровадити mint/burn, totalCirculating та публічні журнали резервів із PoR, інакше вони не пройдуть перевірку платоспроможності.
- Щоб виконати вимоги travel-rule і санкцій, проєктуйте токен із модульним rule-engine-інтерфейсом і сумісністю з будь-якою системою DID; це дасть змогу швидко адаптуватися під різні юрисдикції без переписування коду.
- Для безпечного мультичейна публікуйте офіційні «locker»-адреси, ведіть події про рольові зміни й стандартизований getRoleInfo — це скоротить час аудиту та спростить підключення до канонічних бриджів.
- Вбудуйте параметри fee-rate/maxFee та опціональний ERC-4626-шар: навіть якщо зараз комісії й відсоток нульові, готова інфраструктура дозволить швидко монетизувати продукт або запустити версію з дохідністю, коли регулятор дасть зелене світло.

містками; отже, автор пропонує багато-шаровий протокол, де базове ядро стабільне, а периферійні функції розгортаються за схемою opt-in / plug-in.

Завершальний розділ підкреслює, що відсутність «мінімального спільного знаменника» вже сьогодні заважає регуляторам узгоджувати правила, банкам — інтегрувати стейблкоїни у платіжні коридори, а користувачам — отримувати передбачуваний захист прав, тому автор закликає індустрію, регуляторів і стандартизаторів узгодити описані виміри у вигляді відкритого ERC-стандарту з подальшим імплементаційним гайдом для національних режимів ПВК/ФТ.

Стан Web3 та криптовалют у Франції та Європі [12]

Консалтингова команда Adan і Deloitte оприлюднили четверте щорічне дослідження «Web3 & Crypto in France and Europe — towards sustainable and institutional adoption», об'єднавши репрезентативне соціологічне опитування двох тисяч французів і зріз у 1 000 респондентів по п'яти інших країнах ЄС із глибинними інтерв'ю та анкетою 82 компаній-учасниць екосистеми. Автори фіксують рекордну поінформованість: 92 % французів бодай раз чули про цифрові активи, що на 8 п. більше, ніж 2024-го, тоді як знайомство з NFT підскочило до 45 % (+9 п.). Реальний рівень володіння криптоактивами після стрибка 2023-го стабілізувався на 10 % населення (≈ 5,5 млн осіб), але інтерес до першої покупки зростає: частка «потенційних інвесторів» у Франції піднялася до 33 %, у Німеччині — до 30 %, а в Італії — вже 39 %. У середньому власники тримають у крипті 15 % заощаджень, причому 64 % не перевищують 10 % свого портфеля та 80 % інвестували менше €10 000, що свідчить про зважений ризик-менеджмент після волатильних років . Соціальне ядро інвестора лишається незмінним: 42 % — молодь 18–34, 45 % — вищі соціально-професійні категорії, 67 % — чоловіки.

Французький роздрібний інвестор дедалі більше прагне «банк як шлюз»: 32 % опитаних (+10 п.) уже називають традиційний банк головною довіреною точкою входу у криптоактиви, а чверть готові змінити обслуговуючий банк заради доступу до кастодіальних і торгових функцій; серед чинних інвесторів готовність перейти сягає 65 %. Паралельно 43 % французів хотіли б користуватися цифровим євро, якщо буде гарантовано захист даних, що відкриває прямий попит на регульовані стейблкоїни й токенізовану ліквідність.

У корпоративному зрізі 60 % респондентів — чисті Web3-стартапи, решта 40 % — традиційні корпорації з частковими блокчейн-проєктами. Сектор залишається екосистемою мікро- та малих підприємств: 51 % «чистих» компаній мають річний виторг < €2 млн, тоді як великі інститути входять переважно як пілотні підрозділи. Після 11-відсоткового провалу наймів 2023-го бізнес повернувся до експансії: 63 % компаній збільшили штат, а 76 % планують нові вакансії 2025 р. Насамперед шукають IT-фахівців (64,5 %), комплаєнс-офіцерів (40,3 %), сейлз- і BD-команди (≈ 38 %) — саме ці ролі критичні для дотримання MiCA й виходу на інституційного клієнта.

Фінансування залишається вузьким горлечком: 65 % спеціалізованих підприємств уже залучали капітал, але переважно на pre-seed/seed-етапах; на угоди серій A–C припадає лише 28 %

[12] https://www.adan.eu/wp-content/uploads/2025/04/ETUDE25-ENGLISH.pdf

вибірки. Загальноєвропейська частка у світових Web3-раундах торік скоротилася з 27 % до 21 % (≈ $2,1 млрд), тоді як США утримують 47 % ($4,6 млрд), а Азія зрівнялася з Європою . Дослідники пов'язують відтік з «регуляційним тягарем» і дефіцитом місцевого венчурного капіталу: у 79 % випадків європейські стартапи отримують гроші з-за меж ЄС.

Регуляторика визначає темп ринку: 49 % компаній уже підпадають під MiCA, але ставлення різниться. Великі групи вітають гармонізацію, тоді як Web3-стартапи називають ключовими бар'єрами річні строки та високу вартість доведення комплаєнсу під норми законодавства і відсутність негайних переваг у відносинах із банками; лише 22 % учасників зафіксували покращення доступу до фінпослуг після старту перехідного періоду . Додатковий тиск створюють «Travel Rule» і DORA, а 33 % опитаних зіштовхнулися з обліковими труднощами та 24 % — з податковими колізіями у зарахуванні токенів на баланс.

Попри ці виклики, звіт фіксує фундаментально позитивний тренд: ринок праці знову росте, корпоративний інтерес до токенізації, DeFi й цифрової ідентичності підживлює попит на спеціалістів, а споживачі дедалі частіше очікують криптопродуктів саме від регульованих банків. Автори роблять висновок, що Європа перебуває на стратегічному роздоріжжі: аби уникнути відтоку талантів і капіталу за Атлантику, регуляторам слід поєднати строгі стандарти безпеки з прискореними процедурами, а приватному сектору — консолідувати локальне фінансування та масштабувати освітні ініціативи, щоб перетворити високе зацікавлення у стале масове прийняття.

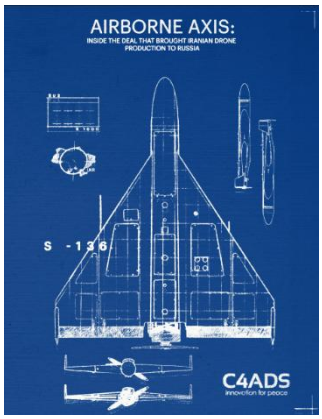
Висновки:

- **Прискорити видачу ліцензій і спростити доступ до банків:** регуляторам слід запровадити спрощені, швидкі процедури для отримання дозволів за MiCA та здешевити дотримання вимог, адже затримки вже змушують стартапи переносити діяльність до США й Азії.
- **Збільшити частку європейського капіталу:** сьогодні лише 32% раундів фінансуються з ЄС; створення спеціалізованих фондів (наприклад, €25 млн від Bpifrance) треба масштабувати до середніх чеків €50–100 млн, щоб утримати лідерів на континенті.
- **Інституалізувати AML/CFT-фреймворк для Web3:** компаніям слід інвестувати в кадри комплаєнсу (40% планують найм) та інтегрувати аналітику блокчейна; для DeFi запропоновано модель сертифікації смарт-контрактів, яку потрібно нормативно закріпити.
- **Банкам — виходити на ринок як довірений провайдер:** 32% французів уже хочуть управляти криптоактивами через свій банк, а 66% потенційних інвесторів очікують банківської пропозиції; інтеграція кастодіальних і платіжних сервісів знизить бар'єр входу й підвищить відслідковування транзакцій.

Як Іран і Росія об'єднали зусилля для виробництва дронів Shahed-136 [13]

Документ підготовлений C4ADS (Центром передових оборонних досліджень), є ґрунтовним аналізом співпраці між Іраном і Росією у сфері виробництва безпілотних літальних апаратів (БПЛА), зокрема моделі Shahed-136, яка активно використовується Росією у війні проти України. Звіт базується на масштабному витоку даних, отриманих хакерською групою Prana Network 4 лютого 2024 року, а також на додаткових відкритих джерелах, що дозволяють детально простежити складну мережу транзакцій, логістичних операцій і державних зв'язків, які забезпечують цю співпрацю. Документ розкриває, як Іран передає технології виробництва

[13] https://c4ads.org/wp-content/uploads/2025/05/SaharaThunder-FinalLayout-1.pdf



дронів російській компанії Alabuga JSC, що дозволяє Росії локалізувати їхнє виробництво, обходячи міжнародні санкції через посередників, альтернативні платіжні системи та логістичні схеми, такі як перевезення через Каспійське море.

Звіт розпочинається з опису контексту, підкреслюючи, що співпраця між Іраном і Росією є частиною їхньої ширшої військової взаємодії, яка поглиблюється через спільні виклики, пов'язані з міжнародними санкціями. Основна увага приділена угоді між іранською компанією Sahara Thunder і російською Alabuga JSC, яка забезпечує передачу технологій, креслень, вихідного коду та навчання для виробництва Shahed-136, відомого в Росії як Geran-2. Ці БПЛА стали ключовим елементом російської стратегії в Україні, де з початку війни було застосовано понад 10 000 таких дронів проти військових, цивільних та економічних цілей. Звіт наголошує, що ця співпраця не лише забезпечує Росію дешевими та ефективними озброєннями, але й демонструє, як країни, що перебувають під санкціями, можуть адаптуватися до глобальних обмежень.

Методологія дослідження є багатошаровою та включає аналіз 10 ГБ даних від Sahara Thunder, що містять 10 685 електронних листів і 45 PDF-файлів, пов'язаних з угодою з Alabuga JSC. Додатково використано витоки від Safiran Airport Services (SAS), компанії, що знаходиться під санкціями США у вересні 2022 року за координацію авіарейсів між Іраном і Росією. Для обробки даних C4ADS застосували машинне навчання, створивши велику мовну модель на основі email-архівів, що дозволило швидко ідентифікувати ключові зв'язки та операції. Аналітики також провели технічне дослідження уламків Shahed-136, знайдених в Україні, щоб підтвердити локалізацію виробництва в Росії. Корпоративні дані з Іранської газети та інших джерел допомогли ідентифікувати компанії та осіб, залучених до угоди, а реєстри суден, дані AIS і позиціонування літаків дозволили відстежити логістичні маршрути, зокрема через Каспійське море.

Ключовими гравцями угоди є Sahara Thunder, іранська компанія, заснована в 1992 році, яка діє як посередник у оборонних операціях і має тісні зв'язки з іранським урядом, та Alabuga JSC, російська компанія в особливій економічній зоні Alabuga SEZ, що підтримується російським урядом для розвитку оборонної промисловості. Sahara Thunder відома своєю участю в закупівлі військових аеростатів у Росії та Китаї з 2016 року, що підкреслює її роль у міжнародних оборонних угодах. Для приховування прямих контактів між сторонами використовувалися посередники з ОАЕ, зокрема компанія Generation Trading FZE, яка в травні 2023 року поставила Alabuga Machinery LLC (дочірній компанії Alabuga JSC) нержавіючу сталь на суму 100 млн дирхамів (27,2 млн доларів США).

Угода, підписана в листопаді 2022 року, мала на меті локалізувати в Росії виробництво 2400 БПЛА Shahed-136 на рік, із планом виготовити 6000 одиниць за 2,5 роки. Загальна вартість контракту склала 108,5 млрд рублів (приблизно 1,75 млрд доларів США), включаючи постачання 6000 комплектів БПЛА, передачу технологій для двигунів MD-550, авіоніки, ракетних прискорювачів і бойових частин, а також 300 000 годин навчання в Ірані та Alabuga SEZ. Початкові інвестиції Alabuga JSC склали 48 млрд рублів, з яких 36 млрд рублів перераховано Ірану, а 12 млрд рублів спрямовано на розвиток інфраструктури в Alabuga SEZ. Вартість одного БПЛА оцінена в 12 млн рублів (193 000 доларів США), що значно вище за історичні оцінки Ірану (30 000–50 000 доларів США) через додаткові витрати на навчання, ліцензії та інфраструктуру. Між квітнем і липнем 2023 року сторони підписали додаткові контракти на постачання матеріалів, таких як нержавіюча сталь і дроти.

Співпраця вже дала результати на полі бою в Україні, де Росія перейшла від імпорту іранських Shahed-136 до виробництва їхнього аналога Geran-2. Аналіз уламків підтверджує, що Росія

досягла значного прогресу в локалізації виробництва. Звіт детально описує характеристики мережі, що забезпечує цю співпрацю: використання посередників з ОАЕ для мінімізації прямих контактів, логістика через Каспійське море, комбіновані платіжні системи (банківські перекази через ОАЕ та поставки золота) для обходу санкцій, а також розвиток відносин через взаємні візити, які вийшли за межі виробництва БПЛА і охоплюють інші оборонні галузі. Хронологія подій включає ключові етапи: підписання угоди в листопаді 2022 року, переговори в січні–лютому 2023 року, початок поставок через ОАЕ в березні 2023 року та додаткові контракти в липні 2023 року.

Звіт завершується висновком, що співпраця між Іраном і Росією є прикладом взаємозалежності країн під санкціями, які використовують складні схеми для підтримки військової діяльності. Для міжнародних організацій та країн, які прагнуть миру в Україні, важливо розглядати Росію та Іран як взаємопов'язаних суб'єктів, а не ізольовано. Документ підкреслює необхідність посилення санкцій проти посередників, моніторингу логістичних шляхів і контролю за альтернативними платіжними системами, щоб ускладнити подібні операції в майбутньому.

Висновки:

- **Посилення санкційного тиску на посередників:** Для припинення співпраці необхідно запровадити цільові санкції проти компаній-посередників, таких як Generation Trading FZE в ОАЕ, які забезпечують логістику та фінансові операції. Рекомендується міжнародним організаціям, зокрема ООН та США, розширити моніторинг діяльності компаній в ОАЕ, які можуть бути залучені до подібних схем.
- **Моніторинг логістичних шляхів через Каспійське море:** Міжнародним партнерам слід посилити відстеження морських перевезень через Каспійське море за допомогою AIS та супутникових даних. Це дозволить виявляти та блокувати поставки обладнання для виробництва БПЛА.
- **Контроль за альтернативними платіжними системами:** Необхідно розробити механізми для відстеження та блокування альтернативних платіжних систем, таких як поставки золота, які використовуються для обходу фінансових санкцій. Фінансові регулятори мають співпрацювати з країнами, що є хабами для таких операцій (наприклад, ОАЕ).
- **Розширення аналізу витоків даних:** Міжнародним аналітичним організаціям варто інвестувати в технології обробки великих обсягів даних, подібних до витоків Sahara Thunder, для швидкого виявлення нових посередників та мереж. Це може включати створення спеціалізованих мовних моделей для аналізу корпоративних даних.

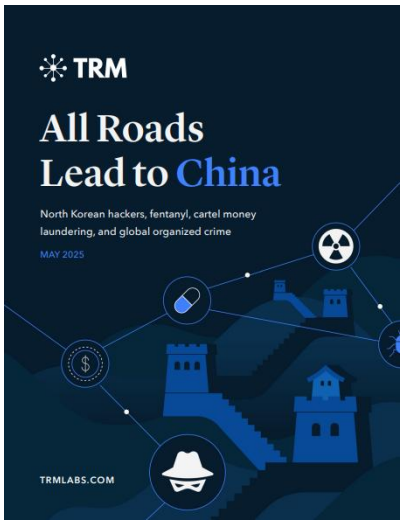
Китайські підпільні мережі та глобальна злочинність [14]

Звіт TRM Labs, є ґрунтовним дослідженням ролі китайських підпільних банківських мереж у глобальній транснаціональній злочинності, зокрема у відмиванні грошей, торгівлі наркотиками, кіберзлочинах та ухиленні від санкцій. Ці мережі, часто відомі як "фей цянь" або "літаючі гроші", функціонують поза межами традиційних фінансових регуляцій, створюючи паралельну банківську систему, яка забезпечує швидкий, псевдонімний рух капіталу через кордони.

Звіт детально описує, як ці мережі використовують криптовалюту для прискорення транзакцій і ускладнення їх відстеження правоохоронними органами, залучаючи до співпраці таких

[14] https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/6830867ef8d6cb74cf00974f_TRM_All%20Roads%20Lead%20to%20China_Report.pdf

суб'єктів, як північнокорейські хакери, мексиканські наркокартелі, російські злочинні синдикати та китайські тріади, які спільно експлуатують ці канали для легалізації незаконних доходів.



Документ розкриває механізми роботи китайських підпільних банків, які діють як фінансова магістраль для злочинців у всьому світі. Одним із ключових методів є так званий "дзеркальний обмін" (mirror exchange), який дозволяє обмінювати кошти без їх фізичного переміщення через кордони. Наприклад, наркодолари, отримані від торгівлі в США, обмінюються на юані в Китаї через посередників, які використовують криптовалюту або торгівлю товарами для розрахунків. У такій схемі долари залишаються в США, юані — в Китаї, а цінність передається без банківських переказів, що мінімізує ризики виявлення регуляторами.

Криптовалюти, зокрема біткойн і стейблкойни, відіграють центральну роль у цих операціях, дозволяючи миттєво переміщувати кошти через блокчейн. Наприклад, наркоторговці можуть конвертувати готівку в криптовалюту через крипто-АТМ у США, після чого ці активи передаються китайським брокерам для подальшого відмивання або інвестування в товари, такі як прекурсори для наркотиків. Ще одним поширеним методом є торгівля на основі відмивання грошей (TBML), де злочинці використовують фальсифіковані інвойси, підставні компанії та товарні операції, щоб замаскувати незаконні кошти під легітимну торгівлю. Криптовалюти посилюють ефективність TBML, оскільки платежі за фіктивні товари можуть здійснюватися через блокчейн, уникаючи банківських перевірок.

Звіт наводить конкретні приклади діяльності злочинних груп, які використовують ці мережі. Північнокорейські хакери, зокрема група Lazarus, викрадають мільярди доларів у криптовалюті через атаки на біржі, як у випадку з Bybit у лютому 2025 року, коли було вкрадено 1,5 мільярда доларів. Ці кошти відмиваються через китайських позабіржових (OTC) брокерів, які конвертують криптовалюту у фіат або товари, обходячи міжнародні санкції. Наприклад, північнокорейський банкір Sim Hyun Seop, знаходячись у китайському місті Дандонг, співпрацював із брокерами в Китаї та Гонконзі, такими як Wu Huihui і Chen Hong Man, для закупівлі санкційних товарів через підставні компанії.

Ці операції дозволяли Пхеньяну фінансувати свої збройні програми. Мексиканські картелі, такі як Сіналоа, також активно співпрацюють із китайськими мережами для відмивання доходів від наркотиків. У Лос-Анджелесі один із осередків відмив понад 50 мільйонів доларів через торгівлю товарами та криптовалютні транзакції, використовуючи криптовалюту для швидкого переказу коштів до Мексики без банківських проводок.

Китайські тріади, такі як 14K і Sun Yee On, інтегрували криптовалюту у свої схеми відмивання через казино (як фізичні, так і онлайн) та шахрайські кол-центри в Південно-Східній Азії. Вони використовують казино для обігу незаконних коштів, видаючи їх за виграші, а також платять криптовалютою за прекурсори для виробництва фентанілу та метамфетаміну. Звіт зазначає, що 97% китайських постачальників таких прекурсорів приймають криптовалютні платежі, що підкреслює глибоку інтеграцію криптовалюти в наркоторгівлю.

Російські злочинці та підсанкційні суб'єкти також використовують китайські мережі для обходу санкцій, оплачуючи військове обладнання, наприклад, дрони та оптику, криптовалютою. TRM виявив перекази на 85 мільйонів доларів із 2021 року між російськими та китайськими суб'єктами, що свідчить про використання криптовалюти для санкційного обходу.

Звіт детально аналізує методи, які дозволяють цим мережам уникати виявлення. Злочинці використовують юрисдикційний арбітраж, проводячи операції в країнах зі слабким регулюванням KYC. Криптовалютні інструменти, такі як міксери, децентралізовані біржі (DEX), крос-чейн містки та приватні монети, дозволяють заплутувати сліди транзакцій.

У кейсі Bybit хакери швидко конвертували вкрадені активи з Ethereum у Bitcoin через THORChain і міксери, такі як Wasabi Wallet, створюючи значні труднощі для відстеження. Шифровані комунікації через WeChat, Telegram і WhatsApp ускладнюють перехоплення інформації, а мовні та культурні бар'єри перешкоджають західним правоохоронцям розшифровувати навіть перехоплені повідомлення. Злочинні мережі демонструють високу адаптивність, швидко переходячи на нові платформи чи методи, коли старі стають уразливими. Наприклад, після закриття російської біржі Garantex, яка була популярною серед північнокорейських і російських хакерів, вони оперативно знайшли альтернативні канали для відмивання.

Висновки:

- **Посилення регулювання криптобірж:** Для зменшення відмивання коштів необхідно запровадити суворіші KYC-вимоги на криптовалютних біржах, особливо в юрисдикціях зі слабким наглядом, щоб обмежити діяльність OTC-брокерів, які співпрацюють із злочинцями.
- **Міжнародна координація правоохоронців:** Успішна боротьба з транснаціональними мережами вимагає співпраці між країнами для обміну розвідданими та координації санкцій проти бірж (як Garantex) і брокерів, що сприяють відмиванню.
- **Використання блокчейн-аналітики:** Правоохоронні органи повинні інвестувати в передові інструменти аналізу блокчейну, які дозволяють відстежувати складні транзакції через міксери та крос-чейн містки, як у кейсі Bybit.
- **Наступальні кібероперації:** Для зриву діяльності злочинних мереж, таких як північнокорейські хакери чи китайські тріади, слід застосовувати активні кіберстратегії, включаючи заморожування активів і блокування доступу до криптобірж.

У висновках звіту підкреслюється, що попри складність цих мереж, вони не є невидимими. Блокчейн-аналітика, міжвідомча співпраця та наступальні кібероперації дозволяють правоохоронцям відстежувати й блокувати незаконні транзакції. Успішні приклади включають санкції проти Garantex і звинувачення проти брокерів, які співпрацювали з Північною Кореєю.

Звіт наголошує, що криптовалюта, хоча й приваблива для злочинців через свою швидкість і псевдонімність, також є інструментом для правоохоронців завдяки прозорості блокчейну. Для ефективної боротьби з цими мережами необхідні посилення регулювання криптобірж, міжнародна координація, інвестиції в аналітичні інструменти та активні кіберстратегії, такі як заморожування активів. TRM Labs, компанія з Сан-Франциско, що спеціалізується на блокчейн-аналітиці, відіграє ключову роль у цьому процесі, надаючи рішення для виявлення та розслідування криптозлочинів, які використовуються правоохоронними органами, фінансовими установами та криптокомпаніями по всьому світу.

Starlink як інструмент війни: трансформація бойових дій і геополітики [15]

Публікація від Global Initiative висвітлює складну й загрозливу ситуацію, що склалася в регіоні Сахелю внаслідок стрімкого розповсюдження супутникової інтернет-технології Starlink серед збройних угруповань і злочинних мереж. Доповідь розкриває, як ця технологія, покликана

[15] https://riskbulletins.globalinitiative.net/wea-obs-012/02-how-starlink-devices-are-shaping-conflict-and-crime-in-Sahel.html

забезпечити віддалені регіони планети доступом до швидкісного Інтернету, перетворилася на інструмент підтримки насильства, терору й незаконної торгівлі в регіонах, де влада держав є слабкою, а конфлікти – хронічними.

Starlink, система супутникового інтернету компанії SpaceX, стала одним із найважливіших технологічних факторів сучасної війни — як на прикладі повномасштабної агресії Росії проти України, так і в конфліктах і збройній злочинності на території країн Сахелю. В обох регіонах ця система забезпечила бойовим структурам високошвидкісний, мобільний і незалежний від місцевої інфраструктури зв'язок.

У випадку України вона відіграла ключову роль у забезпеченні Збройних сил засобами координації, управління дронами, передачі розвідданих і підтримки тилових операцій, особливо у перші критичні місяці вторгнення, коли звичайні системи були виведені з ладу або знищені. Зокрема, Starlink застосовувався в Маріуполі для зв'язку з підрозділами, які обороняли завод «Азовсталь», а також у Херсоні після деокупації, де завдяки системі вдалось швидко відновити зв'язок. Технологія стала опорою для сучасного бойового управління: дрони передавали зображення в реальному часі, артилерія швидше отримувала цілі, а командири оперативно координували дії з планшетів у польових умовах. Україна отримала десятки тисяч терміналів Starlink за підтримки США, Польщі, ЄС та безпосередньо компанії SpaceX, яка на початку надавала послуги безкоштовно.

Однак той самий набір функцій зробив Starlink надзвичайно привабливим і для «сил зла». У Сахелі, де інфраструктура фактично відсутня, а контроль держав слабкий, терористичні організації (такі як ISWAP, JNIM та сепаратисти FLA) й організовані злочинні мережі широко використовують Starlink для координації атак, ухилення від переслідувань, управління контрабандою та пропаганди в інтернеті. Термінали постачаються через добре організовані контрабандні маршрути з Нігерії, Лівії та Чаду. Вони легко ховаються, розбираються на частини й продаються за цінами у 400–600 євро, а прибутки з підписок знімаються через посередників. Ці

Висновки:

- **Starlink став критичним військовим інструментом** — в Україні технологія забезпечує високошвидкісний зв'язок, управління дронами та оперативну координацію ЗСУ, тоді як у Сахелі терористичні й злочинні угруповання використовують Starlink для ухилення від контролю, комунікації в реальному часі та посилення бойових спроможностей у віддалених зонах.
- **Використання Starlink приватними, неконтрольованими суб'єктами створює серйозні ризики безпеки —** система легко потрапляє до рук незаконних користувачів завдяки контрабанді, корупції й слабкому регуляторному нагляду, що підриває національні зусилля зі стабілізації ситуації як у Сахелі, так і в зонах окупації в Україні.
- **Приватний контроль над критичною інфраструктурою породжує геополітичні виклики** — Ілон Маск та компанія SpaceX фактично мають важелі впливу на хід бойових дій, обмежуючи або активуючи доступ до Starlink у конфліктних зонах, що створює прецедент втручання комерційних акторів у питання війни і миру.
- **Технологія Starlink трансформує природу сучасних конфліктів,** підвищуючи роль інформаційної мобільності та комунікаційної переваги. Військова ефективність дедалі більше залежить не лише від озброєння, а й від здатності підтримувати стійкий, зашифрований, незалежний зв'язок у реальному часі, що кардинально змінює стратегії командування і тактики на полі бою.

злочинні мережі також надають «обслуговування» кінцевим користувачам — бойовикам і бандам — збираючи з них плату готівкою. Технологія дає змогу терористам вести бойові операції у повній тиші радіоефіру та координувати зусилля у реальному часі. У липні 2024 року сепаратисти в Малі використали Starlink для координації боїв із військами Малі та найманцями ПВК «Вагнер», а також для розповсюдження пропаганди через соцмережі.

У контексті України з середини 2023 року з'явились підтвердження використання Starlink російськими окупаційними силами, незважаючи на офіційну заборону SpaceX. За даними української розвідки, тисячі терміналів потрапили до армії РФ через треті країни, і використовуються для шифрованого зв'язку, управління дронами та швидкої координації наступів. Це значно підвищило мобільність і живучість російських підрозділів. SpaceX і Пентагон заявили про наміри припинити несанкціоноване використання Starlink і блокування таких терміналів, однак підтвердження про їхню присутність на фронті надходять регулярно.

Усе це викликало широку дискусію про межі контролю приватної компанії над воєнною інфраструктурою. Засновник SpaceX Ілон Маск неодноразово втручався в політичні аспекти війни: у 2022 році він відмовився активувати Starlink над Кримом, вважаючи це актом ескалації проти РФ, що зірвало ударну операцію України. У США почались парламентські слухання про контроль використання Starlink та можливе зловживання монополією у сфері оборонного зв'язку. Маск натомість започаткував ініціативу Starshield — окрему мережу виключно для держав і армій.

Таким чином, у двох дуже різних регіональних контекстах — на Сході Європи та в зоні Сахелю — технологія Starlink стала критично важливим ресурсом, що забезпечує інформаційну перевагу, бойову ефективність і мобільність. Але водночас вона продемонструвала нові виклики: з одного боку, це залежність національних урядів від приватного постачальника комунікацій, з іншого — новий вимір конфлікту, де інформаційна перевага вирішується не стільки арміями, скільки алгоритмами, пропускною здатністю та GPS-координатами.

Рекомендовані матеріали

Про напади на Charlie Hebdo та фінансування тероризму від Франсуа Моліна [16]

Відео, що є частиною серії "Ask the Experts" від EU Global Facility, присвячене ключовій ролі фінансової розвідки у боротьбі з тероризмом та організованою злочинністю. Головним спікером виступає Франсуа Молін, колишній державний прокурор Парижа та почесний генеральний прокурор Касаційного суду.

Франсуа Молін підкреслює, що фінансування є критично важливим елементом для здійснення терористичних атак. Він наводить конкретні приклади вартості таких атак: напад 13 листопада (Vendredi 13) коштував приблизно 100 000 євро, а атаки на Charlie Hebdo та Montrouge оцінюються в 35 000 – 40 000 євро. Ці цифри демонструють, що для терористичної діяльності потрібні значні кошти, навіть якщо здається, що атаки можуть бути "дешевими" за виконанням, їхнє планування та матеріально-технічне забезпечення все ж потребує фінансових ресурсів. Розуміння цієї важливості фінансування призвело до радикальної зміни підходів у боротьбі з тероризмом.

[16] https://www.youtube.com/watch?v=eL1o14qfirw&ab_channel=EUGF-AMLCFTGlobalFacility

Фінансова розвідка стала одним з найпотужніших інструментів у розбитті мереж, що фінансують тероризм та організовану злочинність. Франсуа Молін пояснює, що виявлення підозрілих переказів є ключовим у цьому процесі. Цей підхід дозволяє "тягнути за ниточку, а потім витягувати цілий клубок", що вказує на системний і поступовий характер розслідувань. Завдяки такому підходу, протягом трьох років вдалося виявити та ліквідувати систему збору коштів, призначених для терористів Ісламської держави. Це призвело до ініціювання близько 150 судових переслідувань за фінансування тероризму перед паризьким кримінальним судом. Це свідчить про ефективність нової стратегії та її практичні результати.

Організована злочинність не визнає кордонів і правил. Джерела замовлення та бенефіціари цих коштів часто перебувають за кордоном. Це створює значні виклики для національних правоохоронних органів. Досвід показує, що міжнародна співпраця є "визначальним фактором успіху або невдачі" у боротьбі з відмиванням коштів та фінансуванням тероризму. Це підкреслює необхідність скоординованих зусиль між країнами для ефективної протидії транснаціональним злочинним мережам.

Ініціативи, такі як EU Global Facility з протидії відмиванню грошей та фінансуванню тероризму відіграють життєво важливу роль у оснащенні країн засобами для реагування на транскордонні загрози та захисту їхніх фінансових систем. Франсуа Молін вважає, що ця ініціатива є "дуже цікавим та актуальним інструментом" для країн, які стикаються з труднощами. Вона "виправдовує себе" і "заслуговує на розвиток та отримання ресурсів". Це підкреслює важливість програм технічної допомоги та обміну досвідом у цій сфері.

З огляду на ці дані, можна зробити висновок, що інвестиції у фінансову розвідку та міжнародну співпрацю є не просто бажаними, а критично необхідними для національної безпеки та захисту фінансової системи. Ефективність протидії тероризму та організованій злочинності прямо пропорційна здатності відстежувати фінансові потоки та координувати дії на міжнародному рівні.

Інші новини

Як балканські злочинці озброюються боснійськими паспортами [17]

Розслідування, проведене Центром дослідницької журналістики (CIN) та опубліковане Organized Crime and Corruption Reporting Project (OCCRP), викриває масштабну схему, за якою десятки відомих балканських злочинців, зокрема члени кланів Кавач і Шкалярі, незаконно отримували боснійські паспорти, використовуючи вкрадені документи звичайних громадян Боснії і Герцеговини. Ця схема дозволяла злочинцям вільно пересуватися через кордони, уникати арештів і продовжувати свою діяльність, що включала наркоторгівлю, організацію вбивств та інші тяжкі злочини, використовуючи фальшиві імена. Жертви стикалися з серйозними юридичними та особистими проблемами, оскільки їхні імена асоціювалися з кримінальними справами, що ускладнювало їхнє життя, зокрема під час перетину кордонів.

[17] https://www.occrp.org/en/investigation/using-stolen-identities-balkan-gangsters-armed-themselves-with-bosnian-passports

Схема діяла за чітко відпрацьованим механізмом. Злочинці або їхні посередники отримували доступ до застарілої версії бази даних ідентифікаційних документів Боснії і Герцеговини, що дозволяло їм знаходити громадян, які ніколи не подавали заяв на отримання документів і не мали відбитків пальців у системі. Такі особи часто проживали за кордоном, зокрема в Сербії, що робило їх ідеальними цілями. Використовуючи імена цих громадян, шахраї платили фальшивомонетникам за створення підроблених документів, які містили імена жертв, але фотографії злочинців. На основі цих підробок вони отримували офіційні документи, такі як сертифікати громадянства та довідки про місце проживання, які потім використовувалися для подання заяв на боснійські паспорти. Процес часто завершувався у поліцейських відділках, де злочинці, іноді за супроводу корумпованих інсайдерів, проходили процедуру фотографування та зняття відбитків пальців під фальшивими іменами. Готові паспорти нерідко забирали посередники, що дозволяло злочинцям використовувати їх для перетину кордонів, уникнення арештів або навіть виконання замовних убивств.

Розслідування наводить конкретні приклади, які ілюструють масштаб і зухвалість схеми. Наприклад, Радоє Живкович, високопоставлений член клану Кавач, у 2021 році отримав боснійський паспорт на ім'я Андрея Йовіча за допомогою колишнього поліцейського Далібора Цурлика. Цурлик зареєстрував Живковича за адресою своєї матері в Баня-Луці, щоб той отримав довідку про місце проживання, а також супроводжував його до поліцейського відділку для подання документів. Отримавши паспорт, Живкович вилетів до Стамбула, де організував убивство лідера конкуруючого клану Шкалярі. Турецька поліція затримала його, виявивши підроблений боснійський паспорт, а суд засудив його до довічного ув'язнення. Інший випадок стосується Марка Петровича, сербського злочинця, засудженого за насильство, який отримав паспорт на ім'я Джордже Суша за аналогічною схемою за сприяння Цурлика. Алмір Яхович, ще один член клану Кавач, також намагався отримати паспорт, але був заарештований разом із Цурликом під час передачі документів у Баня-Луці в 2021 році. У районі Брчко ключовим посередником був Нікола Вейн, сербський громадянин, який за 5000 євро за паспорт організував видачу документів для щонайменше 12 членів клану Шкалярі у 2020 році. Вейн також був засуджений у Хорватії за видачу 75 підроблених хорватських паспортів, отримавши за це понад 500 000 євро, але Сербія відмовила в його екстрадиції.

Жертви зазнавали значних труднощів. Наприклад, Джурад Тривунович, чиє ім'я було використано злочинцем Деяном Павловичем, членом клану Шкалярі, був затриманий на кордоні через червоний сигнал Інтерполу. Йому довелося чекати кілька годин у спеку, поки поліція розбиралася в ситуації, а його родина, включно з маленькою дитиною, зазнавала стресу. Для вирішення проблеми Тривуновичу довелося наймати адвоката та отримувати сертифікат від поліції Брчко, що підтверджував крадіжку його документів, але навіть після цього він відчував невизначеність щодо свого статусу. Інший громадянин, Джуро Джураджевич, також зіткнувся з поліцейськими перевірками через використання його імені злочинцем.

Системні проблеми в Боснії і Герцеговині, зокрема децентралізована система управління, що походить від мирної угоди 1990-х років, сприяли вразливості системи видачі документів. Слабка координація між органами, відповідальними за захист даних і видачу паспортів, дозволяла шахраям використовувати прогалини в системі. Боснійська агенція з ідентифікаційних документів (IDDEEA) заперечує витік даних із їхньої бази, стверджуючи, що шахрайство було результатом корупції в місцевих структурах, а не компрометації центрального реєстру. Проте розслідування вказує на систематичну проблему доступу до застарілих баз даних і участі інсайдерів, таких як Цурлик, у видачі документів.

Міжнародний вимір схеми підкреслює її серйозність. Підроблені паспорти використовувалися для скоєння злочинів за кордоном, зокрема вбивств у Туреччині та Греції. Відсутність співпраці між країнами ускладнює боротьбу з такими схемами. Загалом, за даними розслідування, з 2013

по 2022 роки щонайменше 60 членів організованих злочинних груп отримали боснійські паспорти, що свідчить про системний характер проблеми та її вплив на безпеку регіону.

Для загального розвитку

Моделі ризиків у сфері ПВК/ФТ/ФР, що виходять за рамки загроз та вразливостей [18]

Даний матеріал детально аналізує традиційні моделі оцінки ризиків у сфері протидії відмиванню коштів (AML/CFT/CPF), засновані на методології FATF, висвітлює їхні обмеження та пропонує багатовимірну структуру для більш точної та ефективної оцінки ризиків.

У традиційних моделях управління ризиками AML, що використовуються для національних, галузевих або внутрішніх оцінок ризиків компанії, основна увага приділяється співвідношенню загрози та вразливості як способу визначення значення Ризику. Ризик у цих моделях концептуалізується як функція загрози, вразливості та, в ідеалі, наслідків. Однак на практиці багато установ розглядають загрозу та вразливість як первинні фактори.

Загрози стосуються наявності джерел або методів відмивання грошей (наприклад, злочинних мереж або клієнтів високого ризику), які мають потенціал завдати шкоди.

Вразливості — це слабкі місця або особливості системи, які можуть бути використані цими загрозами, такі як неефективний контроль, продукти чи послуги високого ризику або географічний вплив юрисдикцій високого ризику.

Завдяки цим двом факторам організації оцінюють притаманний ризик (ризик до застосування контролю). Потім застосовуються заходи пом'якшення (наприклад, посилена належна перевірка клієнтів, системи моніторингу транзакцій, навчання персоналу), щоб зменшити цей притаманний ризик, що призводить до рівня залишкового ризику. Залишковий ризик — це ризик, що "залишився" після впровадження контролю, і очікується, що керівництво та регулятори будуть ним управляти або приймати.

Ця традиційна модель є простою та зрозумілою. Наприклад, якщо банк виявляє значну схильність до ризику у готівковому бізнесі (високий ризик) і прогалини у своїх заходах контролю за відмиванням коштів (висока вразливість), притаманний ризик буде оцінено як високий. Після впровадження надійних заходів контролю, таких як посилена належна перевірка та моніторинг транзакцій у реальному часі, залишковий ризик може бути знижений до середнього рівня. Ця методологія приваблива завдяки своїй чіткій, лінійній логіці: виявити ризики, застосувати заходи пом'якшення та отримати оцінку залишкового ризику. Вона відповідає регуляторним очікуванням і відносно легко впроваджується різними установами з мінімальним навчанням, оскільки часто використовує якісні бали та прості робочі листи.

[18] https://sites.google.com/view/riskmodels?usp=sharing

Обмеження Традиційних Моделей

Компроміс Між Простотою та Глибиною Аналізу. Простота традиційної моделі є її найбільшим недоліком. Зводячи ризик до двофакторного рівняння (загроза проти вразливості), установи можуть надто спрощувати складні реалії ризиків. FATF у своїх рекомендаціях визнає, що ідеальна оцінка ризиків повинна враховувати не лише загрози та вразливості, але і ймовірність реалізації цих загроз та наслідки, якщо вони настануть. Проте, у багатьох реальних впровадженнях аспект наслідків ігнорується або розглядається поверхово. Це призводить до оцінки, яку легко виконати та повторити, але яка може пропустити нюанси, критично важливі для розуміння та пріоритизації AML-ризиків.

Традиційний підхід, що зосереджений на бінарному фокусі, створює дихотомію між легкістю використання та глибиною аналізу. Це призводить до ігнорування кількох важливих вимірів аналізу ризиків:

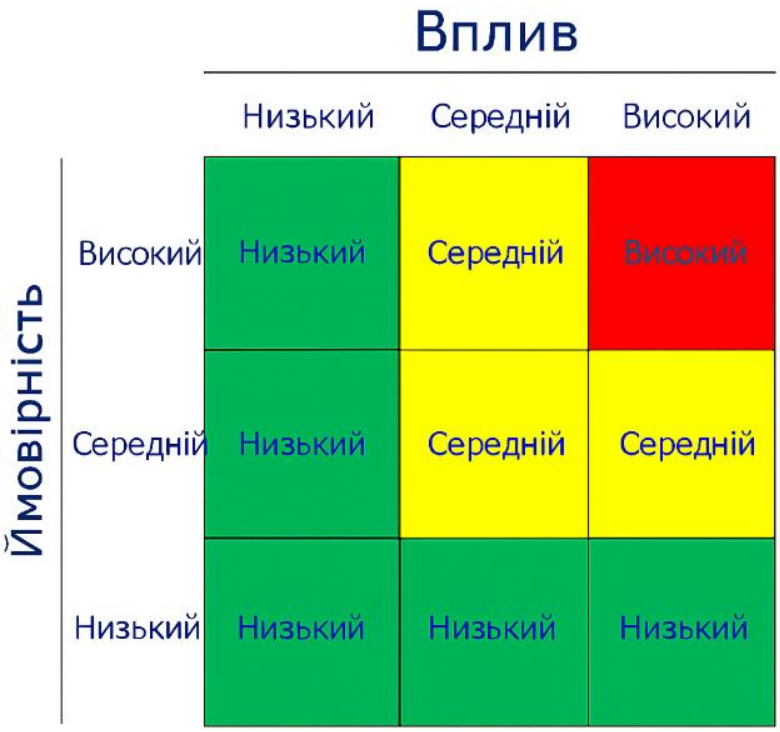
- Нехтування ймовірністю (вірогідністю): Не всі ризики з високою загрозою та високою вразливістю однаково ймовірні. Традиційні моделі іноді припускають, що якщо загроза існує і є вразливість, ризик "високий". Проте, відсутність явної оцінки ймовірності події відмивання коштів означає, що установи можуть переоцінювати одні ризики та недооцінювати інші. Керівництво FATF чітко зазначає, що організації повинні аналізувати інформацію, щоб зрозуміти ймовірність виникнення виявлених ризиків ВК/ФТ.
- Нехтування впливом (серйозністю наслідків): Традиційні моделі схильні зосереджуватися на рівнях притаманного ризику, не розрізняючи, наскільки серйозним буде результат, якщо ризик реалізується. Два різні ризики можуть бути оцінені як "високі", але один може призвести до незначного порушення комплаєнсу, тоді як інший може сприяти протіканню мільйонів незаконних коштів через фінансову систему. FATF визначає наслідки як спричинену шкоду (економічний збиток, репутаційна шкода). Ігнорування цього аспекту може призвести до того, що невелика проблемна ситуація розглядається з такою ж терміновістю, як потенційне масштабне порушення.
- Ігнорування суттєвості та експозиції: Спрощені моделі часто оцінюють фактори ризику ізольовано, без контексту масштабу. Вони можуть не враховувати, наскільки великий фактичний вплив установи на даний ризик. Наприклад, дві фірми можуть оцінити ризик клієнта, який є іноземною політично значущою особою, як високий притаманний ризик, але їхня матеріальна експозиція може бути значно різною. Ігнорування суттєвості, такої як обсяг бізнесу високого ризику, може призвести до неефективного розподілу ресурсів.
- Статичні та загальні оцінки: Багато традиційних оцінок ризиків є одноразовими або щорічними подіями з широкими категоріями, які можуть почати сприйматися як "для галочки". Такі оцінки можуть не відображати нові тенденції або зміну патернів. Простота, що робить оцінку легкою для заповнення, також може зробити її негнучкою або "сліпою" до змін до наступного планового перегляду, що є значним обмеженням у швидкозмінному ландшафті фінансових злочинів.

Наслідком цих обмежень є те, що установи можуть відчувати помилкове почуття безпеки або неправильно розставляти пріоритети у своїх зусиллях. Прикладом є казино та невелика бухгалтерська фірма: традиційна модель може оцінити обидві установи як такі, що мають високий притаманний ризик, але здоровий глузд підказує, що ймовірність та вплив відмивання коштів через казино набагато вищі, ніж через невелику бухгалтерську фірму. Спрощений підхід, який позначає обидві установи як однаково ризикові, може ввести в оману обидві фірми, змушуючи їх думати, що вони мають однаковий профіль ризику, хоча природа та масштаб їхніх ризиків кардинально відрізняються.

Пропонування Багатовимірної Моделі Оцінки AML-Ризиків

Для усунення цих недоліків пропонується розширена структура, яка ґрунтується на основах FATF, але структуровано вводить додаткові виміри ймовірності та впливу. Мета полягає у створенні моделі, достатньо надійної, щоб відображати реальну складність, але при цьому достатньо простої та гнучкої, щоб банки та ВНУП будь-якого розміру могли послідовно застосовувати її з обмеженими даними. Цей підхід переходить від двовимірного погляду (притаманний проти залишкового ризику) до багатовимірного, де ймовірність та наслідки явно оцінюються. Важливо, що це не вимагає складного кількісного моделювання або великих даних, що робить його практичним для швидкого розгортання.

Ключові елементи запропонованої структури:



- Оцінка Притаманної Ймовірності: Замість об'єднання загрози та вразливості в єдиний бал притаманного ризику, їх слід оцінювати з точки зору ймовірності. Розглядаються всі відповідні фактори загрози та вразливості, щоб сформувати судження про те, наскільки ймовірна подія відмивання коштів у даній області. Це може бути якісна оцінка (наприклад, низька/середня/висока ймовірність) на основі експертних знань, минулих випадків та наявних даних.
- Оцінка Потенційного Впливу: Окремо оцінюється вплив або наслідки, якщо інцидент відмивання коштів станеться в цій області. Вплив можна виміряти з точки зору фінансової шкоди, регуляторних/правових наслідків та репутаційної шкоди. Тут також можна використовувати просту шкалу (наприклад, низький, помірний, високий вплив). Явна оцінка впливу гарантує врахування суттєвості ризику.
- Поєднання Ймовірності та Впливу в Матриці Ризиків: Після визначення ймовірності та впливу загальний притаманний ризик може бути отриманий як їх комбінація. Простий, але ефективний спосіб – нанести їх на матрицю ризиків. Ймовірність може утворювати одну вісь, а Вплив – іншу. Перетин цих двох дає рівень ризику. Це дозволяє візуально розрізняти ризики, які є "частими, але м'якими", від ризиків, які є "рідкісними, але катастрофічними". Цей підхід узгоджується зі стандартними практиками управління ризиками, де ризик часто розглядається як функція ймовірності та наслідків: Ризик = (Загроза × Вразливість) × Вплив, де загроза × вразливість дає поняття ймовірності.
- Точне Застосування Заходів Пом'якшення: З урахуванням ймовірності та впливу, заходи пом'якшення можуть бути націлені більш точно. Установа може запитати: чи знизить цей контроль ймовірність події, чи зменшить вплив, якщо вона станеться (або й те, й інше)? Після початкового картографування притаманного ризику, кожен контроль може бути концептуально пов'язаний з однією з осей матриці (зниження ймовірності або впливу), а потім матриця ризиків може бути переглянута для відображення позиції залишкового ризику після контролю.

- Збереження Легкості та Масштабованості Структури: Ця альтернативна модель повинна бути застосовною як великими, так і малими організаціями. Вона не вимагає статистичних моделей або великих історичних даних про втрати, а натомість використовує структурований експертний вхід. Великий банк може використовувати матрицю 5×5 з більш деталізованими шкалами, тоді як невелика фірма може використовувати матрицю 3×3 та експертне судження – концепція залишається тією ж.
- Швидке та Послідовне Застосування: Методологія, що ґрунтується на якісній оцінці, може бути швидко впроваджена. Це дозволяє швидше оновлювати оцінку ризиків при запуску нових продуктів або виникненні нових загроз, ніж чекати наступного річного циклу. Вона також сприяє чіткій документації, а з часом якісні судження щодо ймовірності можуть бути уточнені з появою даних.

Баланс Між Складністю та Практичністю

Хоча може здатися, що введення більшої кількості факторів ускладнює оцінку ризиків, метою є збалансована складність: достатньо факторів для охоплення того, що має значення, але не настільки багато, щоб паралізувати процес. Ймовірність та вплив є інтуїтивно зрозумілими поняттями для керівництва та персоналу, що сприяє обговоренням, які є ключовими для комплаєнс-культури. Цей підхід узгоджується з практиками управління ризиками підприємства, які багато організацій використовують для інших ризиків (наприклад, операційних або кібер-ризиків), створюючи спільну мову. Регуляторні органи та галузеві організації все більше очікують саме такого підходу.

Пропонована структура залишається практичною для швидкого впровадження. Невелика ВНУП може впровадити її за допомогою простої електронної таблиці, а великий банк — інтегрувати її в систему управління ризиками та комплаєнсом (GRC) з більш кількісними вхідними даними. Навчання персоналу цій моделі є простим, оскільки вона допомагає підрозділам краще зрозуміти, чому щось оцінюється як високий ризик (вони бачать, що це або дуже ймовірно, або дуже шкідливе, або і те, й інше, а не абстрактний "бал притаманного ризику"). Якщо регулятори заохочуватимуть цей формат, це призведе до більш порівнянних оцінок ризиків між установами.

Підсумовуючи, хоча традиційні моделі оцінки AML-ризиків, засновані на методології FATF "загроза-вразливість", були хорошою відправною точкою, їх надмірне спрощення може залишати сліпі зони у розумінні ризиків фірмою. Шляхом включення таких вимірів, як ймовірність виникнення та серйозність впливу, а також візуалізації ризиків на простій матриці, фахівці з комплаєнсу можуть отримати більш тривимірний погляд на свій ландшафт ризиків, не втрачаючи здатності діяти швидко.

Прийняття багатшої моделі ризиків має значні переваги. Установи можуть краще розставляти пріоритети у своїх зусиллях з протидії відмиванню коштів, зосереджуючи ресурси на ризиках, які є не лише притаманними, але й правдоподібними та значущими. Це призводить до більш розумних стратегій пом'якшення ризиків, оскільки контроль може бути розроблений для запобігання ймовірним подіям або підготовки до сценаріїв з високим впливом. У світі, де загрози фінансових злочинів продовжують розвиватися, гнучкий, але комплексний підхід до оцінки ризиків є вирішальним. Відхід від старої дихотомії "загроза проти вразливості" та прийняття більш цілісної моделі дозволяє AML-спільноті підвищити як ефективність, так і довіру до комплаєнсу, заснованого на ризиках. Кінцева мета полягає в тому, щоб оцінка ризиків була не просто щорічним зобов'язанням, а живим інструментом, який послідовно керує установами у захисті фінансової системи – без зайвої складності та без сліпих зон

Ваша думка важлива!

1. Враховуючи міжнародні тенденції жорсткого регулювання стейблкоїнів та криптоактивів (досвід Сполученого Королівства та Гонконгу), а також виклики, з якими стикається Web3-сектор в Європі через регуляторний тягар, як ви вважаєте, чи повинна Україна наслідувати ці підходи для інтеграції стейблкоїнів у свою платіжну систему?
2. Які конкретні заходи, на вашу думку, дозволять українським регуляторам знайти оптимальний баланс між посиленням фінансової безпеки, запобіганням відмиванню коштів через криптоактиви, та стимулюванням інновацій у національному Web3-секторі?
3. Які кроки є першочерговими для підвищення ефективності системи оцінки ризиків та покращення якості даних, що надаються ПФР для боротьби з фінансовими злочинами?
4. Які стратегії міжнародної співпраці та внутрішнього контролю є найбільш ефективними для України, щоб протидіяти транснаціональній злочинності, що використовує корупційні схеми, забезпечити надійний захист інформаційних систем та зміцнити довіру до державних інституцій, що є критично важливим для нашої євроінтеграції?
5. Якою має бути ефективна модель запобігання конфлікту інтересів на рівні найвищих виконавчих посад в умовах гібридної демократії та реформування державної служби?
6. Чи становить централізований контроль над супутниковими комунікаціями (наприклад, з боку SpaceX) нову форму цифрової монополії, що впливає на міжнародну безпеку та суверенітет держав?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-24

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

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