Методологічний бюлетень

Серійний номер: МінФін-AML-2025-39

Вересень 2025

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

Кетрін Джонсон

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Регуляторний огляд ПФР Італії за перше півріччя 2025 року [1]

Представлений документ, який є третім випуском серії «Quaderni dell’antiriciclaggio – Rassegna normativa» (Огляд нормативної бази), присвячений ключовим подіям у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР), що відбулися протягом першого півріччя 2025 року. Центральною темою поглибленого аналізу є посилення дисципліни відстеження та повернення незаконно отриманих активів, який FATF визначила пріоритетом у зв'язку зі зростанням складності транскордонних кримінальних схем. Ефективна імплементація стандартів з повернення активів є життєво важливою для стримування злочинних організацій, посилення ПВК та відшкодування збитків жертвам.

[1] https://uif.bancaditalia.it/pubblicazioni/quaderni/2025/quaderno-rn-1-2025/Quaderni_RassegnaNormativa_I_2025.pdf

В рамках цього пріоритету FATF переглянула низку своїх Рекомендацій (зокрема R.4, R.38, R.40, R.30, R.31), запровадивши нові види конфіскації, включаючи конфіскацію без вироку суду (non-conviction based confiscation, NCBC) та розширену конфіскацію (extended confiscation), а також наголосивши на важливості повноважень Фінансових розвідок (ПФР) щодо негайного призупинення підозрілих операцій як інструменту, що передує арешту чи замороженню майна. Зокрема, міжнародне співробітництво, відповідно до оновленої R.38, має надаватися оперативно, навіть щодо процедур NCBC, і визнання іноземних постанов про заморожування/конфіскацію має відбуватися без попередньої умови проведення внутрішніх розслідувань. Також, в рамках R.40, ПФР або інші компетентні органи повинні мати можливість швидко відмовити у згоді або призупинити підозрілу операцію на запит іноземного колеги.

Європейський Союз суттєво посилив свою нормативну базу шляхом ухвалення Директиви ЄС/2024/1260, яка замінює попередні акти і зосереджується на AR. Директива запроваджує широке визначення майна, включаючи криптоактиви, та розширює коло злочинів, включаючи порушення європейських обмежувальних заходів (санкцій). Вона посилює повноваження Офісів з повернення активів (ARO), надаючи їм прямий та негайний доступ до ключових реєстрів, таких як реєстри нерухомості, транспортних засобів та централізовані реєстри банківських рахунків, для швидкого пошуку активів. У невідкладних випадках Директива передбачає можливість негайних заходів заморожування, які можуть тривати до семи робочих днів, навіть за ініціативою ARO, до видачі судового рішення. Важливо, що Директива вимагає від держав-членів прийняття національної стратегії повернення активів до травня 2027 року, а також встановлення офісів з управління активами для збереження вартості замороженого майна, включаючи його можливий продаж до остаточної конфіскації.

На міжнародному рівні FATF також внесла зміни до Рекомендації 1 (щодо ризик-орієнтованого підходу), заохочуючи спрощені заходи належної перевірки клієнтів (SDD) у низькоризикових сферах для сприяння фінансовій інклюзії. Переглянута Рекомендація 16 (Travel Rule) вимагає збагачення інформації

Висновки:

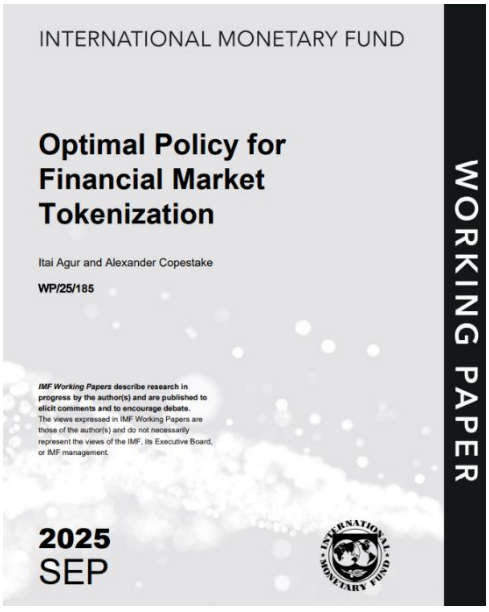
- **Пріоритезація повернення активів вимагає негайного посилення оперативних повноважень ПФР:** Внаслідок перегляду стандартів FATF та Директиви ЄС/2024/1260, ПФР повинні забезпечити негайне використання повноважень щодо призупинення підозрілих операцій (внутрішніх і міжнародних) як критичного інструменту перед арештом, щоб запобігти розпорошуванню активів у високошвидкісному цифровому середовищі.
- **Держави-члени ЄС повинні забезпечити прямий доступ ARO до реєстрів:** Для дотримання вимог Директиви ЄС/2024/1260, національні ARO повинні отримати невідкладний та прямий доступ до широкого спектру централізованих баз даних (включаючи реєстри банківських рахунків, нерухомості та КБВ) для швидкої ідентифікації та трасування незаконних доходів.
- **Потрібна стратегічна адаптація до нових видів конфіскації:** Компетентні органи, включаючи судові та правоохоронні, повинні розробити нові внутрішні методики для використання посилених інструментів, таких як конфіскація без вироку суду (NCBC) та розширена конфіскація, враховуючи необхідність забезпечення належного управління конфіскованими активами та їх цільового використання (наприклад, для відшкодування жертвам або на соціальні цілі).
- **Відстеження криптоактивів та ухилення від санкцій є критичними зонами ризику:** Оператори та регулятори повинні посилити моніторинг щодо використання стейблкоїнів для злочинних цілей та впровадити спеціалізовані індикатори для виявлення складних схем ФР та ухилення від санкцій (наприклад, використання віртуальних рахунків або маніпуляції в морському секторі).

для транскордонних платежів, а також посилює прозорість щодо транскордонного зняття готівки за допомогою карт (вимагаючи надання імені власника картки протягом трьох робочих днів на запит). Крім того, FATF випустила звіти, що деталізують схеми фінансування розповсюдження зброї масового знищення та ухилення від санкцій, а також ризики, пов'язані з використанням криптоактивів і сексуальною експлуатацією дітей в Інтернеті.

В Італії було запроваджено ключові інституційні та законодавчі зміни, зокрема створення нового генерального управління в рамках Міністерства економіки та фінансів (MEF) для координації заходів ПВК/ФТ/ФР. Національне законодавство було оновлено для включення нових понять, таких як "фінансування програм розповсюдження зброї масового знищення" та "цільові фінансові санкції", а Комітету з фінансової безпеки (CSF) було прямо надано повноваження оцінювати національний ризик фінансування розповсюдження. Італійська правова система повернення активів є двоякою: вона включає кримінальні заходи (що вимагають встановлення злочину, наприклад, розширена конфіскація) та превентивні заходи (на основі соціальної небезпеки, що дозволяють NCBC). Роль ПФР є критично важливою, оскільки вона може призупиняти підозрілі операції на термін до п'яти робочих днів для забезпечення збереження коштів до судових заходів. Національний ARO функціонує як координаційний центр для міжнародного співробітництва, маючи доступ до централізованого реєстру банківських рахунків для ідентифікації незаконних доходів.

Судова практика в Італії підтвердила важливі принципи: Верховний суд постановив, що злочин самовідмивання може бути інтегрований навіть через просте використання прозорих (відстежуваних) банківських операцій, якщо вони конкретно перешкоджають ідентифікації походження коштів. Крім того, суд підтвердив, що продаж вкраденого майна третім особам являє собою відмивання коштів, відрізняючись від простого отримання викраденого. Однак, у сфері криптоактивів, Суд анулював ордер на арешт Bitcoin як "прибутку" від податкового злочину, поставивши під сумнів застосування конфіскації за еквівалентом до віртуальної валюти через її немонетарний статус і волатильність.

Оптимальна політика токенізації фінансового ринку [2]



Документ Міжнародного валютного фонду "Оптимальна політика для токенізації фінансового ринку" є глибоким теоретичним дослідженням, що моделює поведінку фінансових посередників (брокерів) в умовах технологічної трансформації, а саме — переходу до токенізованих активів на програмованих платформах. Автори пропонують першу формалізовану модель для аналізу оптимальної державної політики в цій сфері, розглядаючи ключові виклики, як-от ризик фрагментації ринку та стимули для інвестицій в інноваційну інфраструктуру. В основі моделі лежить аналіз взаємодії трьох брокерів із різною ринковою силою, що визначається їхньою початковою клієнтською базою та витратами на перехід клієнтів. Брокери можуть проводити операції трьома способами: всередині власної клієнтської бази (безкоштовно), через існуючу застарілу

[2] https://www.imf.org/en/Publications/WP/Issues/2025/09/19/Optimal-Policy-for-Financial-Market-Tokenization-570540

міжброкерську платформу (з транзакційними витратами) або через нову, більш ефективну токенізовану платформу, яку вони можуть створити спільно.

Центральним елементом дослідження є аналіз стимулів, що спонукають брокерів формувати коаліції для створення токенізованого ринку. Модель демонструє, що приватні інтереси брокерів не збігаються із суспільним оптимумом. Замість створення "великої коаліції" за участю всіх трьох гравців, що повністю б усунуло неефективні операції на застарілій платформі, в рівновазі виникає "часткова коаліція". Як правило, найбільший і найменший брокери об'єднуються, щоб витіснити середнього конкурента, використовуючи переваги нової платформи для переманювання клієнтів та посилення власних позицій. Цей процес, названий "перенаправленням торгівлі" (trade diversion), стає ключовим мотивом, що веде до ринкових викривлень.

У результаті такої поведінки виникають дві основні проблеми. Перша — "надмірне інвестування" (excessive investment), коли приватна вигода від витіснення конкурента спонукає брокерів створювати токенізовану платформу навіть тоді, коли суспільні витрати на її створення перевищують загальну економічну вигоду. Друга — "недостатня токенізація" (insufficient tokenization), коли створення спільної платформи є суспільно вигідним, але приватні стимули до "перенаправлення торгівлі" призводять до створення ексклюзивної коаліції, яка залишає частину ринку на застарілій, менш ефективній інфраструктурі.

Висновки:

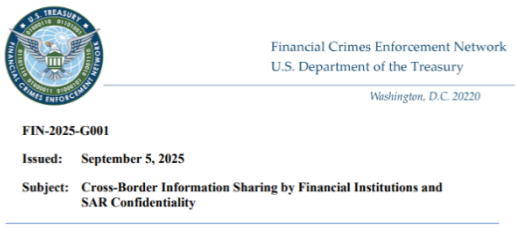
- **Приватні стимули брокерів призводять до фрагментації ринку.** Замість створення єдиної ефективної платформи, брокери формують ексклюзивні коаліції для витіснення конкурентів, що призводить або до надмірних інвестицій в інфраструктуру, або до недостатнього охоплення ринку новою технологією.
- **Окремі політичні інструменти є неефективними.** Ані мандат на інтероперабельність, ані державне субсидування, використані окремо, не здатні повністю вирішити проблему ринкових викривлень. Інтероперабельність може спричинити недоінвестування, тоді як субсидії не усувають стимулів до створення ексклюзивних альянсів.
- **Оптимальна політика вимагає комбінованого підходу.** Для досягнення максимальної суспільної вигоди регуляторам слід одночасно впроваджувати мандат на інтероперабельність (як "батіг" проти фрагментації) та механізми спільного фінансування або субсидування (як "пряник" для стимулювання інвестицій).
- **Наявність публічних блокчейнів не вирішує проблему.** Навіть якщо існує відкрита та безкоштовна інфраструктура, приватні стимули до створення ексклюзивних токенізованих ринків для "перенаправлення торгівлі" залишаються, що зберігає необхідність у проактивній державній політиці.

Автори досліджують два основні інструменти державної політики для вирішення цих проблем: мандат на інтероперабельність (вимога забезпечити можливість приєднання до платформи для всіх учасників ринку) та державно-приватне партнерство у формі субсидування витрат на створення інфраструктури. Аналіз показує, що жоден із цих інструментів, застосований окремо, не є достатнім для досягнення соціального оптимуму. Мандат на інтероперабельність ефективно усуває проблему надмірного інвестування, оскільки робить неможливим витіснення конкурентів, але водночас може призвести до недоінвестування, оскільки найменш зацікавлений брокер може заветувати створення спільної платформи, якщо його приватні вигоди недостатні. З іншого боку, субсидування витрат стимулює інвестиції, але не вирішує проблему ексклюзивних коаліцій та "перенаправлення торгівлі".

Ключовий висновок роботи полягає в тому, що лише комбінація обох політик — мандату на

інтероперабельність та субсидування — дозволяє досягти оптимального результату. Інтероперабельність усуває шкідливі стимули до фрагментації, а субсидія долає проблему недоінвестування, компенсуючи приватним гравцям ту частину суспільної вигоди (зокрема, зниження комісій для інвесторів), яку вони не враховують у своїх рішеннях. Дослідження також показує, що ці висновки залишаються справедливими навіть за наявності незалежної публічної інфраструктури (наприклад, публічного блокчейну) або можливості здійснення побічних платежів між брокерами для стимулювання угод. Таким чином, робота надає регуляторам важливий аналітичний інструментарій, демонструючи, що для ефективного впровадження токенізації потрібен збалансований підхід, який поєднує як регуляторні вимоги, так і фінансові стимули.

Обмін інформацією: нові орієнтири для фінансових установ у боротьбі з відмиванням коштів та фінансуванням тероризму [3]


Financial Crimes Enforcement Network
U.S. Department of the Treasury
Washington, D.C. 20220

FIN-2025-G001

Issued: September 5, 2025

Subject: Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality

У вересні 2025 року FinCEN разом із ключовими банківськими регуляторами США опублікувало нове керівництво, яке стало важливим кроком у роз'ясненні правил обміну інформацією між фінансовими установами.

Протягом багатьох років банки й інші гравці фінансового ринку нерідко помилково вважали, що будь-яке передавання даних про клієнтів чи транзакції за кордон є ризиком порушення Закону про банківську таємницю (BSA). Це створювало атмосферу «обережного мовчання», яка фактично гальмувала міжнародну співпрацю. Документ FinCEN чітко пояснює: обмеження поширюються винятково на Suspicious Activity Reports (SARs) та будь-які дані, які прямо або непрямо вказують на факт їх подання. Водночас сама фактична інформація — дані про транзакції, клієнтів, контрагентів, бенефіціарів чи навіть результати внутрішніх розслідувань — може і має передаватися іноземним фінансовим установам для ефективнішої боротьби з відмиванням коштів і фінансуванням тероризму.

У документі підкреслюється, що злочинні мережі діють глобально, використовуючи багатоступеневі схеми: від дрібних переказів у різних валютах до складних ланцюгів через офшорні юрисдикції. Один банк часто бачить лише «фрагменти» транзакційної картини, які виглядають буденними і не викликають підозри. Проте, коли ці шматки інформації об'єднуються, вимальовується цілісна схема — від структурованих депозитів до багаторівневих ланцюгів переказів. Саме тому FinCEN прямо заохочує банки брати участь у обміні даними: це дозволяє виявляти патерни, які неможливо побачити ізольовано.

У керівництві наведено приклади того, що можна передавати без порушення конфіденційності SAR:

- відомості про конкретні перекази (дати, суми, реквізити рахунків);
- дані про клієнтів і бенефіціарів, включно з типами продуктів, якими вони користуються;
- відомості про джерела коштів або доходів;
- аналітичні витяги з систем моніторингу, наприклад IP-адреси, зв'язки між рахунками чи географічні патерни.

[3] https://www.fincen.gov/system/files/2025-09/Crossborderguidance-508C.pdf

Єдина вимога — уникати навіть натяків на те, що ці факти стали основою для подання SAR. Це означає, що якщо банк описує підозрілі транзакції, він має формулювати повідомлення в нейтральному стилі, уникаючи слів чи конструкцій, які прямо вказували б на SAR.

Водночас документ встановлює юридичні межі й баланс. Фінансові установи зобов'язані враховувати не лише американське законодавство, але й закони юрисдикцій, де перебувають їхні партнери. Це передбачає оцінку надійності іноземних установ, із якими планується обмін: чи мають вони достатній рівень регуляторного контролю, чи здатні забезпечити конфіденційність даних. Такий підхід формує основу для довіри і дозволяє уникати витоків інформації, яка може бути використана проти банку або клієнтів.

Важливим акцентом документа є захист SAR як недоторканного елемента AML-системи. Установа, що отримує судовий запит, чи будь-який інший офіційний запит про надання інформації, зобов'язана негайно повідомити FinCEN і свого регулятора. У відповідях суворо забороняється навіть натякати на факт подання SAR. Рекомендація — використовувати загальні формулювання на кшталт «неконфіденційна наглядова інформація», щоб уникнути порушення. Це чіткий сигнал, що збереження таємниці SAR залишається фундаментом довіри між державою та фінансовими установами.

Окрім юридичних рамок, керівництво має і стратегічне значення. Воно знімає страхи та бар'єри, які утримували банки від міжнародної співпраці. Часто фінансові установи воліли «недодати» інформації, аби уникнути можливих санкцій. Тепер же FinCEN прямо пояснює: інформаційна ізоляція — це не захист, а ризик. В умовах глобалізованої фінансової системи відсутність обміну створює «білі плями», які злочинці активно використовують. Натомість добровільний обмін даними стає інструментом підвищення ефективності й водночас способом зменшити власні регуляторні ризики, адже спільна робота з партнерами дозволяє швидше ідентифікувати підозрілі схеми.

Ще один важливий аспект — культура проактивної співпраці. Керівництво фактично змінює підхід: від обережного, оборонного сприйняття обміну до позиції активного гравця, який ділиться інформацією, щоб ускладнити роботу злочинним мережам. Це дозволяє будувати систему, де банки не лише реагують на злочини постфактум, а й превентивно виявляють загрози. Такий підхід збільшує ефективність боротьби з транснаціональними злочинними мережами, від наркокартелів до терористичних організацій.

Загалом документ можна розглядати як сигнал міжнародній спільноті: США прагнуть бачити фінансову систему більш інтегрованою й здатною давати єдині відповіді на глобальні виклики AML/CFT. Для інших юрисдикцій це запрошення до партнерства й одночасно демонстрація лідерства американського регулятора у встановленні стандартів. Для самих фінансових установ — це нагадування, що сьогоднішня бездіяльність чи ізоляція коштує дорожче, ніж проактивна співпраця.

Висновки:

- **Фінансовим установам слід активно обмінюватися даними** про транзакції та клієнтів із закордонними партнерами, уникаючи лише розкриття самого факту подання SAR.
- **Банки мають впровадити внутрішні політики перевірки надійності іноземних установ-партнерів**, щоб мінімізувати ризики витоку чи неправомірного використання даних.
- **SAR залишаються недоторканними,** тому будь-які запити про їхній зміст потрібно негайно спрямовувати до FinCEN та регуляторів, замінюючи відповіді загальними формулюваннями.
- **Міжнародний обмін інформацією слід сприймати не як ризик**, а як інструмент превентивної безпеки, що підвищує здатність банків виявляти глобальні злочинні схеми.

Таким чином, FinCEN не створює нових обов'язків, але формує нову парадигму мислення: міжнародний обмін інформацією — це не опція, а ключ до ефективної протидії злочинним фінансовим потокам. Банкам і регуляторам варто розглядати його не як потенційне джерело ризиків, а як інструмент для зміцнення власної безпеки й глобальної фінансової стабільності.

Економічна злочинність як виклик національній безпеці: підсумки реалізації стратегічної ініціативи Великої Британії [4]

Звіт, опублікований урядом Великої Британії, є підсумковим документом, що фіксує результати виконання стратегічної ініціативи у сфері боротьби з економічною злочинністю на 2023–2026 роки. Він показує, як держава поступово вибудовує комплексну систему протидії, поєднуючи законодавчі зміни, технологічні інновації, нові підходи до роботи правоохоронних органів та активну взаємодію з приватним сектором. Економічна злочинність визначається не лише як проблема бізнес-середовища, але і як ключова загроза національній безпеці, що безпосередньо впливає на добробут громадян, інвестиційний клімат і репутацію країни на міжнародній арені.

Звіт підкреслює, що головною метою плану є створення у Великій Британії максимально несприятливих умов для злочинців і корумпованих еліт, які прагнуть використовувати її фінансову систему для відмивання доходів, обходу санкцій, шахрайства чи приховування активів. Для цього було розроблено кілька ключових напрямів: зміцнення прозорості корпоративного сектору, підвищення якості фінансового моніторингу, модернізація правоохоронних повноважень та тісна координація з бізнесом. Важливо, що уряд сприймає економічну злочинність як явище, що постійно змінюється, і тому в основі стратегії лежить принцип гнучкості й адаптації до нових викликів.

Одним із головних досягнень звітного періоду стало ухвалення Economic Crime and Corporate Transparency Act, яке суттєво реформує корпоративний реєстр. Вперше у Великій Британії вводиться комплексний механізм перевірки та ідентифікації директорів компаній і кінцевих бенефіціарних власників. Це означає, що створювати «фантомні» компанії для відмивання грошей або обходу санкцій стане набагато складніше. Документ також передбачає введення кримінальної відповідальності за надання неправдивих даних у реєстрі, що значно підвищує його вагу як інструмента прозорості.

Звіт відзначає і розвиток інституційних механізмів: Національне агентство з боротьби зі злочинністю (NCA) отримало розширені повноваження з конфіскації та заморожування активів, у тому числі без попереднього судового рішення у випадках, коли існує високий ризик їх виведення за кордон. Це дозволило більш ефективно реагувати на випадки відмивання коштів, особливо пов'язаних із міжнародними мережами та транскордонними схемами. Крім того, створюються нові спеціалізовані підрозділи у сфері розслідування економічних злочинів, які працюють із використанням великих даних і штучного інтелекту для аналізу підозрілих транзакцій.

Не менш важливою є взаємодія держави з приватним сектором. Банки, фінансові компанії, платіжні системи та технологічні платформи дедалі активніше залучаються до співпраці у виявленні підозрілої активності. Зокрема, втілюються інструменти моніторингу транзакцій у режимі реального часу, що дозволяють блокувати підозрілі операції ще до їх завершення.

[4] https://www.gov.uk/government/publications/economic-crime-plan-2-outcomes-progress-report/economic-crime-plan-2-outcomes-progress-report

Окремо наголошується на важливості партнерства з фінтех-компаніями, адже саме у сфері цифрових платежів та криптовалют сьогодні зосереджені найбільші ризики.

Разом із тим, документ чесно вказує і на обмеження нинішніх результатів. Шахрайство, зокрема онлайн-шахрайство, залишається наймасовішим видом економічної злочинності у Великій Британії. Попри інформаційні кампанії, навчальні програми з кібербезпеки та створення гарячих ліній для потерпілих, кількість інцидентів зростає. Це свідчить, що злочинні групи швидко адаптуються до нових технологій і використовують соціальну інженерію та цифрові канали для досягнення своїх цілей. Саме тому одним із ключових викликів наступних років стане не лише посилення захисту фінансових інституцій, а й підвищення цифрової грамотності населення, аби зменшити кількість жертв шахрайства.

Ще одним важливим аспектом є міжнародний вимір економічної злочинності. Значна частина нелегальних фінансових потоків проходить через офшорні юрисдикції, а також пов'язана з обходом санкцій. У цьому контексті Британія прагне виступати глобальним лідером у сфері прозорості та фінансової безпеки. План спрямований на розширення міжнародної співпраці, зокрема в межах FATF, ЄС та «Великої сімки», а також на укладання двосторонніх угод для обміну фінансовою інформацією. Це підсилює геополітичну роль Лондона та робить боротьбу з економічними злочинами інструментом зовнішньої політики.

Висновки:

- **Запровадження відкритого реєстру бенефіціарних власників** є ключовим інструментом для зменшення зловживань корпоративними структурами.
- **Посилення повноважень правоохоронних органів** у сфері замороження та конфіскації активів дозволяє швидше реагувати на транснаціональні схеми відмивання.
- **Боротьба з онлайн-шахрайством** потребує не лише технічних бар'єрів, а й системного підвищення цифрової грамотності населення.
- **Міжнародна кооперація та обмін фінансовою інформацією** залишаються критично важливими для протидії схемам обходу санкцій і глобальним злочинним мережам.

У підсумку звіт демонструє, що Велика Британія зробила серйозний поступ у реформуванні правового поля, посиленні інституцій та координації з приватним сектором. Проте ключовий висновок документа полягає в тому, що економічна злочинність — це рухома ціль, яка постійно еволюціонує. Тому відповідь на неї має бути комплексною і динамічною: від законодавчих інновацій і технологічних рішень до широкої міжнародної кооперації. Тільки так можна зберегти фінансову систему захищеною, а суспільство — впевненим у справедливості та стійкості держави.

Організована імміграційна злочинність і тіньові фінансові потоки: уроки з британського досвіду [5]

33-й випуск журналу «SARs in Action» від UK Financial Intelligence Unit (UKFIU) став найбільш сфокусованим на темі Organised Immigration Crime (OIC) — організованої імміграційної злочинності, яка дедалі більше визначає кримінальну економіку Великої Британії та Європи. Він підкреслює, що незаконне перевезення мігрантів не обмежується фізичними маршрутами через Середземне море чи Ла-Манш — воно тісно пов'язане з фінансовими потоками, що забезпечують діяльність злочинних угруповань. Саме тут Suspicious Activity Reports (SARs) стають

[5] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/762-sars-in-action-issue-33/file

інструментом, який дозволяє бачити те, що невидиме для класичних правоохоронних методів: схеми переказів, маршрути фінансування, роль «сірого» бізнесу та тіньових систем платежів.

В журналі наводиться детальний опис операцій, які показали ефективність фінансової розвідки. Найбільш показовою стала операція SHEETFUL, у якій агенти NCA виявили схему перевезення мігрантів із Курдистану до ЄС та Великої Британії. Рекрутинг здійснювався через соціальні мережі, а фінансове забезпечення організовувалося за допомогою хавали — традиційної системи неформальних переказів. Кошти мігрантів «заморожувалися» у посередників (хаваладарів) в Іраку й виплачувалися лише після завершення подорожі, а частина грошей інвестувалася у нерухомість і предмети розкоші, що ускладнювало відстеження. Завдяки SARs правоохоронцям вдалося вийти на активи злочинців, що продемонструвало: навіть системи, які спираються на довіру та не залишають цифрового сліду, все одно можна виявити через ретельний аналіз.

Подібні висновки підтвердили й інші операції. Операція WIREWORKER описує історію колишнього рибалки, який перетворився на одного з найбільших перевізників мігрантів через Середземне море. Він отримав вирок у 25 років, і справа стала прецедентом для доведення ролі локальних підприємців у глобальних злочинних мережах. Операція TAKEFUL показала, як невелика компанія, що працювала без належної реєстрації, стала частиною міжнародної системи з відмивання коштів через хавалу, перекачуючи мільйони фунтів стерлінгів. Ці кейси демонструють, що організована імміграційна злочинність часто виглядає «дрібною» на поверхні, але у фінансовому вимірі вона має масштаби транснаціонального бізнесу.

Журнал наводить вражаючу статистику: між 2019 і 2024 роками UKFIU отримала понад 15 000 SARs, пов’язаних із OIC, причому різке зростання припало на останні два роки. Найчастіше повідомлення надходили від банків та платіжних компаній, що вказує на підвищення їхньої настороженості. Однак лише невеликий відсоток SARs напряму стосувався пріоритетних напрямів, які відслідковує NCA (наприклад, перевезення малими човнами). Це свідчить про брак розуміння серед фінансового сектору щодо того, які саме операції становлять інтерес для розслідувань. UKFIU підкреслює необхідність посилення освітніх програм для банків і небанківських установ, щоб вони краще ідентифікували ризики.

Одним із головних досягнень став запуск Joint Fusion Cell (JFC) — міжвідомчої структури, яка об’єднала аналітиків NCA, Home Office та поліції. JFC отримує дані не лише з SARs, а й з мобільних пристроїв, відкритих джерел та партнерських агентств. Це дозволило швидше виявляти фінансові вузли злочинних мереж і блокувати їхні активи. У 2024 році завдяки JFC вдалося заарештувати членів угруповання, яке організовувало переправу мігрантів через Ла-Манш. Цей приклад показує, що поєднання фінансової розвідки та оперативної роботи створює якісно новий рівень боротьби з OIC.

Випуск також підкреслює значення Public-Private Partnerships (PPP). У боротьбі з імміграційною злочинністю беруть участь понад 200 організацій, включаючи банки, платіжні сервіси, телекомунікаційні компанії та технологічні фірми. У результаті співпраці вдалося:

- закрити понад 8 150 рахунків;
- виявити 10 860 нових, раніше невідомих рахунків;
- заморозити активів на суму понад £255 млн.

Ці цифри доводять, що участь приватного сектору є не просто допоміжним, а визначальним чинником успіху.

Окремим блоком журнал аналізує зміни у регуляторній сфері. З 31 липня 2025 року підвищено поріг для Defence Against Money Laundering (DAML) з £1 000 до £3 000. Це полегшує тиск на бізнес, проте не звільняє його від обов'язку подавати SARs у випадках підозри. Навпаки, UKFIU наголошує: навіть дрібні операції можуть бути частиною більшої злочинної схеми, і фінансові інституції повинні залишатися пильними.

У підсумку, журнал чітко демонструє, що організована імміграційна злочинність — це не лише гуманітарний виклик чи питання прикордонної безпеки. Це насамперед фінансове явище, де гроші рухаються складними маршрутами й інтегруються у легальні економіки. SARs, міжнародна співпраця та партнерство з приватним сектором стають головними інструментами виявлення та руйнування цих мереж. Британський досвід доводить: лише через синергію фінансової розвідки, правоохоронних дій і суспільної пильності можна протистояти злочинним структурам, що заробляють на нелегальній міграції.

Висновки:

- **Фінансові розслідування показали, що навіть складні схеми на основі хавали можна викривати**, тому слід активніше інтегрувати фінансовий моніторинг у розслідування злочинів, пов'язаних із міграцією та контрабандою.
- **Приклади операцій довели, що локальні бізнеси можуть бути частиною глобальних злочинних мереж**, отже необхідний жорсткіший контроль за малими підприємствами та неформальними фінансовими сервісами.
- **Public-Private Partnership (PPP) довело свою ефективність** у Британії, тому варто створити аналогічні формати співпраці між банками, платіжними компаніями та правоохоронцями для швидкої ідентифікації підозрілих рахунків.
- **Зміни в регуляції DAML показують, що підвищення порогів може знизити бюрократію,** але водночас посилює роль бізнесу у вчасному поданні SARs, що актуально у контексті реформування AML-системи.

Звіти окремих інституцій та експертів

Канадська асоціація азартних ігор закликає до перегляду режиму ПВК/ФТ на тлі санкцій FINTRAC проти операторів [6]

Документ аналітичного агентства Apeiro присвячений сучасним викликам у сфері ПВК/ФТ у гральному секторі Канади, особливо в контексті нещодавніх штрафних санкцій, накладених FINTRAC на операторів. Центральною темою є дискусія між регуляторами й представниками індустрії щодо ефективності існуючого режиму та необхідності його модернізації.

У першій частині наведено приклади значних адміністративних штрафів, накладених на провідних операторів — British Columbia Lottery Corporation, Canadian National Exhibition Casino та Saskatchewan Indian Gaming Authority. Порушення стосувалися невиконання вимог до

[6] https://media.licdn.com/dms/document/media/v2/D4D1FAQFYi9iRnul2HA/feedshare-document-pdf-analyzed/B4DZlyijepJQAY-/0/1758563287335?e=1759968000&v=beta&t=duRS__UM_sk2W1gMgYvdIjX12VCUeGg9w1yAK8cWsU0

звітування про підозрілі операції, браку належних політик і процедур для роботи з високоризиковими клієнтами та недоліків у документації програм відповідності. Компанії у відповідь подали апеляції, стверджуючи, що дотримуються закону, а санкції мають каральний і бюрократичний характер.

Документ наголошує, що FINTRAC посилив нагляд саме у зв'язку з наближенням нового раунду оцінки FATF. У попередньому MER (2016) було відзначено, що канадські казино розуміють свої зобов'язання, проте застосовують формальний "tick-the-box" підхід без достатнього ризик-орієнтованого підходу. Поточна Національна оцінка ризиків (НОР) визначає як фізичні, так і онлайн-казино високоризиковими, з огляду на роботу з готівкою, клієнтами-нерезидентами та PEP.

Особливе місце відведено результатам "Комісії Каллена", яка досліджувала масштабне відмивання коштів у казино Британської Колумбії. Її висновки продемонстрували наявність "Ванкуверської моделі", де злочинні угруповання через готівкових посередників легалізували кошти через ігрові заклади, з подальшим виведенням грошей за кордон. Це призвело до рекомендацій щодо підвищення прозорості готівкових потоків, запровадження чіткіших правил для онлайн-гемблінгу та криптовалют, а також посилення взаємодії між операторами, регуляторами та правоохоронцями.

Представники індустрії, зокрема Канадська гральна асоціація, різко критикують підхід FINTRAC, наголошуючи, що "галочка заради звіту" та великі штрафи не вирішують проблему. Вони вимагають перегляду законодавства, яке не враховує сучасні форми гемблінгу (онлайн-казино, спортивні ставки, іподроми) та ускладнює роботу через надмірну бюрократизацію процесу звітування. Оператори пропонують дозволити приватним компаніям напряму подавати звіти, аби підвищити ефективність і оперативність виконання вимог.

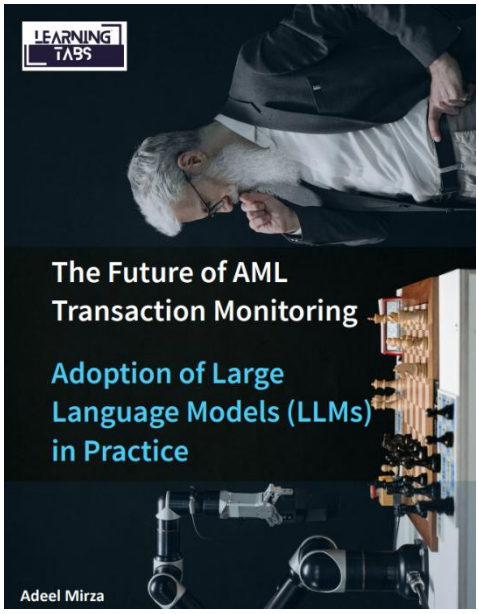
Водночас експерти визнають, що завдяки структурним реформам Канада стала більш підготовленою, ніж під час попередніх оцінок. Йдеться про розширення сфери дії законодавства, посилення санкцій, модернізацію наглядового механізму FINTRAC і врахування міжнародних стандартів щодо криптоактивів. Проте системна проблема полягає у низькому рівні розслідувань та вироків у справах про відмивання коштів, що FATF, ймовірно, знову відзначить як слабке місце.

Висновки:

- **Регуляторний тиск зростає через оцінку FATF:** FINTRAC активно застосовує штрафи для демонстрації жорсткого підходу до виконання вимог з ПВК/ФТ у гральному секторі.
- **Недоліки чинної системи:** Законодавство й механізми звітування застаріли й не враховують специфіку сучасних форматів гемблінгу, створюючи надмірну бюрократію без достатньої ефективності.
- **Уроки "Ванкуверської моделі":** досвід Британської Колумбії показав критичну необхідність кращого відстеження готівки, посилених правил для онлайн-гемблінгу та криптовалют, а також більшої кооперації з правоохоронцями.
- **Практичні кроки для операторів:** перегляд корпоративного управління й ризик-менеджменту, інвестиції у технології моніторингу, підвищення кваліфікації персоналу та використання актуальних даних НОР у програмах відповідності.

Фахівці радять операторам зміцнювати системи управління й підзвітності, забезпечувати належний рівень ресурсів і технологій для моніторингу, покращувати якість звітності для топ-менеджменту, а також системно оновлювати ризик-асесменти відповідно до останньої NRA.

Впровадження великих мовних моделей до моніторингу операцій [7]



Документ за авторством Adeel Mirza присвячений трансформаційному впливу великих мовних моделей (LLM) на процеси ПВК/ФТ, зокрема у сфері моніторингу транзакцій. У вступі наголошується, що традиційні системи моніторингу, які базуються на жорстких правилах та порогових значеннях, більше не справляються з викликами сучасності: високим рівнем хибнопозитивних спрацювань (понад 90% у багатьох банках), складністю нових типологій злочинів (наприклад, використання криптовалют для багаторівневого відмивання чи ФР), а також надмірним навантаженням на аналітиків через ручну підготовку звітів про підозрілі операції. У цьому контексті LLM пропонуються зсув, здатний забезпечити контекстуальне розуміння, безперервне навчання та масштабовану підтримку аналітиків.

Документ детально пояснює природу LLM: це алгоритми, навчені на мільярдах слів із мільйонами чи мільярдами параметрів, які здатні аналізувати тексти, перекладати, узагальнювати інформацію, генерувати звіти й навіть писати код. Вони вже використовуються у ПВК/ФТ для зменшення кількості хибнопозитивних спрацювань, підтримки аналітиків під час розслідувань, складання підсумкових звітів, а також для створення "віртуальних асистентів", які допомагають молодим фахівцям орієнтуватися у складних схемах типу TBML чи ухилення від санкцій. Наведені конкретні приклади пілотних впроваджень у провідних фінансових установах: зменшення часу обробки спрацювань на 30–40% завдяки автоматизованим резюме випадків; ідентифікація підозрілого експорту товарів у зв'язку з попередженням FATF щодо ФР через товари подвійного призначення; автоматизоване формування наративів у звітах до ПФР, що скорочувало час підготовки з годин до хвилин.

Висновки:

- **Оптимізація моніторингу транзакцій:** впровадження LLM дозволяє суттєво знизити кількість хибнопозитивних спрацювань і скоротити час їх обробки на 30–40%, що прямо підвищує ефективність процесів з ПВК/ФТ.
- **Підвищення якості звітності:** використання LLM для автоматизації написання опису у звітах до ПФР зменшує ручне навантаження та стандартизує якість повідомлень.
- **Необхідність регуляторної сумісності:** для масштабного впровадження потрібні чіткі рамки управління моделями, контроль "галюцинацій" та забезпечення прозорості рішень, інакше регулятори не визнають результати прийнятними.
- **Стратегічна інтеграція:** фінансові установи мають застосовувати гібридні архітектури та вузькоспеціалізовані моделі, забезпечуючи постійний аудит і людський контроль, щоб максимально ефективно та безпечно інтегрувати LLM у ПВК/ФТ.

Разом з тим у документі наголошено на значних викликах впровадження LLM. По-перше, це питання конфіденційності та захисту даних: використання відкритих моделей несе ризики витоку, тому банки змушені будувати приватні рішення. По-друге, прозорість та підзвітність: регулятори очікують пояснень, чому

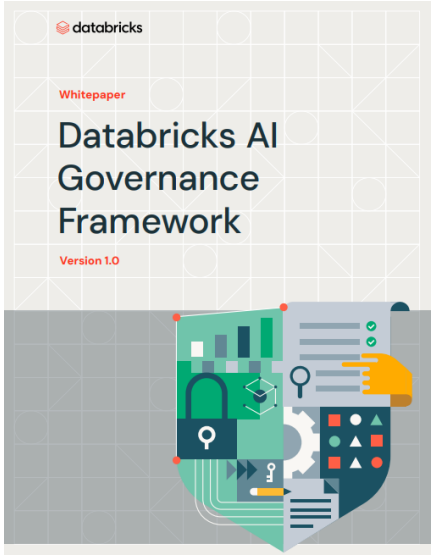
[7] https://media.licdn.com/dms/document/media/v2/D4D1FAQFv-dG7ZjlKUA/feedshare-document-pdf-analyzed/B4DZliBKMXJQAY-/0/1758286099608?e=1759968000&v=beta&t=8n2ZsjuIXgPu-9ux51KvYQjBH6JX2FxsGf-aNS36uss

певний алерт було підвищено або відхилено, тоді як LLM схильні до "галюцинацій" і не завжди можуть надати прозору логіку рішень. По-третє, ризик упередженості та помилок у випадку навчання на нерелевантних даних. По-четверте, висока вартість розгортання — сотні тисяч доларів на місяць для великих установ. Також зазначається, що регулятори загалом відкриті до інновацій, проте вимагають чітких рамок управління моделями, систем валідації та аудиту.

У частині практичних рішень автор пропонує кілька стратегій. По-перше, гібридні моделі розгортання (поєднання локальних і хмарних рішень) для балансу між безпекою та ефективністю. По-друге, використання менших моделей, спеціально адаптованих під завдання ПВК/ФТ, що знижує витрати та підвищує точність. По-третє, створення постійних механізмів моніторингу, перевірки та аудиту результатів з активною участю людини. По-четверте, оптимізація витрат за рахунок пакетної обробки, використання тимчасових обчислювальних ресурсів у хмарі та залучення найпотужніших моделей лише для складних випадків.

У підсумку робиться висновок, що LLM не замінюють класичні системи моніторингу й аналітиків, а виступають інструментом підсилення. Вони здатні зменшити навантаження на персонал, підвищити якість і швидкість аналізу, а також допомогти зосередити людські ресурси на справді складних або високоризикових випадках. Головним фактором успіху стане баланс між інноваційністю та належним управлінням, прозорістю результатів і конструктивним діалогом із регуляторами.

Структура управління штучним інтелектом [8]



Документ “Databricks” є комплексним посібником, що пропонує організаціям структурований та цілісний підхід до управління програмами штучного інтелекту, включно з машинним навчанням (ML) та генеративним AI (GenAI). Хоча документ має універсальний характер, його принципи та компоненти є надзвичайно актуальними для фінансових установ, які впроваджують або планують впроваджувати AI-рішення у свої комплаєнс-функції, зокрема у сфері ПВК/ФТ/ФР. Фреймворк побудований на п'яти фундаментальних стовпах, які разом створюють надійну систему для відповідального, етичного та безпечного використання AI, що повністю відповідає вимогам до сучасних систем ПВК/ФТ.

Перший стовп, "Організація AI", закладає управлінську основу, наголошуючи на необхідності інтеграції AI-стратегії в загальні бізнес-цілі організації. Для сфери ПВК/ФТ це означає, що впровадження AI має бути не просто технічним експериментом, а свідомим кроком для посилення ризик-менеджменту та ефективності комплаєнс-процесів. Документ підкреслює важливість створення чіткої моделі управління (централізованої, розподіленої чи гібридної), визначення ролей та відповідальності (наприклад, Chief AI Officer), а також формування наглядових органів, таких як етичні комітети чи керівні ради. Це прямо корелює з вимогою до фінансових установ мати чітку структуру управління комплаєнс-ризиками, де відповідальність за прийняття рішень, зокрема на основі ШІ, є чітко зафіксованою.

Другий стовп, "Відповідність законодавству та регуляторним вимогам", є центральним для будь-якої комплаєнс-функції. Фреймворк акцентує на необхідності систематичної оцінки

[8] https://media.licdn.com/dms/document/media/v2/D4E1FAQGm-JN_xz2REQ/feedshare-document-pdf-analyzed/B4EZgjWF80HgAY-/0/1752939660297?e=1759968000&v=beta&t=Uj2Fmh9Qu0t0sXxoa3GciKrSO31VZtCwBNzsSVVooq0

правових ризиків, пов'язаних із використанням ШІ, включно з дотриманням галузевих норм (наприклад, банківського регулювання), законів про захист даних (як-от GDPR) та нових спеціалізованих актів, подібних до EU AI Act. Для спеціаліста з ПВК/ФТ це означає необхідність проактивного аналізу того, як AI-моделі для моніторингу транзакцій чи оцінки ризику клієнтів відповідають вимогам регулятора, та розробки стратегій для мінімізації юридичних ризиків, зокрема через чіткі контрактні зобов'язання з постачальниками технологій та ретельне документування процесів.

Третій стовп, "Етика, прозорість та інтерпретованість", торкається однієї з найскладніших проблем AI у фінансовому секторі. Для сфери ПВК/ФТ недостатньо, щоб модель просто виявляла підозрілі операції; установа повинна бути здатною пояснити, чому саме було прийнято те чи інше рішення. Документ розкриває ключові етичні принципи — підзвітність, справедливість (уникнення упередженості), людиноцентричність та інклюзивність. Особливо важливим є розмежування понять інтерпретованості (можливість розуміти логіку роботи моделі) та пояснюваності (можливість обґрунтувати конкретний результат). Це є критичним для валідації моделей, проходження аудитів та обґрунтування рішень перед регуляторами, наприклад, при поданні SAR/STR.

Четвертий стовп, "Операції AI, дані та інфраструктура", описує технічний фундамент, необхідний для стабільної та надійної роботи AI-систем. Для ПВК/ФТ це означає наявність надійних процесів управління даними, від їх збору та очищення до зберігання та використання. Документ підкреслює важливість якості, повноти та репрезентативності даних, що є основою для ефективності будь-якої AI-моделі моніторингу. Крім того, розглядаються аспекти AIOps — практики, що забезпечують автоматизацію, моніторинг та масштабування життєвого циклу ML-моделей, що дозволяє підтримувати їхню ефективність у довгостроковій перспективі (наприклад, своєчасно виявляти "дрейф моделі").

П'ятий стовп, "Безпека AI", присвячений захисту AI-систем від зовнішніх та внутрішніх загроз, що є критичним для збереження цілісності комплаєнс-процесів. Документ

Висновки:

- **Впровадження AI в ПВК/ФТ вимагає створення формалізованої структури управління.** Необхідно створити спеціалізований наглядовий орган (наприклад, комітет з ризиків AI) та призначити відповідальних осіб, які б забезпечували відповідність AI-ініціатив стратегії управління ризиками, нормативним вимогам та етичним стандартам організації.
- **Пояснюваність AI-рішень є ключовою вимогою для комплаєнсу.** Фінансова установа повинна бути готова надати регуляторам та аудиторам чітке обґрунтування будь-якого рішення, прийнятого за допомогою AI (наприклад, чому клієнту присвоєно високий рівень ризику або чому транзакцію визнано підозрілою). Для цього необхідно впроваджувати технічні інструменти (наприклад, SHAP, LIME) та вести детальну документацію всього життєвого циклу моделі.
- **Якість та відстежуваність даних є фундаментом надійності AI-систем у ПВК/ФТ.** Перед впровадженням AI необхідно провести аудит та налагодити процеси управління даними, забезпечивши їх точність, повноту та неупередженість. Впровадження систем відстеження походження даних є обов'язковим для забезпечення прозорості та можливості відтворення результатів моделі.
- **Безпека AI має стати невід'ємною частиною програми кібербезпеки фінансової установи.** Необхідно розробити та впровадити специфічні заходи контролю для захисту AI-моделей від маніпуляцій, таких як "отруєння даних" або зловмисні запити, оскільки компрометація таких систем може призвести до системного збою всієї функції ПВК/ФТ.

відсилає до детального фреймворку DASF, окреслюючи ключові ризики, такі як отруєння даних (data poisoning), викрадення моделей (model theft) та маніпуляція вхідними запитами для отримання бажаного результату. Для сфери ПВК/ФТ це означає необхідність захисту моделей санкційного скринінгу, оцінки ризиків клієнтів та моніторингу транзакцій від спроб їх обійти або "обдурити", що могло б призвести до пропуску фінансових злочинів та серйозних регуляторних наслідків.

Цільові Фінансові Санкції та Фінансування Розповсюдження: Інтеграція в Режими ПВК/ФТ, Схеми Ухилення та Виклики Глобальної Відповідальності [9]

Даний документ є випуском "FIH Insights" (Financial Integrity Hub Insights) за вересень 2025 року, який є продуктом провідного дослідницького центру, присвяченого запобіганню та пом'якшенню фінансових злочинів. Цей звіт представляє глибокий аналіз цільових фінансових санкцій (ЦФС) та боротьби з фінансуванням розповсюдження (ФР), розглядаючи їхню інтеграцію у глобальні та внутрішні режими ПВК/ФТ.

Звіт підкреслює критичну роль санкцій як невійськових заходів, необхідних для реагування на міжнародні загрози, такі як тероризм, торгівля людьми та розповсюдження зброї масового знищення (ЗМЗ). Санкції загалом поділяються на дві категорії: цільові фінансові санкції, які передбачають заморожування активів та заборону надання коштів, та торговельні обмеження. Надійне дотримання санкцій має життєво важливе значення, оскільки воно забезпечує узгодженість внутрішніх практик з міжнародними зобов'язаннями, зокрема Резолюціями Ради Безпеки ООН (РБ ООН) та стандартами FATF, і захищає суб’єкти в середині країни від ненавмисного сприяння незаконній торгівлі або ФР.

Ключовим елементом звіту є аналіз оновленої Консультативної ноти від 25 серпня 2025 року, випущеної Австралійським офісом із питань санкцій (ASO) при Департаменті закордонних справ і торгівлі (DFAT). Ця нота надає "підзвітним суб'єктам" детальне керівництво щодо зобов'язань з дотримання та управління ризиками. DFAT визначає ФР як надання коштів або фінансових послуг для виробництва, придбання, володіння чи транспортування ЗМЗ та їхніх систем доставки в порушення міжнародного чи національного законодавства. Підзвітні суб'єкти повинні застосовувати "розумну обережність та належну обачність", що включає скринінг клієнтів, надійний внутрішній контроль та навчання персоналу, щоб уникнути участі у підсанкційних діях. Консультативна нота DFAT виділяє основні фактори ризику ФР: клієнтські ризики (пов'язані з підсанкційними країнами або підозрілими структурами власності), географічні ризики (зокрема, Іран, КНДР, Росія), ризики продуктів (наприклад, торгове фінансування та товари подвійного призначення) та ризики транзакцій (складні маршрути та використання підставних компаній). Серед високоризикових секторів ідентифіковано постачальників послуг віртуальних активів (VASP), операторів з дорогоцінними металами та камінням, морське судноплавство, а також постачальників послуг трастів і компаній.

Звіт деталізує типові методології ухилення від санкцій, які включають зловживання товарами подвійного призначення, використання відмивання грошей на основі торгівлі, приховування бенефіціарної власності за допомогою підставних компаній та посередників, а також

[9] https://www.mq.edu.au/__data/assets/pdf_file/0003/1355547/FIH-Insights-Sept-25.pdf

використання криптовалют для нашарування та приховування коштів. На міжнародному рівні, FATF вимагає від країн впровадження ЦФС відповідно до Рекомендації 7 (пов'язаної з Резолюціями РБ ООН про розповсюдження ЗМЗ), а також застосування посиленої належної перевірки та контрзаходів щодо юрисдикцій високого ризику, таких як Росія, КНДР та Іран (Рекомендація 19). Санкції, таким чином, є операційним інструментом для досягнення відповідності зобов'язанням FATF. З 31 березня 2026 року в Австралії набудуть чинності реформи до Закону про ПВК/ФТ, які явно інтегрують дотримання санкцій у бізнес-зобов'язання, вимагаючи оцінки ризиків ФР та систематичного скринінгу щодо наявності у Консолідованому санкційному списку DFAT.

Європейський Союз також зміцнює свій режим, інтегруючи ЦФС у законодавство ПВК/ФТ через Директиву AMLD6 та Регламент AMLR. Ці акти вимагають включення ризиків невиконання або ухилення від ЦФС у наднаціональні та національні оцінки ризиків. AMLD6 розширює повноваження державних органів: центральні реєстри бенефіціарної власності повинні звіряти свої дані зі списками санкцій, а нове Управління з питань ПВК/ФТ (AMLA) координуватиме нагляд на рівні ЄС. Фінансові установи в ЄС тепер мають чіткіші обов'язки, включаючи постійний скринінг клієнтів і бенефіціарних власників та негайне заморожування активів.

Незважаючи на міжнародні зусилля, ухилення від санкцій залишається стійким, з використанням посередників, приховуванням бенефіціарної власності та експлуатацією морського сектора. Звіт приділяє особливу увагу інтеграції віртуальних активів, зокрема стейблкоїнів, у схеми ухилення, оскільки вони дозволяють переказувати доларові активи, минаючи банківську інфраструктуру, на яку розраховані санкції (наприклад, SWIFT або кореспондентські банки). Хоча стейблкоїни не є єдиною проблемою, вони посилюють ефективність традиційних методів, таких як підставні компанії та маніпуляції з торговельними рахунками. Недотримання санкцій має високі наслідки, від значних штрафів до кримінальної відповідальності. Регуляторні механізми примусу включають накази про припинення діяльності, фінансові штрафи та накази про конфіскацію, хоча останні рідко застосовуються через побоювання фінансової нестабільності. У цьому контексті

Висновки:

- **Термінова інтеграція санкцій за ФР:** З 31 березня 2026 року всі пілзвітні суб'єкти в Австралії (і паралельно ЄС) повинні забезпечити повну інтеграцію оцінки ризиків ФР та постійного систематичного скринінгу проти Консолідованого санкційного списку DFAT у свої програми ПВК/ФТ, застосовуючи EDD до юрисдикцій високого ризику.
- **Запобігання гібридному ухиленню:** Організації повинні розробити стратегії виявлення гібридних схем ухилення, які поєднують традиційні кримінальні методи (наприклад, підставні компанії, фальсифікація торговельних документів) із сучасними технологіями (використання стейблкоїнів та інших віртуальних активів) для обходу банківської інфраструктури.
- **Контроль за NGO та гуманітарною допомогою:** Необхідно застосовувати суворі правила "Знай свого місцевого партнера" (KYLP) та обов'язково використовувати виключно регульовані, технологічні (наприклад, біометричні картки) канали для передачі коштів у зони конфлікту, категорично забороняючи використання готівки для запобігання зловживанню NGO терористичними групами.
- **Фокус на відповідальності посадових осіб:** Для підвищення ефективності системи ПВК/ФТ глобальні регулятори повинні шукати шляхи для забезпечення цільової відповідальності конкретних державних службовців або установ, які демонструють постійну недбалість у впровадженні стандартів, замість того, щоб накладати широкі санкції, які непропорційно шкодять невинному населенню.

Канада створює прецедент, активно застосовуючи повноваження Special Economic Measures Act (SEMA) для конфіскації підсанкційних активів, як це було продемонстровано у справі літака Антонов Ан-124.

Звіт також висвітлює проблему зловживання неурядовими організаціями (NGO) та шахрайськими благодійними організаціями для фінансування тероризму під виглядом гуманітарної допомоги, що вимагає суворої належної обачності щодо місцевих партнерів та використання лише регульованих каналів передачі коштів, повністю виключаючи готівку в зонах конфлікту. Також піднімається питання про непередбачені наслідки санкцій, включаючи побічний збиток для невинних сторін та явище де-ризикінгу, коли фінансові установи уникають усіх транзакцій, пов'язаних із санкціонованими державами, що може перешкоджати законній гуманітарній допомозі. Звіти FATF про взаємну оцінку часто виявляють недоліки в юрисдикціях, які потрапляють до "сірого списку", що призводить до економічних труднощів для населення. Звіт закликає до цільової відповідальності, стверджуючи, що тягар має лягати на недбалих державних службовців і органи, відповідальні за впровадження ефективних заходів ПВК/ФТ, а не на все населення.

«Піксельні прибутки»: як ігрові економіки перетворюються на нове джерело терористичного фінансування [10]

У статті від GNET досліджується феномен, який донедавна здавався периферійним і майже фантастичним: використання ігрових валют та економік як інструменту для фінансування терористичних структур. Приклад Індонезії, яка має один із найбільших ігрових ринків у Південно-Східній Азії, показує, що зростання цифрових платформ для мобільних ігор, таких як Mobile Legends, Free Fire чи PUBG Mobile, створює не лише ринок розваг і соціальної взаємодії, а й середовище для відмивання коштів і прихованого фінансування. Лише у 2023 році ринок відеоігор в Індонезії оцінювався у понад 3,11 мільярда доларів, із прогнозами швидкого зростання, що робить його привабливим як для легальних інвесторів, так і для кримінальних структур.

Основна загроза полягає у специфіці внутрішньоігрових валют, які функціонують як проміжний фінансовий інструмент між реальними грошима та цифровими активами. Користувач купує валюту за допомогою локальних платіжних систем чи кредитних карт, а потім використовує її для внутрішньоігрових покупок — від скінів (кольорових обгорток на ігрові предмети) до предметів, що дають перевагу в грі. Однак ці валюти мають властивості, що дозволяють їх накопичувати, переказувати між акаунтами або продавати на сторонніх ринках. Саме ця «гнучкість» перетворює їх на ідеальний інструмент для терористичних структур, які шукають способи розмивання коштів через малопомітні й малоконтрольовані канали.

У статті описано кілька типових схем. Одна з них передбачає використання викрадених кредитних карт для масової купівлі внутрішньоігрових валют. Далі ці активи «розмиваються» через десятки акаунтів, іноді навіть у різних іграх, щоб втратити первинне походження. Після цього їх перепродають на сторонніх платформах уже як «законний цифровий товар». У підсумку злочинні мережі отримують «чисті» гроші, походження яких практично неможливо відслідкувати без доступу до всієї транзакційної мережі.

[10] https://gnet-research.org/2025/08/29/pixelated-profits-terrorist-financing-through-in-game-economies-in-indonesia/

Ще одна поширена схема — використання масових мікротранзакцій. Ігри побудовані на дрібних покупках, що виглядають як нормальна поведінка гравців. Терористи та кримінальні мережі дроблять великі суми на сотні чи тисячі малих транзакцій, які не перевищують порогів. Таке «структурування» (structuring) дозволяє обходити навіть автоматизовані алгоритми виявлення підозрілих операцій, оскільки поведінка виглядає органічною для молодої аудиторії геймерів.

Важливим чинником є інфраструктурні слабкості Індонезії. Країна має швидко зростаючу екосистему цифрових платежів, але багато місцевих гаманців і мобільних платіжних сервісів досі не інтегровані з глобальними стандартами фінансового моніторингу. У частини провайдерів ігрових послуг відсутній ефективний KYC або ідентифікація користувачів обмежена лише базовими перевірками. Це створює «сліпі зони», де навіть значні суми можуть циркулювати без уваги державних структур. Саме через це ігрові економіки перетворюються на «тіньові банки» для нелегальних мереж.

Стаття звертає увагу і на реакцію держави. У 2024 році в Індонезії ухвалили закон, який вводить вимоги до регулювання індустрії геймінгу, включаючи положення щодо дотримання стандартів AML/CFT. Фінансовий регулятор OJK і підрозділ фінансової розвідки PPATK почали активніше співпрацювати з ігровими компаніями та платіжними провайдерами. Проте швидкість інновацій у цьому секторі часто випереджає можливості державного контролю. У той час як регулятори лише починають створювати рамки, ігрові валюти вже активно використовуються для схем фінансування, які складно відстежити.

Стаття робить висновок, що індонезійський приклад є симптомом глобальної тенденції. Якщо сьогодні ігрові економіки використовуються як допоміжний канал, завтра вони можуть перетворитися на один із ключових інструментів прихованого фінансування. Це особливо небезпечно у поєднанні з іншими цифровими активами — криптовалютами, DeFi-протоколами та NFT, які теж поступово інтегруються у транснаціональні схеми відмивання коштів.

У цьому контексті автор пропонує низку практичних рішень. По-перше, ігрові компанії повинні впроваджувати суворі системи KYC та моніторингу користувацьких транзакцій, зокрема виявляти нетипові патерни, як-от часті дрібні перекази між акаунтами або надмірно великі покупки за короткий проміжок часу. По-друге, необхідне обмеження можливості обміну ігрової валюти на зовнішніх ринках без належної ідентифікації. По-третє, держава має створювати правові рамки, які охоплюють ігровий сектор як частину фінансової системи, а не лише як розважальну індустрію. Нарешті, необхідна міжнародна координація, адже цифрові активи й ігрові економіки не визнають кордонів.

Загальний меседж статті: світ стоїть перед новим викликом, де розваги й фінансова злочинність перетинаються у несподіваній площині. Якщо ігрові економіки залишаться поза увагою регуляторів і аналітиків, вони можуть перетворитися на приховані фінансові системи для терористів і злочинних організацій. І хоча сьогодні це явище здається маргінальним, його потенційна

Висновки:

- **Ігрові валюти стають новим каналом фінансових зловживань**, тому ігровим платформам слід впровадити суворий KYC та аналітику транзакцій для виявлення підозрілих патернів.
- **Мікротранзакції використовуються для дроблення великих сум**, отже регуляторам потрібно адаптувати AML/CFT-системи до моніторингу дрібних, але масових операцій.
- **Слабкий контроль локальних платіжних сервісів створює «сліпі зони»**, тому країнам необхідно інтегрувати індустрію геймінгу у фінансове регулювання та вимоги прозорості.
- **Міжнародна співпраця має стати ключем**, адже ігрові економіки не визнають кордонів і можуть швидко стати частиною глобальних схем фінансування тероризму.

загроза може швидко зрости, особливо з урахуванням динаміки розвитку цифрових платформ та ігор із мільйонами активних користувачів.

Хто володіє Південною Африкою: як «Система» приватної влади формує нерівність? [11]

Розслідування Open Secrets під назвою The System: Money, Power and Politics відкриває перший том масштабної серії Who Owns South Africa, де автори ставлять фундаментальне питання: хто насправді контролює південно-африканську економіку і як ця влада формується у пост-апартеїдній добі.

Документ демонструє, що, незважаючи на формальні демократичні інститути та перехід до інклюзивної політики, справжні власники ресурсів і капіталу зуміли зберегти контроль і адаптуватися до нових умов. Фактично формується замкнена «Система», де багатство і політична влада не просто співіснують, а взаємно підживлюють одне одного, створюючи цикл, у якому капітал купує вплив, а політичні рішення забезпечують нові вигоди власникам капіталу.

Документ підкреслює драматичний контраст між економічним потенціалом ПАР і соціальною реальністю. Країна має одну з найпотужніших фінансових систем на континенті, розвинений ринок капіталу, доступ до багатих природних ресурсів, високий рівень урбанізації та підприємницької активності. Водночас показники соціальної нерівності залишаються критичними: безробіття сягає 33 %, а серед молоді перевищує 46 %; понад 28 мільйонів громадян змушені виживати завдяки соціальним грантам. Це створює ситуацію, коли економіка працює не на суспільний розвиток, а на відтворення багатства невеликої групи, тоді як більшість населення живе в умовах вразливості.

Центральним елементом аналізу є роль великих корпорацій. В енергетиці, гірничодобувній промисловості, агробізнесі, фінансах і телекомунікаціях ключові гравці мають олігопольний або монопольний контроль. Вони диктують умови ціноутворення, впливають на інвестиційні пріоритети та фактично визначають напрямок розвитку економіки. Ці корпорації формально існують у демократичному середовищі, але через складні корпоративні структури, дочірні компанії, холдинги та офшори реальні бенефіціари залишаються прихованими. Таким чином, громадськість не має можливості відслідкувати, хто контролює стратегічні активи країни та які інтереси стоять за ключовими економічними рішеннями.

Особливої уваги автори приділяють тому, як держава стає інструментом приватних інтересів. Замість того, щоб стримувати надмірну владу капіталу, політичні інститути часто виступають як сервіс для бізнесу. Політичні партії отримують фінансування від корпоративних структур, що створює залежність від їхніх грошей. Натомість компанії отримують державні контракти, пільги чи регуляторні поступки. Це класичний механізм «захоплення держави» (state capture), який, на думку Open Secrets, у ПАР не є поодиноким явищем, а фактично вбудований у системну архітектуру управління.

Окремо розглядається вплив «Системи» на суспільні сфери. У сфері охорони здоров'я приватні корпорації контролюють доступ до якісних медичних послуг, тоді як державна система залишається недофінансованою. В освіті зберігаються відмінності між елітними приватними школами та університетами й масовим доступом до посередніх або обмежених державних

[11] https://www.opensecrets.org.za/wosa_system/

послуг. У транспорті й інфраструктурі великі приватні підрядники диктують умови, а вартість контрактів часто значно перевищує їхню якість. Ці сфери показують, як приватна влада визначає умови життя громадян, підсилюючи розрив між багатими та бідними.

У політичному контексті «Система» проявляється і в кадровій циркуляції: менеджери корпорацій отримують посади в державних структурах і навпаки, що створює тісні мережі особистих і професійних зв'язків. Цей «обіг еліт» означає, що незалежність між державою та бізнесом є умовною: ті самі особи або їхні мережі здатні одночасно впливати на політику, фінанси й економічні пріоритети.

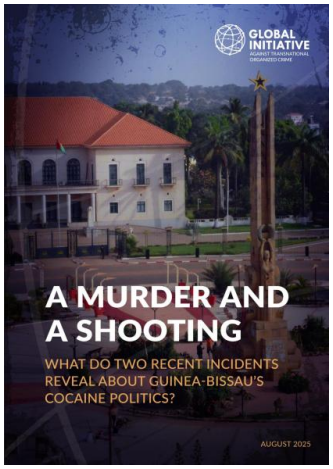
Висновки:

- **Варто розвивати прозорі реєстри бенефіціарних власників**, щоб унеможливити приховування ключових економічних активів за офшорними структурами.
- **Необхідно законодавчо врегулювати політичне фінансування та лобізм**, щоб уникнути захоплення держави приватними інтересами.
- **Слід посилити регуляції проти олігопольних практик** у стратегічних секторах, щоб забезпечити рівний доступ нових гравців і зменшити концентрацію влади.
- **Важливо розбудовувати незалежні механізми нагляду** за державно-приватними контрактами, аби вони служили суспільним інтересам, а не вузькому колу еліт.

Документ підкреслює, що «Система» не є випадковим феноменом чи наслідком хаосу — це добре вибудувана модель, яка має інституційні та правові механізми відтворення. Вона працює через законодавство про приватизацію, через регуляції у сфері конкуренції, через слабкість контролю над лобіюванням і політичним фінансуванням. Навіть демократичні інститути, формально покликані забезпечувати баланс, часто виявляються інструменталізованими, оскільки їхні рішення ухвалюються у контексті тиску й впливу корпоративних інтересів.

У підсумку автори роблять висновок, що без системних змін і радикальної прозорості — від відкритих реєстрів бенефіціарних власників до суворого регулювання політичного фінансування й контролю над офшорними потоками — країна залишатиметься в замкненому циклі нерівності. Open Secrets закликає до побудови нового суспільного договору, у якому корпоративна влада буде підзвітною суспільству, а держава — незалежною від приватних інтересів.

Кокаїнові війни: як вбивства оголили політичну сторону наркоторгівлі [12]



Гвінея-Бісау вже понад два десятиліття вважається класичним прикладом «нарко-держави», у якій політика, військові та кримінальні мережі тісно переплетені навколо міжнародного транзиту кокаїну. Ще у 2000-х країна стала одним з основних перевалочних пунктів для наркотиків з Латинської Америки до Європи. Колумбійські нарко-шляхи проходять через Західну Африку, оскільки цей маршрут менш контрольований, дешевший і дозволяє уникати більшої уваги європейських митниць. Гвінея-Бісау, з її слабкою інституційною системою, корумпованими елітами та вигідним географічним розташуванням, ідеально вписалася у цей сценарій.

Попри багаторічну репутацію «кокаїнової столиці Африки», рівень відкритого насильства в країні залишався дивно низьким. Це

[12] https://globalinitiative.net/wp-content/uploads/2025/08/A-murder-and-a-shooting-What-do-recent-incidents-reveal-about-Guinea-Bissaus-cocaine-politics-GI-TOC-August-2025.pdf

пояснюється балансом інтересів: військові, політики та кримінальні групи розподілили сфери впливу і вміли уникати надмірної публічності. Насильство в минулі роки виникало переважно у формі політичних убивств або переворотів, але не у вигляді відкритих кримінальних воєн. Тому події липня 2025 року стали сигналом серйозних зрушень.

Спершу чутки про вбивство іспанця на архіпелазі Біягос, одному з ключових перевалочних пунктів кокаїну, сколихнули місцеву пресу. Хоча історія виявилася перебільшеною, справжнім потрясінням стала смерть Тано Барі, члена президентської гвардії. Його тіло знайшли зі слідами насильства, що вказувало на поспішне й непрофесійне вбивство. Водночас в іншій частині країни стався інцидент із колумбійським емісаром: його поранили під час конфлікту, який пов'язували з крадіжкою партії кокаїну гвінейським кримінальним авторитетом Данілсоном Фернандесом Гомешом, відомим як «Нік».

Ці події миттєво вплинули на місцеву економіку наркотиків. Оптова ціна кілограма кокаїну в Біссау впала з 10–16 тисяч євро до близько 7 тисяч, оскільки «Нік» поспіхом розпродував товар, щоб конвертувати його у готівку. Така різка зміна цін свідчить, що окремі епізоди насильства здатні руйнувати тендітний баланс і підривати «ринкову стабільність» кокаїнового бізнесу. Для місцевих політиків і військових це має особливе значення, адже торгівля наркотиками фінансує вибори, забезпечує дохідні потоки та тримає вкупі хиткі політичні альянси.

Розслідування Global Initiative наголошує, що інциденти не можна розглядати ізольовано. Вони сталися на тлі політичної турбулентності: за кілька тижнів до цього арештували Тчорно Барі, колишнього голову президентської гвардії й старшого брата загиблого Тано. Його звинувачували у зберіганні документів, які могли викривати президента, а також у змові з метою перевороту. Після арешту Тчорно у владі почалася боротьба за перерозподіл впливу, і смерть його брата стала символічним підтвердженням, що конфлікти в еліті вийшли за рамки закритих переговорів.

Водночас стрілянина з колумбійцем показала крихкість партнерських відносин між латиноамериканськими картелями та місцевими кримінальними групами. Традиційно ці відносини будувалися на взаємній вигоді та протекції з боку державних структур. Коли гвінейські партнери, такі як «Нік», зраджують довіру, продаючи кокаїн у власних інтересах, картелі починають розглядати альтернативні маршрути. Це створює ризик для політичної стабільності: втрата доходів від транзиту може спричинити нові хвилі насильства або навіть падіння уряду, як це вже траплялося в 2006–2009 роках.

Таким чином, липневі інциденти 2025 року оголили кілька ключових рис «кокаїнової політики» Гвінеї-Бісау:

- наркоторгівля є інтегральною частиною політичної системи й фінансування виборів;
- військові й еліти залишаються співучасниками схем, але втрата довіри між гравцями може спровокувати конфлікти;

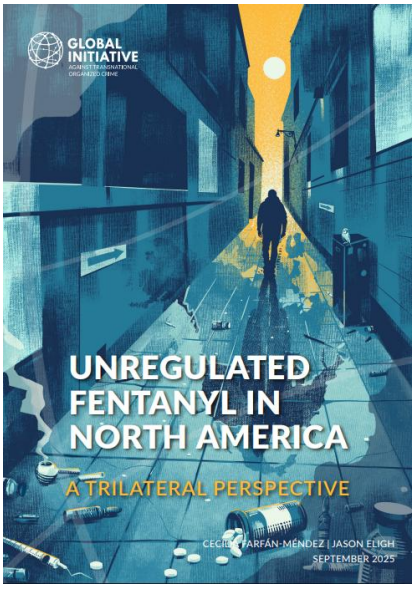
Висновки:

- **Слабкі державні інститути Гвінеї-Бісау дозволяють наркоторгівлі фінансувати політику**, тому міжнародним партнерам варто підтримати розбудову незалежної судової та антикорупційної системи.
- **Падіння довіри між місцевими кланами** та латиноамериканськими картелями може спричинити насильство, отже потрібні механізми регіональної співпраці для моніторингу й стабілізації транзитних маршрутів.
- **Кокаїнова економіка напряму впливає на виборчі процеси**, що вимагає запровадження прозорого фінансування політичних партій і контролю за готівковими потоками.
- **Коливання цін на кокаїн у Біссау свідчать про внутрішні потрясіння**, тому аналітичний моніторинг нарко-ринку слід використовувати як індикатор політичної (не)стабільності.

- ринок кокаїну напряму впливає на політичну стабільність, адже навіть коливання цін стають індикатором внутрішніх потрясінь.

Global Initiative робить висновок: Гвінея-Бісау перебуває на межі. Якщо система «елітного протекціонізму», яка досі утримувала відносний баланс між політиками, військовими та криміналом, ослабне, країну може накрити хвиля насильства. Кокаїн у цьому контексті виступає не просто як товар, а як фундамент політичної економії, що визначає, хто залишиться при владі, хто втратить позиції і навіть хто житиме чи помре.

Фентаніл як стратегічна загроза: спільний виклик для всього регіону [13]



Звіт від Global Initiative концентрується на єдиній, але жахливій ідеї: фентаніл уже не є лише проблемою охорони здоров'я чи окремої кримінальної галузі — це структурна загроза безпеці, що поєднує виробництво, торгівлю, корупцію та політику у єдиний небезпечний ланцюг.

Автори демонструють, що сьогоднішній фентаніл — це продукт північноамериканської екосистеми, у якій складна географія виробництва й збуту поєднується з міжнародними мережами постачання прекурсорів, локальною промисловою інфраструктурою та глибокими соціальними наслідками у вигляді епідемії передозувань. Аналітика підходу «США — Мексика — Канада» дозволяє перейти від спорадичних політичних кроків до розуміння, що без синхронізованих дій одна країна просто «витягує» проблему на себе, а інша — створює умови для її ескалації.

У центрі розгляду — трансформація виробничих ланцюгів: прекурсори фентанілу надходять не лише з традиційних джерел, таких як Китай, але й з інших країн і регіонів — Німеччини, Індії, Гватемали, навіть з окремих потоків всередині США, що демонструє мультиполярну і геоекономічно різноманітну природу проблеми. Частина синтезу концентрується в мексиканських лабораторіях у прикордонних штатах — Баха-Каліфорнія, Сіналоа, Соноро — де поєднуються доступ до логістики, наявність озброєних груп і відносно низький інституційний контроль; таблетування й розпакування партій відбувається у різних точках, у тому числі в Сполучених Штатах та Канаді, що істотно ускладнює відстеження походження та переробки. Канадський випадок вирізняється тим, що країна вже виробляє значну частку свого внутрішнього попиту, що робить проблему не лише транскордонною, а й внутрішньою кризою контролю якості та кримінальної політики. Ці географічні та технологічні розгалуження трансформують традиційні моделі реагування; якщо раніше боротьба з наркотрафіком зосереджувалась на перехопленні великих партій, сьогодні система має реагувати на розпорошену і розподілену мережу виробництва й торгівлі.

Соціальні наслідки цього переходу вже прораховано у страшних цифрах: в США з 2000 року нараховано понад 1,1 мільйона смертей від передозувань, у Канаді — понад 50 тисяч випадків починаючи з 2016 року; в Мексиці кризова динаміка більше виражається у зростанні рівня вбивств і насильницьких зіткнень, пов'язаних із контролем над маршрутами та лабораторіями. Ці відмінності показують, що фентаніл породжує різні ризики у різних національних контекстах: для Півночі проблема — масові передозування і тиск на систему охорони здоров'я, для Півдня — ескалація кримінального насильства й підрив інституційної стабільності. Саме тому політичні

[13] https://globalinitiative.net/wp-content/uploads/2025/09/Cecilia-Farfa%CC%81n-Me%CC%81ndez-Jason-Eligh-Unregulated-fentanyl-in-North-America-A-trilateral-perspective-GI-TOC-September-2025.pdf

інструменти мають бути диференційованими: медичні й профілактичні програми в США й Канаді мають поєднуватися з інституційним підсиленням і реформами в Мексиці, які б унеможливлювали перетворення певних територій на «виробничі хаби» для наркотиків.

Політичні рішення останнього року ілюструють, наскільки важко поєднати медичну й кримінально-правову логіку. Оголошення шести мексиканських картелів «іноземними терористичними організаціями» у США відображає прагнення посилити юридичні засоби тиску, але воно також несе ризики у вигляді дипломатичного напруження й перерозподілу сил у тіньовому секторі. Адже заходи, які ускладнюють одну ланку ланцюга, можуть спричинити адаптацію: картелі міняють маршрути, диверсифікують постачання прекурсорів або стимулюють локальні виробництва далі на півночі. Скасування правила de minimis для китайських і гонконгських вантажів у травні 2025 року — ще один приклад технічного кроку, спрямованого на переривання дрібних потоків прекурсорів, але без узгодженої політики ці заходи ризикують лише частково зменшити доступ до сировини.

В умовах такої складності звіт закликає до комплексного підходу, де заборона і переслідування поєднуються з профілактикою, гарячими лініями, програмами заміщення та реінтеграції, а також з прозорістю даних і спільними науковими програмами з аналізу складів препаратів. Ключовим елементом виступає узгоджена система обміну даними: лабораторні профілі, інформація про прекурсори, митні дані, аналітика транзакцій фінансових потоків — усе це має циркулювати між правоохоронцями та службами громадського здоров'я країн регіону у режимі, що дозволяє одночасно розслідувати та попереджати. Крім того, автори підкреслюють необхідність інвестувати в лабораторні можливості та наукові дослідження, адже ідентифікація нових аналогів фентанілу та їхніх прекурсорів потребує спеціалізованих ресурсів і швидкої наукової реакції.

У практичній площині це означає: створення призначених на національному рівні «координаторів з фентанілу», гармонізацію митних та регуляторних процедур щодо прекурсорів, розбудову каналів для безпечного вилучення та аналізу зразків, розвиток профілактичних програм і доступу до антидотів; для Мексики — підсилення контролю над територіями та розбудова альтернативних економік у вразливих штатах; для Канади — політика протидії внутрішньому виробництву і активна робота з громадським здоров'ям на місцях. Але найголовніше — це не набір поодиноких кроків, а архітектура співпраці: якщо США, Мексика і Канада не створять спільного простору для інформації, ресурсів і політичного реагування, картелі здатні експлуатувати саме ті розриви, що виникають між національними системами.

У підсумку звіт нагадує: боротьба з фентанілом — це не лише локальна правова або медична задача, це геостратегічна операція, де успіх визначається швидкістю обміну

Висновки:

- **Транскордонний характер фентанілового виробництва** вимагає створення спільного механізму обміну даними між США, Канадою та Мексикою для швидкої ідентифікації прекурсорів і логістичних ланцюгів.
- **США повинні поєднувати кримінально-правові заходи проти картелів із фінансуванням програм охорони здоров'я** та доступу до антагоністів опіоїдів, щоб зменшити смертність від передозувань.
- **Мексика має інвестувати у зміцнення інституційного контролю** в прикордонних штатах і пропонувати альтернативні економічні можливості, щоб зменшити залежність місцевих громад від нарковиробництва.
- **Канада повинна розробити національну стратегію протидії внутрішньому виробництву фентанілу**, включно з призначенням координатора та інвестиціями у лабораторні дослідження для моніторингу нових аналогів.

науковою інформацією, узгодженістю регуляторів і здатністю будувати одночасно превентивну та репресивну політику. Без координації регіон ризикує втратити контроль над одним із ключових викликів свого часу — епідемією передозувань на півночі та відверненням політичної та інституційної стабільності на півдні, що має наслідки не лише для регіону, а й для глобальної безпеки.

Рекомендовані та навчальні матеріали

Стратегія використання санкцій [14]

Цей випуск подкасту "STR: Suspicious Transaction Report" під назвою "Strategising the Use of Sanctions: in Conversation with Wally Adeyemo" представляє стратегічний та деталізований аналіз ефективного використання економічних санкцій. У діалозі, який веде Том Кітінг, колишній заступник міністра фінансів США Воллі Адеємо наголошує на фундаментальних вимогах для збереження дієвості санкцій як інструменту зовнішньої політики. Згідно з його позицією, для ефективності санкції потребують чітких, вимірних цілей та очікуваних результатів, обов'язкової багатосторонньої координації та суворого забезпечення виконання (rigorous enforcement). Для того, щоб санкції залишалися надійними та заслуговували на довіру, вони мусять бути інтегровані у ширшу зовнішню політику та забезпечуватися через багатосторонню співпрацю. Обговорення охоплює важливі сучасні питання, включаючи результати Огляду санкцій Міністерства фінансів США 2021 року, стратегію застосування санкцій після повномасштабного вторгнення Росії в Україну, а також складні виклики, які створюють криптовалюти при розробці санкцій у відповідь на жорстокий напад ХАМАС на Ізраїль. Важливим аспектом, на який звертає увагу Адеємо, є ризик надмірного використання санкцій, оскільки це загрожує підірвати вплив США, підштовхуючи супротивників до створення альтернативних фінансових систем. Крім того, надмірне застосування може спричинити ненавмисну гуманітарну шкоду. Загальна тематика цього випуску тісно пов'язана з ширшими дискусіями про американську економічну та фінансову потужність, питання ефективності санкцій як політичного інструменту, людську ціну економічних обмежень, а також контроль США над світовою економікою через механізми, відомі як "Dollar Kill-Switch" та "Sanctions Chokepoints".

Інші новини

Віртуальна валюта як інструмент експлуатації: нові загрози для дітей в онлайн-середовищі [15]

З розвитком цифрових технологій діти дедалі більше інтегровані у віртуальні світи, де навчання, спілкування й розваги відбуваються через ігрові платформи та соціальні простори. Проте одночасно з цим розширюється спектр загроз, серед яких особливу тривогу викликає експлуатація неповнолітніх через віртуальні валюти. Стаття, опублікована на платформі Homeland Security наводить показовий кейс із Північної Кароліни, де 10-річна дівчинка стала

[14] https://open.spotify.com/episode/61RcgYLBOt1Z19yFCXjY9n
[15] https://www.hstoday.us/subject-matter-areas/human-trafficking/perspective-when-virtual-currency-becomes-leverage-against-children/

жертвою сексуального насильства онлайн у популярній грі Roblox: дорослий, видаючи себе за однолітка, поступово завоював її довіру й використав внутрішню валюту Robux як засіб тиску й винагороди, що згодом переросло у вимагання інтимних матеріалів. Цей випадок став предметом судового розгляду, але головне — він демонструє чіткий і тривожний алгоритм дій злочинців.

Автори наголошують: взаємодія в цифровому середовищі має певну послідовність — від початкового контакту і створення довіри у грі, переходу до приватних повідомлень чи сторонніх платформ (наприклад, Discord), далі — пропозицій обміну ігрової валюти на фото, а потім — шантажу, який може призвести навіть до фізичного насильства. Особливу небезпеку становить те, що для дитини обмін Robux виглядає як частина гри, а не злочинна маніпуляція. Таке використання віртуальних валют створює ілюзію легітимності, маскуючи злочинний намір як «обмін» або «подарунок».

Стаття підкреслює масштаб проблеми: Roblox у другому кварталі 2025 року мав 111,8 млн активних користувачів на день і понад 27,4 млрд годин залучення. За таких обсягів навіть мінімальні збої у безпеці можуть означати тисячі жертв. До цього додається низка судових справ у США, де дорослі злочинці зловживали довірою дітей через цю ж платформу, використовуючи схожі схеми. Автори відзначають, що сам Roblox інвестує у кібербезпеку: застосовує технології штучного інтелекту, систему Sentinel, що вже передала понад 1200 випадків потенційної експлуатації до NCMEC, і співпрацює з правоохоронними органами. Проте компанія не може повністю убезпечити користувачів без участі батьків, шкіл і держави.

Важливою є багаторівнева стратегія протидії. На рівні сімей — це постійна комунікація, встановлення «безпечних налаштувань за замовчуванням», блокування підозрілих контактів і моніторинг транзакцій у віртуальних валютах. На рівні шкіл — інтеграція уроків цифрової грамотності, пояснення дітям механізмів шахрайства та експлуатації, впровадження програм фільтрації контенту на шкільних пристроях. На рівні платформ — зміна принципів дизайну: відключення приватних чатів і можливостей торгівлі для акаунтів учасників молодших за 13 років за замовчуванням, верифікація осіб для учасників із високими ризиками, швидке реагування на підозрілі трансакції та прозорість у публікації статистики щодо боротьби з експлуатацією. Нарешті, на рівні правоохоронних органів пріоритетом має бути захист дитини та збереження доказів, швидке реагування на міжплатформні переміщення злочинців і координація з постраждалими родинами для надання психологічної допомоги.

Загальний висновок статті полягає в тому, що цифрова експлуатація дітей через віртуальні валюти не є маргінальною проблемою — це передбачуваний і повторюваний сценарій, який потребує системної відповіді. Якщо чекати, що платформи чи уряди самостійно усунуть загрозу, діти й надалі залишатимуться незахищеними в критичний момент від першого повідомлення до першої вимоги. Лише багаторівнева співпраця — від родини й школи до технологічних компаній і державних структур — здатна скоротити це «вікно вразливості» і зробити цифрове середовище безпечнішим для дітей.

Цифрова ера контенту: між самовираженням і глобальною кримінальною експлуатацією [16]

У статті від Global Initiative, автор Sethasiri Tienpiragul аналізує глибинні трансформації, які відбуваються у сфері створення сексуального контенту під впливом цифровізації. Автор підкреслює, що на відміну від попередніх десятиліть, коли така діяльність була маргіналізованою, прихованою і пов'язувалася передусім із секс-індустрією «офлайн», сьогодні цифрові інструменти створили умови для масштабного й масового виробництва інтимного контенту. Платформи на кшталт OnlyFans, Fansly чи Patreon перетворили індивідуальних користувачів на «творців» (sex creators), які можуть напряму взаємодіяти з аудиторією, монетизувати власний контент і будувати особистий бренд у глобальному просторі.

Цей процес виглядає демократизованим і навіть прогресивним: мільйони молодих людей бачать у ньому легітимний спосіб заробітку чи форму самовираження. Опитування показують, що понад третина «творців» вважає створення інтимного контенту повноцінним джерелом доходу. У суспільстві виникає своєрідна «нормалізація» феномену: присутність оголених фото чи відео в інтернеті перестає вважатися винятком, натомість стає частиною нової економіки.

Однак під фасадом «самостійності» і «контролю над власним тілом» приховані серйозні ризики. Організовані злочинні групи швидко зрозуміли потенціал цифрової секс-індустрії й почали використовувати її у своїх схемах. Вони діють через посередників, агентів або псевдо-продюсерів, які пропонують «роботу» у сфері створення контенту. На практиці це означає прихований контроль над доходами, умовами виробництва й поширенням матеріалів. Молоді люди, особливо з економічно вразливих країн, часто втягнуті у ці мережі через обманливі обіцянки легкого заробітку, віддаленої роботи й «незалежності». У результаті вони фактично втрачають контроль над власним контентом, потрапляють у боргову залежність або піддаються примусу.

Стаття особливо наголошує на проблемі вікової згоди та перевірки особистості. Багато платформ не мають єдиного стандарту верифікації, а підроблені документи дозволяють неповнолітнім видавати себе за повнолітніх. Це створює середовище, де межі між добровільною участю та експлуатацією стають надзвичайно розмитими. Додатково, навіть коли контент створюється за згодою, постає питання «інформованої згоди»: чи усвідомлюють учасники довготривалі наслідки, включно з неможливістю повністю видалити матеріали з інтернету, репутаційними втратами, ризиком шантажу чи булінгу.

Надзвичайно складним викликом стає штучний інтелект. AI-генератори тепер здатні створювати реалістичні зображення та відео сексуального характеру, у тому числі з використанням облич конкретних людей без їхньої згоди. Особливу тривогу викликає те, що вже зафіксовано випадки створення та поширення AI-генерованого дитячого секс-контенту. Цей контент може не мати жодної участі реальних осіб, проте він використовується злочинними мережами так само, як і матеріали експлуатації. Тут постає фундаментальне юридичне питання: як кваліфікувати подібні випадки? Чи можна вважати це злочином без «живої» жертви, і хто нестиме відповідальність — розробник, користувач чи платформа?

Правові системи різних країн виявляються неготовими до таких викликів. У більшості юрисдикцій відсутні чіткі норми, що регулюють онлайн-секс-індустрію, особливо у сфері перевірки віку, згоди, використання deepfake чи AI-контенту. Там, де законодавство існує, воно

[16] https://globalinitiative.net/analysis/sex-creation-in-the-digital-era/

часто не встигає за швидкістю технологічних змін. У результаті з'являється «правова сіра зона», якою активно користуються злочинці.

У статті наголошується, що протидія повинна бути багаторівневою. На рівні суспільства й освіти необхідні кампанії цифрової грамотності, які пояснюють молоді юридичні, етичні та психологічні наслідки участі в секс-контенті. На рівні платформ — запровадження суворих стандартів перевірки віку, алгоритмів для автоматичного виявлення експлуатаційного чи шкідливого контенту, прозорість у статистиці щодо видалення матеріалів і співпраця з правоохоронцями. На рівні держав — посилення законодавчих рамок, гармонізація правил між країнами, міжнародна координація у сфері розслідувань, екстрадиції та обміну доказами.

У фіналі статті звучить чіткий меседж: цифрова секс-індустрія стає новим глобальним простором кримінальної експлуатації. Те, що для частини молодих людей виглядає як спосіб заробітку або самовираження, у руках злочинців перетворюється на інструмент контролю, примусу й прибутку. Баланс між свободою вираження і захистом від експлуатації тут особливо складний, але без системної відповіді ризики для вразливих груп — насамперед неповнолітніх та молодих жінок — лише зростатимуть. В епоху, коли технології розвиваються швидше за законодавство, єдиним реалістичним виходом є скоординована співпраця держав, платформ і громадянського суспільства, яка повинна формувати нові стандарти безпеки, етики й відповідальності у цифровому середовищі.

Ваша думка важлива!

1. Як національні ПФР можуть ефективно застосовувати нові інструменти (наприклад, NCBC), не порушуючи баланс між правами власності та потребою у швидкому заморожуванні активів?
2. Які індикатори або підходи можуть бути найбільш ефективними для виявлення фінансових потоків, що пов'язані з організованою імміграційною злочинністю та системами на кшталт хавали?
3. Які зміни у регулюванні грального сектору могли б забезпечити кращу ефективність систем ПВК/ФТ і водночас зменшити надмірну бюрократію для операторів?
4. Як фінансові установи можуть забезпечити прозорість і пояснюваність рішень великих мовних моделей у процесах моніторингу транзакцій, щоб зберегти довіру регуляторів і клієнтів?
5. Як в Україні врегулювати діяльність онлайн-платформ, що поширюють сексуальний контент, аби одночасно захистити свободу вираження та мінімізувати ризики експлуатації неповнолітніх і вразливих груп?
6. Як Україні запобігти тому, щоб організовані злочинні угруповання перетворилися на ключових «тіньових спонсорів» політиків?
7. Які інструменти цифрової безпеки та освітні програми слід запровадити в Україні, щоб зменшити масштаби онлайн-шахрайства, яке вже набуло загальносвітового характеру?

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-2025-39

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].