



Міністерство
фінансів
України

Методологічний бюлетень AML

№40/2026



Зміст

Стратегічна фінансова розвідка в системі ПВК/ФТ: аналітичний звіт Робочої групи з обміну інформацією (IEWG)	3
Вимірювання корупції на практиці: від національних антикорупційних пріоритетів до доказової політики	7
Оцінка ОБСЄ: як екологічна злочинність і вирубка лісів підривають регіональну безпеку	11
Запобігання використанню НПО у схемах фінансування тероризму	15
Руйнівні наслідки дерискінгу: як канадські заходи ПВК призводять до фінансового виключення	20
Туніс: між жорстким стримуванням та незмінним прагненням до міграції	25
Конвенція ООН проти кіберзлочинності: між надією та геополітичним розколом	29
Мистецтво цифрового розслідування: як шукати тих, хто воліє залишатися невидимим	33
Як найвідоміший командир угруповання Колумбії перетворив злочинність на цифровий контент	37
Анатомія інвестиційного шахрайства	40

**Слухайте цей бюлетень
у форматі подкасту**

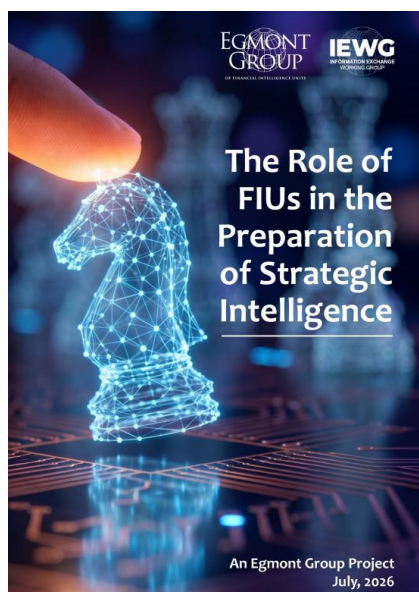


Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для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

Стратегічна фінансова розвідка в системі ПВК/ФТ: аналітичний звіт Робочої групи з обміну інформацією (IEWG) ¹



Аналітичний звіт Робочої групи з питань обміну інформацією Егмонтської групи (IEWG) є всебічним глобальним дослідженням, присвяченим переосмисленню та практичній реалізації функції стратегічної розвідки в діяльності підрозділів фінансової розвідки (ПФР) відповідно до стандартів Рекомендацій 1 та 29 FATF. Документ узагальнює результати комплексного опитування 57 підрозділів фінансової розвідки – членів Егмонтської групи з різних регіонів світу — та обґрунтовує, що стратегічна розвідка не повинна розглядатися як другорядна або суто допоміжна функція чи побічний продукт оперативного аналізу. Навпаки, вона є важливим компонентом національної системи протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ), оскільки дає змогу ПФР виявляти системні тенденції, нові загрози, типології та

вразливості фінансової системи. У такому підході ПФР виконує не лише функцію опрацювання та передачі оперативної фінансової інформації правоохоронним органам, а й роль ключового центру формування стратегічних фінансово-розвідувальних знань для державної системи ПВК/ФТ.

Звіт проводить фундаментальне концептуальне розмежування між оперативним і стратегічним аналізом за шістьма основними вимірами. По-перше, об'єкт аналізу: в оперативній роботі ним є конкретна особа, операція, справа або мережа пов'язаних суб'єктів, тоді як стратегічний аналіз зосереджується на явищах макрорівня, окремих секторах економіки, типологіях, методах і географічних коридорах. По-друге, часовий горизонт: оперативний аналіз орієнтований переважно на короткострокову перспективу – дні або тижні, тоді як стратегічний охоплює середньо- та довгострокові періоди, вимірювані місяцями, а його результати можуть зберігати актуальність протягом року і довше. По-третє, рівень агрегації: оперативний аналіз передбачає детальний розгляд окремих справ та фінансових операцій, тоді як стратегічний передбачає узагальнення значних масивів даних, зокрема сотень і тисяч повідомлень, із застосуванням

¹ <https://egmontgroup.org/wp-content/uploads/2026/09/Annex-1-IEWG-Report-of-Role-of-FIUs-in-preparation-of-Strategic-Reports.pdf>

економетричних методів, машинного навчання та геопросторового аналізу. По-четверте, аналітичні методи: оперативний аналіз переважно використовує дедуктивний підхід, виходячи з уже відомого суб'єкта, операції або обставин справи. Стратегічний аналіз поєднує індуктивні та абдуктивні методи для виявлення прихованих закономірностей, тенденцій і нових ризиків. По-п'яте, кінцеві користувачі: результати оперативного аналізу призначені передусім для слідчих, прокурорів та іноземних компетентних органів, тоді як результати стратегічного аналізу використовуються урядами, регуляторами, розробниками політики, координаторами національних оцінок ризиків та представниками приватного сектору. По-шосте, критерії результативності: ефективність оперативного аналізу може оцінюватися за такими показниками, як кількість кримінальних проваджень, арештованих або конфіскованих активів та інших результатів правоохоронної діяльності. Для стратегічного аналізу ключовими показниками є його вплив на вдосконалення законодавства, зміну наглядних пріоритетів, удосконалення заходів ПВК/ФТ та підвищення якості національної оцінки ризиків. Автори наголошують, що змішування цих двох функцій неминуче породжує деструктивні наслідки, коли постійний тиск невідкладних оперативних запитів систематично витісняє та паралізує довгострокову стратегічну роботу, створюючи замість глибоких аналітичних моделей лише розширені описи старих кримінальних кейсів.

Аналізуючи інституційний ландшафт, автори фіксують абсолютне переважання адміністративної моделі ПФР (близько 74%), тоді як правоохоронні підрозділи становлять 16%, гібридні – 9%, а судові чи прокурорські структури залишаються поодинокими (2%), що закріплює світовий тренд на функціонування фінансових розвідок як незалежних аналітичних центрів. Попри те, що всі респонденти (100%) підтвердили наявність законних повноважень на підготовку стратегічного аналізу, майже половина з них (47%) діє в умовах відсутності чіткого законодавчого визначення цього поняття в первинному праві. Така правова невизначеність породжує асиметрію між високим формальним декларуванням відповідності міжнародним стандартам FATF (середній бал 4,2 з 5) і реальними можливостями інституцій, адже більшість законодавчих формулювань залишаються суто ретроспективними та діагностичними – орієнтованими на опис минулих трендів і фіксацію вже скоєних злочинів, а не на прогностичне моделювання, виявлення слабких сигналів чи сканування горизонту майбутніх загроз. Це, своєю чергою, суттєво послаблює правові позиції ПФР у суперечках щодо розширення доступу до чутливих баз даних або виділення окремих бюджетів. Крім того, аналіз періодичності роботи свідчить, що більшість органів обирає випуск продуктів «за потребою», намагаючись поєднати високу гнучкість реагування на нові виклики зі стабільними щорічними чи квартальними зобов'язаннями.

Одним із найгостріших сигналів звіту є кадровий та матеріально-технічний дефіцит: хоча 81% установ створили профільні підрозділи стратегічного аналізу, їхня фактична чисельність є вкрай невеликою (медіана становить лише 5 штатних одиниць або 10% персоналу ПФР проти 40% в оперативному блоці), а майже половина аналітиків (47%) змушена суміщати стратегічні задачі з оперативними справами в межах гібридних ролей. Це поєднується з дисбалансом фахових навичок: аналітики демонструють високий рівень критичного мислення (4,0/5) та якісного аналізу політик (3,7/5), проте відчутно відстають у галузі Data Science (3,3/5), економетрики (3,3/5) та

прогнозного моделювання (3,5/5). Наявні програми навчання лише поглиблюють цей розрив, зосереджуючись на базових методологіях (79%) і підготовці звітів (59%), тоді як роботі з великими даними навчали лише 40%, а технологіям машинного навчання – лише чверть персоналу. Ситуація ускладнюється інформаційною фрагментацією: за наявності практично вільного доступу до власних повідомлень про підозрілі транзакції (100%), реєстрів компаній (93%) та відкритих джерел (96%), фінансові розвідки відчують значний дефіцит зовнішніх контекстних даних, зокрема реєстрів кінцевих бенефіціарних власників (77%), митної інформації (86%), даних пасажирських авіаманіфестів, доступних через API (63%) та матеріалів регуляторного нагляду (68%), без яких неможливо встановити приховані транскордонні та міжсекторальні схеми. Понад половина ПФР прямо визнає свою поточну ІТ-інфраструктуру непридатною для масштабної стратегічної розвідки, а 77% заявляють про критичну необхідність регулярного перекалібрування правил виявлення та алгоритмів через постійне відставання аналітичних моделей від динаміки кримінального середовища.

У частині продуктів і каналів доведення інформації звіт фіксує переважання традиційних типологічних звітів, досліджень тенденцій та індикаторів ризику, орієнтованих переважно на банківський сектор (до 90%), правоохоронні структури (близько 70%) та регуляторів (близько 70%). Водночас більш змістовні та прогнозні оцінки загрози випускаються менш регулярно. Хоча переважна більшість ПФР організовує роз'яснювальні семінари та звітує про наявність каналів зворотного зв'язку (86%), в інституціях практично відсутні прозорі показники ефективності (KPI), які б вимірювали, наскільки ці продукти реально підвищують якість фінансового моніторингу або змінюють наглядові практики. Окремо документ підкреслює високу роль стратегічної аналітики у підготовці Національних оцінок ризиків (НОР, оцінка 4,3 з 5) та фіксує, що в 70% юрисдикцій стратегічні матеріали ПФР стали прямим рушієм змін законів чи підзаконних актів. При цьому звіт рішуче спростовує хибне уявлення про те, що операційна незалежність ПФР за Рекомендацією 29 FATF поширюється лише на оперативні розслідування окремих фігурантів, доводячи, що аналітична автономія у формулюванні висновків, виборі пріоритетів дослідження та публікації викритих вразливостей (навіть на базі цілком анонімізованих даних) повинна залишатися непорушною та суворо захищеною від політичного цензурування, лобістського тиску чи спроб міністерств приховати системні недоліки чутливих галузей.

Узагальнюючи рівень розвитку стратегічної аналітичної функції ПФР, звіт пропонує чотирирівневу модель зрілості: початковий (15–20% ПФР – без окремих команд і з обмеженим доступом до даних), такий, що розвивається (40–45% – із гібридними аналітиками, базовими типологіями та розрізненими системами), сформований (30–35% – зі стабільними виділеними підрозділами та глибокою інтеграцією в національні ризик-оцінки) і передовий (5–10% – із повною інституціоналізацією, використанням штучного інтелекту, централізованих сховищ великих масивів даних та оцінюванням їхнього впливу на формування державних стратегій). У заключному блоці документ формулює систему прагматичних рекомендацій: закріпити прямий мандат і законодавче визначення стратегічного аналізу в законах про ПВК/ФТ, створити структурно відокремлені аналітичні підрозділи із захищеним часом, укласти обов'язкові міжвідомчі шлюзи для обміну даними про бенефіціарів, розробити систему внутрішніх KPI та започаткувати другу

фазу проекту Егмонтської групи для розробки прикладних інструментів – типових каталогів стратегічних продуктів, шаблонів логічного виведення, спільних бібліотек типологій і практичних навчальних модулів з аналізу великих даних.

Висновки

У законодавстві майже половини ПФР немає чіткого визначення стратегічного аналізу. **Потрібно прямо прописати це повноваження у законі, щоб гарантувати незалежність висновків розвідки від політичного тиску та захистити фінансування таких підрозділів.**

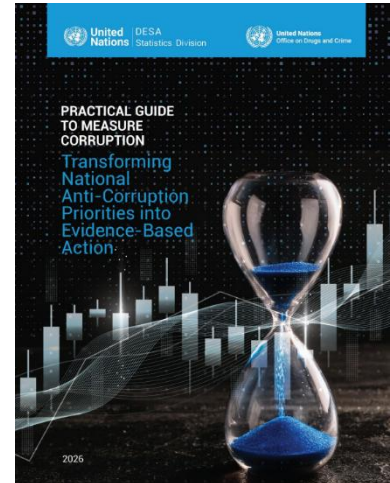
У багатьох ПФР ті самі працівники ведуть і поточні розслідування, і стратегічні проекти, через що на довгостроковий аналіз бракує часу. **Потрібно виділити окремі посади суто для стратегічної роботи та навчати фахівців аналізу даних і машинному навчанню.**

Для якісного аналізу аналітикам недостатньо лише банківських звітів про підозрілі операції. **Необхідно налагодити передачу даних із реєстрів компаній, бенефіціарних власників, митниці та податкової, а також оновити застарілі аналітичні ІТ-системи.**

ПФР рідко вимірюють, як їхні дослідження та типології змінюють роботу банків чи закони. **Необхідно запровадити показники ефективності (KPI), налагодити постійний зворотний зв'язок зі споживачами інформації та регулярно оновлювати бібліотеки схем відмивання коштів.**

Вимірювання корупції на практиці: від національних антикорупційних пріоритетів до доказової політики²

Практичний посібник, підготовлений спільно Статистичним відділом ООН (UNSD) та Управлінням ООН з наркотиків і злочинності (УНЗ ООН) за підтримки глобальної ініціативи «Data for Now», є комплексним прикладним керівництвом, покликаним допомогти державам реалізувати «Статистичну рамку УНЗ ООН щодо вимірювання корупції» та вибудувати життєздатну систему виробництва офіційної статистики у сфері доброчесності. Документ розроблено на виконання резолюцій 8/10, 10/4 та 11/5 Конференції держав-членів Конвенції ООН проти корупції (UNCAC) і рішень Статистичної комісії ООН, що закріпили вимогу переходу від суб'єктивних абстрактних оцінок до об'єктивних, контекстно-чутливих національних вимірювань. Емпіричну й фактологічну основу посібника становить прямий досвід реалізації пілотних проектів у Колумбії, Домініканській Республіці та Кенії, а також стратегічні обміни з профільними інституціями Бразилії та Мексики. Окрім того, враховано результати широких міжнародних консультацій за участі наукових установ, асоціацій громадянського суспільства та відповідей 27 держав-членів на опитувальник УНЗ ООН 2024 року. Принциповою методологічною вимогою авторів є те, що керівництво не створено для міждержавних рейтингів, комбінування показників у єдиний індекс чи нав'язування універсальних шаблонів: воно пропонує гнучкий, поетапний маршрут розбудови національної спроможності з урахуванням ресурсних, правових і політичних обмежень кожної країни.



Основна теза посібника полягає в тому, що корупція є складним і багатовимірним явищем, яке принципово неможливо досягнути одним числовим показником або винятково через суб'єктивні опитування сприйняття, які часто віддзеркалюють медійний резонанс чи політичний клімат, а не реальний стан справ. Державна антикорупційна політика втрачає дієвість, якщо спирається на фрагментарні відомчі звіти чи абстрактні індекси; їй необхідна повноцінна доказова база. На противагу спрощеним підходам посібник пропонує збалансовану систему збирання та аналізу доказів, яка охоплює адміністративні дані, соціологічні опитування досвіду взаємодії з державою, параметри внутрішнього контролю в органах влади та показники доступності правосуддя. При цьому автори застерігають проти перевантаження даних надмірними аналітичними претензіями: офіційна статистика має залишатися стриманою, відображати лише

фактично зафіксовані процеси і не підміняти собою політичні висновки чи причинно-наслідкові гіпотези, які перебувають у площині окремого експертного аналізу. Особливе значення надається фактору доступу громадян до правосуддя та захищених каналів скарг: у середовищі, де люди побоюються переслідувань або не мають можливості повідомити про вимагання неправомірної вигоди, низька кількість офіційних скарг вказує не на відсутність проблеми, а на дефіцит правового захисту й закритість державних інституцій.

Архітектура статистичного виробництва структурована у вигляді семи послідовних ітеративних кроків, які відповідають логіці Загальної моделі статистичних бізнес-процесів (GSBPM) і спираються на Фундаментальні принципи офіційної статистики ООН — незалежність, прозорість методів, конфіденційність та захист джерел. Перший крок – координація – закладає інституційний фундамент усього процесу. Він передбачає ретельне картування ключових державних суб'єктів: від органів прокуратури, поліції та судів до регуляторів публічних закупівель, аудиторських палат, фіскальних відомств і підрозділів фінансової розвідки. Керівництво рекомендує формувати дієву міжвідомчу робочу групу з призначенням оперативних координаторів (focal points), у якій національний статистичний орган забезпечує методологічну точність і якість метаданих, а антикорупційне відомство задає стратегічний вектор відповідно до національних пріоритетів. Замість спроб охопити одразу всі 145 індикаторів Статистичної рамки УНЗ ООН країнам пропонується обрати для першого циклу вузький і керований пакет із 3–5 пріоритетних тем і 3–4 конкретних індикаторів, що довів досвід Кенії, яка сконцентрувалася на прозорості закупівель, конфіскації активів та засудженнях за розтрату, та Домініканської Республіки, де сфокусувалися на розслідуванні хабарництва й аудиторських перевірках.

На другому кроці – зборі даних – інформаційні потоки систематизуються за трьома базовими напрямками Статистичної рамки: кримінальні правопорушення, превентивні заходи та сприятливе середовище. Автори всебічно оцінюють потенціал адміністративних даних, соціологічних опитувань, цифрових платформ і додаткових відомостей громадського сектору. Адміністративні масиви мають вирішальну перевагу регулярності та фіксації дій держави, проте страждають через закритість окремих етапів та інституційні бар'єри. Опитування дозволяють оцінити масштаби незареєстрованого хабарництва («темне число» правопорушень) та рівень суспільної довіри, хоча вимагають фінансових витрат і захисту респондентів. Окреме місце посідають цифрові інструменти: прозорі портали закупівель, відкриті реєстри бенефіціарів та системи е-декларування, до яких усе частіше додаються модулі штучного інтелекту. Досвід Офісу Генерального контролера Бразилії (CGU) демонструє дієвість моделей машинного навчання та обробки природної мови: системи щоденного аналізу оголошень про закупівлі (ALICE), інтелектуального опрацювання запитів на доступ до інформації (LAION) та автоматичного скорингу скарг (FARO) інтегровані безпосередньо у внутрішні системи контролю, що суттєво прискорило виявлення системних зловживань. Поряд із цим важливими залишаються дослідження аналітичних центрів і журналістів, які надають цінний контекст і виявляють приховані схеми, хоча їх залучення до офіційної статистики потребує попередньої методологічної верифікації.

Третій крок присвячено технічній валідації даних, яку очолює статистичне відомство. Тут первинні джерела тестуються на предмет повноти заповнення полів, відсутності дублювань, внутрішньої логічної узгодженості статусів справ і часових рядів, а також ясності метаданих. За підсумками валідації робоча група приймає формальне рішення щодо кожного джерела: готовність до негайного використання, придатність із застереженнями, неготовність або потреба заміни показника більш надійним проксі-індикатором.

Четвертий крок – інтеграція даних та статистичне виробництво – фокусується на узгодженні інформаційних масивів між різними відомствами. У посібнику обґрунтовано концепцію чотирьох рівнів інтероперабельності: правової (наявність законодавчих прав на обмін), організаційної (практична взаємодія та взаємна довіра посадовців), семантичної (однакове тлумачення термінів і правових категорій, таких як «справа», «підозра», «скарга») та технічної (сумісність кодів, протоколів і реєстрів). Державам рекомендовано відмовитися від поспішного створення мега-баз даних і обирати комфортний рівень складності: від простої координації незалежних показників чи стандартизованого обміну агрегованими таблицями без передачі конфіденційних персональних даних до вибіркового зв'язування за єдиними ідентифікаторами або побудови інтегрованих систем, закріплюючи це міжурядовими протоколами.

П'ятий крок – аналіз та інтерпретація – спрямований на встановлення об'єктивного змісту показників і унеможливлення маніпуляцій. Головне аналітичне правило полягає в тому, що показники правоохоронної діяльності (кількість відкритих проваджень, арештів чи вироків) відображають активність і пропускну спроможність органів юстиції, а не загальний рівень поширеності корупції в суспільстві. Крім того, критичне значення має вивчення процесуального звуження масиву справ, або «атриції» (attrition): систематичне відстеження того, на яких саме стадіях – реєстрації, досудового розслідування, судового розгляду та виконання судових рішень – відбувається найбільше скорочення кількості справ. Такий аналіз дає змогу виявити структурні та процедурні «вразливі місця» системи, зокрема тривалі затримки, припинення або закриття проваджень, недостатність доказової бази, обмеженість інституційної спроможності чи інші фактори, що перешкоджають просуванню справи до наступної стадії. Водночас виявлення атриції на певному етапі саме по собі не свідчить про конкретну причину її виникнення; для цього необхідне додаткове дослідження процесуальних рішень, строків, ресурсного забезпечення, якості доказування та інших релевантних факторів.

Шостий крок – поширення – вибудовує прозору комунікацію з суспільством, де статистичне відомство зберігає нейтральність, а антикорупційний орган бере лідерство у поясненні практичного значення даних для державної політики. Прикладом зрілої координації слугує досвід Мексики, де конституційна незалежність статистичного інституту (INEGI) поєднана зі створенням Національної цифрової платформи (PDN), що зв'язує реєстри декларацій, закупівель і санкцій під егідою Секретаріату Національної антикорупційної системи (SESNA), створюючи постійний канал інформування уряду й суспільства. Завершальний сьомий крок – моніторинг та сталість – забезпечує регулярний зворотний зв'язок між статистиками й антикорупційними практиками, проведення щорічних ревізій системи, вилучення застарілих та включення нових

індикаторів, перетворюючи тимчасову міжвідомчу ініціативу на стабільну рутинну державну функцію.

У цілому посібник демонструє якісну зміну філософії антикорупційного моніторингу: фокус переноситься з абстрактних зовнішніх індексів на створення стійкої, інституційно керованої національної екосистеми збору та аналізу даних. Державні органи отримують не просто теоретичний опис, а деталізовані практичні опитувальники, матриці вибору джерел і чеклісти валідації, включені в додатки до посібника. Належна організація цього процесу дозволяє трансформувати відомчу звітність із засобу формального контролю на стратегічний інструмент управління, що допомагає вчасно виявляти системні ризики, підвищувати прозорість державних функцій та підтримувати суспільну довіру на основі перевірених фактів.

Висновки

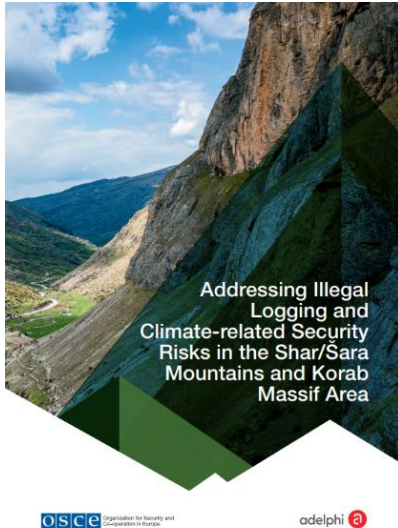
Необхідно відмовитися від спроб виміряти всю корупцію одразу та зосередитися на конкретних сферах з надійними реєстрами – наприклад, перевірці декларацій, тендерах чи арешті активів, де дані вже збираються регулярно.

Доцільно чітко розмежувати інституційні повноваження, закріпивши за органом державної статистики технічну валідацію метаданих і методологічну незалежність, а за антикорупційними відомствами – змістовне використання результатів у публічній політиці.

Слід надавати пріоритет обміну знеособленими агрегованими даними, розвиваючи правову, організаційну, семантичну й технічну сумісність реєстрів без передчасного злиття персональних мікроданих задля захисту викривачів і конфіденційної інформації.

Важливо розмежовувати показники правоохоронної активності та реальний рівень корупції, системно досліджуючи процесуальне відсіювання справ («атрицію») від реєстрації до вироку та супроводжуючи всі оприлюднені дані обов'язковими технічними застереженнями.

Оцінка ОБСЄ: як екологічна злочинність і вирубка лісів підривають регіональну безпеку³



Аналітична записка спільно підготовлена Організацією з безпеки та співробітництва в Європі (ОБСЄ) та берлінським аналітичним центром Adelphi, становить собою всебічне й ґрунтовне дослідження складних взаємозв'язків між масштабною вирубкою лісів, зміною клімату, діяльністю організованої злочинності та комплексними викликами регіональній стабільності в Південно-Східній Європі. Емпіричний фундамент аналізу спирається на результати регіонального експертного воркшопу в місті Пешкопія (Албанія), ґрунтовні кабінетні й польові дослідження групи провідних регіональних і міжнародних науковців, прямі консультації з парковими адміністраціями, міністерствами внутрішніх справ, лісовими агентствами, судовими органами та представниками місцевих громад трьох

прикордонних юрисдикцій. Географічним і предметним фокусом дослідження визначено транскордонну екологічну зону загальною площею понад 240 000 гектарів, закріплену тристоронньою міжурядовою угодою 2022 року між Албанією, Косово та Північною Македонією, яка об'єднала чотири суміжні природоохоронні парки: «Кораб-Корітнік», «Маврово», «Шар-Планина» («Шар Планина») та «Шаррі/Шара». Ця заповідна територія є однією з найбільших безперервних природоохоронних зон у всій Європі та осередком виняткового біорізноманіття світового значення, ресурси якого слугують головною основою для підтримки життєдіяльності та економіки місцевих гірських громад, однак сьогодні цей природний капітал опинився під подвійним деструктивним впливом кліматичного стресу та неконтрольованої антропогенної експлуатації.

Центральна концептуальна рамка документа розкриває наявність глибокого, самопідсилювального циклу взаємопов'язаних процесів деградації екосистем і безпекового середовища, каталізатором якого виступають хронічні соціально-економічні вразливості та системні прогалини в державному врядуванні. Кліматичні чинники – стійке підвищення температури повітря, кардинальні зсуви у режимах сезонних опадів, пересихання поверхневих водних джерел, частіші та триваліші хвилі посухи, а також спалахи масштабних неконтрольованих лісових пожеж – критично виснажують стійкість гірських лісових екосистем, суттєво уповільнюючи процеси їх природного самовідновлення та прискорюючи структурну вирубку. У міру скорочення площі й щільності лісового покриву знижується природна здатність

ґрунтів утримувати вологу, вичерпуються підземні водоносні горизонти, руйнуються цінні природні біотопи та стрімко зростає ризик масштабних ерозійних процесів, сходження зсувів і спустошливих паводків під час екстремальних злив. Руйнування цих базових екосистемних послуг безпосередньо б'є по традиційних галузях зайнятості гірського населення – сільському господарству, тваринництву, лісовому збору та перспективному екологічному туризму. В умовах стрімкої трудової депопуляції та відтоку молоді до великих міст у поєднанні з обмеженим вибором альтернативних джерел доходу й високими тарифами на комерційні енергоносії дрібні несанкціоновані вирубки стають для багатьох збіднілих домогосподарств чи не єдиною доступною стратегією виживання і заготівлі дров перед суворими гірськими зимами. Цей процес має також виразний гендерний вимір, оскільки жінки в сільських громадах традиційно сильніше залежать від збору недеревинної лісової продукції та набагато гостріше відчують наслідки виснаження природних багатств. У такий спосіб утворюється замкнене коло, де місцеві громади водночас потерпають від кліматичної деградації лісів і самі змушені брати участь у їх винищенні, концентруючи побутові рубки навколо власних сіл.

Паралельно з побутовим винищенням лісів документ детально описує значно небезпечніший вимір – масштабну комерційну вирубку лісових масивів, контрольовану організованими злочинними мережами. Слабкість державного нагляду, дефіцит правоохоронного контролю та поширення корупційних практик створили ідеальне живильне середовище для тіньових лісозаготівельних синдикатів. Нелегальна вирубка в регіоні дедалі тісніше переплітається з транснаціональною злочинністю: високий регіональний і міжнародний попит на лісоматеріали робить цей промисел надзвичайно високоприбутковим бізнесом, прибутки від якого легалізуються через готівкові розрахунки, непрозорі фінансові ланцюги та неформальні канали, перетікаючи у перехресне фінансування інших видів тяжкої злочинності. Кримінальні угруповання діють злагоджено, адаптивно та застосовують сучасні методи розвідки: вони використовують важку лісозаготівельну техніку, системно відстежують маршрути пересування лісової охорони й поліцейських патрулів, а в деяких випадках вдаються до залякування, саботажу й відкритих збройних нападів на інспекторів задля безперешкодного доступу до цінних ділянок лісу. Знищення деревостану унеможливорює поглинання вуглецю природним шляхом і призводить до викиду додаткових мільйонів тонн парникових газів в атмосферу, що ще більше розганяє кліматичну кризу, робить ліси легкозаймистими для нових пожеж і породжує дефіцит ресурсів, провокуючи відкрите соціальне протистояння та підриваючи верховенство права в усьому транскордонному регіоні.

Аналіз інституційної системи виявляє критичну невідповідність між задекларованими політичними цілями та реальними можливостями правозастосування на місцях. Хоча уряди Албанії, Косова та Північної Македонії розробили галузеві нормативні акти та десятирічні плани управління для всіх чотирьох заповідників, їх практична реалізація паралізована хронічним дефіцитом фінансових, людських і технічних ресурсів. Паркові адміністрації та лісові інспекції натрапляють на гостру нестачу штатної чисельності працівників лісової охорони, мізерні заробітні плати та фактичну відсутність необхідного спорядження. Інспекторам бракує всюдихідних патрульних автомобілів, спеціальних захисних засобів, надійних рацій для зв'язку в

умовах складного гірського рельєфу та безпілотних літальних апаратів, що робить регулярне патрулювання високогірних віддалених урочищ практично неможливим. Крім того, ситуацію суттєво ускладнює регуляторна неоднорідність: значні розбіжності у визначенні складів правопорушень, неоднакові рівні штрафів та кримінальних санкцій, дублювання обов'язків між міністерствами охорони довкілля, сільського господарства та внутрішніх справ, а також відсутність налагодженої співпраці між прикордонними судовими органами трьох країн створюють численні прогалини у правовому регулюванні, завдяки яким організатори незаконних схем безперешкодно уникають арешту, судового переслідування та обов'язкової конфіскації знарядь злочину.

Окремим вагомим блоком дослідження є аналіз проблеми глибокого інформаційного вакууму та небезпечної латентності правопорушень. Офіційні звіти національних органів часто демонструють парадоксальну картину зменшення кількості зафіксованих незаконних рубок: наприклад, в албанській зоні «Кораб-Корітнік» зареєстровані обсяги незаконно зрубаної деревини формально знизилися з 430,7 кубічних метрів у 2002 році до 17,3 кубометрів у 2022 році. Однак автори доводять, що ця динаміка є наслідком катастрофічного недовиявлення злочинів, а не їхнього реального викорінення. Незалежні супутникові спостереження глобальної радарної системи Land Use Change Alerts (що використовує радарні знімки супутників Sentinel-1 Європейського космічного агентства в майже реальному часі) зафіксували істотне порушення лісового покриву на площі понад 1135 гектарів у парку «Шаррі/Шара» та 476 гектарів у парку «Кораб-Корітнік» лише за період 2018–2023 років. Водночас супутниковий моніторинг без наземного обстеження не здатен самостійно відрізнити антропогенну нелегальну рубку від природних пошкоджень — хвороб лісу, вітровалів чи наслідків пожеж. Непрямі ж розрахунки через порівняння реальних потреб населення у паливі з офіційно дозволеними лімітами заготівлі показують колосальний дисбаланс, який свідчить про те, що значна частина дров видобувається незаконно без будь-якого відображення у статистиці державних відомств.

Підсумовуючи, керівні настаннови ОБСЄ пропонують комплексний і взаємопов'язаний пакет дій, спрямований на виведення лісового сектору з кризи та зміцнення транскордонної довіри. Наголошується, що класичні природоохоронні заходи більше не можуть працювати ізольовано від питань безпеки, економічного розвитку та соціальної політики. Першочерговим кроком має стати розгортання Регіональної цільової групи з даних щодо лісових правопорушень задля стандартизації звітності, запровадження формалізованих протоколів оперативного обміну інформацією між прикордонними службами, лісовими інспекціями та муніципалітетами, а також координації міжнародної донорської підтримки (через такі інструменти, як фонди PONT, EU IPA, EU4Nature, проекти GIZ, JICA та екологічні програми Інтерполу). У сфері юстиції країни мають уніфікувати законодавчі норми на засадах Директиви ЄС про кримінально-правову охорону довкілля (2024/1203), посилити відповідальність за нелегальну заготівлю лісу та гарантувати невідворотну конфіскацію пилорам, лісовозів і техніки порушників. На операційному рівні необхідні термінові цільові інвестиції у навчання, захисне спорядження, засоби зв'язку та мобільність працівників лісової охорони. Нарешті, ключовим елементом визнано подолання першопричин побутового браконьєрства шляхом підтримки енергетичного переходу: держави

повинні надати гірським громадам пряму підтримку для термоізоляції будинків, встановлення високоефективних пічок на біомасі та монтажу сонячних панелей, паралельно залучаючи місцевих мешканців, жінок і маргіналізовані групи до спільного управління парками та стимулюючи розвиток легального збору лікарських рослин і зеленого туризму. Лише такий комплексний транскордонний підхід здатний зупинити деградацію екосистем, захистити природну спадщину та зміцнити кліматичну стійкість, мир і довгострокову стабільність на Балканах.

Висновки

Офіційні звіти значно занижують масштаби вирубок через нестачу даних та приховування порушень. Реальний обсяг нелегальної заготівлі деревини стає очевидним лише за умови зіставлення супутникових знімків із реальними потребами населення, а також налагодження прямого обміну інформацією між прикордонними парками.

Відмінності в законах і розмірах штрафів між сусідніми юрисдикціями дозволяють порушникам уникати відповідальності. Для припинення контрабанди державам слід зрівняти покарання за стандартами європейського права та обов'язково конфісковувати транспортні засоби, пилорами й обладнання правопорушників.

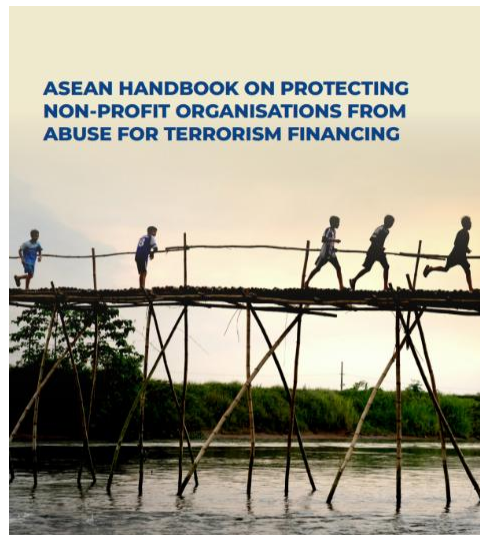
Службам охорони заповідних зон критично бракує фінансування, техніки та захисного спорядження. Лісові патрулі стикаються з фізичними нападами з боку злочинних груп і не мають змоги дістатися віддалених урочищ, тому ресурси необхідно спрямувати на закупівлю дронів, зв'язку, всюдиходів і запуск спільних транскордонних патрулювань.

Селяни в горах здійснюють незаконні вирубки переважно через бідність та потребу в опаленні осель. Громадам потрібна державна підтримка на утеплення будинків, заміну застарілих дров'яних печей на енергоефективні та встановлення сонячних панелей.

Запобігання використанню НПО у схемах фінансування тероризму⁴

Документ, розроблений Секретаріатом АСЕАН є ґрунтовним, масштабним і практично орієнтованим дослідженням, покликаним встановити новий якісний стандарт у сфері регулювання благодійної діяльності та імплементації Рекомендації 8 FATF. Цей документ синтезує передові напрацювання регіональних безпекових органів, передусім Наради старших посадових осіб з питань транснаціональної злочинності (SOMTC), практичні здобутки Робочої групи АСЕАН з протидії тероризму (SOMTC-WG on CT) під провідним лідерством Індонезії, положення Балійського плану дій (2019–2026 роки) щодо запобігання поширенню радикалізації та насильницького екстремізму, а також підсумкові матеріали спеціалізованого семінару АСЕАН–ЄС, проведеного у листопаді 2025 року в Бангкоку за участі представників регуляторних і правоохоронних органів усіх одинадцяти держав регіону. Головна мета посібника полягає у подоланні системного інституційного конфлікту між необхідністю забезпечення прозорості фінансових каналів та збереженням спроможності легітимного громадянського суспільства функціонувати без непропорційного регуляторного та комплаєнс-навантаження. Особливу увагу приділено явищу масового де-ріскінгу, за якого банки та платіжні провайдери можуть відмовляти громадським організаціям у відкритті рахунків, обмежувати проведення благодійних зборів або припиняти ділові відносини на підставі оцінки ризиків, яка не завжди є пропорційною характеру та рівню відповідного ризику.

Автори детально відтворюють генезис цієї глобальної проблеми, що бере свій початок одразу після подій 11 вересня 2001 року, коли після прийняття Резолюції Ради Безпеки ООН 1373 боротьба з фінансуванням тероризму стала ключовим світовим пріоритетом, а FATF у межах Спеціальної рекомендації VIII без належного фактологічного аналізу оголосила весь неприбутковий сектор планети «особливо вразливим» до терористичних маніпуляцій. Цей підхід сприяв формуванню протягом понад двох десятиліть практик надмірного комплаєнсу, за яких уряди, прагнучи мінімізувати ризик невідповідності міжнародним стандартам та пов'язаних із цим санкційних наслідків, запроваджували суворі реєстраційні та ліцензійні вимоги, обмежували міжнародне грантове фінансування, передавали окремі функції нагляду за діяльністю



The Financial Action Task Force Recommendation 8
and its Effective Implementation to Mitigate Terrorism
Financing Risks for Non-Profit Organisations



⁴ https://asean.org/wp-content/uploads/2026/09/endorsed-ad-ref_SOMTC_07092026_ASEAN-Handbook-on-Protecting-NPOs-from-Abuse-for-TF_FINAL_12092026.pdf

благодійних організацій підрозділам фінансової розвідки (ПФР) або правоохоронним органам, а також поширювали на громадські організації окремі обов'язки, передбачені для підзвітних суб'єктів у сфері ПВК/ФТ. У результаті виник комплекс тяжких негативних наслідків: масове закриття банківських рахунків, кількомісячне заморожування пожертв, критичні затримки гуманітарних вантажів у зонах збройних конфліктів та парадоксальне руйнування місцевих програм запобігання насильницькому екстремізму (P/CVE), адже регуляторний удар найсильніше вражав саме ті низові громадські ініціативи, які розбудовували стійкість громад. Крім того, надмірне регулювання прямо порушувало базові міжнародні конвенції, включаючи Міжнародний пакт про громадянські і політичні права (ICCPR), звужуючи фундаментальні права на свободу слова, мирних зібрань і свободу асоціацій.

Посібник висвітлює тривалу боротьбу за перегляд цих підходів, ініційовану створеною у 2013 році Глобальною коаліцією НПО при FATF (Global NPO Coalition on FATF), зусилля якої спершу привели до вилучення у 2016 році тези про «особливу вразливість», а згодом — до запуску у 2021 році офіційного напрямку FATF з вивчення ненавмисних наслідків надмірного регулювання за чотирма напрямками: де-ріскінг, фінансова ізоляція, неправомірне переслідування НПО та порушення прав людини й процесуальних гарантій. Кульмінацією цієї роботи стало ухвалення у листопаді 2023 року оновленої редакції Рекомендації 8, нової Інтерпретаційної записки та комплексного Документа про найкращі практики, які базуються на непорушному принципі «не нашкодь». Сучасний міжнародний стандарт докорінно змінює логіку нагляду: він встановлює, що регуляторні вимоги повинні поширюватися не на весь універсум громадських об'єднань країни, а виключно на їхню функціонально визначену підмножину за критеріями FATF — тобто юридичні особи чи структури, які займаються переважно збором або розподілом коштів на благодійні, релігійні, культурні, освітні чи соціальні цілі. Документ чітко наголошує, що НПО не повинні автоматично розглядатися як підзвітні суб'єкти у сфері ПВК/ФТ та підлягати вимогам, які застосовуються до фінансових установ і визначених нефінансових підприємств та професій. Зокрема, на НПО не слід поширювати загальні обов'язки щодо проведення належної перевірки клієнтів (CDD) або перевірки їхніх бенефіціарів, якщо такі вимоги не обґрунтовані відповідним ризиком. Нагляд і моніторинг діяльності НПО мають здійснюватися пропорційно ризикам, з урахуванням специфіки їхньої діяльності, а застосування заходів контролю не повинно створювати необґрунтованих перешкод для здійснення гуманітарної діяльності, забезпечення прав біженців та дотримання норм міжнародного гуманітарного права. Цей підхід додатково посилюється низкою новацій у міжнародних стандартах та практиці їх застосування: оновленням у 2025 році Рекомендації 1 FATF щодо обов'язкового заохочення держав до застосування спрощених заходів перевірки у випадках низького ризику; переглядом у червні 2026 року Рекомендації 6 щодо закріплення обов'язкових гуманітарних винятків із санкційних режимів Ради Безпеки ООН, зокрема передбачених резолюціями 2664 та 2761; спільними настановами Контртерористичного управління ООН (CTED) та Управління Верховного комісара ООН з прав людини 2025 року щодо врахування прав людини у заходах протидії фінансуванню тероризму; а також запровадженням спеціального механізму фіксації та розгляду ненавмисних наслідків під час проведення взаємних оцінок.

Попри прогресивні нормативні кроки на глобальному рівні, регіональний огляд свідчить про наявність глибокого розриву між теорією та практикою в державах Азійсько-Тихоокеанського регіону: за даними горизонтального звіту регіонального органу APG, майже половина держав-членів (47%) і 60% країн світу не змогли продемонструвати технічну відповідність або ефективність за Рекомендацією 8 через формалізм і застарілі репресивні методи. Головна проблема полягає в тому, що значна частина юрисдикцій замість оцінювання фактичних результатів за Immediate Outcome 10 фактично зводить оцінку до формальної перевірки наявності відповідних законодавчих та інституційних заходів і автоматично відносить увесь неприбутковий сектор до категорії високого ризику. Такий підхід не враховує відмінності між притаманним ризиком, пов'язаним із потенційною вразливістю сектору до зловживань, та залишковим ризиком, який зберігається після врахування чинних законодавчих, регуляторних та інших заходів контролю, а також механізмів саморегулювання і внутрішнього контролю самого сектору.

Для реагування на виявлені проблеми посібник пропонує практичні моделі та підходи, які можуть бути застосовані на національному рівні. У Малайзії профільний підкомітет SCONPO при Національному координаційному комітеті (NCC) провів секторальну оцінку в межах NPORA 2024, поєднавши п'ятирічні дані органів фінансової розвідки, поліції та податкових органів із результатами опитування 997 фінансових установ і матеріалами фокус-груп за участю НПО. На основі трьох кількісних кластерів показників – структури організації, характеру операцій та статистики правопорушень – і чотирьох типів контрольних заходів малайзійська влада здійснила диференційоване оцінювання ризиків та віднесла спортивні й соціальні організації до категорії низького ризику. Такий підхід дає змогу зосереджувати наглядові ресурси на суб'єктах і операціях, які характеризуються вищим рівнем ризику, зокрема на підозрілих транскордонних операціях. У Таїланді відомство фінансового моніторингу AMLO систематизувало оцінювання сектору за 21 параметром і встановило, що значна частина виявлених порушень стосувалася недоліків бухгалтерського обліку та організаційного управління, а не безпосередньо ознак фінансування тероризму. Це сприяло переходу до більш диференційованого підходу до нагляду, орієнтованого не лише на контроль, а й на підвищення організаційної спроможності благодійних організацій, а також інтеграції ризиків, пов'язаних із діяльністю НПО, до НОР. Водночас досвід Індонезії, яка стикається з реальними ризиками використання краудфандингових механізмів і благодійних зборів терористичними мережами, зокрема пов'язаними з Jemaah Islamiyah, демонструє важливість пропорційного та ризик-орієнтованого підходу. За результатами комплексної секторальної оцінки, із понад 491 тисячі зареєстрованих організацій лише 32 суб'єкти були визначені як такі, що становлять високий ризик фінансування тероризму. Це створює підстави для концентрації правоохоронних та наглядових заходів на конкретних суб'єктах і механізмах, щодо яких виявлено підвищений ризик, без поширення надмірних обмежень на весь неприбутковий сектор.

Критично важливою умовою подолання проблеми фінансового виключення неприбуткових організацій автори називають формування постійного тристороннього діалогу між відповідними державними органами, фінансовими установами та представниками громадянського суспільства. Як один із прикладів такого підходу посібник наводить досвід Нідерландів, де в

межах формалізованого круглого столу за координації Нідерландської банківської асоціації (NVB) взаємодіють представники міністерств фінансів, закордонних справ і юстиції, а порядок денний формується за участю громадських організацій. Результатом цього діалогу, зокрема, стала доповідь Центрального банку Нідерландів (DNB) «Від відновлення до балансу». Подальшим елементом розвитку такого підходу стало запровадження галузевих базових стандартів для оцінювання ризиків НПО, а також розвиток спеціалізованих банківських сервісів, зокрема порталу ABN AMRO. За даними, наведеними в посібнику, частка фондів, визначених як такі, що становлять підвищений ризик, у банківських портфелях зменшилася з 21 % до 9 %, одночасно зі скороченням витрат банків і клієнтів на повторні та дубльовані процедури перевірки.

Схожий формат взаємодії описується на прикладі Нігерії, де тристороння робоча група MSWGC об'єднала представників Спеціального підрозділу з питань боротьби з відмиванням коштів при Комісії з корпоративних справ (SCUML/EFCC), ПФР Нігерії та Асоціації комплаєнс-офіцерів банків Нігерії. Робоча група проводила навчальні заходи для представників банківського сектору та брала участь у розвитку нормативного підходу до регулювання діяльності НПО. Британський досвід робочої групи при Міністерстві внутрішніх справ (Home Office) також ілюструє значення узгоджених інформаційних роз'яснень щодо застосування санкційних вимог до благодійних організацій, які здійснюють діяльність у зонах конфлікту.

Окрему увагу посібник приділяє внутрішнім механізмам управління ризиками в самих НПО: чіткому плануванню програм, розподілу повноважень під час здійснення фінансових операцій, незалежному аудиту та належній перевірці партнерів відповідно до характеру й рівня ризику. Важливим доповненням є розвиток механізмів саморегулювання та незалежної сертифікації, зокрема застосування міжнародного стандарту управління ризиками ISO 31000, нідерландського знака якості CBF із диференційованими вимогами залежно від річного доходу організації, балканського механізму TrustMark та багаторівневого підходу до належної перевірки, що застосовується Start Network у благодійній сфері.

Наявність незалежних стандартів і сертифікаційних механізмів потенційно може сприяти зменшенню дублювання процедур перевірки з боку фінансових установ, якщо такі механізми інтегровані в їхні ризик-орієнтовані процеси належної перевірки. Загальний висновок посібника полягає в тому, що забезпечення фінансової доброчесності неприбуткового сектору потребує збалансованого поєднання ефективного управління ризиками, належного контролю та збереження доступу законних організацій до фінансової системи. Такий підхід має ґрунтуватися на пропорційності регуляторних заходів, об'єктивному аналізі фактичних ризиків, захисті гуманітарного простору та дотриманні принципів верховенства права і фундаментальних прав людини.

Висновки

Оцінка ризиків має охоплювати лише функціонально визначені організації та враховувати залишковий ризик. Регуляторам слід виокремлювати з усього неприбуткового сектору лише ті НПО, які збирають і розподіляють кошти, а під час визначення рівня загрози обов'язково враховувати наявні внутрішні системи контролю.

Необхідно переглянути статус НПО та відмовитися від надмірного регуляторного нагляду. Громадські та благодійні організації не є фінансовими установами, тому закони мають замінити тотальний фінансовий контроль на ризик-орієнтований моніторинг виключно високовразливих груп.

Слід запровадити постійний тристоронній діалог між урядом, банками та благодійним сектором. Створення спільних консультативних платформ за прикладом Нідерландів і Нігерії дозволяє встановити єдині галузеві стандарти належної перевірки та усунути необґрунтований де-ріскінг.

Визнання систем галузевого саморегулювання має стати підставою для спрощеного комплаєнсу. Впровадження міжнародних стандартів прозорості (зокрема ISO 31000 чи незалежних знаків довіри) повинно офіційно визнаватися банками як фактор зниження ризику для спрощення фінансових операцій.

Руйнівні наслідки дерискінгу: як канадські заходи протидії фінансуванню тероризму призводять до фінансового виключення⁵

International Civil Liberties Monitoring Group

The Damage of De-risking

How Canada's Policies to Counter
Terrorism Financing Drive Financial
Exclusion

Tim McSorley
National Coordinator, ICLMG
Sept. 2026

Звіт, підготовлений національною правозахисною коаліцією International Civil Liberties Monitoring Group (ICLMG), є комплексним, системним і безпрецедентно детальним дослідженням проблеми фінансового де-ріскінгу та масового позбавлення доступу до банківських послуг неприбуткових організацій (НПО), зареєстрованих благодійних фондів, правозахисних ініціатив та гуманітарних місій у Канаді. Цей документ виступає прямою аналітичною лінією продовження фундаментальної доповіді ICLMG 2021 року «The CRA's Prejudiced Audits», яка вперше на основі публічних даних довела наявність інституційної дискримінації та упередженості у діяльності спеціалізованого підрозділу Податкового агентства Канади – Відділу перегляду та аналізу (RAD CRA). Та попередня

публікація викликала широкий суспільний резонанс і започаткувала низку офіційних розслідувань: обговорення на Національному саміті з протидії ісламофобії, вивчення практики Омбудсменом платників податків, спеціальне розслідування Сенату Канади щодо ісламофобії та ґрунтовний огляд Агентства з перегляду питань національної безпеки та розвідки (NSIRA) у 2025 році. Нове дослідження 2026 року переносить фокус уваги з суто фіскального тиску на приватний банківський сектор, доводячи, що масове закриття рахунків, блокування платежів і витіснення благодійних організацій за межі формальної фінансової систем є не ланцюгом розрізнених комерційних рішень приватних банків, а закономірним, структурно зумовленим і передбачуваним результатом роботи канадської державної архітектури протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ). Доказову базу звіту сформовано на ретельному аналізі норм Закону про доходи від злочинної діяльності та фінансування тероризму (PCMLTFA), законів Bank Act і United Nations Act, матеріалів трьох національних оцінок ризиків (NIRA 2015, NIRA 2023 та оновленої NRA 2025 року), настанов регуляторів FINTRAC, OSFI та FCAC, прецедентів Банківського омбудсмена (OBSI), академічних досліджень Інституту ісламських студій

⁵ https://fatfplatform.org/assets/Derisking_report-1.pdf

Університету Торонто, а також серії з шести ґрунтовних анонімізованих кейсів, наданих постраждалими організаціями та активістами.

Центральна концептуальна ідея дослідження полягає у викритті штучно створеної регуляторної асиметрії, закладеної канадським законодавством, яка підштовхує фінансові інституції до тотального уникнення ризику замість кваліфікованого управління ним. З одного боку, чинна нормативна система покладає на банки, кредитні спілки, платіжні системи та страхові компанії надзвичайно суворі зобов'язання щодо виявлення та попередження підозрілих операцій, підкріплені загрозою колосальних адміністративних грошових штрафів (AMPs) та руйнівними репутаційними наслідками. Якщо міжнародними орієнтирами катастрофічної відповідальності тривалий час слугували штрафи HSBC у 2012 році на 1,9 млрд доларів США та TD Bank у 2024 році на понад 3,1 млрд доларів США за порушення американського Bank Secrecy Act, то на внутрішньому ринку Канади регулятор FINTRAC у жовтні 2025 року створив власний прецедент, наклавши рекордний штраф у розмірі 177 млн доларів на криптовалютну біржу Cryptomus, а на початку 2026 року канадське законодавство суттєво посилило санкції, піднявши максимальний штраф із 500 тис. доларів до 20 млн доларів або 3% від глобального річного доходу установи (залежно від того, яка сума є вищою). З іншого боку, в канадському законодавстві існує абсолютний нульовий фінансовий і правовий ризик за безпідставне видворення законного клієнта чи розірвання ділових відносин із чесним благодійним фондом. Опинившись перед вибором між витратним, ресурсомістким індивідуальним аналізом благодійної організації та миттєвим закриттям її рахунків, комплаєнс-департаменти приймають рішення про припинення клієнтських відносин як єдино раціональне комерційне рішення, яке повністю знімає юридичну відповідальність перед наглядовими органами. Це прямо спотворює так званий «ризик-орієнтований підхід» (RBA), що офіційно декларується міжнародними стандартами FATF. Хоча FATF ще з 2016 року оновила свою фундаментальну Рекомендацію 8, офіційно спростувавши міф про те, що всі НПО є «особливо вразливими» до фінансування тероризму, і прямо заборонила країнам вдаватися до секторального де-ріскінгу, канадський регуляторний ландшафт протягом цілого десятиліття діяв у діаметрально протилежному напрямі.

Головним каталізатором укорінення системного упередження та надлишкової підозрілості стали офіційні державні документи – Національні оцінки притаманних ризиків (NIRA) 2015 та 2023 років, підготовлені Департаментом фінансів Канади за участі щонайменше 13 федеральних міністерств і розвідувальних служб. У цих звітах весь масив зареєстрованих благодійних організацій було беззастережно віднесено до категорії «високого ризику» щодо фінансування тероризму без жодних конкретних статистичних даних, емпіричних доказів чи обвинувальних судових вироків (жоден канадський благодійний фонд чи його посадовець за історію ніколи не був засуджений за злочин фінансування тероризму). Оцінки 2015 та 2023 років штучно сконструювали уявлення про загрозу через призму гіпотетичних сценаріїв зловживань та зосередили майже всю увагу виключно на ісламістських угрупованнях (9 з 11 організацій у звіті 2015 року) і фондах, пов'язаних із мусульманськими громадами або тими, що надають допомогу у зонах геополітичних конфліктів. Державні оцінки ризиків сформували стійку презумпцію винуватості, яка була автоматично закладена в математичні моделі та алгоритми приватних банківських систем. Поява у серпні 2025

року Національної оцінки ризиків (НОР), у назві якої уряд свідомо відмовився від терміну «притаманний» (Inherent) на користь оцінки «пом'якшеного ризику», знизила рейтинг НПО з високого до середнього та прямо визнала дерискінг реальною загрозою, проте не змогла переломити десятирічну інерцію системи. Банківські комплаєнс-підрозділи, сформовані під впливом багаторічних підходів до оцінювання загроз, часто продовжують застосовувати застарілі моделі та критерії ризик-орієнтованого підходу. Ситуацію значно поглиблюють оприлюднені у 2025 році висновки розслідування наглядового органу NSIRA щодо спеціального підрозділу RAD Податкового агентства Канади: перевірка довела, що державні податкові аудити проти мусульманських благодійних організацій ініціювалися на основі неперевірених, застарілих розвідданих, без належного письмового обґрунтування та під впливом системних упереджень. Коли такі закриті урядові підозри циркулюють між розвідкою CSIS, поліцією RCMP, агентством FINTRAC та податковою, вони неминуче транслюються у банківський сектор, провокуючи миттєвий захисний де-ріскінг. Якщо державне відомство під суворим законодавчим контролем припускається грубих аналітичних помилок, то в банках, закритих комерційною таємницею, цей процес набуває масштабів неконтрольованої «чорної скриньки», де навіть топменеджери корпорацій не мають повноважень скасувати або зрозуміти рішення власного комплаєнс-підрозділу.

Практичний вимір звіту демонструє наслідки такої політики на основі низки задокументованих кейсів, зокрема поширення ефекту фінансового виключення на пов'язаних суб'єктів та цілі сектори. Практика де-ріскінгу уже не обмежується традиційним розрахунково-касовим обслуговуванням юридичних осіб, а поширюється на ширший спектр сучасної цифрової фінансової інфраструктури, включно з провайдерами платіжних послуг, платформами для збору пожертв, CRM-сервісами та міжнародними картковими платіжними системами. Звіт демонструє суттєву невідповідність між змінами у законодавстві та практикою їх застосування фінансовими установами. Зокрема, після внесення Канадою у лютому 2025 року змін до санкційного режиму відповідно до SEMA щодо Сирії, а також ухвалення Bill C-41, який передбачив гуманітарні винятки щодо Афганістану, платіжні оператори, за даними звіту, продовжували утримувати заблокованими близько 1 млн доларів пожертв канадського фонду протягом майже року. При цьому оператори посилалися на недостатню обізнаність щодо запроваджених урядом винятків та, за твердженням звіту, вимагали припинення діяльності фонду в Сирії як умови відновлення платіжних послуг. Не менш небезпечним є де-ріскінг на підставі спростованих або сфабрикованих медійних повідомлень: канадська внутрішня благодійна організація втратила банківські рахунки через неправдиву статтю в медіа, і навіть після офіційного судового спростування матеріалу банки відмовилися поновити договори. Водночас практика де-ріскінгу може впливати й на доступ фізичних осіб до фінансових послуг. Згідно з наведеним у звіті кейсом, через правозахисну діяльність директора однієї з пропалестинських організацій банк припинив обслуговування його рахунків, кредитних карток та іпотеки, а також одночасно припинив надання фінансових послуг 13 членам його родини, включно з літніми батьками. За даними звіту, несплачені внаслідок блокування рахунків зобов'язання батьків були передані колекторам. Автори звіту розглядають цей випадок як приклад застосування обмежень до пов'язаних осіб на

підставі їхнього зв'язку з клієнтом. Крім того, звіт наводить приклад потенційного впливу надмірних процедур перевірки на благодійні пожертви. Зокрема, після отримання понад 50 запитань щодо приватного внеску в розмірі 400 тис. доларів США донор відкликав кошти, а відповідний фонд, за даними звіту, припинив приймати міжнародні пожертви.

Усе це супроводжується абсолютним колапсом інституційних механізмів оскарження та підзвітності в Канаді. Згідно з Bank Act, фінансові установи мають повне право розривати відносини з клієнтами без пояснення конкретних причин, використовуючи шаблонну фразу про перегляд внутрішнього «ризик-апетиту». Єдиний спеціалізований орган зовнішнього розгляду спорів у банківській сфері – Банківський омбудсмен (OBSI) – не має повноважень розглядати скарги щодо політик і практик управління комплаєнс-ризиками. Крім того, юрисдикція OBSI не поширюється на спори з організаціями, річний дохід яких перевищує 5 млн доларів США, що може охоплювати великі благодійні фонди. Регулятор захисту споживачів FCAC слідкує виключно за формальним виконанням процедурних строків, не маючи законодавчого мандата оцінювати дискримінаційність де-ріскінгу, а розвідка FINTRAC спирається на звіти про підозрілі операції (STRs), сформовані на суб'єктивному і критично низькому порозі «обґрунтованих підстав для підозри». Це може створювати ризики для реалізації низки фундаментальних прав і свобод, гарантованих Канадською хартією прав і свобод, зокрема права на рівність та захист від дискримінації, свободи совісті та віросповідання, свободи асоціацій і свободи вираження поглядів. Практика припинення або обмеження доступу до фінансових послуг може ускладнювати діяльність законних громадських і благодійних організацій, зокрема через блокування або припинення платіжних операцій. У гуманітарному контексті такі обмеження також можуть створювати перешкоди для своєчасного надходження коштів, необхідних для придбання та доставки продовольства, медикаментів та інших предметів першої необхідності до населення кризових регіонів.

Для реагування на виявлені проблеми ICLMG формулює комплекс із 12 практичних рекомендацій, адресованих федеральному уряду, фінансовим наглядовим органам та приватному сектору. Федеральному уряду та Департаменту фінансів рекомендовано внести зміни до законодавства у сфері ПВК/ФТ, зокрема до PCMLTFA, передбачивши вимоги щодо наявності в банківських комплаєнс-програмах належних запобіжників від непропорційного застосування де-ріскінгу. Серед інших пропозицій – запровадження щорічної публічної звітності підзвітних суб'єктів про кількість і причини припинення обслуговування клієнтів, а також розроблення обов'язкових міжвідомчих рекомендацій для банків щодо застосування гуманітарних винятків із санкційних режимів. Наглядовим органам – FINTRAC, OSFI та FCAC – рекомендовано розробити спільне регуляторне керівництво щодо пропорційного управління ризиками, встановити вимоги до документування рішень у сфері комплаєнсу та переглянути повноваження омбудсмена OBSI щодо розгляду спорів, пов'язаних із рішеннями про управління ризиками. Для приватного сектору, зокрема банків і платіжних провайдерів, ICLMG пропонує запровадити стандарти належної процедури під час припинення або обмеження обслуговування клієнтів. Вони передбачають надання клієнтам зрозумілої інформації про підстави відповідного рішення, можливість надати пояснення та оскаржити рішення, а також створення незалежного

внутрішнього механізму перегляду комплаєнс-рішень. Загалом запропонований підхід спрямований на посилення пропорційності, прозорості та обґрунтованості рішень щодо припинення або обмеження фінансового обслуговування, одночасно зберігаючи можливість фінансових установ ефективно управляти ризиками ВК/ФТ та дотримуватися санкційних вимог.

Висновки

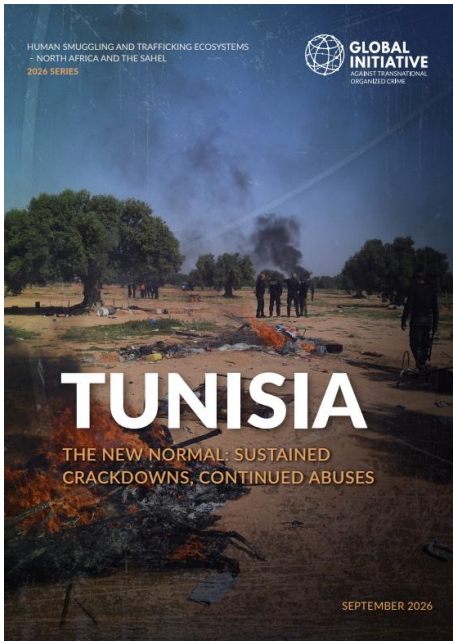
Необхідно законодавчо закріпити підзвітність банків за необґрунтований дерискінг. Внесення змін до закону PCMLTFA має визнати практику поголовного відсікання клієнтів дефектом системи комплаєнсу, зобов'язавши фінансові установи щорічно звітувати перед регулятором про кількість і мотиви розірвання контрактів.

Доцільно впровадити стандарти належного процесу та розкриття причин закриття рахунків. Банки та платіжні процесори повинні надавати клієнтам вмотивовані пояснення замість формальних посилань на «ризик-апетит», забезпечувати право на відповідь та створювати незалежні внутрішні механізми перегляду комплаєнс-рішень.

Слід розширити юрисдикцію омбудсмена OBSI на спори щодо оцінки комплаєнс-ризиків. Неприбуткові організації та фізичні особи повинні мати дієвий інструмент незалежного оскарження банківського дерискінгу, що усуне монополію банківських комплаєнс-підрозділів на ухвалення безконтрольних рішень.

Варто чітко роз'яснити банкам правила проведення гуманітарних платежів під час санкцій. Уряд має надати фінансовому сектору обов'язкові інструкції, щоб банки не блокували законну допомогу благодійників для зон конфліктів через страх покарання.

Туніс: між жорстким стримуванням та незмінним прагненням до міграції⁶



Протягом періоду з січня 2025 по червень 2026 року Туніс перетворився на своєрідний полігон для випробування найжорсткіших методів міграційного контролю, які, попри безпрецедентний тиск на мережі контрабандистів та безпосередньо на мігрантів, не змогли викоринити структурні причини незаконного переміщення. Звіт GI-TOC малює картину країни, яка перетворилася з головного транзитного хабу на територію «пригніченої мобільності», де успішні прибуття до Європи впали до історичних мінімумів, але ціна цього стримування виявилася надзвичайно високою з точки зору гуманітарних ризиків, регіональної нестабільності та адаптації злочинних угруповань.

Починаючи з вересня 2023 року, Туніс послідовно впроваджував курс на зменшення привабливості країни як транзитного та кінцевого пункту для нерегулярних мігрантів. До 2025 року цей підхід набув рис усталеної системи, що поєднує морські перехоплення, примусові депортації до сухопутних кордонів та систематичне знищення неформальних поселень. Як зазначається у звіті, стратегія Тунісу більше не обмежувалася імпровізованими діями; вона трансформувалася у структурований набір механізмів видалення мігрантів з території країни. Це призвело до різкого скорочення морських переправлень до Італії: у 2025 році було зафіксовано лише 4 861 прибуття з Тунісу, що становить 25% від показників 2024 року та менше 5% від піку 2023 року, коли Туніс тимчасово випередив Лівію як головну точку відправлення в Центральному Середземномор'ї. У першій половині 2026 року ця тенденція збереглася: лише 1 074 прибуття, що на 46% менше, ніж за аналогічний період попереднього року.

Однак, як наголошують аналітики GI-TOC, зниження кількості успішних переправлень не означає зниження попиту на міграцію. Між початком 2025 року та серединою 2026 року було зафіксовано від 19 600 до 21 600 спроб морських відправлень. Це свідчить про те, що мобільність була не стільки знищена, скільки штучно пригнічена безпрецедентним тиском правоохоронних органів. Берегова охорона Тунісу перехопила близько 12 000 мігрантів у 2025 році, а до березня 2026 року, за даними італійського МВС, ще 2 528 осіб. Ці перехоплення, своєю чергою, призвели до

⁶ <https://globalinitiative.net/wp-content/uploads/2026/09/Tunisia-The-new-normal-Sustained-crackdowns-continued-abuses-GI-TOC-September-2026.pdf>

повторного повернення мігрантів на туніську територію, що лише поглибило внутрішню соціальну напругу та посилило тиск на й без того обмежені ресурси країни.

Одним із найбільш тривожних аспектів, висвітлених у звіті, є практика примусових переміщень до сухопутних кордонів з Алжиром та Лівією. За оцінками Всесвітньої організації проти катувань (ОМСТ), у 2025 році було здійснено понад 26 600 депортацій, з яких 19 100 – до Алжиру та 7 500 – до Лівії. Ці дії часто відбуваються поза офіційними процедурами: мігрантів затримують під час рейдів, вуличних перевірок або після морських перехоплень, утримують у переповнених та антисанітарних умовах, а потім перевозять у закритих конвоях до кордону. На кордоні практики різняться: у випадку з Лівією мігрантів або передають лівійським силовикам, або кидають у віддалених пустельних районах, де вони змушені самотійно перетинати кордон.

Внутрішня політика Тунісу також зазнала значних змін. З березня 2025 року влада розпочала систематичну кампанію з ліквідації неформальних поселень мігрантів у районі Сфакса, зокрема в оливкових гаях аль-Амра та вздовж коридору KM21-KM37. Ці операції, які офіційно подавалися як заходи з відновлення порядку, призвели до переміщення близько 7 000 осіб, переважно вихідців з країн Африки на південь від Сахари. Хоча влада заявляла про дотримання прав людини, свідчення з місць вказують на примусові виселення, відмову в доступі до майна та випадки насильства. Ліквідація таборів не вирішила проблему присутності мігрантів, а лише розпорошила їх, змусивши шукати притулок у менших, більш розкиданих поселеннях або вирушати до міст у пошуках засобів для існування.

Паралельно з цим, у червні 2025 року уряд Тунісу запровадив власну програму «добровільного повернення», яка функціонує поза рамками Міжнародної організації з міграції (МОМ). Ця програма, презентована як швидша альтернатива, не передбачає реінтеграційної допомоги після повернення і діє в контексті посиленого примусу та ліквідації таборів. Станом на червень 2026 року через неї було репатрійовано 4 620 осіб, переважно громадян Гвінеї та Кот-д'Івуару. Водночас програма МОМ продовжувала демонструвати високі показники, репатріювавши 8 853 особи у 2025 році, що на 28% більше, ніж у 2024 році. Таким чином, повернення стало одним із небагатьох доступних виходів для мігрантів, які опинилися в пастці між жорстокістю правоохоронної системи та відсутністю перспектив легалізації.

Попри безпрецедентний тиск, мережі контрабандистів не зникли, а зазнали глибокої структурної трансформації. Замість великих, ієрархічних угруповань з'явилися менші, гнучкі та розосереджені осередки. Сфакс залишається головним морським хабом, але відправлення часто здійснюються з інших локацій, таких як Махдія, Монастір, Набуль та Зарзіс, що ускладнює прогнозування та перехоплення. Контрабандисти все частіше використовують тактику одночасних запусків човнів для розпорошення ресурсів берегової охорони, використовують судна-приманки та максимально обмежують інформаційні потоки.

Особливу увагу в звіті приділено зростанню ролі вихідців з країн Африки на південь від Сахари як координаторів, посередників та навіть капітанів човнів. Ця тенденція, яка розпочалася у 2024 році, значно прискорилося, оскільки туніські організатори, перебуваючи під тиском

правоохоронців, все більше перекладають операційні ризики на представників мігрантських спільнот. Така структура «взаємної залежності» дозволяє туніським організаторам зберігати стратегічний контроль, але водночас робить мережі менш вразливими до викриття. Однак для самих мігрантів це обертається підвищеним ризиком: втрата можливості перевірити надійність контрабандиста призводить до використання перевантажених, технічно несправних суден та недосвідчених капітанів, що збільшує ймовірність катастроф.

Звіт GI-TOC наголошує, що поточна модель стримування має три стратегічні вразливості. По-перше, замість ліквідації мереж контрабанди, вона підвищила їхню адаптивність, що робить їх більш стійкими до зовнішнього тиску. По-друге, структурні драйвери міграції залишаються незмінними: попри підвищені ризики, маршрут через Туніс залишається значно дешевшим (450–600 євро) порівняно з Лівією (від 1 000 євро) і сприймається як менш жорстокий. По-третє, жорсткі та непрозорі методи правоохоронної діяльності ускладнюють міжнародну співпрацю та підвищують репутаційні ризики для зовнішніх партнерів, які підтримують туніські прикордонні ініціативи.

Домашні умови також сприяють збереженню міграційного тиску. Економічна стагнація, високий рівень безробіття, інфляція та фіскальний стрес, а також подальша централізація виконавчої влади та звуження інституційного плюралізму створюють потужний фон для соціального невдоволення. Організації, які надають допомогу мігрантам, стикаються з адміністративними перешкодами, судовим переслідуванням та навіть ув'язненням співробітників.

У короткостроковій перспективі Туніс, ймовірно, збереже рівновагу. Однак вона залишається вкрай вразливою до регіональних та внутрішніх шоків. Відновлення нестабільності в Лівії, збої в міжнародній співпраці або внутрішні заворушення можуть миттєво змінити міграційну динаміку. Більше того, висока кількість смертей та зникнень, зафіксована протягом звітного періоду, демонструє, що зменшення відправлень до Європи не означає зменшення гуманітарних втрат. Замість вирішення міграційних проблем, поточний підхід Тунісу, найімовірніше, лише перерозподіляє їх географічно, водночас збільшуючи вразливість тих, хто продовжує рухатися. Туніс залишається «тихим, але не стабільним».

Висновки

Скорочення переправлень не означає зниження попиту. Попри падіння морських переправлень до Італії на 75% у 2025 році та ще на 46% у першій половині 2026 року, кількість спроб перетину морського кордону залишається високою (19 600–21 600 за півтора року), що свідчить про штучне придушення мобільності, а не усунення її причин.

Мережі контрабандистів адаптувалися, а не зникли. Замість великих ієрархічних структур з'явилися менші, гнучкі осередки, де вихідці з країн Африки на південь від Сахари дедалі частіше виконують ролі координаторів і капітанів, що ускладнює виявлення та підвищує ризики для самих мігрантів.

Ціна стримування — гуманітарні зловживання та регіональна нестабільність. Примусові депортації до Алжиру та Лівії, ліквідація таборів і «добровільні» повернення під тиском створили систему, де мігранти зазнають повторюваних циклів насильства, вимагання та незаконного утримання, а тиск перерозподіляється на сусідні країни.

Поточна рівновага є крихкою і вразливою до шоків. Модель стримування залежить від постійного політичного тиску, фінансування та операційної спроможності; будь-яке послаблення контролю, регіональний конфлікт або внутрішні заворушення можуть спричинити швидку реактивацію маршрутів.

Конвенція ООН проти кіберзлочинності: між надією та геополітичним розколом ⁷



Ухвалення Конвенції ООН проти кіберзлочинності (відомої як Ханойська конвенція) на Генеральній Асамблеї у жовтні 2025 року та подальше підписання її 75 державами-членами у Ханой стало визначною віхою, яка, втім, аж ніяк не була неминуchoю. Цей документ, розроблений в умовах безпрецедентної геополітичної фрагментації, є компромісом між протилежними баченнями глобального управління кіберпростором. З одного боку, він пропонує безперечні переваги для боротьби з транскордонною злочинністю, а з іншого — несе в собі потенційні ризики використання як інструменту для посилення авторитарного контролю та порушення прав людини. Майбутнє цього договору, як і його ефективність, залежить від здатності держав подолати взаємну недовіру та забезпечити відкритий і інклюзивний процес впровадження.

Екосистема кіберзлочинності, що включає фінансово мотивоване шахрайство, атаки програм-вимагачів, торгівлю людьми з використанням онлайн-платформ та незаконні ринки, є надзвичайно адаптивною та транснаціональною. За оцінками INTERPOL, щорічні світові втрати від кіберзлочинності можна порівняти з ВВП великих економік. В умовах, коли існуючі регіональні інструменти, такі як Будапештська конвенція 2001 року, мають обмежене коло учасників, потреба в універсальному глобальному механізмі стала нагальною. Однак шлях до його створення був сповнений протиріч. Ініційована росією та Китаєм, ця конвенція з самого початку розглядалася Заходом як спроба легітимізувати державний контроль над інтернетом. Росія та її союзники просували ідею широкого договору, який би криміналізував максимально широке коло діянь, пов'язаних з використанням інформаційно-комунікаційних технологій, включаючи навіть боротьбу з тероризмом та екстремізмом. Натомість країни Заходу, такі як Канада, Нова Зеландія та держави ЄС, наполягали на вузькому фокусі на конкретних кібер-злочинах із обов'язковим включенням надійних гарантій захисту прав людини та даних. Результатом став складний компроміс, який, хоч і задовольнив усі сторони формально, залишив багато питань відкритими.

⁷ <https://globalinitiative.net/wp-content/uploads/2026/09/Ian-Tennant-and-Helena-Yixin-Huang-The-present-and-future-of-the-UN-cybercrime-convention-GI-TOC-September-2026.pdf>

На сьогоднішній день конвенція вже має перших учасників — Катар, Азербайджан та В'єтнам, і, за прогнозами, набуде чинності вже у 2027 році після ратифікації 40 державами. Проте її майбутнє виглядає неоднозначним. США, де зосереджені найбільші технологічні компанії, зайняли вичікувальну позицію і, ймовірно, не приєднаються до договору найближчим часом. Приватний сектор, зокрема такі гіганти, як Cisco, та галузеві об'єднання, як-от Cybersecurity Tech Accord, відкрито критикують конвенцію, називаючи її "договором стеження", який вимагає від компаній надавати дані та докази, що збільшує витрати та ускладнює операційну діяльність. Правозахисні організації також висловлюють серйозне занепокоєння, попереджаючи, що конвенція може легітимізувати репресії під виглядом боротьби з кіберзлочинністю, особливо в країнах з слабкими верховенством права. Водночас частина громадянського суспільства, яка опікується захистом жертв, бачить у ній позитивний потенціал, зокрема щодо криміналізації несанкціонованого поширення інтимних зображень.

Ключовим викликом для майбутнього конвенції є переведення її положень у практичну площину. Для цього необхідно подолати три взаємопов'язані розриви: у знаннях, спроможностях та довірі. Перший стосується переходу до спільного використання розвідданих. Кіберзлочинність використовує фрагментацію інформації, тому жодна установа не має повної картини загроз. Існуючі тактичні, оперативні та стратегічні дані розпорошені між телекомунікаційними компаніями, фінансовими установами, правоохоронними органами та дослідниками. Без механізмів інтеграції цих рівнів реагування залишається реактивним. Прикладом можуть слугувати масштабні шахрайські операції в Південно-Східній Азії, які часто виявляються неурядовими організаціями та журналістами-розслідувачами, а не правоохоронними каналами. Для вирішення цієї проблеми необхідно перейти від принципу "потреби знати" до принципу "потреби поділитися", створивши координаційні механізми для синтезу даних від національних CERT, правоохоронців та приватного сектору, як це робить, наприклад, Cybercrime Atlas Всесвітнього економічного форуму або Європейський центр кіберзлочинності Europol.

Другий розрив — це розрив у спроможностях, який вимагає не лише технічного оснащення, а й процедурної сумісності. Кіберрозслідування є надзвичайно чутливими до часу, оскільки цифрові докази можуть бути швидко втрачені. Хоча конвенція передбачає створення цілодобових контактних пунктів, на практиці затримки виникають через відмінності в судових процедурах, адміністративних процесах та рівнях технічної експертизи. У той час як одні країни мають спеціалізовані підрозділи з передовими криміналістичними можливостями, інші обмежені в доступі до інструментів та навчання. Це призводить до нерівномірності координації, коли одна юрисдикція може обробити запит швидко, а інша — ні, що ускладнює розслідування фінансових злочинів, де гроші переказуються між рахунками за лічені хвилини. Для подолання цього необхідно розробити стандартизовані шаблони для запитів про взаємну правову допомогу, що включатимуть криптографічні хеш-значення, стандартні часові посилення та узгоджені метадані, а також посилити інституційну координацію між технічними експертами, слідчими, прокурорами та суддями, виходячи за межі регіональних ініціатив, таких як Круглий стіл прокурорів АСЕАН.

Третій, і найважливіший, розрив — це довіра. Міжнародна співпраця у сфері кіберзлочинності вимагає обміну чутливими даними, що робить довіру одночасно передумовою та результатом співпраці. Держави можуть бути обережними через побоювання щодо захисту даних, потенційного зловживання або політично мотивованих запитів. Довіра не може бути встановлена лише юридичними положеннями; вона розвивається через послідовне впровадження, прозорість та демонстрацію надійних гарантій. У цьому контексті важливу роль відіграють положення конвенції щодо захисту даних та пропорційності. Для зміцнення довіри можна використовувати добровільне звітування про впровадження, подібне до взаємних оцінок FATF, що дозволило б державам публікувати періодичні звіти про законодавчі зміни, показники співпраці та механізми нагляду, не розкриваючи чутливих оперативних деталей. Це сприяло б формуванню спільних очікувань та норм, зменшуючи невизначеність.

Окремої уваги заслуговує роль багатосторонніх зацікавлених сторін. Ханойська конвенція значно відрізняється від попередніх конвенцій ООН, таких як Конвенція проти транснаціональної організованої злочинності (UNTOC) та Конвенція проти корупції (UNCAC), набагато ширшим залученням неурядових суб'єктів. Приватний сектор, громадянське суспільство та наукові кола згадуються в багатьох контекстах: від захисту жертв і запобігання злочинам до нарощування потенціалу та технічної допомоги. Це визнання того, що успіх конвенції неможливий без участі багатьох різних груп. Неурядові організації допомагають відстежувати тенденції, надають аналітику на основі різноманітних даних, підтримують ініціативи з нарощування потенціалу та доносять голоси жертв. Вони також відіграють ключову роль у надгляді за дотриманням гарантій прав людини, які є невід'ємною частиною цього компромісного договору.

Однак на шляху до повноцінного впровадження конвенції виникла серйозна перешкода. У січні 2026 року на зустрічі Спеціального комітету держави-члени не змогли узгодити правила процедури для Конференції сторін (CoP), включаючи механізми взаємодії з багатосторонніми зацікавленими сторонами. Це призвело до глухого кута та відтермінування прогресу, оскільки наступна зустріч запланована лише на січень 2027 року. Відсутність консенсусу щодо правил процедури є тривожним сигналом, особливо на тлі фінансової кризи ООН та фрагментації багатосторонності. UNODC, яке виконує функції секретаріату конвенції, стикається з безпрецедентними бюджетними скороченнями, що ставить під сумнів можливість реалізації мандату з нарощування потенціалу на тому ж рівні, що й для UNTOC та UNCAC. Існує ризик, що політичні розбіжності та фінансові обмеження призведуть до стагнації конвенції. Ще більшим ризиком є те, що вона може бути використана для зловмисних цілей, наприклад, для переслідування дисидентів, журналістів або активістів під приводом боротьби з кіберзлочинністю, особливо в країнах з авторитарними тенденціями, використовуючи потенціал, наданий UNODC.

Таким чином, успіх Конвенції ООН проти кіберзлочинності не вимірюється кількістю підписів чи ратифікацій. Він залежить від здатності держав перетворити юридичні зобов'язання на практичні механізми для розслідування, обміну доказами та правозастосування. Це вимагає подолання розривів у знаннях, спроможностях та довірі, а також забезпечення відкритого та інклюзивного

процесу впровадження. Конвенція більше не належить тим, хто її пропонував, чи тим, хто спочатку її відкидав. Вона має стати спільним надбанням усіх зацікавлених сторін — держав з різними політичними поглядами, бізнесу та громадянського суспільства, які усвідомлюють свою важливу роль у втіленні її в життя під егідою ООН. Якщо держави не зможуть домовитися про інклюзивний, гнучкий та ефективний механізм участі через Конференцію сторін, конвенція може бути приречена на провал. Лише відкрита та довірлива взаємодія з приватним сектором і громадянським суспільством може забезпечити її життєздатність та перетворити на дієвий інструмент міжнародної співпраці в цифрову епоху.

Висновки

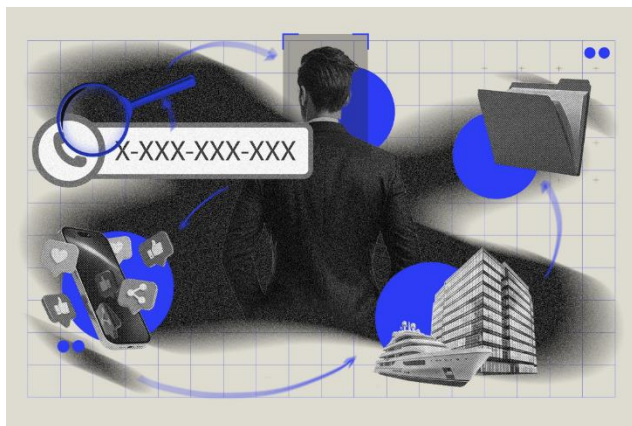
Компроміс замість консенсусу. Конвенція є результатом складного компромісу між авторитарним баченням (широкий контроль над інтернетом) і західним підходом (вузький фокус на злочинах із гарантіями прав людини), що робить її вразливою до різних тлумачень.

Розрив між підписанням і дією. Попри підписання 75 державами, конвенція стикається з серйозними викликами: відсутність США та великих технологічних компаній, а також глухий кут у Відні щодо правил процедури Конференції сторін (CoP) ставлять під сумнів її практичну реалізацію.

Три виміри впровадження. Ефективність конвенції залежить від подолання трьох розривів: у знаннях (перехід до спільного використання розвідданих), у спроможностях (процедурна сумісність і стандартизація) та в довірі (прозорість і надійні гарантії захисту даних).

Ключова роль неурядових суб'єктів. Конвенція значно ширше залучає приватний сектор і громадянське суспільство, ніж попередні договори ООН, визнаючи їхню незамінну роль у нарощуванні потенціалу, захисті жертв та нагляді за дотриманням прав людини.

Мистецтво цифрового розслідування: як шукати тих, хто воліє залишатися невидимим⁸



У сучасному світі, де цифровий слід залишається навіть після видалення акаунтів, а інформація про людину може бути розкидана по десятках баз даних, платформ і архівів, розслідування перетворилися на справжню науку. Організація OCCRP опублікувала методичний посібник, який розкриває внутрішню кухню своїх дослідників — тих, хто щодня займається пошуком людей, які не бажають бути знайденими.

Перше, на чому наголошують автори — це безпека самого дослідника. Розслідування, особливо коли воно стосується організованої злочинності чи корупції, вимагає повної анонімності. Використання особистих акаунтів у соціальних мережах під час пошуку інформації про підозрюваного є грубою помилкою, яка може не лише попередити об'єкт про інтерес до нього, а й наразити слідчих на небезпеку. Замість цього OCCRP рекомендує створювати окремі акаунти. Такі акаунти повинні виглядати природно: мати відповідну електронну пошту, регулярні публікації та активність, щоб алгоритми соціальних мереж не визначили їх як фальшиві. Особливо це стосується LinkedIn, де автоматизовані системи особливо ретельно виявляють підозрілі профілі. Крім того, обов'язковим є використання VPN для шифрування з'єднання та приховування фізичного місцезнаходження. Ці заходи не є надмірною параноєю — вони є базовою гігієною безпеки, адже випадковий лайк на старому фото може мати катастрофічні наслідки, якщо об'єкт розслідування є небезпечною особою.

Другий критичний аспект — архівування. Злочинці та корумповані чиновники часто реагують на загрозу викриття миттєвим видаленням своїх цифрових слідів. Тому дослідники OCCRP навчають фіксувати кожну знахідку: робити скріншоти із видимою датою, зберігати URL-адреси та використовувати Wayback Machine для створення незмінних копій веб-сторінок. Це дозволяє зберегти докази навіть тоді, коли оригінальний контент буде видалено. У посібнику наводиться яскравий приклад: колега OCCRP досліджував дружину бізнесмена, пов'язаного з Prince Group — камбоджійським конгломератом кібершахрайства. Через три роки всі її соціальні мережі були очищені, але завдяки заздалегідь зробленим скріншотам докази вдалося зберегти. Це підкреслює важливість дисциплінованого підходу до збору інформації: те, що сьогодні доступне, завтра може зникнути назавжди.

⁸ <https://www.occrp.org/en/feature/reporters-notebook-how-to-build-a-dossier-on-someone-from-a-single-clue>

Початковий етап розслідування, за методологією OCCRP, завжди починається з широкого пошуку. Перш ніж витратити тижні на глибоке занурення, необхідно переконатися, що ця історія ще не була розкрита журналістами. Для цього використовуються розширені оператори Google, а також штучний інтелект — але з великою обережністю. ШІ може надати корисні підказки, проте його відповіді завжди повинні супроводжуватися посиланнями на першоджерела, а будь-які дані, отримані від нього, потребують обов'язкової перевірки. Крім того, дослідники звертаються до архівів преси, таких як LexisNexis та Dow Jones Factiva, які містять десятиліття газетних вирізок. Це дозволяє не лише уникнути дублювання, а й отримати ґрунтовну базу для подальшого аналізу.

Після широкого огляду настає етап цілеспрямованих запитань. Замість розпливчастої мети «знайти все про особу А», що неминуче призводить до інформаційного перевантаження, OCCRP радить формулювати конкретні питання: «Чи пов'язана особа А з чиновником Х?» або «Які її фінансові зв'язки з компанією Y?». Такий підхід дозволяє зосередитися на ключових аспектах, глибше проаналізувати дані та знайти саме ті докази, які стануть основою матеріалу.

Одним із найскладніших завдань є ідентифікація людини. Імена можуть бути оманливими, особливо при транслітерації з арабської, кирилиці чи інших алфавітів. Наприклад, ім'я Mohammed може мати десятки варіантів написання. Тому дослідники використовують так звані «золоті ідентифікатори»: дату народження, електронну пошту, номер телефону, нікнейми в соціальних мережах. У поєднанні з інформацією про місце роботи чи родинні зв'язки ці деталі дозволяють відрізнити одну людину від мільйонів інших з таким самим ім'ям. Особлива увага приділяється структурним нюансам імен, які можуть вказувати на походження та родинні зв'язки.

Офіційні реєстри — це справжнє золото для розслідувачів. OCCRP радить починати з комерційних, земельних, авіаційних та судноплавних реєстрів. Однак у країнах, де такі дані закриті, доводиться виявляти креативність. Наприклад, якщо компанія з Венесуели не доступна в публічному реєстрі, її сліди можуть знайтися в судових справах США, де розкривається структура власності. Крім того, офіційні газети та державні архіви часто публікують інформацію про акціонерів компаній. Для полегшення пошуку OCCRP створила каталог дослідницьких ресурсів, який постійно оновлюється, а також список реєстрів компаній Європейського Союзу.

Треті сторонні бази даних, такі як OpenCorporates, Equasis, FlightRadar24, Sayari, Moody's Orbis та Offshore Alerts, значно скорочують час дослідження. Вони агрегують глобальні структури власності, судові справи та фінансову інформацію. Однак, як наголошує OCCRP, ці дані можуть містити помилки, тому їх завжди слід перевіряти за офіційними джерелами. Крім того, дослідники активно використовують витоки даних, доступні через бази ICIJ та AlephPro.

Соціальні мережі — це окремий всесвіт, де навіть найсуворіші налаштування приватності не гарантують повної анонімності. OCCRP використовує концепцію «найслабшої ланки»: навіть якщо об'єкт має закритий профіль, його родичі, друзі чи колеги можуть публікувати відкриту інформацію. Наприклад, африканський дослідник витратив тижні, щоб знайти шахрая, який видавав себе за дубайського принца, але саме дружина злочинця опублікувала фото їхньої вілли, що розкрило місцезнаходження. Крім того, зворотний пошук зображень через PimEyes дозволяє

знайти додаткові місця, де з'являлися фотографії, — іноді навіть весільні альбоми, які розкривають родинні зв'язки.

Світ пошукових інструментів (people search tools) стає дедалі потужнішим. OSINT Industries та Darkside by District4Labs перевіряють ідентифікатори на сотнях сайтів, миттєво створюючи карту публічного цифрового сліду. Вони можуть показати, які ресторани любить відвідувач Google Maps, які книги читає користувач Goodreads, яку мову вивчає студент Duolingo. Ці дані надзвичайно чутливі, і OCCRP наголошує на етичній відповідальності: використовувати їх слід лише за суворої необхідності та з повагою до приватності. Особливо корисними такі інструменти є для розрізнення людей з поширеними іменами: якщо в телефонній книзі збережено «Ахмед з компанії ABC», це може стати ключем до ідентифікації.

Цифрове розслідування — це мистецтво, яке поєднує науку та інтуїцію. Незважаючи на доступ до потужних баз даних, найціннішими інструментами залишаються цікавість, інстинкт та вміння читати між рядками. OCCRP закликає довіряти своїй інтуїції, коли підказка здається перспективною, але водночас залишатися дисциплінованими у верифікації. Кожен знайдений фрагмент — це частина пазлу, і лише наполегливість, креативність та увага до деталей дозволяють скласти повну картину.

Висновки

Безпека понад усе: Розслідувач ніколи не повинен використовувати особисті акаунти для пошуку. Створення спеціальних профілів, використання VPN та постійне архівування знахідок є обов'язковою базою, адже об'єкт розслідування може миттєво знищити всі цифрові сліди.

Від широкого до конкретного: Ефективний пошук починається з перевірки вже відкритих даних (архіви преси, ШІ з обов'язковою верифікацією), а потім звужується до конкретних запитань. Це дозволяє уникнути інформаційного шуму та зосередитися на реальних доказах.

Ідентифікація через «золоті» дані: Через складність транслітерації імен, ключовими стають унікальні ідентифікатори: дата народження, email, номер телефону та нікнейми. Поєднання цих деталей з інформацією про роботу та родину дозволяє відрізнити конкретну.

Слабка ланка та етика: Навіть найзакритіші профілі можна розкрити через оточення (родичів, друзів), які публікують фото чи геолокації. Водночас використання потужних OSINT-інструментів (на кшталт OSINT Industries) вимагає суворої етичної відповідальності, адже вони розкривають надчутливі особисті дані.



Як найвідоміший командир угруповання Колумбії перетворив злочинність на цифровий контент ⁹

Сучасний світ цифрових комунікацій створив безпрецедентні можливості не лише для законного бізнесу та соціальних ініціатив, але й для тих, хто перебуває по інший бік закону. Історія Наїна Переса, відомого під псевдонімом Бендіто Менор («Маленьке благословення»), яскраво демонструє, як лідери незаконних збройних формувань можуть використовувати соціальні мережі для побудови власного бренду, вербування нових членів та легітимізації своєї діяльності в очах місцевого населення. Цей феномен, який дослідники називають «наркокультурою» нового покоління, ставить серйозні питання перед суспільством і технологічними платформами.

Наїн Перес народився у 1999 році в Ріоача — бідному місті на півострові Гуахіра, розташованому між Карибським морем та ізольованим гірським масивом Сьєрра-Невада-де-Санта-Марта. Цей регіон, ближчий до Венесуели, ніж до Боготи, традиційно характеризується слабкістю державної влади та процвітанням організованої злочинності. Саме тут, у середовищі, де держава не могла забезпечити базові потреби населення, а злочинні угруповання контролювали ключові транспортні маршрути для кокаїну та контрабандного палива, формувався світогляд майбутнього «наркоінфлюенсера».

Незважаючи на те, що Перес не був найвпливовішим членом ACSN, він, безсумнівно, став найвідомішим. Його шлях до слави розпочався з соціальних мереж, де він створив образ, що поєднував елементи гламурного способу життя та відвертої демонстрації злочинної діяльності. З легкою усмішкою та стильною зачіскою, 27-річний колумбієць будував величезну аудиторію на Facebook, Instagram та TikTok. Але за цими романтичними знімками та мемами ховалася темніша реальність: Перес відкрито транслиував свою роль як командира незаконного збройного

⁹ <https://www.occrp.org/en/feature/the-dramatic-death-of-a-social-media-star-shines-a-light-on-colombias-narcoinfluencer-culture>

угруповання, демонструючи кадри боїв у джунглях, патрулювання на човнах та військові тренування.

Феномен Бендіто Менора не був поодиноким випадком. Дослідники відзначають, що він представляє «нову стадію» наркокультури — явища, яке існує в Колумбії та інших країнах Латинської Америки з часів розквіту кокаїнової торгівлі у 1990-х роках. Пісні та теленовели, що оспівують наркоторгівлю, десятиліттями користувалися популярністю, а серіали про таких «королів» наркотиків, як Пабло Ескобар, захоплювали аудиторію в США. Однак раніше ці історії передавалися усно або через піратські записи. Сьогодні ж самі злочинці можуть миттєво поширювати власний контент, а платформи на кшталт Spotify навіть розміщують оригінальні пісні, що прославляють їхні подвиги.

Незважаючи на те, що неясно, чи мав Перес прямий контроль над якимось конкретним акаунтом, він явно створював власний контент. Результатом стали переконливі пости та відео, які представляли «наркоторгівлю як повсякденну, бажану або навіть веселу діяльність». Було не рідкістю, коли його пости збирали коментарі із запитаннями про те, як до нього приєднатися, або про можливості працевлаштування.

Ця привабливість була особливо сильною для підлітків, які ставали його реальними послідовниками. Їх приваблювали нелегальні мотоциклетні гонки, які він організовував на вулицях Ріоачі, а також подарунки у вигляді телефонів, зброї та грошей. Такий підхід дозволяв йому вербувати нових членів до свого угруповання та створювати ореол «успішної» людини, яка піклується про своїх.

Однак контент Бендіто Менора не обмежувався демонстрацією розкоші та гламуру. Експерти та місцеві жителі розповіли OCCRP, що він також поширював кадри вбивств та інших насильницьких злочинів, які вчиняв, іноді в режимі реального часу. Хоча наразі ці відео, схоже, недоступні в мережі, сам факт їх існування свідчить про безпрецедентний рівень відкритості злочинця. Така поведінка викликала подив навіть у старших командирів ACSN, які звикли до іншої епохи збройного конфлікту.

Політичний контекст додав історії Бендіто Менора додаткової напруги. ACSN з 2022 року вела переговори з попереднім урядом Густаво Петро, чия політика «Тотального миру» мала на меті роззброїти менші партизанські угруповання шляхом укладання індивідуальних угод. Однак угода була скасована після того, як Петро залишив посаду влітку. Його наступник, Абелардо де ла Еспріелья, ультраправий колишній адвокат у кримінальних справах, який отримав підтримку президента США Дональда Трампа, обіцяв жорсткішу лінію щодо безпеки. 9 липня, після обрання, але до вступу на посаду, де ла Еспріелья оголосив, що Бендіто Менор є однією з «цілей високої цінності» для його майбутньої адміністрації. У відповідь акаунти, пов'язані з Бендіто Менором, почали глузувати з новообраного президента.

Смерть Бендіто Менора настала в ранні години 4 вересня, коли він та Роза Анхеліка Таразона, були застрелені під час драматичної нічної операції. Протягом трьох тижнів після цього уряд також націлювався на інших лідерів ACSN, що призвело до значного спалаху вуличного насильства в їхньому оплоті Санта-Марта та розгортання військ там. Президент особисто супроводжував патрулі, поділившись відео, де він іде вулицями в бронезилеті та з пістолетом.

Похорон Бендіто Менора, який відбувся через два дні після його смерті, був настільки масштабним, що паралізував рух у Ріоачі. Місцеві газети повідомляли, що ACSN використала цю подію, щоб продемонструвати свою незмінну владу та підтримку в регіоні, можливо, надсилаючи повідомлення уряду. Через кілька днів репортер OCCRP відвідав район Ла-Напіта в Ріоачі, де мати

Бендіто Менора досі живе в маленькому будинку. На вулиці було встановлено білий намет, щоб приймати постійний потік скорботних. Молоді чоловіки в чорних футболках їздили вулицею на мотоциклах, спостерігаючи за обстановкою. Сестра Бендіто Менора, Роза, вийшла з будинку, щоб коротко поговорити з репортером.

Ця подвійність — жорстокий злочинець і водночас «благодійник» — є ключовою для розуміння феномену Бендіто Менора та подібних до нього. Вони використовують соціальні мережі не лише для самопросування, але й для створення паралельної системи влади та легітимності, яка конкурує з державною. У регіонах, де держава не виконує своїх функцій, такі фігури заповнюють вакуум, пропонуючи населенню те, чого воно не отримує від офіційної влади: захист, порядок і навіть соціальну допомогу. Однак ціна цієї «допомоги» — підтримка злочинної діяльності, страх і підкорення кримінальним законам.

Після смерті Бендіто Менора його цифрове життя продовжилося. Кілька акаунтів, які поширювали його контент, продовжували публікувати повідомлення від його імені, ніби він живий, та ділитися зображеннями, які, ймовірно, згенеровані штучним інтелектом, де Бендіто Менор роздає подарунки та гроші бідним. Його шанувальники відповідали взаємністю.

Ця цифрова спадщина викликає серйозні питання про роль соціальних мереж у сприянні таким фігурам. Хоча Meta, материнська компанія Facebook та Instagram, оголосила в своєму періодичному звіті про загрози, що призупинила понад 1000 акаунтів, груп або сторінок у Колумбії, пов'язаних з невказаним «терористичним угрупованням», яке використовувало акаунти для «поширення ідеологічного матеріалу та вербування нових членів», неясно, чи знала компанія про популярність Бендіто Менора на своїх платформах.

Історія Бендіто Менора — це не просто історія одного злочинця. Це історія про те, як технології змінюють природу злочинності та влади. У світі, де кожен може стати «інфлюенсером», лідери незаконних збройних формувань використовують ті самі інструменти, що й законні бізнеси та публічні особи, для побудови власного бренду, залучення прихильників та легітимізації своєї діяльності. Вони створюють контент, який резонує з молоддю, яка шукає соціальної мобільності та визнання, пропонуючи їм альтернативний шлях до «успіху» — шлях, який веде до насильства, страху та смерті.

Цей феномен ставить перед суспільством низку складних питань. Як регулювати контент, який прославляє злочинність, не порушуючи свободу слова? Як платформи можуть ефективно виявляти та видаляти матеріали, які створюються самими злочинцями, особливо коли вони маскуються під розважальний контент? Як держава може конкурувати з привабливістю «інфлюенсерів» у регіонах, де її присутність слабка? І, можливо, найважливіше: як суспільство може запропонувати молоді альтернативні моделі успіху, які не вимагають участі в злочинній діяльності?

Анатомія інвестиційного шахрайства ¹⁰

Сучасний ландшафт фінансових злочинів демонструє стрімку трансформацію методів соціальної інженерії, серед яких інвестиційне шахрайство посідає одне з провідних місць за рівнем матеріальних збитків для громадян. Відповідно до матеріалів, підготовлених Національним агентством з боротьби зі злочинністю Великої Британії (NCA) у співпраці з Управлінням з фінансового регулювання і нагляду (FCA), цей тип фінансового злочину здебільшого зароджується в цифровому просторі, зокрема через таргетовану онлайн-рекламу та публікації в соціальних мережах. Механізм протиправної схеми полягає у введенні потенційних інвесторів в оману щодо існування високодохідних інвестиційних планів чи торговельних стратегій, які насправді є фіктивними та мають єдину мету — протиправне заволодіння коштами потерпілих.

Основним інструментом залучення жертв виступає експлуатація психологічних факторів: бажання швидкого збагачення, надмірної довіри до медійних осіб та страху втраченої вигоди. Зловмисники масово використовують рекламні кампанії, що обіцяють гарантовану прибутковість при мінімальних чи взагалі відсутніх ризиках, що саме по собі суперечить базовим економічним законам функціонування фінансових ринків. Додатковим фактором легітимізації часто слугує фейкова підтримка з боку відомих публічних постатей чи знаменитостей, чиї образи використовуються без їхнього відома для створення ілюзії надійності.

У процесі взаємодії шахраї намагаються перевести комунікацію в неконтрольоване русло, наполягаючи на використанні месенджерів або закритих груп у соцмережах замість офіційних каналів зв'язку. Практика створення штучної ексклюзивності через запрошення до «обраних інвестиційних клубів» поєднується з жорсткими вимогами конфіденційності, коли жертві прямо забороняють радитися з родичами, друзями чи фахівцями. Такий тиск ізолює людину від критичної оцінки ситуації ззовні. На етапі, коли потерпілий намагається повернути свої вкладення або отримати нібито нарахований прибуток, шахраї висувають нові фінансові вимоги під виглядом сплати вигаданих податків, комісій за розблокування коштів або плат за верифікацію. Увесь цей процес супроводжується безперервним психологічним тиском та маніпуляціями, що підштовхують до нових фінансових транзакцій.

Ефективна протидія подібним деструктивним схемам ґрунтується передусім на глибокій обізнаності та системній попередній перевірці. Перед перерахуванням будь-яких коштів критично важливо провести процедуру належної обачності (due diligence), перевіривши компанію через спеціалізовані державні реєстри: реєстр регулятора FCA (Firm Checker) для підтвердження наявності відповідної ліцензії та повноважень на надання фінансових послуг, а також реєстраційну палату Companies House для з'ясування реального статусу юридичної особи.

¹⁰ <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/828-stop-investment-fraud-info-sheet/file>

Якщо протиправний інцидент уже стався або є обґрунтовані підозри щодо шахрайства, протокол дій вимагає негайної та скоординованої реакції. Першочерговим кроком є невідкладне звернення до банківської установи з вимогою заблокувати рахунки та зупинити рух коштів на час проведення внутрішнього розслідування. Наступний крок передбачає офіційну фіксацію правопорушення через передачу детального звіту уповноваженим органам протидії шахрайству через онлайн-форму або за офіційною лінією зв'язку.

Особливу увагу необхідно приділити збереженню доказової бази: будь-яких листувань, квитанцій, повідомлень та історії транзакцій, які слугуватимуть матеріалами для розслідування. Водночас варто зберігати пильність щодо так званих послуг із «повернення коштів» (chargeback-шахрайство), оскільки зловмисники або пов'язані з ними групи нерідко повторно контактують із потерпілими під виглядом детективів чи юристів, вимагаючи нових платежів за фіктивне повернення викрадених активів.

Ваша думка важлива!

Яку відповідальність повинні нести цифрові платформи (Facebook, Instagram, TikTok) за поширення контенту, що прославляє злочинність, і як це узгодити зі свободою слова?

Враховуючи, що багато українських реєстрів були закриті або обмежені під час війни, наскільки на вашу думку ефективними є міжнародні сторонні бази даних (OpenCorporates) для виявлення українських активів за кордоном?

Як Україні гарантувати, що нові механізми конвенції ООН проти кіберзлочинності не будуть використані росією проти українських військових, активістів чи журналістів під виглядом боротьби з "екстремізмом" чи "тероризмом"?

Як в умовах збройної агресії та масштабного повоєнного відновлення знайти дієву рівновагу між закриттям чутливої інформації оборонного характеру та забезпеченням публічного доступу до даних про закупівлі й відбудову для якісного вимірювання корупційних ризиків?

Контакуйте щодо цього документу з Міністерством фінансів України:

Email: aml_bulletin@minfin.gov.ua

Поштова адреса: Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11

Ідентифікація контакту: стосовно Методологічного Бюлетеня № Мінфін-AML-2026-40



Архів

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

