

“Ким би ви не були, будьте кращими”

сентенція XIX століття

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій



Протидія відмиванню коштів у юридичному секторі Великої Британії¹



Звіт Solicitors Regulation Authority (SRA) за 2024/25 фінансовий рік представляє комплексне дослідження стану британської правової системи. Цей

документ, пронизаний дуалізмом досягнутого прогресу та невблаганної стійкості ризиків, служить своєрідною лінзою, через яку можна розглянути не лише механізми регулювання, але й внутрішню культуру юридичних фірм, їхню сприйнятливість до технологічної еволюції та постійну битву між легальністю та кримінальною винахідливістю.

У передмові Пол Філіп, головний виконавчий директор SRA, одночасно констатує значні успіхи в пріоритизації AML-ініціатив та висловлює розчарування через майбутню втрату повноважень на користь Управління з фінансового регулювання (FCA), що додає звіту відтінок перехідного періоду та невизначеності.

Аналіз показує, що SRA активно впроваджує стратегію кількісного та якісного розширення нагляду, різко збільшивши кількість проактивних заходів з 545 до 935 порівняно з попереднім періодом. Ця інтенсифікація, що включає 317 виїзних інспекцій та 671 документальний огляд, є

¹ <https://www.sra.org.uk/pdfcentre/?type=ld&data=1888107460>

свідомою реакцією на високий ризик-профіль сектору, підтверджений Національною оцінкою ризиків Великої Британії. Регулятор явно переходить від вибірових перевірок до систематичного моніторингу, використовуючи щорічний збір даних від усіх 5 569 фірм, що підпадають під дію AML-регламенту, для створення динамічних профілів ризику. Однак найважливішим висновком є те, що це масштабування нагляду не просто виявляє більше порушень, але й розкриває системні слабкості в управлінні ризиками на рівні окремих фірм, які не були вирішені протягом багатьох років.

Серцевину проблеми, на думку SRA, становить часто формальне та нефункціональне застосування керівних принципів оцінки ризиків. Хоча відсоток фірм, що мають відповідну оцінку ризиків на рівні компанії (FWRA), зріс до 47%, аналіз 833 таких документів виявив тривожну тенденцію: бездумне використання шаблонів без адаптації під специфіку бізнесу. Багато FWRA нагадують абстрактні академічні нариси, що описують теоретичні ризики юридичної професії загалом, а не конкретні загрози, з якими стикається дана фірма в своїй практиці, з урахуванням її клієнтської бази, географії операцій та спектру послуг. Наприклад, документи часто містять загальні фрази про високоризикові юрисдикції, але не розкривають, чи взаємодіє фірма з клієнтами з цих регіонів, і якщо так, то які конкретні заходи запроваджено для пом'якшення ризику. Це свідчить про дефіцит культури глибокого, інтроспективного аналізу, коли процес створення FWRA сприймається як обов'язкова формальність, а не як живий інструмент стратегічного управління. Ще більш критична ситуація спостерігається на операційному рівні — у оцінках ризиків клієнтів (CMRA). Те, що 16% з 5873 перевірених справ взагалі не мали такої оцінки, а 39% наявних були визнані неефективними (часто зводяться до простих галочок «високий», «середній» або «низький» ризик без жодного обґрунтування), — це прямий шлях до сліпоти щодо відмивання коштів. Цей розрив між високорівневими політиками та їх реалізацією в щоденній роботі юристів свідчить про глибоку прогалину між теорією комплаєнсу та практикою.

Окремої уваги заслуговує тематика перевірки джерела коштів (Source of Funds, SOF), яку SRA ідентифікує як одну з найбільш проблемних зон. Звіт підкреслює, що розуміння легітимності джерела коштів є фундаментальним бар'єром для відмивання, проте дані демонструють тривожну неспроможність багатьох фірм виконувати цю функцію належним чином. У 10% справ, де SOF-перевірка була обов'язковою, вона взагалі відсутня. Ще більш показовим є те, що у 18% справ, де документи були зібрані (наприклад, банківські виписки), вони не піддавалися критичному аналізу. Типовий сценарій, описаний SRA: фірма приймає виписку з рахунку клієнта як доказ наявності коштів для покупки нерухомості, але навіть не намагається зрозуміти, як така значна сума з'явилася на цьому рахунку. Чи надійшли кошти від продажу активів, отримання спадщини, бізнес-доходів чи в один день від невідомої третьої сторони? Відсутність таких запитів робить всю процедуру CDD марною, перетворюючи її на збір паперів, а не на процедуру захисту. SRA прямо закликає фірми перестати сприймати SOF як формальність і розглядати це як можливість захистити свою репутацію та уникнути кримінальної відповідальності.

Контекст фінансових санкцій, яким в звіті присвячено окремий великий розділ, розкриває новий рівень складності регуляторного середовища. Санкційний режим перестав бути нішевою темою для спеціалізованих практик; дані SRA показують, що 34% фірм, які пройшли інспекцію, випадково стикалися з обслуговуванням підсанкційних осіб у рамках своєї звичайної роботи. Це означає, що кожна фірма, яка веде міжнародну діяльність або працює з корпоративними структурами, потенційно знаходиться в зоні ризику. Хоча базові контролю, такі як скринінг клієнтів (83% фірм), широко поширені, детальні інспекції виявили болючі точки на етапі дотримання умов ліцензій. Це вказує на недостатню операційну злагодженість: фінансові відділи можуть не повідомляти про заморожені кошти комплаєнс-офіцерам, а адміністративні системи можуть не відстежувати мінливі терміни звітності по ліцензіях. Успішні фірми, за даними SRA, характеризуються високим рівнем координації між експертами з питань санкцій,

комплаєнс-командами та фінансовими відділами, що забезпечує цілісний контроль над усіма аспектами справи.

Технології в звіті представлені як дві сторони медалі. З одного боку, електронна ідентифікація та верифікація (eIDV) стають стандартом, їх використовують 90% фірм, що значно пришвидшує та автоматизує процес CDD. Деякі системи навіть пропонують моніторинг негативних новин та змін у санкційних списках. З іншого боку, SRA попереджає про небезпеку технологічного фетишизму: електронний звіт корисний лише тоді, коли особа, що його переглядає, розуміє його обмеження та може інтерпретувати результати. Крім того, нові технології створюють нові вразливості: платформи для збору коштів устаткування можуть маскувати справжнє джерело капіталу, а глибокі підробки (deepfakes) відео та аудіо стають серйозною загрозою для дистанційної ідентифікації. SRA наголошує, що впровадження будь-якої нової технології зобов'язане супроводжуватися оцінкою AML-ризиків, які вона несе, та заходами щодо їх пом'якшення.

Висновки:

- **Прогрес у масштабах, але криза у глибині.** Регулятор (SRA) різко активізував проактивний нагляд, збільшивши кількість перевірок на 71%. Однак це виявило стійкі системні проблеми: майже третина перевірених фірм не відповідала вимогам, а головні недоліки лежать у площині неякісних оцінок ризиків та формального підходу до перевірки джерел коштів.
- **Розрив між політикою та практикою — найбільша загроза.** Найнебезпечнішою виявилася відсутність зв'язку між формально прийнятими процедурами та їх виконанням. Це свідчить про те, що AML-комплаєнс у багатьох фірмах залишається паперовим, а не практичним інструментом захисту.
- **Санкційний режим перетворився з нішевої теми на повсякденний ризик:** кожна третя перевірена фірма випадково стикалася з обслуговуванням санкційованих осіб. Основні порушення тепер стосуються не виявлення, а складного операційного дотримання умов.
- **Електронні засоби ідентифікації покращують ефективність, але породжують нові загрози:** надмірна довіра до автоматичних звітів без їхнього розуміння та ускладнення контролю в децентралізованих моделях роботи фірм.

Динаміка правозастосування в звіті відображає наслідки активізації нагляду: кількість внутрішніх санкцій зросла майже вдвічі (до 137), а суми штрафів (661 200 фунтів) свідчать про готовність застосовувати економічно відчутні заходи. Примітно, що більшість порушень, що призводять до санкцій, не є складними схемами, а базовими недоліками: відсутність FWRA або CMRA, неефективні політики та невиконання перевірок SOF. Це ще раз доводить, що основна боротьба відбувається не на рівні витончених схем, а на рівні рутинної недбалості та недоінформованості.

У перспективі SRA окреслює низку нових та повторюваних ризиків, що формують порядок денний на майбутнє. Децентралізовані бізнес-моделі, популярність яких зростає, створюють виклики для контролю якості AML-процедур серед незалежних консультантів. Звіт також фіксує появу нового явища — інфільтрації, коли злочинні групи набувають контроль над фірмами для проведення підозрілих операцій.

Таким чином, стійкість базових недоліків у оцінці ризиків і перевірці джерел коштів вказує на недостатнє інтегрування принципів AML в повсякденне мислення та дії кожного фахівця. У цьому контексті найважливішим висновком є те, що в умовах постійної еволюції загроз найнадійнішим активом юридичної фірми стає не лише набір політик, але й культура критичного професійного скептицизму та неупередженого аналізу, вкорінена в кожному етапі юридичної роботи.

Глибинна трансформація санкцій Великої Британії: стратегічний перехід до уніфікованої системи²



Історична зміна, ініційована британським урядом на початку 2026 року, що полягає в консолідації всіх санкційних дій в єдиний, централізований UK Sanctions List (UKSL), є стратегічним переформатуванням всієї філософії імплементації

та контролю за дотриманням міжнародних обмежувальних заходів. Цей перехід, ретельно підготовлений протягом попередніх років та детально врегульований керівництвом, опублікованим від імені трьох ключових державних органів — Міністерства закордонних справ, Співдружності та розвитку (FCDO), Казначейства її Величності (HM Treasury) та Офісу з виконання фінансових санкцій (OFSI) — відображає глибоке розуміння сучасних викликів, з якими стикаються як регулятори, так і приватний сектор в епоху надзвичайно динамічних геополітичних зрушень, ускладнення фінансових потоків та необхідності безпрецедентної швидкості реагування на загрози національній та міжнародній безпеці.

Цей масштабний проект пройшов тривалий етап консультацій з бізнес-спільнотою, яка неодноразово висловлювала стурбованість щодо неефективності, породженої необхідністю паралельного моніторингу кількох, іноді технічно не синхронізованих, джерел даних. Фрагментація інформації між списком OFSI, який охоплював виключно аспекти фінансових заморожень, та ширшим UKSL, що включав імміграційні та торгові обмеження, створювала реальні операційні ризики. Могла виникнути ситуація, коли юридична особа ідентифікувалася б як чиста за фінансовими санкціями, але при цьому потрапляла під суворі торгові ембарго, інформація про які містилася в іншому місці. Така дисперсія даних не тільки збільшувала витрати на комплаєнс, але й підвищувала ймовірність людської чи технічної помилки, що в контексті жорсткої регуляторної відповідальності могло призвести до значних штрафів та репутаційних втрат. Таким чином, об'єднання інформації про всі санкційні дії у рамках UKSL, який з моменту свого створення у 2020 році на підставі Закону про санкції та боротьбу з відмиванням коштів (SAMLА) слугував основним законодавчим каркасом, є логічним кроком для усунення цих системних вад та створення єдиного джерела істини, що охоплює весь спектр примусових заходів: від заборони на фінансові операції до обмежень на в'їзд на територію країни та обіг конкретних товарів.

Імплементація цього переходу вимагає від усіх учасників ринку, незалежно від їх розміру чи галузі, проведення ретельного аудиту власних внутрішніх процесів, технологічних систем та контрактів з третіми сторонами. Найбільш критичним завданням є оновлення автоматизованих систем скринінгу, які раніше були налаштовані на регулярне отримання та обробку даних з OFSI Consolidated List. Відтепер джерелом цих даних має стати виключно UKSL. Більш того, ключова технічна зміна стосується ідентифікаторів. Історичний ідентифікатор «OFSI Group ID», який протягом багатьох років був стандартом де-факто для посилання на суб'єкт фінансових санкцій у внутрішніх і зовнішніх звітах, заявках на ліцензії та повідомленнях про порушення, більше не призначатиметься для осіб, що додаються до списку після 28 січня 2026 року. На заміну йому приходить загальний «Unique ID» UKSL, який призначається всім суб'єктам санкцій незалежно від їх типу. Це вимагає переконфігурації баз даних, оновлення бізнес-логіки програмного забезпечення та перепідготовки персоналу. Проте, для забезпечення плавного переходу та збереження історичного контексту, британські органи влади збережуть усі «OFSI Group ID», призначені до цієї дати, в усіх форматах UKSL, гарантуючи, що старі посилання, ліцензійні номери та звіти залишаться дійсними та зрозумілими для регуляторів. Це мудре рішення

² <https://www.gov.uk/guidance/moving-to-a-single-list-for-uk-sanctions-designations-28-january-2026>

демонструє баланс між інновацією та стабільністю, дозволяючи бізнесу адаптуватися без необхідності миттєвої та вартісної міграції всіх архівів.

Окремо варто відзначити значне розширення технічних можливостей та форматів подання даних. Окрім чотирьох початкових форматів UKSL, таких як ODT для людино-читаних документів та XML для машинної обробки, були додані три знайомих і широко використовуваних в автоматизованих системах формати: TXT, CSV та PDF. Це пряме дослухання до запитів бізнесу, який прагне мінімізувати зусилля з переформатування даних. Ще важливішим є впровадження статичних URL-адрес для кожного з семи форматів. Ця, на перший погляд, технічна деталь має велике практичне значення: посилання на файл CSV або XML більше не змінюватиметься з кожним оновленням списку. Це дозволяє організаціям налаштувати автоматизовані завантаження лише один раз, усуваючи ризик збоїв через «застарілі» посилання та значно спрощуючи процес підтримки актуальності даних.

Висновки:

- **З 28 січня 2026 року Велика Британія повністю відмовилася від оновлення окремого Консолідованого списку OFSI** на користь єдиного UK Sanctions List (UKSL), що тепер містить усі типи санкцій.
- **Для технічної інтеграції бізнесу критично важливо оновити всі системи скринінгу**, перейшовши на дані UKSL.
- **Уряд значно вдосконалив доступ до даних:** додано три нові формати файлів, що спрощує автоматизацію, а також оновлено онлайн-інструмент пошуку з функціями розмитої логіки та підсвічування збігів.
- **Незважаючи на уніфікацію, деякі спеціалізовані списки залишаються поза межами UKSL**, що означає необхідність для бізнесу проводити паралельні перевірки за кількома джерелами в окремих випадках.

Важливу роль в новій екосистемі відіграє оновлений інструмент пошуку по UKSL, доступний як окремий онлайн-сервіс. Його модернізація з акцентом на «розмиту логіку» (fuzzy logic) та ранжування результатів є прямим відгуком на складність пошуку через варіації в написанні імен, транскрипціях або неточностях у вхідних даних. Це особливо актуально в міжнародному контексті, коли скринінг має охоплювати осіб з різних культурних та мовних середовищ. Покращена система виділення збігів полегшує візуальну перевірку, зменшуючи навантаження на операторів. Одночасно відбулася централізація інформаційних потоків: замість окремих фінансових санкційних

повідомлень OFSI, тепер FCDO публікує єдині санкційні повідомлення щодо всіх типів обмежень. Це дозволяє суб'єктам господарювання отримувати цілісну картину всіх змін одним підписом на електронні сповіщення, мінімізуючи ризик пропустити критичне оновлення через розсіяність джерел.

Однак, незважаючи на прагнення до повної уніфікації, існує важливий виняток, який підкреслює специфічність окремих санкційних режимів. Перелік «росія: список осіб, позначених у зв'язку з фінансовими та інвестиційними обмеженнями», що стосується 11 ключових юридичних осіб у відповідності до Додатку 2 російських санкційних положень, залишається окремим від UKSL. Це свідчить про те, що британський уряд визнає особливу природу цільових секторальних обмежень, які можуть вимагати окремого адміністрування. Для бізнесу це означає, що процедури скринінгу повинні включати дволанкову перевірку: первинну — за основним UKSL, і вторинну — за цим спеціалізованим переліком, особливо для операцій, пов'язаних з чутливими секторами економіки.

У глобальному контексті перехід Великої Британії до єдиного санкційного списку можна розглядати як частину світової тенденції до гармонізації, стандартизації та технологічного вдосконалення регуляторних практик. Це крок до створення більш ефективного, зрозумілого та

передбачуваного регуляторного середовища, що є критично важливим для підтримки довіри інвесторів та функціонування відкритої економіки в умовах геополітичної напруженості. Успіх цієї трансформації залежатиме не лише від чітких дій уряду, але й від здатності приватного сектора до оперативної адаптації.

Дотримання рекомендацій стане вирішальним фактором для мінімізації операційних ризиків та уникнення суворих регуляторних наслідків. Таким чином, дана реформа є не просто зміною джерела даних, а скоріше фундаментальним оновленням інфраструктури національної безпеки та економічної стійкості, що вимагає від кожної компанії, яка працює в британській юрисдикції чи з британськими контрагентами, повної усвідомленості та проактивних дій.

Європейська боротьба за культурну спадщину: аналіз стратегії протидії незаконному обігу артефактів³



У світлі глобалізації ринків та цифрової трансформації торгівлі незаконний обіг культурних цінностей перетворився з нішевою проблеми археологів та мистецтвознавців на серйозну загрозу національній безпеці, фінансовій стабільності та культурній ідентичності народів Європи.

Опубліковане директором Європейської комісії з питань міграції та внутрішніх справ, дослідження розкриває масштабну та багатогранну картину цього явища, пропонуючи не просто окремі заходи, а комплексну архітектуру захисту, побудовану на принципах прослідковуваності, стандартизації та транснаціональної співпраці.

Дослідження виходить далеко за рамки традиційного уявлення про "крадіжку картин". Воно концептуалізує незаконний обіг культурних цінностей як складний конгломерат злочинних діянь, що включає три основні явища: крадіжку оригіналів

витворів мистецтва; розкрадання (незаконне вивезення артефактів з археологічних пам'яток); та підробку. Однак справжня небезпека криється у вторинному використанні цих предметів — легалізованих чи ні — як інструментів для відмивання коштів, ухилення від міжнародних санкцій та фінансування терористичної діяльності.

Арт-ринок з його традиційною культурою конфіденційності, суб'єктивною оцінкою вартості, використанням офшорних компаній та можливістю великих готівкових розрахунків створює ідеальне середовище для спотворення фінансових потоків. Високий рівень невиявлених або незареєстрованих випадків робить точну оцінку масштабів неможливою, але численні резонансні справи, проілюстровані в доповіді, свідчать про системний характер проблеми. Від арешту групи з дев'яти громадян Грузії, які викрали понад 170 рідкісних книг з європейських бібліотек, до виявлення мережі, що займалася одночасно торгівлею зброєю та розкраданням археологічних пам'яток в Іспанії, — усі ці приклади вказують на участь організованих злочинних груп, які вправно експлуатують транснаціональні ланцюги поставок та правові прогалини.

Особливу загрозу становить використання культурних цінностей у фінансових злочинах. Як зазначається в дослідженні, ризик відмивання коштів через торгівлю культурними цінностями в ЄС оцінюється як "високий". Сучасне мистецтво, через легкість логістики та значні коливання цін, часто використовується для швидкого перетворення незаконних коштів на ліквідні активи.

³ <https://euagenda.eu/publications/study-on-measures-to-increase-traceability-of-cultural-goods-in-the-fight-against-cultural-goods-trafficking-at-the-member-state-level-and-at-the-eu-level>

Наприклад, недорогі роботи можуть бути "продані" співучасникам за значно завищеною ціною, створюючи легальну інвойсну документацію для трансферу коштів. Водночас "блакитні фішки" — роботи визнаних майстрів на кшталт Моне, Вархола або Пікассо — слугують стабільним активом для зберігання вартості, який можна тримати роками, не побоюючись втрати ліквідності. Онлайн-простір лише посилив ці тенденції. Хоча "темна павутина" не є основним каналом продажу через обмежену аудиторію, легальні соціальні мережі, спеціалізовані онлайн-аукціони та маркетплейси стали головними майданчиками для злочинної діяльності. Анонімність, швидкість операцій та складність перехресної юрисдикції роблять розслідування таких справ надзвичайно ресурсомісткими та технічно складними. Ця фрагментація проявляється у кількох ключових вимірах.

По-перше, правова роздробленість. Хоча існує низка міжнародних конвенцій (ЮНЕСКО 1970 року, UNIDROIT 1995 року, Нікосійська конвенція 2017 року) та європейських директив (про повернення культурних цінностей, проти відмивання коштів, тощо), їх імплементація в державах-членах суттєво відрізняється. Національні законодавства криміналізують різні аспекти незаконного обігу (наприклад, незаконні розкопки, крадіжку культурних цінностей), мають різні строки давності та різні санкції. Італія, наприклад, має суворі статті за відмивання саме культурних цінностей, тоді як в інших країнах такі дії кваліфікуються в загальних рамках. Це створює "яскраві" та "слабкі" зони в правовому просторі ЄС, якими злочинці активно маніпулюють, вибудовуючи маршрути переміщення артефактів через юрисдикції з найменш суворими правилами.

По-друге, операційна та технологічна розрізненість: бази даних викрадених культурних цінностей та зобов'язання щодо реєстрації операцій. Ситуація з базами даних є показовою: лише частина держав-членів має спеціалізовані системи. Там, де вони існують (як "Леонардо" в Італії, Treima II у Франції), вони розрізняються за типами даних, що збираються, системою категоризації предметів, технічними можливостями (наявність пошуку за зображенням, сумісність API) та рівнем доступу. Деякі бази закриті для публіки та навіть для правоохоронних органів інших країн, інші — частково відкриті. Відсутність єдиного стандарту, подібного до Object ID ICOM, робить автоматизований обмін інформацією технічно неможливим.

Ще гірша ситуація з реєстрацією операцій. Лише кілька країн (Франція, Італія, Іспанія, Румунія) мають розвинені системи "поліцейських книг" для антикварів та арт-дилерів. В інших покладаються на загальні принципи належної перевірки в рамках законодавства про протидію відмиванню коштів, яке застосовується лише до угод понад 10 000 євро. Навіть у країнах із розвиненими системами записи часто ведуться в паперових журналах, що робить їх непридатними для швидкого обміну. Онлайн-транзакції, особливо на платформах типу C2C (споживач-споживач), практично випадають з-під будь-якого контролю.

По-третє, ресурсна нерівність. Дослідження чітко демонструє прірву між державами-членами в плані можливостей боротьби з цими злочинами. Спеціалізовані підрозділи, такі як Команда карабінерів із захисту культурної спадщини (Carabinieri TPC) в Італії (219 офіцерів) або Центральне бюро з боротьби з обігом культурних цінностей (OCBC) у Франції, мають десятилітній досвід, експертизу та технологічні розробки (наприклад, систему Swoads для моніторингу аукціонів за допомогою AI). Інші країни мають лише кількох призначених офіцерів або покладаються на загальні підрозділи, яким бракує знань з історії мистецтва та археології. Ця нерівність означає, що навіть за наявності гарних інструментів у одній країні, їх ефективність обмежена неможливістю ефективної співпраці з сусідами, які не мають аналогічних можливостей для аналізу, перевірки та просування розслідувань.

Виходячи з цієї діагностики, доповідь не просто пропонує список рекомендацій, а будує логічну архітектуру політичних заходів, де кожен наступний крок залежить від реалізації попереднього.

Замість революційних, але непрактичних рішень (на кшталт єдиної бази даних ЄС), автори віддають перевагу еволюційному, модульному підходу.

Перший і найважливіший модуль — стандартизація (захід А.1 та Б.1/Б.2). Це фундамент усієї подальшої будівлі. Для баз даних викрадених цінностей це означає прийняття обов'язкового мінімального стандарту для всіх держав-членів. Стандарт має включати: 1) єдиний перелік категорій культурних цінностей (зброя, дерев'яні вироби, археологічні фрагменти, картини тощо); 2) обов'язковий набір полів даних (типологія, опис, розміри, ім'я автора, дата, високоякісні зображення) на основі Object ID; 3) технічні вимоги до якості зображень та форматів файлів; 4) обов'язкові базові функції, такі як текстовий пошук. Аналогічно, для реєстрів операцій пропонується встановити обов'язкові мінімальні стандарти того, яку інформацію повинні фіксувати дилери (детальний опис предмета, дані покупця та продавця, фотографії, ціна, дата) та забезпечити обов'язковий цифровий формат цих записів. Цей крок не вимагає негайної дорогої інтероперабельності, але створює умови для неї, зрівнюючи правила гри.

Другий модуль — інтероперабельність та доступ (захід А.2). Лише після стандартизації стає технічно та економічно доцільним наступний крок: створення механізму для взаємних запитів між національними базами даних. Доповідь пропонує модель, аналогічну системі Prüm II для обміну відбитками пальців та даними ДНК. Це передбачає створення центрального маршрутизатора під управлінням агентства ЄС EU-Lisa, через який уповноважений орган однієї країни зможе відправити запит до баз даних усіх інших держав-членів. Така система зберігає суверенітет над даними (вони не зливаються в єдину базу), але забезпечує безпрецедентну швидкість та масштаб пошуку. Для реєстрів операцій аналогічним кроком могло б стати

Висновки:

- **Незаконний обіг культурних цінностей — це системна загроза безпеці ЄС.** Арт-ринок через свою конфіденційність, суб'єктивність оцінок та використання офшорних схем є ідеальним середовищем для злочинних операцій.
- **Головною перешкодою ефективної боротьби є фрагментація.** Держави-члени ЄС мають різне законодавство, розрізнені стандарти баз даних викрадених цінностей, несумісні формати реєстрації операцій та нерівні операційні можливості правоохоронних органів. Це створює "сірі зони", якими зловмисники активно користуються.
- **Стратегія ЄС будується на поетапному підході.** Першочерговий крок — запровадити обов'язкові мінімальні стандарти для національних баз даних і реєстрів операцій. Лише потім технічно можливим стане створення системи взаємних запитів між країнами.
- **Технології — важливий помічник, але не панацея.** Штучний інтелект та блокчейн можуть значно посилити моніторинг і аналіз, але їх ефективність залежить від наявності стандартизованих, якісних даних та правових механізмів для обміну інформацією.

створення можливості для правоохоронців отримувати доступ до цифрових реєстрів компаній інших країн у рамках конкретних розслідувань, з дотриманням усіх процедурних гарантій.

Третій модуль — інтеграція з існуючими європейськими системами. Доповідь обережно оцінює можливості підключення до потужних інфраструктур ЄС, таких як Шенгенська інформаційна система (SIS) або митні системи (ICS2, система імпорту культурних цінностей). Аналіз показує, що технічні перешкоди тут значно вищі. SIS, наприклад, розрахована на об'єкти з унікальними ідентифікаторами (на кшталт VIN-коду автомобіля), яких у культурних цінностей немає. Впровадження пошуку за зображенням у SIS вимагало б колосальних переробок. Тому доповідь радше розглядає це як довгострокову перспективу, акцентуючи зараз на більш досяжних цілях.

Особлива увага приділяється принципу пропорційності (захід Б.5). Автори визнають, що арт-ринок ЄС на 96,4% складається з мікропідприємств. Тому нав'язування їм складних та дорогих зобов'язань щодо реєстрації кожної операції може завдати непоправної шкоди галузі. Як збалансоване рішення пропонується впровадження на рівні ЄС єдиного обов'язку щодо посиленої належної перевірки (due diligence) для угод із культурними цінностями, вартість яких перевищує певний поріг (наприклад, 10 000 євро). Цей обов'язок включав би перевірку походження, консультації з публічними базами даних викрадених цінностей, перевірку імпоротно-експортних ліцензій та отримання письмових гарантій від продавця. Таким чином, регулятивне навантаження лягає на операції з найвищим ризиком, не обтяжуючи дрібних колекціонерів та дилерів.

Доповідь реалістично оцінює роль нових технологій. Вона описує перспективні європейські проекти, такі як ENIGMA (веб-інтерфейс для моніторингу онлайн-майданчиків), AURORA (хімічне маркування та блокчейн для трекінгу) та Anchise (інструментарій для інтеперабельності). Особливо виділяється італійська система Swoads 2.0, яка використовує AI не тільки для аналізу зображень, але й для розуміння текстових описів, а також для автоматичного створення методів відстеження нових аукціонних сайтів.

Однак ключове послання полягає в тому, що технології — це лише інструмент. Без стандартизованих даних, які потрібно аналізувати, і без правової основи для обміну результатами аналізу, навіть найдосконаліший штучний інтелект буде марним. Технологічна модернізація має йти рука об руку з правовою та інституційною гармонізацією.

Квантова загроза і фінансові системи: як провести перехід до пост-квантової криптографії⁴



Документ є прикладним аналітичним дослідженням, спрямованим на переведення теми постквантової криптографії (PQC) з площини абстрактних майбутніх загроз у площину конкретних управлінських і технологічних рішень для фінансового сектору. Його ключовий меседж полягає в тому, що квантова загроза для криптографії вже сьогодні має безпосереднє значення для фінансових установ, навіть за відсутності повномасштабних квантових комп'ютерів, здатних зламувати сучасні алгоритми. Це зумовлено асиметрією у часі між моментом компрометації зашифрованих даних і моментом фактичного зламу, що створює реалістичний сценарій «перехоплення сьогодні — розшифрування в майбутньому», особливо критичний для даних із тривалим строком чутливості та зберігання

Автори документа послідовно обґрунтовують, що для фінансових установ перехід до постквантової криптографії не може розглядатися як разова технічна заміна алгоритмів. Натомість він є довготривалим, багатофазним і міжорганізаційним процесом, який потребує раннього планування, інтеграції у корпоративні рамки управління ризиками та узгодження з життєвими циклами IT-активів, стандартами ринку, регуляторними очікуваннями та можливостями постачальників. Саме тому центральним елементом документа стає запропонована методологія пріоритизації міграції, яка дозволяє структурувати цей процес та уникнути як передчасних, так і запізнілих рішень.

⁴ <https://www.europol.europa.eu/cms/sites/default/files/documents/Post-quantum-cryptography-report.pdf>

У методологічному вимірі документ пропонує починати з повної інвентаризації бізнес-процесів, що покладаються на криптографію з відкритим ключем. Така інвентаризація розглядається не як формальність, а як аналітичний процес, що дозволяє виявити приховані залежності, ланцюги довіри та критичні точки взаємодії з третіми сторонами. Для кожного такого бізнес-процесу пропонується оцінювати квантовий ризик, який визначається трьома ключовими параметрами: тривалістю збереження чутливості даних, рівнем експозиції до потенційних зловмисників та тяжкістю наслідків компрометації. Ці параметри дозволяють перевести абстрактну «квантову загрозу» у вимірювану категорію, зрозумілу для керівництва, ризик-менеджменту та наглядових функцій.

Паралельно документ вводить концепцію часу міграції, яка відображає реальну складність і тривалість переходу до квантово-стійких рішень. Тут увага зосереджується не лише на технічній доступності постквантових алгоритмів, а й на вартості впровадження, глибині необхідних архітектурних змін та рівні зовнішніх залежностей. Особливо наголошується, що у фінансовому секторі саме зовнішні залежності — від стандартів, вендорів, платіжних схем, браузерів, постачальників хмарних і мережевих сервісів — часто є визначальним фактором, який суттєво подовжує реальні строки міграції незалежно від внутрішньої готовності організації.

Комбінування оцінки квантового ризику та часу міграції формує основу для визначення пріоритетності дій. Документ підкреслює, що цінність цього підходу полягає не стільки в самій класифікації бізнес-випадків, скільки у процесі аналітичного осмислення, який змушує організацію критично переглянути власні криптографічні залежності, технічний борг і стратегічні припущення. Таким чином, пріоритизація виступає інструментом управлінської зрілості, а не просто технічним чеклистом.

Для демонстрації практичної застосовності підходу документ детально розглядає два контрастні приклади. Екосистема платіжних терміналів (PoS) показує ситуацію, де квантовий ризик є помірним, але час міграції — надзвичайно високим через апаратну природу рішень, довгі цикли заміни обладнання та складну багатосторонню систему стандартів і відповідальностей. У цьому випадку автори роблять акцент на необхідності раннього стратегічного планування, узгодження з життєвими циклами активів і підготовчих дій, які не залежать від остаточної стандартизації PQC. Натомість приклад публічних вебсайтів демонструє протилежну ситуацію, де квантовий ризик є значущим через загрозу довготривалої компрометації даних, але час міграції є мінімальним завдяки вже наявній

Висновки:

- **Фінансовим установам необхідно вже зараз провести повну інвентаризацію бізнес-процесів, що використовують криптографію з відкритим ключем, і застосувати двовимірну модель «квантовий ризик / час міграції» для формування реалістичної дорожньої карти переходу.**
- **Публічні вебсайти та TLS-інфраструктура є найбільш доцільною точкою входу для раннього впровадження PQC, оскільки гібридні постквантові механізми вже доступні та можуть бути інтегровані з мінімальними витратами у рамках поточної операційної діяльності.**
- **Апаратно-залежні екосистеми (PoS, платіжна інфраструктура) мають бути включені в довгострокове стратегічне планування вже сьогодні, щоб уникнути передчасної заміни обладнання та неузгоджених рішень у майбутньому.**
- **Системне виявлення та усунення криптографічних анти-патернів має розглядатися як обов'язковий етап безумовно доцільних заходів у процесі міграції, який одночасно знижує поточні ризики, підвищує криптографічну зрілість та забезпечує криптографічну гнучкість організації.**

підтримці гібридних постквантових механізмів у браузерях, CDN і криптографічних бібліотеках. Саме такі кейси позиціонуються як найкраща можливість для раннього практичного впровадження постквантових рішень у режимі звичайної операційної діяльності.

Важливим концептуальним доповненням до теми пріоритизації є розділ, присвячений криптографічним антипатернам. Документ розглядає їх як системну проблему фінансового сектору, що підвищує як поточні ризики, так і складність майбутньої міграції. Усунення таких практик подається як стратегічно вигідний і безпечний крок, який одночасно зменшує технічний борг, підвищує криптографічну зрілість і створює передумови для криптоагильності, необхідної в умовах швидкої еволюції загроз.

У підсумку документ формує цілісне бачення постквантової криптографії як стратегічного виклику для фінансового сектору, що потребує поєднання технічної експертизи, управління ризиками, міжорганізаційної координації та довгострокового планування. Він переконливо демонструє, що організації, які почнуть цей шлях уже зараз, отримають не лише підвищений рівень захисту даних у майбутньому, але й конкурентну перевагу у вигляді більш зрілої, гнучкої та стійкої цифрової інфраструктури

Між соціальними мережами та маркетплейсами: як працює екосистема прихованих посилань⁵



Документ UNICRI розглядає феномен «прихованих посилань» (hidden links) як одну з найбільш адаптивних, стійких і складних для викриття схем незаконного обігу контрафактних товарів у сучасній електронній комерції. У центрі дослідження лежить теза про те, що розвиток цифрових маркетплейсів, зростання ролі сторонніх продавців та масове використання автоматизованих інструментів контролю з боку платформ і правовласників не зменшили масштаби контрафакту, а, навпаки, стимулювали еволюцію злочинних моделей. Приховані посилання постають як відповідь організованих мереж контрафактників на підвищення ефективності алгоритмічних фільтрів, систем розпізнавання зображень і ключових слів та процедур перевірки продавців.

У звіті детально пояснюється, що сутність прихованих посилань полягає у навмисному створенні розриву між тим, що задекларовано на платформі електронної комерції, і тим, що фактично постачається покупцеві. Формально оголошення може виглядати як продаж абсолютно нейтрального товару без ознак порушення прав інтелектуальної власності, однак після оформлення замовлення споживач отримує конкретний контрафактний брендований продукт. Така модель фактично знецінює класичні механізми виявлення контрафакту, адже ні візуальний аналіз, ні текстовий пошук, ні порівняння цін не дозволяють зафіксувати порушення до моменту фізичної доставки товару.

Автори наголошують, що ключова небезпека прихованих посилань полягає не лише в ухиленні від контролю, а й у використанні законної інфраструктури електронної комерції для незаконної діяльності. Контрафактні товари потрапляють до споживачів через ті самі платформи, логістичні

⁵ https://unicri.org/sites/default/files/2026-01/Hidden-Links-Facilitating-Criminal-Activities-While-Exploiting-E-Commerce-Jan-2026_0.pdf

сервіси та платіжні механізми, які асоціюються з довірою, зручністю та законністю. Це розширює аудиторію покупців за межі тих, хто свідомо звертається до «чорного ринку», і призводить до системного перетікання доходів від правовласників до злочинних мереж у межах одного й того ж цифрового середовища.

Значна частина документа присвячена розкриттю екосистемного характеру цієї моделі. Приховані посилання не функціонують ізольовано, а є центральним елементом складної мережі взаємодії між виробниками контрафакту, продавцями на маркетплейсах, інфлюенсерами, соціальними мережами, месенджерами та допоміжними цифровими сервісами. Виробники та продавці створюють обфусковані або «відволікаючі» оголошення, після чого поширення інформації про реальний товар відбувається через закриті групи, приватні канали або напівпублічні сторінки в соціальних мережах. Саме приховане посилання виконує функцію містка між нелегальним маркетингом і формально легальним процесом купівлі.

Документ детально аналізує еволюцію технік маскування, демонструючи, що вони постійно ускладнюються у відповідь на розвиток технологій виявлення. Якщо на ранніх етапах достатньо було просто вилучити назву бренду з опису, то згодом з'явилися розмиті зображення, навмисно змінені логотипи, повністю не пов'язані з реальним товаром продукти-приманки, а також кодована мова в коментарях і інструкціях для покупців. Окремо підкреслюється використання кількох прихованих посилань одночасно, що підвищує стійкість мережі до блокувань і дозволяє швидко перенаправляти трафік у разі втручання платформи.

Висновки:

- Приховані посилання руйнують ефективність традиційних механізмів виявлення обігу контрафактних товарів в електронній комерції, оскільки розривають зв'язок між оголошенням і фактично доставленим товаром.
- Ключовою інфраструктурою таких схем є інфлюенсери та закриті соціальні групи, що зумовлюють необхідність координації між платформами та посилення контролю за повторною реєстрацією акаунтів.
- Масштабна протидія прихованим посиланням можлива лише за умови використання автоматизованих інструментів поведінкового та мережевого аналізу.
- Кримінально-правові механізми є більш ефективними, ніж цивільно-правові, для припинення організованих схем обігу контрафактних товарів.

Особливу увагу в документі приділено ролі інфлюенсерів, які фактично стають центральними посередниками в цій схемі. Інфлюенсери не лише поширюють приховані посилання, а й легітимізують купівлю контрафакту через особистий бренд і довіру аудиторії. Вони формують наратив «доступної альтернативи», «вигідної знахідки» або «дюпу» (стилістична імітація оригінальних брендових виробів), водночас навчаючи підписників правилам безпечної комунікації, уникненню згадування брендів і правильному проходженню процедури замовлення. Така діяльність розмиває межу між свідомим співучастю та удаваною необізнаністю, що ускладнює як цивільне, так і кримінальне переслідування.

У завершальній частині звіту автори переходять до аналізу можливих шляхів протидії. Підкреслюється, що ручні методи розслідування та вибіркові

контрольні покупки не відповідають масштабам і швидкості адаптації прихованих посилань. У зв'язку з цим пропонується системний перехід до використання інструментів штучного інтелекту, здатних автоматизувати виявлення поведінкових і мережевих аномалій, імітувати процес купівлі без завершення транзакції та акумулювати експертні знання через підходи на кшталт Retrieval-Augmented Generation. Водночас наголошується, що жодне технологічне рішення не буде ефективним без поглибленої співпраці між маркетплейсами, соціальними

мережами, правовласниками та правоохоронними органами, адже саме закриті соціальні простори є критичною інфраструктурою для масштабування цієї злочинної моделі.

Загальний висновок документа полягає в тому, що приховані посилання є не тимчасовою тактикою, а стійкою структурною відповіддю контрафактних мереж на цифрову трансформацію торгівлі. Вони демонструють, наскільки ефективно організована злочинність здатна інтегруватися в легітимні цифрові екосистеми та використовувати їхні переваги проти самих регуляторів і платформ. Тому протидія прихованим посиланням має розглядатися не як вузьке питання захисту прав інтелектуальної власності, а як комплексна проблема економічної безпеки, цифрового врядування та кримінального правозастосування у глобалізованому онлайн-середовищі.

Від нашарування до узгодженості: методологія спрощення фінансового регулювання ЄС⁶



У звіті Європейського банківського інституту здійснено ґрунтовний, концептуально побудований аналіз проблеми надмірної складності фінансового права Європейського Союзу та запропоновано методологічні підходи до його спрощення без підризу базових публічних цілей регулювання. Документ виходить із того, що фінансове регулювання ЄС за останні два десятиліття істотно посилило фінансову стабільність, захист споживачів і доброчесність ринків, однак водночас накопичило багатшарову систему норм, інституцій і процедур, яка дедалі більше ускладнює правозастосування, знижує правову визначеність, послаблює наглядову конвергенцію та негативно впливає на конкурентоспроможність і здатність до інновацій. Автори підкреслюють, що ця складність не є побічним або випадковим явищем, а має системний характер і є результатом поступового нашарування законодавчих і наглядових рішень, ухвалених у відповідь на різні, часто взаємопов'язані політичні імперативи.

Звіт чітко вбудований у сучасний політичний і стратегічний контекст ЄС, зокрема в межах порядку денного Союзу заощаджень та інвестицій, висновків доповідей Летти й Драгі, а також ініціатив Європейської Комісії щодо зменшення адміністративного та регуляторного навантаження. Водночас автори принципово відмежовують запропонований підхід від дерегуляції чи зниження стандартів. Спрощення розглядається не як ослаблення фінансового права, а як необхідна умова збереження його ефективності, легітимності та довгострокової стійкості, за незмінного пріоритету фінансової стабільності як ключової публічної мети, покликаної запобігати системним кризам і негативним зовнішнім ефектам.

Центральною аналітичною тезою документа є твердження, що сучасна складність фінансового права ЄС сформувалася внаслідок послідовних хвиль регуляторного розвитку, кожна з яких переслідувала легітимні цілі, але рідко супроводжувалася повною консолідацією попередніх режимів. Після глобальної фінансової кризи 2007–2009 років ЄС істотно розширив і поглибив регуляторну базу, інтегрувавши у фінансове право вимоги щодо пруденційної стійкості, управління кризами, захисту споживачів, а згодом — цифрових інновацій, управління даними, сталого розвитку та протидії фінансовим злочинам. У результаті виникла регуляторна архітектура, що характеризується перекриттям правових джерел, фрагментованими дефініціями, розмитими інституційними межами та високим рівнем технічної деталізації.

⁶ <https://ebi-europa.eu/wp-content/uploads/2026/01/the-EBI-SIMPLIFICATION-REPORT-16-January-2026-FINAL.pdf>

Значну увагу звіт приділяє внутрішнім чинникам регуляторної складності, передусім інституційній архітектурі нагляду в ЄС. Автори демонструють асиметрію між фінансовими секторами: банківський союз є найбільш інтегрованою та централізованою моделлю, яка забезпечила відносно високий рівень наглядової конвергенції, тоді як ринки капіталу та страхування залишаються переважно децентралізованими й координуються через європейські наглядові органи та національні компетентні органи. Паралельно відбулося суттєве розширення кола наглядових учасників, включно зі створенням нових органів, таких як AMLA, що призвело до перетину мандатів і множинності наглядових ліній. У практичному вимірі це означає, що одна й та сама фінансова установа може одночасно підпадати під пруденційний, поведінковий, резолюційний та нагляд у сфері ПВК/ФТ, які здійснюються різними органами на основі різних правових режимів і методологій.

Одним із ключових концептуальних висновків звіту є констатація ерозії ламфалюссівського процесу, який мав забезпечувати чітку ієрархію між політичними рішеннями, технічним регулюванням і наглядовою конвергенцією. З часом законодавство рівня 1 стало надмірно технічним і деталізованим, акти рівня 2 суттєво розрослися, а інструменти «м'якого права» рівня 3 набули фактичної квазінормативної сили. Судова практика Суду ЄС посилила цю тенденцію, що створює ризики для правової визначеності, пропорційності, підзвітності регуляторів і ефективного судового захисту суб'єктів ринку.

Змістова фрагментація фінансового права, за висновками учасників, є не менш серйозною проблемою. Базові поняття, такі як «фінансовий інструмент», «кредитна установа» або «клієнт», визначаються по-різному в різних секторальних актах, часто через перелічувальні або колові формулювання, що ускладнює їх уніфіковане застосування. Часті зміни ключових регламентів і директив, інтенсивне перехресне посилення між актами та включення складних методологій безпосередньо в первинне законодавство перетворюють *acquis* ЄС на нестабільну систему, яка є складною як для суб'єктів ринку, так і для наглядових органів, без гарантованого підвищення регуляторної ефективності.

Окремо проаналізовано зовнішні чинники складності, зокрема вплив міжнародних фінансових стандартів, технологічних інновацій, цифрового регулювання та інтеграції нефінансових цілей. Постійне оновлення та непослідовне впровадження міжнародних стандартів, розвиток

цифрових фінансів і паралельне застосування таких режимів, як MiCAR, DORA, GDPR та AI Act, а також фрагментовані вимоги у сфері сталого фінансування (SFDR, CSRD, Таксономія) створюють дублювання обов'язків, зростання звітного навантаження та правову невизначеність, особливо для міжсекторальних учасників ринку.

Висновки:

- **Спрощення має бути структурною реформою, а не дерегуляцією:** ЄС потребує методологічного перегляду архітектури фінансового права з відновленням чіткої ієрархії норм, а не вибіркового скорочення вимог.
- **Інституційна фрагментація є одним із головних джерел регуляторної неефективності:** множинність наглядових органів і перехресні мандати потребують чіткого перерозподілу повноважень і підзвітності.
- **Відсутність уніфікованих дефініцій і таксономії підриває правову визначеність:** практичним пріоритетом має стати кодифікація ключових понять і усунення міжсекторальних розбіжностей у базових категоріях фінансового права.
- **Найбільший потенціал швидкого ефекту — у спрощенні звітності та даних:** інтегровані системи звітності й спільні стандарти даних можуть суттєво зменшити навантаження на ринок без шкоди для наглядових цілей.

На цьому тлі звіт формулює концепцію спрощення як методологічного та архітектурного процесу, спрямованого на раціоналізацію джерел права, стабілізацію дефініцій і таксономій, усунення перекриттів і відновлення внутрішньої узгодженості системи фінансового регулювання. Спрощення розуміється як постійне завдання управління, яке має охоплювати як перегляд чинного законодавства, так і дисципліну у формуванні майбутніх норм. У фінальному висновку автори наголошують, що фінансове право ЄС перебуває на критичному етапі розвитку: без свідомого й системного підходу до спрощення подальше нашарування норм може підірвати функціонування внутрішнього ринку, тоді як належно спроектоване спрощення є передумовою збереження стійкості, ефективності та легітимності фінансового регулювання ЄС у довгостроковій перспективі.

Коли корупція стає порушенням прав людини: правозахисний вимір антикорупційної політики⁷



A Practical Guide



Документ формує цілісну концептуальну та практичну рамку розуміння корупції як системного явища, що безпосередньо та опосередковано підриває реалізацію всього комплексу прав людини і водночас обмежує здатність держав виконувати свої міжнародні правозахисні зобов'язання. Посібник виходить із принципового твердження, що корупція не є нейтральною з точки зору прав людини та не може розглядатися виключно як кримінально-правова чи адміністративна проблема, оскільки її наслідки завжди матеріалізуються у формі конкретної шкоди для осіб, груп та суспільства загалом. Корупція підриває демократію, верховенство права, довіру до інституцій, сприяє зростанню нерівності та створює сприятливе середовище для системних і повторюваних порушень прав людини.

У Посібнику послідовно обґрунтовується теза про нерозривний взаємозв'язок між корупцією та правами людини, який

проявляється через відволікання публічних ресурсів від соціально значущих сфер, викривлення процесів прийняття рішень, підміну публічного інтересу приватною вигодою та інституціоналізацію безкарності. Корупція ослаблює спроможність держави забезпечувати доступ до базових послуг, таких як охорона здоров'я, освіта, соціальний захист, житло, правосуддя, і водночас перетворює ці сфери на зони підвищеного ризику експлуатації, дискримінації та зловживань владою. Документ наголошує, що в умовах системної корупції порушення прав людини часто перестають сприйматися як виняток і стають нормалізованими практиками, що додатково ускладнює їх виявлення, оскарження та відшкодування шкоди.

Значна частина Посібника присвячена детальному аналізу характеру та масштабів негативного впливу корупції на реалізацію прав людини, який розглядається через призму прямого, непрямого та віддаленого причинно-наслідкового зв'язку. Корупція може безпосередньо порушувати права людини, коли доступ до суду, медичної допомоги, соціальних виплат або адміністративних послуг ставиться в залежність від надання неправомірної вигоди. Водночас вона часто діє як ключовий елемент ширшого ланцюга подій, наприклад у сфері продовольчої безпеки, екологічного контролю чи регулювання бізнесу, де корупційні дії створюють умови для появи небезпечних продуктів, екологічної шкоди або масових порушень соціально-економічних прав. У ще ширшій перспективі корупція підриває легітимність демократичних процесів,

⁷ <https://www.ohchr.org/sites/default/files/documents/issues/corruption/corruption-human-rights-a-practical-guide-2025.pdf>

зокрема виборів, що може призводити до політичної нестабільності, репресивних реакцій держави та серйозних порушень громадянських і політичних прав.

Посібник докладно демонструє, що корупція становить структурну перешкоду для реалізації конкретних прав, зокрема права на достатній життєвий рівень, харчування, житло, соціальне забезпечення, охорону здоров'я та освіти. Вказується, що корупція у сфері житлової політики, землекористування та містобудування призводить до примусових виселень, дискримінації, затримок у доступі до соціального житла та позбавлення правового захисту. У продовольчих системах корупція підриває всі ключові елементи права на їжу — доступність, безпечність, адекватність і сталість, сприяючи незаконному обігу продуктів, розкраданню субсидій і зловживанням у сфері контролю якості. У системах соціального захисту корупція знижує охоплення населення соціальними програмами, ускладнює доступ до виплат і підриває довіру до державних механізмів підтримки.

Окремо підкреслюється згубний вплив корупції на реалізацію права на охорону здоров'я, зокрема через розкрадання бюджетних коштів, маніпуляції з публічними закупівлями, поширення неякісних або небезпечних медичних засобів та створення бар'єрів доступу до лікування для соціально вразливих груп. Аналогічно у сфері освіти корупція підриває рівний доступ, якість та інклюзивність освітніх послуг, сприяє дискримінації та відтворенню соціальної нерівності. У сфері правосуддя корупція безпосередньо руйнує право на справедливий суд і ефективний засіб правового захисту, підриваючи незалежність суддів, прокурорів і адвокатів та позбавляючи потерпілих реальних можливостей домогтися відновлення порушених прав.

Висновки:

- **Антикорупційні політики без правозахисного виміру є неповними:** держави мають інтегрувати обов'язки щодо прав людини (поважати, захищати, забезпечувати) у всі антикорупційні стратегії, а не обмежуватися кримінальним переслідуванням.
- **Корупція повинна розглядатися як джерело конкретної шкоди,** що вимагає визнання жертв, забезпечення доступу до правового захисту, відшкодування шкоди та ефективних механізмів скарг.
- **Вразливі групи мають бути у фокусі антикорупційних заходів,** оскільки саме вони зазнають непропорційного впливу корупції у сферах житла, соціального захисту, охорони здоров'я, освіти та правосуддя.
- **Підхід, заснований на правах людини,** підвищує стійкість боротьби з корупцією, оскільки зміцнює довіру до інституцій, зменшує безкарність і створює довгострокові запобіжники повторного відтворення корупційних практик.

Посібник також наголошує, що корупція має непропорційний вплив на окремі групи правовласників, зокрема жінок, дітей, мігрантів, осіб з інвалідністю, корінні народи, осіб, позбавлених волі, та людей, які живуть у бідності. У таких випадках корупція часто поєднується з іншими формами дискримінації, посилюючи вразливість цих груп та обмежуючи їх здатність захищати свої права. Документ підкреслює, що ігнорування цього аспекту робить антикорупційні заходи формальними та неефективними з точки зору реального впливу на життя людей.

Важливим концептуальним елементом Посібника є обґрунтування необхідності застосування підходу, заснованого на правах людини, у боротьбі з корупцією. Такий підхід розглядається як доповнення, а не альтернатива кримінально-правовим механізмам і передбачає фокус на підзвітності, участі, недискримінації, прозорості та орієнтації на потерпілих.

Документ підкреслює, що Конвенція ООН проти корупції повинна імплементуватися у спосіб, сумісний з міжнародними стандартами прав людини, а антикорупційна політика має

оцінюватися не лише за кількістю розслідувань чи вироків, а й за її здатністю запобігати порушенням прав та відновлювати справедливість.

Загалом Посібник формує системне бачення корупції як глибинного чинника порушення прав людини та водночас підкреслює, що ефективна протидія корупції неможлива без інтеграції правозахисного виміру у всі етапи політики, правозастосування та інституційних реформ.

Коли законність стає фікцією: як корупція підриває ефективність EUDR⁸

Документ є комплексним аналітичним дослідженням того, яким чином корупція у сфері землекористування, управління лісами та аграрними ресурсами може системно підірвати реалізацію Регламенту ЄС щодо продуктів, що не пов'язана з вирубкою лісів (EUDR), навіть за наявності формально жорсткої та технічно розвиненої моделі належної перевірки

В основі документа лежить констатація того, що ліси залишаються критично важливим глобальним ресурсом для збереження біорізноманіття, кліматичної стабільності та засобів до існування мільярдів людей, водночас аграрна діяльність залишається домінуючим чинником глобальних втрат лісів. Європейський Союз, усвідомлюючи власну роль як одного з ключових центрів споживчого попиту на лісоризикові товари, розробив EUDR як інструмент, спрямований на розрив зв'язку між доступом до ринку ЄС та глобальною дефористацією. Однак автор наголошує, що сам по собі регламент не може бути ефективним у відриві від реальних умов управління землею та лісами у країнах походження сировини, де слабкі інституції, непрозорі реєстри та політична корупція є структурними, а не випадковими явищами.

Документ детально розкриває логіку та механіку EUDR, який ґрунтується на трьох взаємопов'язаних вимогах: підтвердженні того, що продукція є дефористаційно нейтральною, дотриманні законодавства країни виробництва та здійсненні належної перевірки з боку операторів і трейдерів. При цьому особливий акцент робиться на тому, що поняття законності в межах EUDR охоплює не лише земельне та екологічне право, а й антикорупційні норми, трудові стандарти, права людини та принцип вільної, попередньої та поінформованої згоди корінних народів. Саме ця інтеграція антикорупційного виміру робить EUDR першим регуляторним актом ЄС, який прямо визнає корупцію як чинник дефористації, але водночас робить його вразливим до маніпуляцій у корумпованих правових системах.

Центральною аналітичною лінією документа є твердження, що корупція у земельному секторі має системний, багаторівневий характер і діє одночасно на локальному, національному та транснаціональному рівнях. Автор показує, як підкуп посадових осіб, фальсифікація кадастрових даних, політичне захоплення ліцензійних процедур і використання підставних компаній дозволяють незаконній або напівзаконній вирубці лісів набувати вигляду формально легальної діяльності. У такому контексті корупція не лише порушує закон, а й трансформує саму правову рамку, створюючи ситуацію, коли документи, дозволи та реєстри більше не є надійним джерелом істини для операторів, що здійснюють належну перевірку.



⁸ https://knowledgehub.transparencycdn.org/helpdesk/ForPublishing_Land-corruption-risks-in-the-implementation-of-the-EU-Regulation-on-Deforestation-free-Products-EUDR.pdf

Особлива увага приділяється ризикам у сфері простежуваності ланцюгів постачання, які є ключовим елементом EUDR. Документ демонструє, що у складних, фрагментованих ланцюгах, характерних для какао, сої, пальмової олії чи деревини, корупція дозволяє системно змішувати легальну та нелегальну продукцію, підробляти сертифікати походження та маніпулювати геолокаційними даними. Навіть використання супутникового моніторингу та цифрових карт не гарантує достовірності, якщо базові кадастрові та дозвільні системи є неповними або скомпрометованими. Таким чином, простежуваність може перетворюватися на технічну ілюзію відповідності, не відображаючи реальних практик на землі.

Аналізуючи вимогу законності, автор розкриває феномен так званої «захопленої законності», коли корупційні практики не просто порушують норми, а вбудовуються в сам механізм їх застосування. Приклади з Індонезії, Бразилії, Камеруну, Ліберії та інших країн демонструють, як незаконне захоплення земель може бути легалізоване заднім числом через корумповані реєстраційні процедури, як екологічне законодавство застосовується вибірково, а політично пов'язані учасники отримують дозволи, які формально відповідають праву, але фактично є результатом зловживання владою. У таких умовах оператори, що покладаються виключно на перевірку документів, ризикують стати частиною системи відмивання дефористаційної продукції.

Окремий пласт дослідження присвячений ризикам належної перевірки як такої. Документ переконливо показує, що формальне виконання процедур належної перевірки, зосереджене на заповненні декларацій і збиранні паперових підтверджень, не здатне виявити глибинні корупційні ризики. Наводяться кейси, коли аудитори, інспектори або сертифікаційні органи були залучені до корупційних схем, а компанії ігнорували добре задокументовані ризики у висококорумпованих юрисдикціях. Це підкреслює, що без переходу від формальної відповідності до змістовної оцінки інституційного контексту EUDR може стати інструментом «процедурного прикриття» проблем, а не їх вирішення.

Документ також містить критичний аналіз внутрішніх вразливостей самого EUDR, зокрема системи країнового бенчмаркінгу ризиків. Автор звертає увагу на те, що орієнтація переважно на історичні показники дефористації без належного врахування якості врядування, рівня корупції та ефективності правозастосування створює ризик помилкової класифікації країн як «низькоризикових». Запропоновані спрощення режиму для окремих операторів і юрисдикцій,

Висновки:

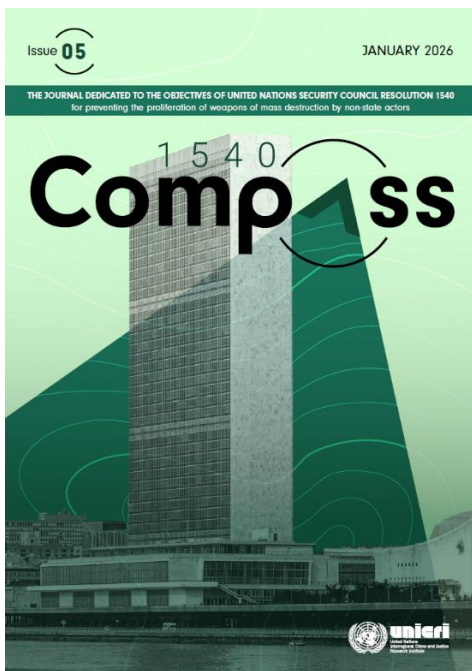
- **Корупція у сфері землекористування створює «ефект доміно»**, одночасно підриваючи простежуваність, законність і належну перевірку за EUDR; ізольовані контрольні заходи неефективні без системних реформ управління землею та лісами.
- **Формальна законність не дорівнює доброчесності**: у країнах з високим рівнем корупції документи та дозволи можуть маскувати незаконну вирубку, тому оператори мають інтегрувати оцінку корупційних ризиків і якості врядування в належній перевірці незалежно від рейтингу країн EUDR.
- **Інтегровані державні дані та прозорість бенефіціарної власності є ключовими інструментами** запобігання «відмиванню» продукції; приклади Гани та багатосторонніх платформ демонструють практичну ефективність такого підходу.
- **Довгостроковий успіх EUDR залежить від поєднання ринкової умовності з антикорупційними та фінансовими механізмами**, включно з використанням стандартів FATF, потенціалу ПФР та активної ролі громадянського суспільства для виявлення прихованих схем і політичного захоплення ресурсів.

на думку автора та цитованих експертів, можуть ще більше послабити превентивний потенціал регламенту та створити нові можливості для зловживань.

У завершальній частині документа EUDR розглядається не лише як торговельний чи екологічний інструмент, а як потенційний каталізатор ширших реформ у сфері управління землею та боротьби з корупцією. Автор детально аналізує практики інтегрованих державних інформаційних систем, зокрема приклад Гани, де поєднання лісових, земельних, аграрних і дозвільних даних створює цілісну та прозору картину землекористування. Особливо підкреслюється значення прозорості кінцевої бенефіціарної власності, залучення фінансової розвідки для виявлення відмивання доходів від лісових злочинів, а також критична роль громадянського суспільства, журналістських розслідувань і міжнародних антикорупційних механізмів, зокрема UNCAC та стандартів FATF.

У підсумку документ формує чіткий висновок: без системного врахування корупційних ризиків у сфері землекористування EUDR ризикує залишитися формально ефективним, але фактично обмеженим інструментом, тоді як його реальний потенціал полягає у здатності поєднати доступ до ринку ЄС із глибшими інституційними та антикорупційними трансформаціями у країнах-виробниках.

Фінансування розповсюдження ЗМЗ як виклик для сучасної архітектури міжнародної безпеки⁹



Документ, підготовлений під егідою UNICRI та присвячений реалізації цілей Резолюції Ради Безпеки ООН 1540 (2004) у контексті запобігання розповсюдженню зброї масового знищення недержавними суб'єктами. Центральною наскрізною темою є порушення та нейтралізація механізмів фінансування і торговельного забезпечення розповсюдження ЗМЗ, з особливим акцентом на сучасні фінансові, регуляторні та технологічні виклики.

Документ відкривається інституційним і політичним контекстом діяльності Комітету 1540 у 2025 році. Після періоду фактичної паузи, спричиненої тривалим узгодженням кандидатури голови, обрання Панами та нового Голови Комітету у червні 2025 року відновило активну роботу з просування повної та ефективної імплементації резолюції. Підкреслюється, що, попри понад двадцять років з моменту ухвалення Резолюції 1540,

її виконання залишається довгостроковим процесом, який вимагає постійного оновлення інструментів у відповідь на нові ризики, технології та моделі обходу контролю.

Суттєвим змістовним елементом документу є аналіз першого Добровільного технічного довідника Комітету 1540, оприлюдненого у вересні 2025 року та присвяченого експортному контролю. Документ розглядає експортний контроль як один із ключових стовпів виконання Резолюції 1540, наголошуючи на необхідності наявності комплексної нормативної бази, ефективних процедур ліцензування, актуальних контрольних списків, а також таких інструментів, як загальні контрольні заходи типу «catch-all», контроль кінцевого користувача, контроль транзиту, контроль реекспорту, контроль брокерської (посередницької) діяльності, нематеріальна передача технологій та фінансування експортних операцій. Експортний контроль

⁹ <https://unicri.org/Publications/Magazine-1540%20Compass>

у цьому контексті трактується не лише як митно-торговельний інструмент, а як елемент ширшої архітектури запобігання розповсюдженню ЗМЗ, тісно пов'язаний із фінансовим моніторингом і санкційними режимами.

Окремий концептуальний блок присвячено поясненню сутності фінансування розповсюдження ЗМЗ як багатовимірного явища. Документ демонструє, що фінансування розповсюдження не зводиться виключно до порушень санкцій, а охоплює складні транснаціональні фінансові та торговельні мережі, використання товарів подвійного призначення, посередників, юридичних осіб, непрозорих структур власності та легальних каналів міжнародної торгівлі. Підкреслюється, що саме «нормальність» і легальне прикриття таких операцій роблять їх особливо складними для виявлення в межах традиційних підходів ПВК/ФТ.

Значну аналітичну глибину випуску забезпечують інтерв'ю з провідними міжнародними експертами, зокрема колишніми та чинними представниками Комітету 1540, FATF і її регіональних органів. У цих матеріалах послідовно розкривається проблема відсутності універсального визначення фінансування розповсюдження на рівні ООН і, як наслідок, фрагментованість національних підходів. Наголошується, що на практиці більшість держав формують свої оцінки ризиків фінансування розповсюдження виходячи з вимог FATF щодо цільових фінансових санкцій, не інтегруючи ширші зобов'язання, які випливають безпосередньо з Резолюції 1540, особливо у частині недержавних суб'єктів.

Документ детально висвітлює роль FATF у формуванні глобальної архітектури протидії фінансуванню розповсюдження, зокрема після запровадження з 2020 року обов'язку для держав і підзвітних суб'єктів ідентифікувати, оцінювати та пом'якшувати відповідні ризики. Водночас наводяться тривожні дані про низький рівень ефективності імплементації цих стандартів у більшості юрисдикцій, що створює системні вразливості глобальної фінансової системи.

Окрему увагу приділено сучасним типологіям фінансування розповсюдження, серед яких ключове місце займають зловживання юридичними особами, компаніями-оболонками, складними ланцюгами контролю та бенефіціарної власності, а також використання торговельного фінансування, вільних економічних зон, морських перевезень і логістичних хабів. Значний акцент зроблено на зростаючій ролі віртуальних активів і постачальників послуг з обігу віртуальних активів, які дедалі частіше використовуються для переміщення коштів, отриманих злочинним шляхом, з подальшим їх залученням у схемах розповсюдження ЗМЗ, при цьому механізми конвертації таких активів у фіат залишаються недостатньо прозорими.

Висновки:

- **Фінансування розповсюдження ЗМЗ залишається слабкою ланкою глобальної безпеки**, оскільки більшість держав формально виконують санкції, але не вибудували цілісні системи ідентифікації та пом'якшення ризиків ФРЗМЗ відповідно до Резолюції 1540.
- **Експортний контроль і фінансовий моніторинг повинні працювати як єдина система**, із залученням митних, ліцензійних, фінансових та правоохоронних органів; ізолювані підходи не дозволяють виявляти складні транснаціональні схеми.
- **Юридичні особи, посередники та непрозора структура бенефіціарної власності є ключовими інструментами ФР**, що вимагає посилення контролю КБВ, міждержавного обміну інформацією та аналітичних типологій.
- **Віртуальні активи та нові платіжні технології формують новий фронт ризиків**, і без жорсткого нагляду за VASP, ефективного аналізу конвертації криптоактивів у фіатні валюти та державно-приватного партнерства ці канали залишатимуться вразливими.



Наскрізним висновком усього документу є твердження, що ефективна реалізація Резолюції 1540 в сучасних умовах можлива лише за умови інтегрованого, ризик-орієнтованого та міжвідомчого підходу, який поєднує фінансовий моніторинг, експортний контроль, санкційну політику, митні та ліцензійні механізми, а також активну участь приватного сектору. Резолюція 1540 у документі постає не як вузькоспеціалізований інструмент нерозповсюдження, а як елемент ширшої системи глобальної фінансової, торговельної та безпекової архітектури, що має постійно адаптуватися до еволюції загроз.

Звіти окремих інституцій та експертів

Мовчання океану: як розслідують торгівлю людьми у світових водах¹⁰



Global Investigative Journalism Network

На морських просторах, де хвилі охоплюють не лише географічні простори, але й межі національних юрисдикцій, відбувається одна з найбільш масштабних та прихованих

гуманітарних катастроф сучасності — системна експлуатація людей, яка набуває форм примусової праці, торгівлі людьми та сучасного рабства.

Океан, що забезпечує функціонування понад 80% глобальної торгівлі, опинився парадоксальним чином одночасно і найважливішою артерією світової економіки, і найменш захищеною зоною для десятків тисяч моряків, рибалок та працівників плавучих фабрик, чиї права регулярно ігноруються в умовах організованої безвідповідальності. Глибинна суть проблеми криється не просто в окремих злочинах окремих судновласників, а в складній системі регулювання, яка завдяки таким інструментам, як "зручні прапори", навмисне розмиває ланцюги власності та контролю, створюючи ідеальне середовище для злочинної діяльності. Саме ця системність і становить найбільший виклик для розслідувачів, які мусять протистояти не окремому злочинцю, а цілій архітектурі ухилення від відповідальності, побудованій на міжнародному рівні.

Технологічний прогрес, парадоксально, став як потужним союзником злочинців, так і ключовим інструментом для тих, хто намагається їх викрити. Судна, залучені до незаконної діяльності, від неконтрольованого вилову риби до транспортування крадених природних ресурсів і людей, все частіше перетворюються на високотехнологічні "примари" — вони здатні вимикати системи автоматичної ідентифікації (AIS), змінювати назви та прапори прямо посеред океану, здійснювати перевалювання вантажу в нейтральних водах з "темних" суден на "легальні". Ці практики породжують так звані "темні флоти", які є буквально невидимими для офіційних систем моніторингу.

Однак саме технології, які дозволяють злочинцям ховатися, стали основою для нових методологій журналістських розслідувань. Проекти на кшталт Global Fishing Watch, що базуються на супутникових даних та алгоритмах машинного навчання для відстеження рибальських суден, та платформи, подібні до Marine Traffic, які акумулюють масиви AIS-даних, тепер надають журналістам можливості, раніше доступні лише державним спецслужбам. Але справжнє мистецтво полягає не у використанні одного інструмента, а в їх синергії. Так, розслідування Абдуса Сомата в Арафурському та Натунському морях показало, як поєднання даних про рух суден із супутниковими знімками високої роздільної здатності від Planet Labs дозволяє виявити не лише факт незаконного вилову, а й встановити зв'язок між певними суднами та впливовими бізнес-структурами чи політичними фігурами, які часто стоять за цими операціями. Аналіз паттернів поведінки — тривалі стоянки в міжнародних водах, нелогічні зміни курсу, регулярні "зникнення" з радарів у конкретних регіонах — перетворюється на мову доказів, яка може бути представлена суду.

Надзвичайно важливим виміром сучасного розслідування стало залучення цифрових слідів, які залишають самі постраждалі та учасники системи. Соціальні мережі перетворилися на велетенський невпорядкований архів свідчень життя на морі. Журналісти, такі як Ketі МакК'ю, систематично "прочісують" Facebook, Instagram, TikTok та YouTube, де моряки діляться

¹⁰ <https://gijn.org/stories/gijc25-exposing-forced-labor-trafficking-oceans/>

буденними деталями свого існування. Фотографія гнилої їжі в кают-компанії, відео з ламаним обладнанням, пости про затримку зарплати на кілька місяців, або навіть знімки поранень після конфліктів з офіцерами — все це перестає бути лише приватним вираженням розчарування, а стає публічним доказом. Коментарі під такими постами часто розкривають мережу зв'язків: інші моряки розпізнають назви суден, імена капітанів або агенцій з найму, що дозволяє журналістам будувати картину не поодиноких випадків, а системної практики певних гравців ринку. Окремим джерелом інформації стають національні спільноти моряків у месенджерах, де обговорюються умови праці на конкретних суднах чи в конкретних компаніях. Ця цифрова енциклопедія людських страждань вимагає від журналіста не лише вміння вести пошук, але й критичної оцінки інформації, перевірки джерел та встановлення особистості того, хто публікує матеріал, щоб уникнути маніпуляцій або дезінформації.

Однак найбільш складним завданням часто є не зібрати технічні докази руху судна чи навіть отримати свідчення, а встановити юридичну відповідальність. Судноплавна індустрія побудована на каскадних контрактах, офшорних компаніях-одноденках та складних чартерних угодах. Коли стається трагедія або викривається експлуатація, останнім ланцюжком у цій конструкції завжди виявляється капітан або невелика компанія-оператор, тоді як справжні бенефіціари залишаються в тіні. Розплутування цієї павутини вимагає колосальної роботи з документами, які часто мають фізичну форму та знаходяться прямо на судні. Розслідувачі навчаються ідентифікувати ключові папери: договори про найм моряків, де можуть бути приховані кабальні умови; судові документи, що фіксують особовий склад; вантажні маніфести, які можуть свідчити про контрабанду; судові журнали, де офіцери іноді фіксують аварійні ситуації чи конфлікти. Цінність мають навіть, здавалося б, побутові речі — фоторамки з фотографіями родини в каюті моряка можуть містити на звороті записи з номерами телефонів або іменами, листівки з портів можуть слугувати підтвердженням маршруту. Найважливішим завданням є фіксація унікального семизначного номера IMO, викарбуваного на корпусі судна, — це "ДНК" судна, що не змінюється ніколи. Поєднання цього номера з даними про останні зміни прапора в базі даних Міжнародної морської організації та відкритими реєстрами компаній у офшорних юрисдикціях може поступово вивести розслідувачів на кінцевого бенефіціара.

Моряки, які потрапляють у пастку системи, часто переживають не лише фізичні позбавлення, а й глибоку психологічну травму, що посилюється почуттям ізоляції, страхом за свої сім'ї на батьківщині (агенти часто конфіскують паспорти та прямо погрожують родичам) і соромом за свою ситуацію. Журналіст, який виходить на контакт, несе подвійну відповідальність: отримати правду і не нашкодити джерелу. Досвідчені розслідувачі, такі як МакК'ю, виробляють чіткі протоколи: з перших слів ідентифікувати себе як журналіста, а не рятувальника чи представника влади; одразу надавати контакти організацій, які можуть надати реальну юридичну чи гуманітарну допомогу, як-от ITF або Apostleship of the Sea; детально обговорювати умови анонімності, пояснюючи, які ризики може нести публікація; а в разі роботи з особливо травматичними спогадами — співпрацювати з психологами або консультантами. Критично важливим є принцип "не нашкоди", який на практиці означає, що іноді публікацію матеріалу треба відкласти або змінити, якщо вона становить загрозу для безпеки моряка або його родини.

Останнім, але не менш важливим бар'єром на шляху правди є складність самої теми для широкої аудиторії. Тому інновації в розповіді та форматі стають не менш важливими, ніж якість самого розслідування. Команда Thomson Reuters Foundation, презентуючи проєкт "Темні води", показала, як можна трансформувати складне технічне розслідування в багатопланову історію для різної аудиторії. Короткі новинні статті висвітлювали головні висновки; інтерактивні графіки та карти візуалізували маршрути "темних флотів"; довгі розповіді з акцентом на людські долі давали глибину; пояснювальні відео розкривали механізми злочинів; а Q&A-сесії з авторами розвіювали ауру таємничості навколо журналістської роботи. Особливу роль відіграли

ілюстрації та фотографії, які не лише доповнювали текст, а й створювали емоційний зв'язок, перетворюючи абстрактне "судно" на конкретне місце страждань конкретних людей.

Висновки:

- **Системна непрозорість морської індустрії** — використання «зручних прапорів», офшорних схем власності та навмисне вимкнення супутникових систем (AIS) створюють умови для експлуатації людей та ухилення від відповідальності.
- **Технології — інструмент як злочинців, так і журналістів** — сучасні методи розслідувань поєднують аналіз супутникових даних, моніторинг AIS, соціальні мережі та документацію суден, щоб відстежувати «темні флоти» та встановлювати зв'язки між злочинами та їхніми організаторами.
- **Інновації в поданні інформації** — для залучення широкої аудиторії до складної теми необхідні різноманітні формати: від довгих текстів і візуалізацій до коротких новин, соціального медіа-контенту та інтерактивних матеріалів.

Отже, розслідування злочинів в океані сьогодні — це багатовимірна дисципліна, що поєднує в собі елементи журналістики, кіберрозслідувань, документальної кримінології, етичної психології та інноваційного сторителінгу. Це боротьба не просто з окремими злочинцями, а з цілою глобалізованою системою, що використовує прогалини в міжнародному праві, технологічний прогрес та соціальну вразливість мільйонів людей для отримання прибутку.

Кожне таке розслідування нагадує, що глобальна економіка, з її ланцюгами поставок, які здаються абстрактними, в реальності

тримається на плечах конкретних людей, і що право на гідність не повинно зникати за обрієм територіальних вод.

Інші новини

Аналіз санкційної політики США щодо ірансько-венесуельської збройної співпраці: стратегічні цілі та наслідки ¹¹



У середині грудня 2025 року Міністерство фінансів США через Управління з контролю за іноземними активами (OFAC) запровадило черговий пакет санкцій, цього разу спрямований на

перекриття каналів військово-технічного співробітництва між Іраном та Венесуелою. Ця акція, яка стосується десяти фізичних та юридичних осіб у обох країнах, є логічним продовженням політики адміністрації США, спрямованої на протидію поширенню зброї та обмеження військового потенціалу Ірану та його союзників. Санкції, введені на підставі виконавчих указів 13382 та 13949, мають на меті не лише заблокувати конкретні угоди з продажу безпілотників, але й продемонструвати готовність Вашингтона використовувати весь спектр фінансово-економічних інструментів для захисту своїх національних інтересів у Західній півкулі та на Близькому Сході.

Детальний огляд об'єктів санкцій виявляє чітку та цілеспрямовану архітектуру. Центральним елементом у відносинах Ірану з Венесуелою стала компанія Empresa Aeronautica Nacional SA (EANSA). Її діяльність далеко виходить за межі простого посередництва; згідно з матеріалами OFAC, EANSA займається прямою координацією з іранською Qods Aviation Industries (QAI), підтримкою, складанням та, ймовірно, навіть локалізацією виробництва безпілотних літальних апаратів серії «Mohajer». Ці БПЛА, що переробляються в Венесуелі під маркою ANSU, трансформуються з розвідувальних платформ у повноцінні ударні системи, здатні нести іранські керовані бомби «Qaem». Цей крок безпосередньо атакує операційну логістику партнерства, намагаючись паралізувати ключову інституційну ланку, відповідальну за інтеграцію іранських технологій у венесуельський арсенал.

Таким чином, дії проти EANSA є логічним «розширенням периметра»: якщо ядро іранського виробника вже ізольовано, то наступний удар завдається по зовнішнім агентам та партнерам, які забезпечують йому зовнішні ринки збуту та виробничі майданчики. Це відображає сучасну філософію санкцій, спрямовану на створення ефекту «удушення» – системи переплетених обмежень, які роблять будь-яку зовнішню діяльність цільового суб'єкта надзвичайно складною та ризикованою для третіх сторін. Постачання БПЛА Венесуелі розглядається Вашингтоном не просто як продаж зброї, а як частину ширшої іранської стратегії створення опорних пунктів за межами Близького Сходу, здатних тиснути на США на їхніх традиційних периферіях, порушуючи тим самим американську стратегічну рівновагу.

Паралельно з атакою на ланцюг постачання безпілотників, OFAC розгорнуло другий фронт, спрямований на серце іранської ракетної програми – її хімічну та матеріальну базу. Санкції проти трьох іранських суб'єктів, пов'язаних із закупівлями хімікатів для Parchin Chemical Industries (PCI). Такі речовини, як перхлорат натрію (попередник перхлорату амонію), себацінова кислота та нітроцелюлоза, є критичними, спеціалізованими та контрольованими на міжнародному рівні в рамках Режиму контролю за ракетними технологіями (MTCR). Сутність цього удару полягає в превентивному саботуванні: ускладнити та збільшити витрати на

¹¹ <https://home.treasury.gov/news/press-releases/sb0347>

відтворення ракетного арсеналу, особливо в контексті повної заборони на іранський імпорт та експорт зброї, відновленої Радою Безпеки ООН у вересні 2025 року.

Третій компонент санкційного пакету зачіпає технологічну та дослідницьку інфраструктуру, яка живить іранські програми розвитку озброєнь, зокрема під егідою Корпусу Вартових Ісламської революції (KBIP). Мережа компаній, що об'єднана навколо Rayan Fan Kav Andish Co (Rayan Fan Group), є характерним прикладом того, як сучасні оборонно-технологічні комплекси в умовах санкцій організовуються у вигляді розгалужених конгломератів. Вони поєднують холдингові структури (RFKA), виробничі дочірні підприємства (Rayan Roshd Afzar), спеціалізовані технологічні фірми (Fanavari Electro Moj Mobin, Kavoshgaran Asman Moj Ghadir) і навіть програмне забезпечення. Атака на технологічну базу KBIP є особливо важливою, оскільки ця структура відповідає за найбільш інноваційні та асиметричні проекти Ірану, включаючи БПЛА, які загрожують судноплавству або використовуються проксі-силами.

Правові та економічні наслідки цих дій є суворими й створюють ефект заморожування, що поширюється далеко за межі безпосередніх цілей. Згідно з механізмом OFAC, заблоковуються не лише активи перелічених осіб у США, але й будь-яка юридична особа, яка на 50% і більше належить їм прямо або опосередковано, автоматично потрапляє під ті самі обмеження. Це правило «50%» є критичним інструментом для боротьби зі спробами обійти санкції через створення нових юридичних оболонок. Більш того, загроза вторинних санкцій проти іноземних фінансових установ, які «свідомо проводять або сприяють будь-якій значній операції» від імені зазначених осіб, є, мабуть, найпотужнішим стримуючим фактором. Це означає, що будь-який банк у будь-якій країні світу, який обробляє платежі для EANSА або Rayan Fan Group, ризикує втратити доступ до американської фінансової системи та доларових розрахунків, що в сучасних умовах є смертним вироком для міжнародної діяльності. Таким чином, реальна сила санкцій OFAC полягає не в заморожуванні кількох рахунків, а в створенні навколо цілей неприступного «санкційного поля», через яке не наважуються переступати глобальні фінансові посередники.

У довгостроковій перспективі ефективність цих санкцій залежатиме від кількох факторів: здатності Ірану та Венесуели розвивати ще більш засекречені та децентралізовані мережі обміну, використовуючи криптовалюту або бартерні угоди; готовності таких гравців, як росія чи Китай, надавати альтернативні фінансові канали; та згоди ключових союзників США, особливо в Європі та Латинській Америці, дотримуватися аналогічних обмежень. Однак ясно одне: США послідовно розширюють визначення «іранської загрози», включаючи до неї не лише ядерну програму, а й весь спектр її військових можливостей та зовнішніх альянсів.

Санкції проти ірансько-венесуельської збройної торгівлі є сигналом усьому світу, що Вашингтон готовий застосовувати свою фінансову гегемонію для боротьби з цією загрозою на будь-якому географічному напрямку, розглядаючи Західну півкулю не як окремий регіон, а як частину єдиного глобального стратегічного поля бою.

Глобальна гра: Meta, регулятори та мільярди в тіні шахрайської реклами ¹²

Зростаючий тиск регуляторних органів по всьому світу на соціальні мережі з вимогами забезпечити цифрову безпеку користувачів наштовхується на складну систему корпоративного опору, детально викладену у внутрішніх документах компанії Meta, що потрапили до агенції Reuters. Ці матеріали, що охоплюють період останніх чотирьох років розкривають не просто окремі випадки ухилення, а цілеспрямовану, систематизовану та глобальну стратегію захисту

¹² <https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/>

бізнес-моделі, що отримує мільярди доларів від реклами, навіть якщо частина цих коштів походить від явно шахрайської діяльності.

Замість того, щоб викорінювати проблему в її основі через універсальну верифікацію рекламодавців, Meta розробила та вдосконалила механізми створення ретельно сконструйованого фасаду дотримання вимог, який має заспокоїти наглядові органи, водночас мінімізуючи фінансові та операційні витрати для самої компанії.



Ця стратегія отримала кодову назву «керівництво» (playbook) і представляє собою детальний план дій на випадок регуляторних загроз у різних юрисдикціях. Її витoki сягають ситуації в Японії, де на початку 2024 року регулятори були стурбовані хвилею явно шахрайської реклами на Facebook та Instagram, від фальшивих інвестиційних схем до підроблених за допомогою штучного інтелекту рекомендацій знаменитостей. Побоюючись, що країна може запровадити обов'язкову верифікацію всіх рекламодавців, Meta зосередилася не на запобіганні шахрайству, а на управлінні сприйняттям цього явища. Ключовим інструментом стала публічна Бібліотека реклами (Ad Library), створена раніше як жест прозорості. Японські наглядові органи використовували її пошук як простий тест ефективності боротьби Meta з аферами. У відповідь співробітники компанії розробили механізм впливу на те, що вони назвали «сприйняттям поширеності» (prevalence perception). Вони ідентифікували ключові слова та імена знаменитостей, які, на їхню думку, використовували регулятори для пошуку обманних оголошень, і почали масово та автоматично видаляти такі результати з вибірки пошуку в бібліотеці, паралельно видаляючи їх з платформ.

Внутрішні меморандуми з гордістю констатували, що після кількох місяців такої «чистки» кількість знайдених шахрайських оголошень впала до нуля. Це справило враження на японських законодавців, один з яких публічно похвалив покращення. Таким чином, Meta досягла своєї головної мети: створення статистичної картини успіху, яка дозволила уникнути введення обов'язкових, але витратних для компанії правил верифікації. Колишній розслідувач шахрайства Сандіп Абрахам дав цій практиці точне визначення — «регуляторний театр», підкреслюючи, що інструмент прозорості перетворився на інструмент обману, що спотворює реальний стан речей для тих, хто намагається його оцінити.

Успіх японської операції призвів до її канонізації та включення в арсенал глобальної стратегії. «Керівництво» детально описує, як уповільнити або зірвати регуляторні ініціативи в будь-якій країні. Один з центральних елементів — це відстрочка. За рік до очікуваного впровадження нових правил, Meta радить запропонувати регуляторам створити добровільний процес верифікації, просячи час на його впровадження та оцінку ефективності. Через півроку компанія повинна запровадити верифікацію лише для «нових та ризикованих» рекламодавців, що є мінімальною поступкою, яка дозволяє виграти ще більше часу. Кінцева мета — уникнути обов'язкової універсальної верифікації, поки це юридично можливо.

Документи наповнені свідченнями успіху цієї тактики. Наприклад, в Гонконзі лобісти Meta, координуючись з Google, запропонували фінансовим регуляторам альтернативу у вигляді добровільної «антишахрайської хартії». Це дозволило уникнути жорстких обов'язкових правил, які вимагали б верифікації фінансових рекламодавців. Працівники, святкуючи цю перемогу, зазначали, що остаточний текст не містить «нових зобов'язань або вимог щодо додаткової розробки продуктів». Подібні зусилля докладалися в Європі, Сінгапурі та Британії.

Фінансові мотиви цієї позиції розкриті в документах з кричущою ясністю. Внутрішні аналізи визнають, що універсальна верифікація є надзвичайно ефективним засобом. Впровадження в будь-якій країні займає менше шести тижнів і може миттєво знизити кількість шахрайської реклами на 29%. Проте розрахунки показують, що одноразова вартість впровадження такої системи склала б близько 2 мільярдів доларів. Для компанії з річним доходом у 164.5 мільярди доларів ця сума сама по собі, мабуть, не є непереборною. Справжнім стримуючим фактором є очікувана втрата доходу. Блокування неверифікованих рекламодавців, серед яких, за власним аналізом Meta 2022 року, 70% нових активних облікових записів просували шахрайство або заборонені товари, могло б позбавити компанію до 4.8% загальної виручки. Крім того, запровадження безкоштовної обов'язкової верифікації підірвало б платну програму «Verified for Business», за яку компанія стягує з клієнтів до 349.99 доларів на місяць. Таким чином, бізнес-модель, що отримує значну частину прибутків від низькобар'єрного доступу до рекламних інструментів, опиняється під загрозою.

Коли регуляторний тиск стає невідворотним і загрожує катастрофічними штрафами, Meta підкоряється, але навіть це підкорення стає для неї джерелом стратегічних даних. Яскравий приклад — Тайвань, який у 2023 році ввів жорсткі правила верифікації після спалаху інвестиційних шахрайств. Загроза штрафу у 180 000 доларів за кожне неверифіковане шахрайське оголошення зробила недотримання економічно неможливим. Meta виконала вимоги, що призвело до різкого падіння шахрайської реклами на острові. Однак внутрішній аналіз компанії виявив тривожний ефект: алгоритми Meta, які дозволяють рекламодавцям вибирати кілька географічних цільових аудиторій, просто перенаправили заблоковані в Тайвані шахрайські оголошення в інші регіони, такі як Гонконг, Малайзія та Філіппіни. Внутрішні документи прямо констатують: якщо верифікація не застосовується глобально, Meta не бореться зі шахрайством, а лише географічно його перерозподіляє. Цей ключовий висновок був підготовлений у вигляді брифінгу для генерального директора Марка Цукерберга, що вказує на усвідомлення проблеми на найвищому рівні.

Окрім реактивного «керівництва», Meta інвестувала в проактивні технології управління сприйняттям (perception management). Компанія розробила систему, яка за країнами будує величезні списки ключових слів, що імітують можливі пошукові запити регуляторів (наприклад, «безкоштовний подарунок», «гарантований прибуток»). Ці списки використовуються для проактивного сканування та видалення відповідних оголошень з вибірок пошуку, знову ж таки, змінюючи «сприйняття поширеності» проблеми. Компанія навіть технічно модифікувала бібліотеку, зробивши типовим пошук лише по активних оголошеннях, що автоматично приховувало вже видалені шахрайські матеріали, і запровадила повторне сканування всіх оголошень, які з'являються в нових пошукових запитах, надаючи собі «другий шанс» вилучити порушників. Ці зусилля принесли плоди на міжнародних форумах, таких як конференція Global Anti-Scam Alliance в Лондоні, де, за відгуками співробітників Meta, критичний тон на адресу компанії різко змінився на більш примирливий порівняно з попередніми подіями.

Підсумовуючи, отримані документи розкривають не просто окремі недоліки в системі модерації, а фундаментальний конфлікт інтересів у серці бізнес-моделі однієї з найвпливовіших технологічних компаній світу. Meta, володіючи технологічними можливостями, фінансовими ресурсами та внутрішніми знаннями про ефективність верифікації, свідомо обирає шлях найменшого опору, який полягає в мінімізації регуляторних ризиків, а не в мінімізації шкоди для користувачів. Вона будує складну архітектуру управління, де реальні показники шахрайства затьмарюються статистичними маніпуляціями, а глобальні проблеми не вирішуються, а експортуються в інші юрисдикції. Ця стратегія, закріплена в «керівництві», перетворює боротьбу з цифровою злочинністю на нескінченну гру між регуляторами та корпоративними лобістами, де безпека мільярдів користувачів залишається розмінною монетою в боротьбі за збереження мільярдних потоків рекламних доходів.

Як організована злочинність використовує світову торгівлю рибою¹³



В глибинах Каліфорнійської затоки, відомої також як Море Кортеса, розігрується одна з найбільш похмурих та складних екологічно-кримінальних драм сучасності. Її центром є величезна риба тотуаба, ендемік цих вод, чий плавальний міхур, висушений і перетворений на товар, цінується в найдорожчих ресторанах та аптеках Гонконгу, Шанхаю та Гуанчжоу.

Ця історія — не просто про браконьєрство. Вона про складну, багаторівневу

транснаціональну злочинну індустрію, яка вправно експлуатує розрив між законодавством та його виконанням, між традиційними віруваннями та сучасним кримінальним капіталізмом, між локальною бідністю та глобальною жагою до статусу і прибутку. Попит на «морський кокаїн», як його іноді називають, створює ланцюг, де кожна ланка — від рибалки, що кидає сіті, до чиновника, що закриває очі, і фінансиста, що відмиває гроші — посилює спіраль руйнування.

Культурно-економічне підґрунтя цього явища глибоке та давнє. У китайській традиційній медицині плавальні міхури риб, відомі як «хуа тао» або «фіш ма», століттями цінувалися за їхню нібито здатність покращувати стан шкіри, підвищувати фертильність, зміцнювати життєву силу та лікувати болі в суглобах. Однак у останні десятиліття цей продукт перетворився з ліків на символ статусу та об'єкт фінансових спекуляцій. В контексті стрімкого зростання багатства в Азії володіння рідкісним та дорогим міхуром тотуаби стало демонстрацією соціального положення, а його дарування — могутнім жестом благословіння або хабарем. Ціни, що досягають 81 000 доларів за кілограм, перевершують вартість золота та кокаїну, створюючи економічну тягу настільки потужну, що вона з легкістю подолала всі юридичні бар'єри. Цей попит не просто існує паралельно з боротьбою за збереження видів; він активно формує нову, паралельну реальність, в якій виживання виду визначається не екологічними факторами, а коливаннями ринкових цін на його органи.

Мексика, як країна походження, опинилася в епіцентрі цього шторму. Незважаючи на заборону вилову з 1976 року та включення до CITES, практика показала повну відсутність реального контролю над просторами Каліфорнійської затоки. Рибачькі громади в штатах Баха-Каліфорнія та Сонора, багато з яких живуть в умовах глибокої економічної нестабільності, стикаються з моральною та фінансовою дилемою: дотримуватися закону та бідувати, чи піти на угоду з кримінальними угрупованнями, які пропонують готові логістичні ланцюги та готівкові гроші.

Картелі, такі як Сіналоа та Халіско, зрозуміли прибутковість цього бізнесу. Вони не лише організовують вилов і транспортування, але й встановлюють фактичну монополію на рибальські угіддя, збираючи «податки» з рибалок або просто застосовуючи силу для контролю території. Їхня інфраструктура, розвинена для торгівлі наркотиками, — таємні схованки, коридори для контрабанди, корупційні зв'язки в поліції, армії та митних органах — ідеально підходить і для транспортування висушених міхурів.

Технології обходу закону постійно вдосконалюються. Контрабанда маскується з хитрістю, гідною шпигунських романів. Міхури ховають у контейнерах з замороженими морепродуктами, змішують з легальними товарами, переправляють у валізах пасажирів авіарейсів або посилками під виглядом «сувенірів» чи «одягу». Критичними вузлами в цій системі є транзитні території з

¹³ <https://globalinitiative.net/analysis/the-totoaba-trafficking-route/>

гнучким законодавством або слабким наглядом. Гонконг з його вільним портом і складними ланцюгами реекспорту, Тайвань, В'єтнам, Сінгапур — усі вони використовуються для перепакуння, фальсифікації документів і приховування справжнього маршруту. Часто товар робить декілька «стрибків» між юрисдикціями, перш ніж дістатися кінцевого споживача, що повністю заплутує слід для правоохоронців. Дослідження таких організацій, як C4ADS, виявили наявність цілих кластерів китайських торговців, які осіли в прибережних мексиканських містах. Вони є ключовою ланкою, що забезпечує безпосередній зв'язок між місцевими постачальниками сировини та ринком в Азії, володіючи знанням мови, культури споживачів та каналів розповсюдження.

Однак найбільш трагічним і непоправним наслідком цієї незаконної діяльності є майже повне знищення вакити — найменшого та найрідкіснішого морського ссавця на Землі, який мешкає лише у Каліфорнійській затоці. Вакити гинуть, потрапляючи в заборонені сіті «пальянґери», які браконьєри ставлять саме на тотауабу. Розмір сіток ідеально підходить для великої тотауаби, але в них так само гинуть і малі вакити, які не можуть вивільнитися. Популяція вакити, яка в 1997 році налічувала близько 600 особин, зменшилася до, за останніми оцінками, менше 10. Кожна виловлена тотауаба несе прямі ризики загибелі вакити, роблячи торгівлю міхурами прямим знаряддям біологічного знищення цілого виду. Це кричущий приклад того, як цілісність екосистеми жертвується заради отримання одного комерційного продукту.

Глобальний індекс організованої злочинності дає цьому явищу чітку оцінку. Мексика отримує високий бал (7.50/10) за злочини проти фауни, що відображає масштаб проблеми. Але ще важливішим є показник слабкої стійкості — нездатності держави ефективно протистояти загрозі. Індекс вказує на корупцію як на системну проблему, що пронизує всі рівні, від місцевої поліції до вищих ешелонів влади, а також на хронічну нестачу ресурсів і координації між численними відомствами, відповідальними за охорону природи, рибальство, безпеку та митницю. Результат — практична безкарність. За шість років лише 16 вироків за торгівлю тотауабою є жалюгідним показником ефективності правосуддя на тлі тисяч щорічно виловлених риб.

На іншому кінці ланцюга, у Китаї, ситуація також суперечлива. З одного боку, існують суворі закони, а у 2020 році було запроваджено загальну заборону на споживання диких тварин у відповідь на пандемію COVID-19. З іншого боку, Індекс послідовно оцінює Китай як країну з найвищим у світі рівнем злочинів проти фауни (9.0/10). Ця розбіжність між законодавством та реальністю пояснюється низкою факторів: вкоріненими культурними практиками, що змінюються повільніше, ніж закони; потужним підпільним ринком; обмеженими можливостями правоохоронних органів відстежувати та переривати кримінальні мережі, що часто маскують свою діяльність під легальний бізнес; а також тим, що попит зберігається серед могутніх та заможних верств населення. Крім того, дозвіл CITES на торгівлю тотауабою, вирощеною в аквакультурі, створює небезпечний прецедент для легалізації та відмивання продукції дикого вилову, оскільки відрізнити одне від іншого без дорогих ДНК-експертиз практично неможливо, а різниця в розмірі та якості очевидна для покупця.

Фінансова складова цієї торгівлі є її життєво важливим нервом і водночас ахіллесовою п'ятою. Прибутки від продажу міхурів, як і від інших видів злочинної діяльності, потрібно інтегрувати в легальну економіку. Розслідування виявляють складні схеми відмивання грошей: інвестиції в нерухомість у престижних районах мексиканських курортів, Майамі або самого Гонконгу; створення павутини офшорних компаній у зонах з пільговим оподаткуванням; використання неформальних систем грошових переказів, таких як «фей ч'єн» або криптовалютні гаманці. Часто ці самі механізми обслуговують суміш злочинних доходів — від наркотиків, торгівлі людьми, вирубки лісів та контрабанди фауни, ще більше змішуючи та ускладнюючи картину для слідчих.



Таким чином, боротьба з торгівлею тотаубою не може бути лише екологічною ініціативою. Це комплексне завдання в сфері національної та міжнародної безпеки. Ефективна стратегія повинна включати в себе паралельне руйнування як кримінальних мереж, так і попиту. З боку пропозиції це означає не просто патрулювання моря, а проведення фінансових розслідувань, направлених на виявлення та конфіскацію активів; боротьбу з корупцією на всіх рівнях; підвищення рівня життя в прибережних громадах, надаючи їм альтернативні джерела доходу; та зміцнення міжвідомчої та міжнародної координації. З боку попиту потрібна не лише інформаційна кампанія, але і цілеспрямована робота з бізнес-спільнотою в Азії, представниками традиційної медицини для пошуку альтернатив, а також суворе кримінальне переслідування ключових фігур в імперії торгівлі дикими тваринами.

Ваша думка важлива!

1. У світлі активного українського санкційного законодавства та міжнародних режимів, які націлені на російську агресію, як українські юридичні фірми можуть вибудувати ефективні, але не надмірно бюрократичні, процедури скринінгу клієнтів та контролю за дотриманням санкцій, особливо з огляду на можливі спроби обходу санкцій через треті юрисдикції чи складні корпоративні структури?
2. Чи може досвід США щодо протидії іранським поставкам БПЛА та ракетних технологій бути корисним для України у контексті боротьби з аналогічними загрозами? Які практичні кроки може вжити Україна спільно з міжнародними союзниками, щоб посилити ефект від існуючих санкцій проти РФ через механізми тиску на треті країни та фінансові інституції, які свідомо обходять обмеження?
3. Враховуючи високу оцінку ризику відмивання коштів через мистецтво, чи повинна Україна вже зараз посилювати національне законодавство щодо фінансового моніторингу операцій з культурними цінностями, особливо для предметів з нечітким походженням або тих, що з'являються на ринку під час війни?
4. Які інституційні рішення дозволяють забезпечити сталість реформ у сфері ПВК/ФТ в умовах тривалих криз, війни та обмежених ресурсів, і які уроки з досвіду інших держав можуть бути релевантними для післявоєнного відновлення України?
5. Яку роль має відігравати приватний сектор в Україні — банки, ВНУП, логістичні та торговельні компанії — у протидії фінансуванню розповсюдження ЗМЗ, і де проходить межа між добровільною співпрацею та регуляторним примусом?

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-2026-05

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

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