Методологічний бюлетень

Серійний номер: МінФін-AML-2026-29

Липень 2026

“Прогрес неможливий без змін, а ті, хто не може змінити мислення, не здатні змінити нічого!”

Бернард Шоу

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

Тероризм у Європейському Союзі в 2025 році: статистика, типології фінансування та вплив геополітичного контексту [1]

Європейське поліцейське управління (Європол) оприлюднило щорічний звіт «European Union Terrorism Situation and Trend Report» (EU TE-SAT) за 2026 рік – консолідований ситуаційний огляд стану тероризму в Європейському Союзі за 2025 рік, підготовлений на основі кількісних і якісних даних держав-членів щодо терористичних атак і арештів, а також інформації Євроюсту щодо вироків і покарань за терористичні злочини. Звіт спирається на гармонізоване, але не уніфіковане правове підґрунтя: Директива (ЄС) 2017/541 про боротьбу з тероризмом встановлює лише мінімальні спільні стандарти визначення терористичних злочинів, тоді як класифікація конкретних діянь як терористичних залишається прерогативою національного законодавства держав-членів. Це означає, що наведена в звіті статистика відображає не уніфіковану, а гармонізовану на мінімальному рівні практику кваліфікації, що є суттєвим методологічним застереженням для будь-якого порівняльного аналізу даних звіту.

У 2025 році держави-члени повідомили про 45 терористичних атак (22 завершені, 20 відвернені, 3 невдалі) у 10 державах-членах - це менше, ніж 58 атак у 2024 році (34 завершені),

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-TE-SAT-2026.pdf

однак кількість арештів за злочини, пов'язані з тероризмом, продовжила зростати - 486 осіб у 21 державі-члені (порівняно з 449 у 2024 році та 426 у 2023 році). Джихадизм лишається домінантною ідеологічною категорією, на яку припадає 24 атаки (зокрема 9 завершених - більше, ніж 6 у 2024 році) та 347 арештів, тобто майже 71% усіх арештів за 2025 рік. Європол прямо застерігає, що зниження кількості атак на тлі зростання арештів не можна інтерпретувати як послаблення загрози - радше це може свідчити про ефективність превентивної роботи правоохоронних органів, тоді як масштаб непроявленої (у вигляді атак) активності залишається невідомим через велику кількість незавершених розслідувань, які не враховані у наведеній статистиці.

Найбільш значущим розділом звіту є фіксація розмивання ідеологічних меж класичних категорій тероризму (джихадизм, право- та ліворадикальний тероризм, етнонаціоналістичний і сепаратистський тероризм). Окрім усталених ідеологій, звіт виокремлює нові дестабілізаційні феномени: антиінституційні групи, що живляться конспірологічними наративами і підривають довіру до демократичних інституцій; гібридних акторів, які інструменталізують проксі для скоєння терористичних злочинів у межах довгострокової стратегії кумулятивної дестабілізації, а не одноразової масштабної атаки; і нігілістичний насильницький екстремізм, уособлений мережею The Com - децентралізованою онлайн-екосистемою з трьома гілками (Cyber Com - DDoS-атаки, доксинг, свотинг, програми-вимагачі; (S)extortion Com - грумінг і сексуальне вимагання переважно неповнолітніх жертв; Offline Com - підпали, напади з ножем, вбивства). Показово, що окремі підгрупи The Com уже визнані терористичними організаціями за межами ЄС (Канада - грудень 2025 року, Велика Британія - червень 2025 року), тоді як усередині Союзу кваліфікація відповідних інцидентів залишається неоднорідною між державами-членами.

Розділ звіту, присвячений фінансуванню тероризму, фіксує співіснування традиційних і новітніх методів акумулювання та переміщення коштів. Джерелами фінансування залишаються заробітна плата, пожертви, краудфандингові кампанії, продаж пропагандистських матеріалів, вхідні внески на заходи, крадіжки, продаж нелегальних товарів і створення фіктивних неурядових організацій, причому кошти надходять як із легальних, так і з нелегальних джерел. Що стосується переміщення та зберігання коштів, традиційні канали (системи хавала, готівкові кур'єри) співіснують із новішими технологіями - криптоактивами та трансфером вартості через ігрові платформи; окремо зазначено, що самі провайдери хавали розширюють спектр своїх послуг, додаючи онлайн-сервіси, що ускладнює традиційні підходи до моніторингу цього каналу. Ця констатація має пряме значення для оновлення типологій фінансового моніторингу, оскільки традиційні індикатори підозрілості, орієнтовані на готівкові операції, дедалі менше відповідають фактичній структурі каналів фінансування тероризму.

Окремої уваги заслуговує зафіксоване звітом зловживання штучним інтелектом - від використання генеративних інструментів для створення дипфейків, мемів і пропагандистських матеріалів (переважно у формі «квазі-летального» контенту, оскільки більшість AI-інструментів навчені не генерувати прямо протиправний контент) до застосування чат-ботів на основі великих мовних моделей для оптимізації вербування й пропаганди та проведення попереднього дослідження перед підготовкою атак. Паралельно терористичні актори продовжують використовувати наскрізно зашифровані месенджери, VPN, darknet-браузери та децентралізовані блокчейн-сервіси, причому останні є особливо проблемними для правоохоронних органів, оскільки децентралізована архітектура унеможливлює повне видалення контенту - користувачі створюють резервні та фіктивні канали й псевдоніми, які автоматично «відновлюються» в разі видалення одного з примірників.

Звіт детально аналізує вплив геополітичного контексту на радикалізацію в межах ЄС, насамперед конфлікту на Близькому Сході. Атака ХАМАС 7 жовтня 2023 року та подальша ескалація конфлікту між Ізраїлем, Іраном і його проксі-мережею (так звана «вісь опору» - Хезболла, ХАМАС, Ансар Аллах та угруповання в Іраку) продовжують живити антисемітські наративи, що об'єднують акторів різних ідеологічних таборів. Знаковою подією 2026 року

стало офіційне визнання Радою ЄС Корпусу вартових ісламської революції Ірану (КВІР) терористичною організацією рішенням (ЗЗБП) 2026/421 від 19 лютого 2026 року, після чого Європол у лютому-квітні 2026 року координував операцію проти пропагандистської онлайн-екосистеми КВІР. Звіт також окремо фіксує, що війна росії проти України продовжує фігурувати в наративах право-радикальних акторів (хоча й менш помітно, ніж у попередні роки), і застерігає щодо ризиків використання війни для набуття екстремістських навичок, незаконного обігу зброї та експлуатації міграційних потоків.

Висновки:

- **Межі між класичними ідеологіями (джихадизм, ультраправі чи ультраліві рухи) розмиваються.** Зростає загроза від антиінституційних груп, нігілістичного екстремізму та гібридних акторів, які використовують кримінальні елементи як "проксі" для системної дестабілізації суспільства. Такі зловмисники часто не мають чіткої політичної мети, окрім поширення хаосу.
- **Більшість терористичних актів та змов планується і здійснюється терористами-одинаками або невеликими самоорганізованими осередками**. Вони найчастіше використовують прості, але доступні та ефективні методи (холодна зброя, підпали тощо). Відсутність розгалуженої мережі зв'язків критично ускладнює їхнє завчасне виявлення традиційними методами стеження.
- **Інтернет залишається головним інструментом не лише для споживання екстремістського контенту, але й для швидкого залучення до закритих спільнот.** Цифровий простір прискорює процеси радикалізації та дозволяє здійснювати приховану оперативну координацію між однодумцями без необхідності фізичних зустрічей.
- **Складний геополітичний контекст та збройні конфлікти за межами ЄС безпосередньо впливають на внутрішню безпеку.** Вони розпалюють екстремістські настрої, сприяють вербуванню та призводять до цілеспрямованих загроз проти конкретних спільнот.

Статистика вироків, надана Євроюстом, демонструє показову розбіжність, яка варта окремого коментаря: у 2025 році судові провадження, завершені у 21 державі-члені, дали 406 обвинувальних вироків і 99 виправдань, причому рівень засудження суттєво відрізняється залежно від ідеологічної категорії - 88% для джихадистського й право-радикального тероризму та лише 41% для ліво-радикального й анархістського тероризму. Це не обов'язково свідчить про різну тяжкість доказової бази, радше вказує на структурні відмінності в характері справ (ліво-радикальні дії частіше кваліфікуються як напади на майно без постраждалих, що потенційно ускладнює доведення терористичного мотиву за стандартами національного кримінального права) і має враховуватися аналітиками, які використовують дані про вироки як проксі-показник ефективності протидії тероризму за окремими типологіями.

Загалом звіт EU TE-SAT 2026 підтверджує тезу, що ефективна протидія фінансуванню тероризму дедалі більше вимагає виходу за межі традиційної парадигми моніторингу готівкових потоків і фокусування на гібридних каналах - поєднанні хавала-мереж з онлайн-сервісами, криптоактивів, ігрових платформ і фіктивних благодійних структур, - а також врахування динамічного геополітичного контексту, зокрема ролі проксі-мереж держав, визнаних джерелами дестабілізації.

Золото в резервах центральних банків: стратегічні міркування, ринкові ризики та практичні рекомендації МВФ [2]

Міжнародний валютний фонд оприлюднив методологічну нотатку присвячену відродженню ролі золота в резервах центральних банків та практичним рекомендаціям для управителів резервів.

Частка монетарного золота в міжнародних резервах зросла з 10% у січні 2019 року до понад 22% станом на серпень 2025 року, однак це зростання зумовлене переважно переоцінкою вартості на тлі стрімкого зростання цін на золото, а не масштабним фізичним накопиченням: за 2018–2025 роки ринкова вартість золотих резервів центральних банків зросла приблизно на 3,2 трлн дол. США (+268%), тоді як сукупний обсяг накопиченого золота зріс лише на 8,5%, причому майже дві третини приросту вартості припадає на центральні банки, які взагалі не збільшували фізичний обсяг своїх запасів.

Автори застерігають, що властивості золота як інструменту хеджування є умовними й режимозалежними: золото послідовно демонструє надійний захист лише від процентного ризику, тоді як його захисні властивості проти обвалів на ринках акцій, інфляційних шоків і геополітичних потрясінь суттєво послабилися після пандемії – кореляція золота з S&P 500, яка була близькою до нуля чи від'ємною до пандемії, стала додатною після 2022 року. Ба більше, золото не демонструє надійних властивостей «безпечної гавані» під час екстремальних подій. Методологічно значущим є висновок про ліквідність: попри значні обсяги торгів на лондонському ринку злитків (близько 134 млрд дол. США щоденно), золото забезпечує суттєво менш ефективну ліквідність, ніж свідчить його номінальна ринкова вартість, тому нотатка рекомендує застосовувати VaR-методологію для розрахунку вартості золота в ліквідній транші резервів – на рівні 6–12% залежно від ринкового режиму, що приблизно вдвічі перевищує стандартну вартість для 10-річних казначейських облігацій США (4% за базельською методологією).

Окремої уваги заслуговує визначена нотаткою властивість золота слугувати інструментом хеджування санкційних ризиків – властивість, що набула актуальності на тлі геополітичної фрагментації та розширення застосування фінансових санкцій. На відміну від валютних резервів, розміщених на рахунках чи в цінних паперах, що підпадають під юрисдикцію країн-емітентів, золото, яке зберігається поза міжнародною фінансовою системою, не є зобов'язанням жодного іноземного суверена і тому в принципі захищене від заморожування активів чи платіжних обмежень. Водночас автори підкреслюють, що ефективність такого захисту прямо залежить від місця зберігання: що ближче золото зберігається до внутрішніх сховищ країни-власника, то сильніший захист від зовнішнього юридичного чи операційного втручання, але то нижча його негайна придатність до використання – фізично розміщене у внутрішніх сховищах золото стає практично повністю неліквідним для потреб валютних інтервенцій чи міжнародних платежів. Це методологічне спостереження безпосередньо пояснює логіку нарощування золотих резервів країнами, що перебувають під санкційним тиском або очікують його посилення.

Значну частину нотатки присвячено ризикам програм внутрішньої закупівлі золота центральними банками (domestic gold purchases, DGP), які автори прямо застерігають не вважати панацеєю. Ключове методологічне розрізнення проведено між закупівлею монетарного золота (яке вже відповідає стандартам резервного активу і придатне до негайного продажу) та немонетарного золота (що потребує афінажу, пробірного аналізу й сертифікації перед визнанням резервним активом) – останнє створює істотно вищі ризики для мандата, врядування, балансу, операційної спроможності та імплементації монетарної політики центрального банку, оскільки за своєю природою нагадує квазіфіскальну діяльність, невластиву традиційним функціям центрального банку.

[2] https://www.imf.org/-/media/files/publications/imf-notes/2026/english/insea2026007.pdf

Методологічно найважливішим для сфери фінансового моніторингу є визначення нотаткою ризиків фінансової доброчесності (financial integrity risks) як окремого й системно недооціненого виміру програм DGP. Золото – особливо здобуте кустарним і дрібномасштабним видобутком або отримане через складні посередницькі ланцюги – може використовуватися для легалізації доходів, одержаних злочинним шляхом, або для обходу санкційних і податкових зобов'язань. Коли центральний банк купує золото безпосередньо у внутрішніх постачальників, він бере на себе відповідальність за забезпечення повноцінного контролю у сфері ПВК/ФТ, включно з належною перевіркою клієнтів, верифікацією кінцевих бенефіціарних власників, моніторингом операцій і веденням обліку, що забезпечує перевірюваний ланцюг від джерела видобутку до резервного активу; нездатність запровадити такий контроль створює ризик включення незаконно набутої вартості до офіційних резервів держави з потенційно серйозними репутаційними, юридичними та фінансовими наслідками для центрального банку.

Висновки:

- **Різке зростання частки золота в резервах центробанків останнім часом зумовлене насамперед стрімким зростанням його ринкової ціни, а не масштабним фізичним накопиченням.** Через це покращення загальних показників достатності резервів може бути ілюзорним. Ба більше, на практиці золото забезпечує значно меншу ефективну ліквідність, ніж його номінальна ринкова вартість.
- **Хоча золото не несе кредитного ризику і може діяти як захисний актив, воно є волатильним.** Дослідження показують, що після пандемії COVID-19 його властивості як "тихої гавані" та інструменту хеджування проти інфляції, падіння акцій чи геополітичних шоків значно послабилися. Воно не здатне надійно замінити ліквідні іноземні активи у кризових ситуаціях.
- **Практика купівлі золота на внутрішньому ринку (особливо немонетарного золота, яке ще потребує афінажу та монетизації) створює серйозні ризики:** проблеми з прозорістю, операційні загрози, викривлення балансу та перешкоди для реалізації монетарної політики.

У розділі, підготовленому Правовим департаментом МВФ, сформульовано конкретні законодавчі запобіжники: законодавство має в принципі забороняти центральним банкам здійснювати програми закупівлі немонетарного, неафінованого золота як квазіфіскальну діяльність; якщо політичні обставини унеможливлюють відмову від уже запущеної програми, вона має отримати чітку законодавчу підставу з вузько визначеною метою, ціновими правилами зі знижками на афінаж і логістику, кількісними лімітами експозиції, своєчасною монетизацією, правилами розподілу збитків через механізми прибуткового розподілу та рекапіталізації центрального банку, а також обов'язковою прозорістю – регулярною звітністю перед парламентом і міністерством фінансів та незалежним зовнішнім аудитом.

Хоча Україна не є значним виробником золота і Національний банк наразі не здійснює програм внутрішньої закупівлі золота, методологічний апарат нотатки має пряме прикладне значення для української системи ПВК/ФТ/ФР у двох аспектах. По-перше, задокументована властивість золота слугувати інструментом обходу заморожування активів безпосередньо стосується методології відстеження та прогнозування поведінки резервів росії в умовах санкційного тиску. По-друге, викладена структура контролю фінансової доброчесності – від верифікації постачальника до забезпечення перевірюваного ланцюга походження активу – є готовою методологічною основою для оцінки ризиків відмивання коштів через операції з дорогоцінними металами, включно з ризиками, пов'язаними з неформальними транскордонними потоками золота в умовах війни.

Як Італія переосмислює боротьбу з фінансовими злочинами [3]

Минулий рік став періодом значної трансформації ландшафту фінансових злочинів, на який глибокий вплив мали як технологічні інновації, так і геополітична нестабільність. Документ, опублікований Банком Італії та Італійським ПФР (UIF), малює картину динамічної боротьби, де традиційні методи відмивання грошей еволюціонують, адаптуючись до цифрової ери, а UIF, у свою чергу, модернізує свої підходи, роблячи акцент на технологічному лідерстві та міжнародній співпраці. Центральна тема звіту – це не просто статистика зростання чи спаду кількості підозрілих операцій, а якісна зміна характеру загроз, які стають все більш складними, транснаціональними та технологічно витонченими.

У 2025 році UIF зафіксував відновлення зростання кількості повідомлень про підозрілі операції, яке зросло на 11,5% порівняно з попереднім роком, що становить загалом 162,059 звітів. Це зростання, однак, не було рівномірним для всіх категорій підзвітних суб'єктів. Основний приріст забезпечили банки та Пошта Італії, де кількість звітів зросла на 26,8%, що значною мірою пов'язано з діяльністю нових, переважно онлайн-банків. Одночасно з цим спостерігалося значне скорочення на 20,3% повідомлень від інших фінансових посередників, зокрема електронних грошових установ та платіжних інститутів. Це може свідчити про перерозподіл ринку фінансових послуг на користь більш традиційних, але технологічно оновлених гравців. Найбільш вражаюче зростання, на 77,6%, продемонстрували не фінансові оператори, такі як торговці золотом та дорогоцінними металами (зростання на 96,6%) та оператори з віртуальними валютами (зростання на 85,1%). Це чітко вказує на посилену увагу до цих секторів, які, очевидно, стають все більш привабливими для зловмисників. Внесок професіоналів, зокрема нотаріусів, залишився стабільним, а ось від публічних адміністрацій надійшло на 58,8% менше повідомлень, що може вказувати на проблеми у виконанні ними своїх зобов'язань у сфері ПВК/ФТ.

Одним з ключових висновків звіту є визнання того, що фінансові та технологічні інновації стали подвійним мечем. З одного боку, такі інструменти, як криптоактиви, віртуальні IBAN, віртуальні карти та небанківські банкомати, ускладнюють відстеження фінансових потоків. З іншого боку, вони розширюють масштаби та ускладнюють структуру злочинної діяльності. UIF відзначає значне зростання повідомлень, пов'язаних з шахрайством та комп'ютерним шахрайством, яких у 2025 році було близько 31,600, тобто майже п'ята частина від загального потоку. У звіті детально описуються різноманітні схеми, від психологічних маніпуляцій жертвами до використання підроблених документів, створених за допомогою штучного інтелекту, для відкриття рахунків. Крім того, аналітики UIF виявили, що організована злочинність все активніше використовує платформи FinTech та криптовалюти для відмивання коштів, отриманих від ухилення від сплати податків, зловживання державними коштами та корупції. Складність полягає в тому, що злочинці все частіше використовують децентралізовані фінанси (DeFi), смарт-контракти та стейблкоїни, які часто прив'язані до долара США, що дозволяє їм переміщувати капітали без необхідності конвертації у фіатні валюти, створюючи додатковий рівень анонімності. Особливу тривогу викликає використання стейблкоїнів, які, на відміну від біткоїна, не схильні до різких коливань курсу, що робить їх ідеальним інструментом для збереження та переміщення незаконних доходів.

Звіт не оминає увагою і тему фінансової вразливості підприємств. Дослідження, проведене UIF спільно з Університетом Бокконі, демонструє прямий зв'язок між погіршенням кредитоспроможності компанії та підвищеним ризиком її проникнення з боку організованої злочинності. У ситуації, коли банки обмежують кредитування, злочинні угруповання виступають у ролі «кредитора останньої інстанції», дозволяючи фінансово слабким компаніям виживати. Це не тільки спотворює ринкові механізми та знижує продуктивність, але й створює ілюзію економічної активності, за якою ховається злочинний вплив. Таким чином, фінансове здоров'я підприємств стає не лише питанням бізнесу, а й питанням національної безпеки,

[3] https://uif.bancaditalia.it/pubblicazioni/rapporto-annuale/2026/UIF-Annual-Report-2025.pdf?language_id=1

оскільки створює сприятливе середовище для мафіозних структур. Крім того, в аналітичній частині підкреслюється, що організована злочинність, зокрема така могутня, як мафія 'Ndrangheta, використовує свої величезні транснаціональні мережі не лише для традиційних злочинів, але й для впливу на геополітичні процеси, що вимагає абсолютно нового рівня розуміння та реагування з боку фінансової розвідки.

Діяльність UIF у 2025 році не обмежувалася пасивним збором даних. Агентство активно вдосконалювало свої аналітичні потужності. Ключовим напрямком стало впровадження передових технологій, включаючи експерименти з генеративним штучним інтелектом (великі мовні моделі). Ці моделі використовувалися для вилучення структурованих даних з текстових звітів, узагальнення інформації з транскордонних повідомлень та навіть для створення помічника з питань декларування золота, що дозволило скоротити час відповідей на запити приблизно на 30%. Одночасно з цим UIF посилив і контроль за якістю інформації, яку надають звітувачі, впроваджуючи нові «зворотні картки» для оцінки їхньої роботи та наголошуючи на необхідності збереження людського контролю над автоматизованими системами моніторингу. Аналіз виявив, що некритичне використання штучного інтелекту самими фінансовими установами для виявлення підозрілих транзакцій може призводити до хибних спрацьовувань та стандартизованих, малозмістовних звітів. Таким чином, UIF виступає за збалансований підхід, де технології є інструментом, але не замінюють професійне судження.

Висновки:

- **Домінування цифрового шахрайства:** У 2025 році відбулося вибухове зростання підозрілих операцій, пов’язаних з комп’ютерним шахрайством та фішинговими. Це свідчить про те, що кіберзлочинність стала головним драйвером зростання фінансових правопорушень, витісняючи на другий план традиційні схеми.
- **Еволюція інструментів відмивання:** Відбувається остаточний перехід від переважно готівкових розрахунків до складних цифрових екосистем. Криптоактиви, віртуальні IBAN, стейблкоїни та платформи DeFi все частіше використовуються для приховування походження коштів, що робить класичні методи фінансового моніторингу недостатньо ефективними.
- **Критична роль фінансової вразливості:** Дослідження UIF підтвердило прямий зв'язок між кредитними труднощами компаній та ризиком їх поглинання організованою злочинністю. Злочинні угруповання виступають «кредиторами останньої інстанції», що дозволяє їм отримувати контроль над реальним сектором економіки, спотворюючи ринкову конкуренцію.
- **Пріоритет технологічного суверенітету:** UIF робить ставку на власні технологічні розробки, зокрема на використання великих мовних моделей (LLM) для аналізу даних. Це дозволяє автоматизувати рутинні процеси, підвищити якість аналітики та значно скоротити час реагування на запити, зберігаючи при цьому критичний людський контроль.

Геополітичний вимір діяльності UIF у 2025 році набув особливої ваги через посилення міжнародних санкцій, зокрема проти росії, білорусі та Ірану. Відновлення санкцій ООН проти Ірану призвело до різкого збільшення обсягу заморожених активів, загальна сума яких зросла до 340,4 млн євро, що було зумовлено переважно активами, пов'язаними з Іраном. UIF не лише забезпечувала імплементацію цих санкцій, але й активно виявляла та блокувала активи, співпрацюючи з Комітетом з фінансової безпеки. Важливо, що у 2025 році Італія імплементувала європейську директиву, яка криміналізує порушення та ухилення від міжнародних фінансових санкцій. Це робить боротьбу з обходом санкцій не лише адміністративною, а й кримінальною справою.

Підсумовуючи, звіт UIF за 2025 рік демонструє, що італійська фінансова розвідка перебуває на передовій боротьби з новим поколінням фінансових злочинів. Вона реагує на виклики, що швидко змінюються, інвестуючи в аналітичні технології, поглиблюючи міжнародну співпрацю та активно взаємодіючи з національними та європейськими регуляторами. Головним висновком є те, що ефективний протидія фінансовим злочинам у XXI столітті вимагає не просто більшої кількості регуляцій, а глибокого розуміння технологій, тісної міжнародної координації та постійної адаптації до нових, часто непередбачуваних, злочинних схем, які дедалі більше стирають межі між легальною та нелегальною економікою.

Кібершахрайські центри та торгівля людьми: фінансові потоки, примусова злочинність і міжнародні механізми протидії [4]

Типологічний звіт Азійсько-Тихоокеанської групи з протидії відмиванню коштів (APG) присвячений комплексному дослідженню центрів кібершахрайства як однієї з найбільш динамічних форм сучасної транснаціональної організованої злочинності. Документ розкриває нерозривний зв'язок між масштабним онлайн-шахрайством, торгівлею людьми з метою примусової злочинної діяльності, корупцією, приховуванням бенефіціарної власності та відмиванням доходів, одержаних злочинним шляхом. Основний висновок авторів полягає в тому, що центри кібершахрайства не можна розглядати виключно як шахрайські кол-центри або сукупність окремих цифрових злочинів. Насправді вони функціонують як складні кримінальні підприємства, що мають власну фізичну, кадрову, корпоративну, технологічну та фінансову інфраструктуру, працюють одночасно у кількох юрисдикціях та використовують легальні фінансові й комерційні системи для підтримання незаконної діяльності. У межах такої моделі одночасно існують дві великі категорії потерпілих: люди, яких обманом, примусом або через боргову залежність змушують здійснювати шахрайські операції, та особи з різних країн світу, у яких ці працівники під контролем організованих злочинних груп виманюють гроші.

Звіт був підготовлений на основі типологічного проєкту APG, реалізованого під спільним керівництвом Індонезії та Управління ООН з наркотиків і злочинності. Дослідження поєднує огляд відкритих джерел, відповіді державних органів і приватного сектору, інформацію компаній блокчейн-аналітики та постачальника послуг у сфері віртуальних активів, експертні інтерв'ю, матеріали тематичних обговорень і значну кількість практичних кейсів. В опитуванні взяли участь державні органи сімнадцяти юрисдикцій і 156 представників приватного сектору, переважно банків, платіжних установ та інших суб'єктів фінансового моніторингу. Завдяки цьому звіт не обмежується загальним описом явища, а детально аналізує механізми функціонування шахрайських центрів, способи вербування людей, профілі потерпілих, джерела доходів, маршрути переміщення коштів, типології відмивання, індикатори підозрілої діяльності та проблеми, з якими стикаються правоохоронні органи й підрозділи фінансової розвідки. Водночас автори визнають, що реальні масштаби явища можуть бути значно більшими, оскільки багато держав не ведуть окремої статистики щодо доходів, кримінальних проваджень, повідомлень про підозрілі операції або арештованих активів, безпосередньо пов'язаних із центрами кібершахрайства, включаючи такі випадки до ширших категорій кіберзлочинності, шахрайства, торгівлі людьми або організованої злочинності.

У документі центри кібершахрайства описуються як вертикально інтегровані кримінальні екосистеми, у яких різні етапи злочинного процесу контролюються однією мережею або групою взаємопов'язаних організацій. До цієї екосистеми можуть входити рекрутингові агентства, посередники з оформлення документів і перевезення людей, власники або орендарі нерухомості, охоронні структури, оператори телекомунікацій, IT-фахівці, адміністратори

[4] https://apgml.org/sites/default/files/2026-07/APG%20Cyber%20Scam%20Hubs%20%26%20Human%20Trafficking%20Report%202026.pdf

підроблених інвестиційних платформ, організатори мереж грошових мулів, нелегальні надавачі платіжних послуг, нерегульовані криптовалютні брокери, підставні юридичні особи та професійні посередники. Кримінальна мережа може самостійно забезпечувати розроблення шахрайських сценаріїв, придбання персональних даних потенційних жертв, створення фальшивих сайтів і мобільних застосунків, комунікацію через соціальні мережі та месенджери, приймання платежів, їх швидке розпорошення між рахунками, конвертацію у віртуальні активи та подальше інвестування у нерухомість, дорогі товари або нові кримінальні проєкти. Така структура дозволяє організаторам не лише отримувати надприбутки, а й швидко відновлювати діяльність після окремих правоохоронних операцій, змінюючи юридичні особи, рахунки, місця розташування та технологічні платформи.

Особливу увагу у звіті приділено умовам, які дозволяють центрам кібершахрайства виникати та функціонувати протягом тривалого часу. Однією з головних передумов є використання територій із недостатнім регуляторним та правоохоронним контролем. Йдеться про спеціальні економічні зони, вільні торговельні зони, прикордонні райони, території з нестабільною безпековою ситуацією, колишні гральні комплекси та інші простори, де повноваження різних державних органів є нечіткими або реалізуються непослідовно. Такі території часто мають розвинену інтернет-інфраструктуру, значні площі для розміщення працівників, готелі, казино, офісні приміщення та зручний доступ до міжнародних транспортних маршрутів. Найбільш відомі центри зосереджені у прикордонних районах М’янми, Камбоджі, Лаоської Народно-Демократичної Республіки та Таїланду, однак звіт також фіксує поширення подібних операцій в інших частинах Азії, Африки, Південної Америки та Тихоокеанського регіону. За результатами опитування, більшість державних респондентів вказували на міські центри та прикордонні території як на основні місця розташування таких комплексів.

Історично значна частина цієї інфраструктури сформувалася на основі казино, готелів і підприємств офшорного грального бізнесу, які втратили попередні джерела доходів під час пандемії COVID-19 та після посилення державних обмежень щодо азартних ігор. Організовані злочинні групи переобладнали приміщення, телекомунікаційні мережі, системи безпеки й платіжну інфраструктуру для здійснення масового онлайн-шахрайства. Таким чином, перехід від незаконного грального бізнесу до кібершахрайства не означав створення принципово нових кримінальних структур, а став адаптацією вже існуючих мереж до більш прибуткової та технологічно гнучкої діяльності. Показовим прикладом ефективного державного втручання стало запровадження на Філіппінах законодавчої заборони діяльності офшорних операторів азартних ігор, що суттєво вплинуло на поширеність пов’язаних із ними шахрайських комплексів. Водночас автори застерігають, що ліквідація великих центрів може спричинити не повне припинення діяльності, а її переміщення до інших країн або децентралізацію на менші, менш помітні підрозділи.

Ще одним базовим елементом функціонування шахрайських центрів є використання складних корпоративних структур для приховування реальних організаторів і бенефіціарів. Злочинні групи створюють багаторівневі ланцюги володіння, підставні компанії, компанії-оболонки, фіктивні рекрутингові, аутсорсингові, IT-, інвестиційні та гральні підприємства, залучають номінальних директорів і акціонерів. Через такі юридичні особи орендується або купується нерухомість, оформлюються дозволи, відкриваються рахунки, укладаються договори з постачальниками послуг доступу до мережі Інтернет, електроенергії та інших послуг, здійснюється формальне працевлаштування персоналу і переміщуються злочинні доходи. За даними опитування APG, 65% державних респондентів назвали складні корпоративні структури одним із головних способів відмивання коштів, а 76% відзначили участь професійних сприячів. Серед них згадуються юристи, бухгалтери, секретарі компаній, надавачі корпоративних і трастових послуг та інші представники визначених нефінансових установ і професій. Звіт наголошує, що такі особи можуть діяти як свідомо, так і через недостатню перевірку клієнтів, однак у будь-якому випадку їхня участь у створенні непрозорих структур суттєво ускладнює встановлення КБВ і відстеження активів. Саме тому автори підкреслюють необхідність ефективного ризик-орієнтованого нагляду за

професійними посередниками та забезпечення доступу компетентних органів до точної, актуальної і перевіреної інформації про бенефіціарну власність.

Важливим чинником, без якого центри кібершахрайства часто не могли б працювати у великих масштабах, є корупція. Організовані злочинні групи можуть підкуповувати місцевих посадовців, працівників поліції, прикордонних і міграційних органів, ліцензійних служб, осіб, відповідальних за земельні питання, будівництво та телекомунікації. Це дозволяє отримувати дозвільні документи, забезпечувати безперешкодне переміщення працівників, уникати перевірок, отримувати попередження про правоохоронні операції або переміщувати центр до іншого району до початку втручання держави. Про корумпованість або співучасть місцевих органів влади як про суттєву умову діяльності шахрайських центрів повідомили 41% опитаних членів APG. Приклад філіппінського оператора офшорних азартних ігор, пов'язаного з політично значущою особою, демонструє, як романтичні та інвестиційні шахрайства, торгівля людьми, незаконний гральний бізнес, придбання нерухомості, використання підставних компаній і рух коштів через віртуальні активи можуть бути об'єднані в одну кримінально-фінансову систему. У цьому випадку фінансовий аналіз виявив різке зростання обсягів операцій після початку діяльності гральних компаній, численні перекази між пов'язаними рахунками, великі зняття коштів після депозитів, використання транзитних рахунків, невідповідності у документах належної перевірки клієнта, придбання нерухомості та створення підприємств, пов'язаних із дорогими автомобілями й розвитком нерухомості.

Центральною складовою кримінальної моделі є торгівля людьми з метою примусової злочинної діяльності. Потенційних працівників здебільшого вербують через соціальні мережі, месенджери, онлайн-платформи з працевлаштування та неформальні особисті контакти. Їм пропонують роботу у сфері обслуговування клієнтів, цифрового маркетингу, IT, онлайн-торгівлі, криптовалют, грального бізнесу або технічної підтримки. Вакансії часто передбачають високу заробітну плату, безоплатне проживання, харчування, оплату авіаквитків та оформлення документів, але при цьому не містять чітких вимог до досвіду, не передбачають повноцінної співбесіди або вимагають швидкого переїзду. Для підвищення довіри використовуються фальшиві сайти компаній, професійно оформлені профілі, підроблені трудові договори та корпоративні електронні адреси. За результатами опитування, неправдиві пропозиції роботи або бізнес-можливостей були одним із найпоширеніших способів вербування.

Організатори цілеспрямовано шукають молодих дорослих, студентів, безробітних, трудових мігрантів, осіб із фінансовими труднощами, знанням іноземних мов, IT-навичками, досвідом використання соціальних мереж або розумінням віртуальних активів. Після прибуття до країни призначення у людей вилучають паспорти й телефони, обмежують можливість залишати територію комплексу, нав'язують борги за транспорт, проживання, харчування, оформлення документів або «навчання». Працівників змушують підписувати договори, умови яких вони не розуміють або не можуть реально оскаржити, а строк роботи може односторонньо продовжуватися. Їм встановлюють норми щодо кількості контактів, залучених жертв і отриманих платежів. Невиконання таких норм може призводити до фінансових штрафів, погіршення умов утримання, погроз або інших форм примусу. У деяких випадках людей продають або передають між різними комплексами та кримінальними синдикатами як робочу силу, що створює своєрідний внутрішній ринок експлуатованих осіб.

Звіт особливо наголошує на складності правового статусу таких працівників. Формально вони можуть бути безпосередніми виконавцями шахрайських операцій, спілкуватися з потерпілими, створювати фальшиві акаунти, надсилати інструкції щодо переказу коштів або управляти підробленими платформами. Однак значна частина цих осіб діє під примусом і фактично є потерпілими від торгівлі людьми. Нерозпізнавання цього статусу може призводити до їх затримання, кримінального переслідування або депортації без належного розслідування обставин експлуатації. Тому APG підтримує орієнтований на потерпілих підхід, який передбачає ранню ідентифікацію ознак примусу, координацію між правоохоронними,

міграційними, соціальними та фінансовими органами, а також розмежування організаторів, добровільних учасників і людей, змушених до вчинення злочинів.

Профіль жертв торгівлі людьми постійно змінюється відповідно до еволюції шахрайських схем. Коли злочинні групи починають орієнтуватися на нову країну або мовну аудиторію, їм потрібні працівники, які знають місцеву мову, культурні особливості, стиль спілкування та фінансові звички потенційних потерпілих. Це сприяє розширенню географії вербування. Водночас автоматизація частини комунікацій за допомогою штучного інтелекту може поступово зменшувати потребу у великій кількості операторів, але не усуває торгівлю людьми повністю, оскільки люди все ще потрібні для персоналізованого спілкування, контролю за платформами, фінансових операцій і обслуговування технологічної інфраструктури. Автори також звертають увагу на недостатність довгострокової підтримки репатрійованих осіб. Після повернення додому вони можуть залишатися без засобів існування, психологічної, правової та соціальної допомоги, що підвищує ризик повторного вербування.

Іншою масштабною групою потерпілих є особи, у яких виманюють кошти. За даними звіту, діяльність центрів кібершахрайства охопила жертв у понад ста юрисдикціях. Основними цілями є громадяни країн із відносно високими доходами, значними приватними заощадженнями, розвиненою банківською системою, доступом до кредитування, пенсійних накопичень та віртуальних активів. Водночас єдиного профілю потерпілого не існує, оскільки різні типи шахрайства орієнтуються на різні категорії населення. Інвестиційні шахрайства спрямовуються на осіб, які мають заощадження або шукають високодохідні можливості; романтичні схеми – на людей, які прагнуть емоційного зв’язку; шахрайство з працевлаштуванням і онлайн-завданнями – на тих, хто шукає додатковий заробіток; схеми з видаванням себе за державних службовців – на осіб, які можуть злякатися кримінальної відповідальності, податкової заборгованості або проблем із міграційним статусом.

Найбільш поширеними є фіктивні інвестиційні схеми, зокрема шахрайство, засноване на поступовому встановленні довірчих відносин із потерпілим. Злочинці протягом тривалого часу формують у нього довіру, після чого переконують вкладати дедалі більші суми коштів через підроблені торговельні, інвестиційні або криптовалютні платформи. Потерпілому демонструють фальшивий особистий кабінет, графіки прибутковості та вигадані успішні операції. На початковому етапі йому можуть навіть повернути невелику суму, щоб підтвердити нібито надійність інвестиції. Після цього розмір платежів поступово збільшується, а при спробі вивести кошти з’являються вимоги сплатити податок, комісію, страховий депозит, витрати на верифікацію або розблокування рахунку. Після припинення платежів зв’язок із шахраями зникає.

Романтичні шахрайства будуються на створенні підробленої емоційної близькості через соціальні мережі та застосунки для знайомств. Після формування довіри шахрай повідомляє про фінансову проблему, просить допомогти у надзвичайній ситуації або пропонує вигідну інвестиційну можливість. У такий спосіб романтична схема нерідко перетворюється на інвестиційне шахрайство. Поширеними є також схеми з видаванням себе за працівників банків, поліції, податкових або міграційних органів, членів родини чи знайомих. Шахраї можуть використовувати викрадені персональні дані, підроблені документи, телефонні номери, що імітують офіційні контакти, клонування голосу та відеодіпфейки. Окремою моделлю є шахрайство за принципом «завдання – винагорода – повернення коштів», коли людині пропонують виконувати прості онлайн-завдання, наприклад переглядати рекламу або оцінювати товари. Перші невеликі виплати створюють довіру, після чого потерпілого змушують переказувати дедалі більші суми для доступу до нових завдань або «розблокування» зароблено прибутку.

Особливо небезпечною є повторна віктимізація. Після втрати коштів із потерпілими можуть зв’язуватися особи, які представляються спеціалістами з повернення активів, працівниками правоохоронних органів, юристами або компаніями блокчейн-аналітики. Вони стверджують, що знайшли викрадені кошти та можуть їх повернути після сплати комісії, податку або

адміністративного збору. Насправді це є продовженням шахрайської схеми, побудованої на використанні вразливості людини, яка вже зазнала фінансових збитків.

Масштаби доходів центрів кібершахрайства оцінюються у десятки мільярдів доларів США на рік, хоча точне визначення обсягів ускладнюється прихованим характером операцій, транскордонністю потоків і недостатньою статистикою. Доходи формуються з кількох взаємопов'язаних джерел. Найбільшу частину становлять безпосередні платежі жертв шахрайства. Додатково кримінальні групи отримують кошти за вербування і транспортування людей, продаж або передавання працівників між комплексами, штучні борги, утримання заробітної плати та штрафи за невиконання встановлених норм. Родичів потерпілих можуть змушувати сплачувати викуп за звільнення, причому платежі можуть здійснюватися як у фіатних коштах, так і у стейблкоїнах. У деяких випадках замість грошей від утримуваної особи вимагають завербувати нових працівників, що забезпечує постійне самовідтворення злочинної системи.

Процес відмивання доходів поєднує традиційні методи з новими цифровими інструментами. На початковому етапі кошти потерпілих надходять на банківські рахунки фізичних або юридичних осіб, електронні гаманці, рахунки платіжних установ, рахунки продавців чи адреси віртуальних активів. Далі вони швидко переміщуються через численні рахунки й юрисдикції, розподіляються між великою кількістю учасників, конвертуються у готівку або віртуальні активи та змішуються з іншими надходженнями. На завершальному етапі доходи використовуються для придбання нерухомості, землі, автомобілів, золота, коштовностей, предметів розкоші, фінансування підставних підприємств або створення нових шахрайських центрів.

Найпоширенішим інструментом є рахунки грошових мулів. Їх використання відзначили 76% державних респондентів. Для відкриття таких рахунків залучають студентів, безробітних, малозабезпечених осіб, трудових мігрантів або людей, які шукають роботу. Вони можуть добровільно передавати рахунок за винагороду, бути введеними в оману або діяти під примусом. Організатори отримують банківські картки, SIM-картки, паролі, доступ до онлайн-банкінгу та засоби автентифікації. Рахунки використовуються протягом короткого часу, після чого їх замінюють новими. Типовими ознаками є невеликі тестові перекази перед великими операціями, численні платежі від не пов'язаних між собою осіб, негайне перерахування отриманих коштів, відсутність накопичення залишку, однакові або близькі суми надходжень і списань, а також активність, що не відповідає доходам, професії чи звичайній поведінці клієнта.

Велику роль відіграють нелегальні або незареєстровані надавачі послуг із переказу коштів, системи «hawala», неформальні брокери та підпільні банківські мережі. За допомогою таких систем готівка може передаватися посереднику в одній країні, тоді як еквівалентна сума виплачується або конвертується у віртуальні активи в іншій юрисдикції без формального міжнародного переказу. Це ускладнює встановлення зв'язку між початковим платежем і кінцевим отримувачем та дозволяє обходити банківський контроль.

Особливе місце посідають віртуальні активи. Про їх використання як одного з основних механізмів відмивання повідомили 71% державних респондентів. Після надходження коштів на рахунки мулів вони можуть бути негайно конвертовані у USDT, біткоїн, ефір або інші віртуальні активи. Далі кошти переміщуються через численні гаманці, P2P-платформи, нерегульованих OTC-брокерів, офшорні біржі, міжмережеві мости, міксери та активи з підвищеною конфіденційністю. Окремою новою типологією є внесення готівки до криптоматів із подальшим переказом віртуальних активів на гаманці, пов'язані зі злочинною мережею. Такі операції дозволяють обходити банківські обмеження та ускладнюють визначення особи, яка фактично контролює кошти. Водночас автори підкреслюють, що публічність блокчейну може бути використана правоохоронними органами. За наявності кваліфікованих аналітиків, відповідного програмного забезпечення і швидкої співпраці з

VASP можна відстежувати ланцюги транзакцій, визначати точки конвертації, пов’язувати гаманці між собою та заморожувати активи.

Аналіз правоохоронної практики показує, що більшість розслідувань починається надто пізно. У 82% юрисдикцій основним приводом були заяви або скарги потерпілих, тоді як повідомлення про підозрілі операції стали джерелом для 59% респондентів. Менше третини юрисдикцій отримували повідомлення, у яких прямо встановлювався зв’язок між фінансовою операцією та центром кібершахрайства. Це свідчить про те, що банки й інші суб’єкти фінансового моніторингу часто виявляють окремий рахунок грошового мула, шахрайський платіж або підозрілу криптовалютну операцію, але не бачать ширшого зв’язку з торгівлею людьми, організованою злочинністю, корупцією та міжнародною мережею відмивання доходів.

Однією з найсерйозніших проблем є транскордонний характер злочинів. Потерпілий, рахунок першого отримувача, криптовалютна біржа, організатор, шахрайський центр і активи можуть перебувати у різних державах. Традиційні процедури міжнародної правової допомоги часто є повільнішими за рух коштів, які можуть пройти через десятки рахунків протягом кількох годин. Окремі юрисдикції не мають достатньої правової основи для оперативного обміну інформацією, не відповідають на запити або не повідомляють, як використали отримані відомості. У результаті національне розслідування може обмежитися затриманням локальних грошових мулів і посередників, тоді як організатори та бенефіціари залишаються поза межами досяжності.

Низькою залишається й ефективність повернення активів. Лише незначна частина опитаних юрисдикцій вважала себе успішною у відстеженні, арешті та поверненні доходів, пов’язаних із центрами кібершахрайства. Перешкодами є швидкість переказів, використання підставних осіб, іноземних компаній, віртуальних активів, неформальних систем розрахунків, недостатня міжнародна координація та нестача спеціалізованих знань. Більшість респондентів назвали відстеження операцій із віртуальними активами та недостатню експертизу у сфері блокчейн-аналітики, цифрових доказів і розслідування кібершахрайства одними з головних проблем.

Звіт закликає перейти від розслідування окремих платежів до системного картографування кримінальних мереж. Підрозділи фінансової розвідки та правоохоронні органи мають об’єднувати інформацію з повідомлень про підозрілі операції, банківських і платіжних даних, інформації VASP, податкових і корпоративних реєстрів, відкритих джерел, соціальних мереж, IP-адрес, геолокації, ідентифікаторів пристроїв та даних про телекомунікації. Такий підхід дозволяє встановлювати зв’язки між зовні не пов’язаними рахунками, виявляти спільні пристрої, адреси, контактні дані, гаманці, номінальних власників і юридичних осіб, а також переходити від виявлення першого одержувача коштів до ідентифікації організаторів та контролерів мережі.

Серед найефективніших моделей реагування названо створення спеціалізованих національних антишахрайських центрів, постійних міжвідомчих груп і державно-приватних партнерств. Такі механізми можуть об’єднувати підрозділи фінансової розвідки, поліцію, кіберпідрозділи, органи протидії торгівлі людьми, регуляторів, банки, платіжні установи, телекомунікаційні компанії та VASP. Їхньою головною перевагою є можливість швидко обмінюватися інформацією, зупиняти платежі та заморожувати кошти до їх подальшого переміщення. Практичні кейси у звіті показують, що оперативна міжнародна взаємодія та участь банків можуть дозволити не лише затримати учасників шахрайського центру, а й повернути значну частину коштів потерпілим та запобігти новим втратам.

Для приватного сектору рекомендується запроваджувати посилену перевірку клієнтів і спеціалізовані сценарії транзакційного моніторингу. Необхідно аналізувати незвичайні входи до рахунків за IP-адресами, геолокацією та ідентифікаторами пристроїв, виявляти випадки використання одного пристрою для управління численними рахунками, відстежувати швидке проходження коштів через ланцюги контрагентів, перевіряти відповідність операцій заявленому профілю клієнта та його цифровому сліду. Додатковими заходами можуть бути

відеоідентифікація, повторна перевірка клієнта при істотній зміні поведінки, аналіз зв'язків між бенефіціарами, адресами, номерами телефонів і корпоративними структурами.

У додатках до документа наведено розгорнуті індикатори, які охоплюють як фінансову, так і нефінансову поведінку. До нефінансових ознак функціонування великого шахрайського центру можуть належати надзвичайно високі обсяги споживання електроенергії та інтернет-трафіку, активність у нічний час, масове постачання комп'ютерного обладнання, SIM-карток і продуктів харчування, велика кількість іноземних працівників, організовані перевезення між місцями проживання та роботи, колишні казино або готелі з обмеженим виходом працівників. Ознаками підозрілого вербування є пропозиція дуже високої заробітної плати за мінімальних кваліфікаційних вимог, відсутність формальної співбесіди, вимога передати паспорт, оплата поїздки роботодавцем, наполягання на терміновому переїзді та переведення комунікації до закритих месенджерів.

Фінансовими індикаторами є численні надходження від не пов'язаних між собою осіб, структуровані операції нижче встановлених порогів, різке збільшення кількості контрагентів, швидке надходження і подальше списання однакових сум, активізація нового або раніше неактивного рахунку, невідповідність оборотів доходам чи професії клієнта, часті платежі до високоризикових юрисдикцій, придбання дорогих активів без зрозумілого джерела коштів, використання персональних рахунків замість корпоративних та складні зміни у структурі власності. У сфері віртуальних активів увагу мають привертати негайна конвертація отриманих коштів у стейблкоїни, перекази з великої кількості нових гаманців на невелику кількість агрегаторів, використання міксерів або міжмережевих мостів одразу після отримання активів, спільні IP-адреси й пристрої, операції з нерегульованими OTC-посередниками та неможливість клієнта пояснити економічну мету транзакцій.

Висновки:

- **Необхідно розглядати центри кібершахрайства як єдину кримінальну екосистему.** Національні органи мають проводити паралельні розслідування шахрайства, торгівлі людьми, корупції та відмивання коштів, а не обмежуватися переслідуванням окремих грошових мулів або виконавців.
- **Потрібно створити механізм негайного фінансового реагування.** Необхідні постійно діючі центри протидії шахрайству або міжвідомчі групи, цілодобові канали зв'язку з банками, платіжними установами та VASP, а також процедури оперативного зупинення платежів, заморожування рахунків і віртуальних активів.
- **Необхідно перетворити типології на конкретні сценарії моніторингу.** Суб'єкти фінансового моніторингу повинні виявляти мережі рахунків за сукупністю транзакційних, геолокаційних і корпоративних даних, окремо контролюючи P2P-платформи, OTC-брокерів, криптовалютні автомати, швидку конвертацію у стейблкоїни та приховування бенефіціарної власності.
- **Потрібно посилити міжнародну та орієнтовану на потерпілих відповідь.** Пріоритетами мають стати швидкий транскордонний обмін фінансовою розвідкою, розвиток блокчейн-аналітики та повернення активів, належний нагляд за професійними посередниками й VASP, а також гарантування того, що особи, примушені до шахрайської діяльності, ідентифікуються та захищаються як потерпілі від торгівлі людьми.

Водночас APG встановила, що лише невелика частина юрисдикцій надала суб'єктам фінансового моніторингу комплексні та регулярно оновлювані рекомендації, спеціально присвячені взаємозв'язку між центрами кібершахрайства, відмиванням коштів і торгівлею людьми. У багатьох державах використовуються загальні індикатори шахрайства, які не

дозволяють встановити ширшу кримінальну модель. Це означає, що накопичені типологічні знання ще недостатньо інтегровані у практичні системи моніторингу, підготовку повідомлень про підозрілі операції та аналітичну діяльність підрозділів фінансової розвідки.

У заключній частині звіту автори аналізують подальшу еволюцію загрози. Після посилення правоохоронного тиску великі комплекси можуть децентралізуватися та переміщуватися до приватних будинків, квартир, готельних номерів або окремих офісних приміщень. Така модель зменшує видимість діяльності, ускладнює використання традиційних індикаторів і дозволяє швидко змінювати місцезнаходження. Іншим визначальним фактором є штучний інтелект. Більшість опитаних юрисдикцій повідомили про використання діпфейків, клонування голосу, чатботів і автоматично створених повідомлень. AI дозволяє вести спілкування різними мовами, персоналізувати звернення до потерпілих, імітувати голоси родичів або посадових осіб, створювати переконливі фальшиві вакансії та обслуговувати одночасно значну кількість потенційних жертв. Автоматизація може зменшити потребу у великій кількості працівників, але водночас суттєво збільшує масштаб, швидкість і глобальне охоплення шахрайських кампаній.

Узагальнюючи, звіт APG демонструє, що центри кібершахрайства є не тимчасовим або локальним явищем, а стійкою транснаціональною бізнес-моделлю організованої злочинності, яка об’єднує цифрове шахрайство, торгівлю людьми, корупцію, непрозорі корпоративні структури, професійних сприячів, мережі грошових мулів, нелегальні платіжні системи та віртуальні активи. Ефективна протидія потребує політичної волі, належного нормативного регулювання, посилення нагляду за VASP і ВНУП, оперативного міжнародного обміну інформацією, розвитку блокчейн-аналітики, паралельних фінансових розслідувань, швидкого заморожування активів і створення міжвідомчих державно-приватних механізмів. Одночасно правоохоронна відповідь має залишатися орієнтованою на потерпілих і враховувати, що значна частина осіб, які безпосередньо здійснюють шахрайські дії, могла бути залучена до них через обман, примус і торгівлю людьми.

Звіти окремих інституцій та експертів

AI-врядування в банках [5]

Міжнародна аудиторсько-консалтингова мережа Deloitte оприлюднила звіт, присвячений стану врядування штучним інтелектом (AI governance) у глобальному банківському секторі. В основі дослідження – розроблений авторами Trustworthy AI Governance Index, що оцінює зрілість врядування AI за п'ятьма компонентами (принципи та політики, організаційна структура, процедури та контролі, персонал і навички, моніторинг та звітність) на основі 41 індикатора. Індекс застосовано до відповідей 135 керівників глобальних та національних системно важливих банків (G-SIB, D-SIB) та інших великих банків із 16 країн, отриманих через два інструменти опитування – 24 поглиблені інтерв'ю з керівниками напряму AI governance в G-SIB/D-SIB та 111 анкет від старших виконавчих директорів ширшої вибірки банків.

Результати свідчать про системний розрив між темпами впровадження AI та зрілістю механізмів контролю: 87% глобальних банків мають істотний простір для вдосконалення врядування ШІ, лише 13% банків досягли «оптимізованого» рівня зрілості, а 10% банків досі перебувають на «безсистемному» рівні. Найслабшою складовою для більшості банків є організаційна структура – понад чверть банків (27%) не мають навіть базового розподілу відповідальності за ризики ШІ, а лише 37% банків повідомили про те, що вище керівництво явно й видимо реалізує підзвітність за рішення щодо ризиків ШІ. Показово, що оцінки зрілості суттєво різняться залежно від того, хто відповідає: керівники підрозділів AI governance систематично оцінюють організаційну структуру своїх банків на 20 пунктів нижче (за шкалою

[5] https://www.deloitte.com/content/dam/assets-zone1/apac/en/docs/collections/2026/banking-on-trust.pdf

0–100), ніж інші старші керівники, що свідчить про розрив між формальною і фактичною підзвітністю.

Звіт фіксує різке зростання інцидентів, пов'язаних із застосуванням AI у фінансовому секторі: за даними моніторингу OECD AI Incidents and Hazards Monitor, частка інцидентів у фінансових послугах серед усіх публічно зафіксованих інцидентів AI зросла з 1,8% у 2021 році до 5,2% у 2025 році, а станом на травень 2026 року сектор зафіксував 247 публічно оприлюднених інцидентів – на 20% більше, ніж за аналогічний період 2025 року, і на 72% більше, ніж у 2024 році. Дослідники також встановили, що майже всі (97%) зафіксовані порушення безпеки, пов'язані зі ШІ, стосувалися систем без належного контролю доступу, а середня вартість витоку даних у фінансових послугах у 2025 році становила 5,56 млн дол. США, зростаючи на додаткові 670 тис. дол. США у випадках виявлення «тіньового» AI (shadow AI) – застосунків, розгорнутих без формального затвердження чи нагляду.

Особливої уваги в контексті фінансового моніторингу заслуговує виявлений розрив у контролі за агентним (agentic) AI – системами, здатними самостійно ухвалювати рішення та виконувати комплексні процеси без покрокового втручання людини. Якщо моніторинг ризиків упродовж усього життєвого циклу впровадження забезпечено для 61% застосувань традиційного AI та 59% генеративного ШІ, для агентного AI цей показник падає до 44%. Оскільки банки дедалі активніше застосовують AI саме для автоматизованого моніторингу транзакцій, скринінгу на відповідність санкційним спискам та спискам PEP, а також формування первинних підозр щодо операцій, розрив у контролі за агентними системами створює прямий ризик для надійності автоматизованих механізмів фінансового моніторингу: рішення про ескалацію чи неескалацію підозрілої операції, ухвалене автономною системою без адекватного нагляду, є вразливим до систематичних помилок першого й другого роду, які складно виявити постфактум.

Висновки:

- **Дослідження доводить, що надійна система управління AI напряму пов'язана з розширенням його використання та збільшенням доходів** (підвищення показника Trustworthy AI governance Index на 10 пунктів дає в середньому 10% приросту доходу). Тобто регулювання AI – це інструмент зростання, а не гальмо для інновацій.
- **У період з 2022 по 2025 роки кількість порушень безпеки, пов'язаних із AI у фінансовому секторі, зросла майже у 8 разів.** При цьому лише 15% банків регулярно оновлюють тренінги з управління AI для персоналу, а третина банків світу взагалі не проводить такого навчання або робить це хаотично.
- **Клієнтська довіра залишається крихкою:** 84% споживачів готові змінити свого фінансового провайдера, якщо їхні дані будуть оброблені або використані неналежним чином.

Методологічно цінним є емпіричний аналіз зв'язку між зрілістю врядування AI та фінансовими показниками банків: економетричне моделювання (з контролем за масштабом використання ШІ, розташуванням головного офісу, чисельністю персоналу та роками діяльності банку) показує, що підвищення індексу врядування на 10 пунктів асоціюється зі зростанням доходу приблизно на 10 відсоткових пунктів швидше. Для банку із середнім у вибірці річним доходом 500 млн дол. США це означає різницю між приростом доходу в 50 млн та 100 млн дол. США за рік. Автори звіту прямо застерігають, що результат описує статистичну асоціацію в межах вибірки переважно менших банків (жоден банк у вибірці не має доходу понад 4 млрд дол. США) і не має екстраполюватися на глобально системно важливі банки без застережень, однак сам факт документованого зв'язку є аргументом для переосмислення врядування AI не як витратного центру контролю, а як фактора, що уможливлює безпечне масштабування.

Звіт також фіксує розбіжність підходів регуляторів до врядування AI у банківському секторі: Рада фінансової стабільності (FSB) у червні 2026 року оприлюднила рамкові «Sound Practices

for Responsible Adoption of Artificial Intelligence» з дванадцятьма практиками за двома напрямами – врядування та управління життєвим циклом ШІ, тоді як Міжнародна організація комісій з цінних паперів (IOSCO) опублікувала наглядовий інструментарій для застосування AI на ринках капіталу. Найбільш методологічно релевантним для сфери ПВК/ФТ є режим Акта ЄС про штучний інтелект (набув чинності 1 серпня 2024 року, більшість зобов'язань застосовується з 2 серпня 2026 року), який класифікує застосування AI для оцінки кредитоспроможності та формування кредитного скорингу фізичних осіб як «високоризикове», встановлюючи вимоги щодо управління ризиками, врядування даними, прозорості та людського нагляду під загрозою штрафів до 35 млн євро або 7% глобального річного обороту компанії (стаття 99).

Хоча звіт Deloitte безпосередньо не присвячений фінансовому моніторингу, його висновки мають пряме методологічне значення для нагляду за застосуванням AI в системах ПВК/ФТ/ФР: транзакційний моніторинг, скринінг контрагентів на відповідність санкційним переліками, автоматизоване визначення рівня ризику клієнта і навіть попереднє формування повідомлень про підозрілі операції дедалі частіше спираються на моделі штучного інтелекту, зокрема агентні системи з обмеженим людським наглядом. Задокументований у звіті розрив між темпами впровадження та зрілістю врядування – включно з непрозорістю щодо переліку застосувань AI (72% банків фіксують менше половини випадків використання AI в централізованому реєстрі) – створює операційний ризик для банківського нагляду в Україні: Національний банк України та Держфінмоніторинг, оцінюючи ефективність автоматизованих систем фінансового моніторингу банків, мають враховувати не лише формальну наявність такої системи, а й задокументованість її врядування впродовж усього життєвого циклу, включно з поясненістю (explainability) автоматизованих рішень про ескалацію підозрілих операцій.

AMLA: нова архітектура системи протидії відмиванню коштів та фінансуванню тероризму в Європейському Союзі [6]

Документ є комплексним аналітичним дослідженням, присвяченим створенню нового європейського органу з питань протидії відмиванню коштів та фінансуванню тероризму (AMLA), його майбутній ролі у трансформації системи фінансового моніторингу Європейського Союзу та потенціалу для підвищення ефективності міжнародної боротьби з фінансовою злочинністю. Автори виходять із того, що сучасна система ПВК/ФТ стикається з безпрецедентними викликами, пов'язаними зі стрімким зростанням обсягів незаконних фінансових потоків, розвитком організованої транснаціональної злочинності, поширенням кіберзлочинності, використанням криптоактивів, новітніх платіжних технологій та штучного інтелекту злочинними угрупованнями. На цьому тлі існуюча модель нагляду, заснована переважно на діяльності окремих національних органів, дедалі більше демонструє свої обмеження, особливо щодо виявлення складних транскордонних схем відмивання коштів і фінансування тероризму. Саме тому створення AMLA розглядається як найбільш масштабна інституційна реформа системи ПВК/ФТ Європейського Союзу за останні десятиліття, покликана забезпечити єдиний підхід до регулювання, нагляду, координації та управління ризиками на рівні всього Союзу.

Автори наголошують, що необхідність створення AMLA зумовлена не лише масштабами сучасної фінансової злочинності, але й низькою ефективністю чинної міжнародної системи її протидії. У документі зазначається, що глобальні незаконні фінансові потоки вже оцінюються у кілька трильйонів доларів США, тоді як частка коштів, які вдається виявити та конфіскувати, залишається вкрай незначною. Одночасно швидко зростають доходи від торгівлі наркотиками, торгівлі людьми, кібершахрайства, організованого шахрайства, екологічної злочинності та інших видів тяжких злочинів. Особливу небезпеку становить швидкість, з якою злочинці

[6] https://www.deloitte.com/content/dam/assets-zone2/at/de/docs/services/consulting/2026/amla-whitepaper.pdf

адаптуються до нових технологій: криптовалюти, нові платіжні рішення, анонімізовані канали комунікації, VPN-технології, наскрізне шифрування та інструменти штучного інтелекту дедалі активніше використовуються для приховування злочинної діяльності, автоматизації шахрайських схем та уникнення виявлення. Додатково геополітична нестабільність, міжнародні конфлікти, фінансування тероризму, обходження санкцій та фінансування розповсюдження зброї масового знищення значно посилюють навантаження на існуючі системи ПВК/ФТ.

Значна увага приділяється аналізу специфічних проблем Європейського Союзу. Попри високий рівень розвитку фінансового сектору та тривалу еволюцію законодавства у сфері ПВК/ФТ, держави-члени продовжують застосовувати різні підходи до нагляду, оцінювання ризиків, процедур перевірки клієнтів та обміну інформацією. Це створює нерівномірний рівень ефективності систем фінансового моніторингу, сприяє виникненню регуляторного арбітражу та дозволяє злочинцям використовувати слабкі місця окремих юрисдикцій. Особливе занепокоєння викликає сектор криптоактивів, де більшість компетентних органів ЄС оцінюють ризики відмивання коштів та фінансування тероризму як високі або такі, що постійно зростають. Документ підкреслює, що саме фрагментованість нагляду, відсутність єдиних стандартів та неоднакове застосування законодавства є одними з головних причин недостатньої ефективності чинної системи ПВК/ФТ у Європі.

Далі автори детально розглядають законодавчу основу створення AMLA та його місце в новій архітектурі європейського фінансового моніторингу. Пояснюється, що AMLA є центральним елементом нового пакета законодавства ЄС у сфері ПВК/ФТ, який включає Регламент AMLR, Шосту директиву AMLD6, а також оновлені правила щодо переказів криптоактивів. Новий орган отримує принципово нову модель повноважень порівняно з попередньою системою координації. Він здійснюватиме прямий нагляд за приблизно сорока найбільшими транскордонними фінансовими установами, які мають найвищий ризик використання для ВК/ФТ, координуватиме діяльність національних наглядових органів, забезпечуватиме взаємодію між підрозділами фінансової розвідки держав-членів, розроблятиме технічні стандарти, керівні принципи та інші нормативні документи, необхідні для однакового застосування законодавства в усіх країнах ЄС. Документ також описує поетапне розгортання діяльності AMLA, включаючи формування організаційної структури, створення інформаційної інфраструктури, розроблення нормативної бази, підготовку до прямого нагляду та реалізацію програм розвитку на 2026–2028 роки.

Водночас автори наголошують, що навіть найкраща нормативна база сама по собі не гарантує успіху реформи. Одним із найбільших викликів вони називають необхідність подолання інституційної фрагментованості між державами-членами, різного рівня розвитку національних органів нагляду та відсутності єдиної наглядової культури. Окремо підкреслюється, що AMLA повинен забезпечити інтеграцію оцінювання ризиків ВК/ФТ у загальну систему фінансового нагляду, а також побудувати ефективну взаємодію між наглядовими органами, підрозділами фінансової розвідки, правоохоронними органами та міжнародними партнерами. Автори застерігають, що існує ризик перетворення діяльності нового органу на перевірку формального виконання нормативних вимог, коли основна увага приділятиметься технічній відповідності законодавству, а не фактичному зниженню рівня фінансової злочинності. Саме тому пропонується максимально інтегрувати у діяльність AMLA підхід FATF, який орієнтується насамперед на досягнення вимірюваних результатів, а не на кількість виконаних процедур чи формальних перевірок.

Однією з центральних тем документа є розвиток ризик-орієнтованого підходу як фундаментального принципу майбутньої діяльності AMLA. Автори наголошують, що ефективна система ПВК/ФТ повинна концентрувати свої ресурси на найбільш суттєвих ризиках, а не намагатися однаково контролювати всі сфери діяльності. На їхню думку, фінансові установи, наглядові органи та аудитори повинні працювати відповідно до чітко визначених національних і наднаціональних пріоритетів, що дозволить ефективніше розподіляти ресурси та підвищити якість виявлення найбільш небезпечних схем. Документ

підтримує концепцію FATF щодо оцінювання систем ПВК/ФТ через досягнення безпосередніх результатів (Immediate Outcomes), коли основним критерієм стає не виконання нормативних вимог, а реальне виявлення ризиків, припинення незаконної діяльності, конфіскація активів та ефективність міжнародного співробітництва. У цьому контексті AMLA має розробити власну систему аналізу ризиків, яка поєднуватиме інформацію від наглядових органів, ПФР, інших інституцій ЄС та міжнародних партнерів для формування єдиного бачення ризиків ВК/ФТ на рівні всього Союзу.

Великий розділ присвячений гармонізації правил фінансового моніторингу в межах Європейського Союзу. Автори розглядають створення єдиного нормативного простору як одну з головних переваг AMLA. На їхню думку, гармонізація повинна охоплювати не лише законодавство, а й практичні аспекти діяльності суб'єктів фінансового моніторингу, включаючи єдині формати повідомлень про підозрілі операції, стандартизовані процедури належної перевірки клієнтів, єдині підходи до ідентифікації кінцевих бенефіціарних власників, однакові вимоги до процедур KYC та уніфіковані механізми обміну інформацією між державами-членами. Особливо підкреслюється, що різні формати SAR сьогодні суттєво ускладнюють аналіз транскордонних схем відмивання коштів, тоді як стандартизована звітність дозволить формувати комплексну картину злочинної діяльності одночасно в кількох юрисдикціях. Крім того, уніфікація нормативних вимог повинна сприяти скороченню адміністративних витрат фінансових установ, підвищенню якості аналітики та зменшенню кількості ресурсів, які сьогодні витрачаються на виконання різних технічних вимог окремих держав. Водночас автори наголошують, що гармонізація не повинна завершитися встановленням лише мінімальних стандартів, які країни потім почнуть доповнювати власними вимогами, оскільки це фактично збереже нинішню фрагментованість системи.

Висновки:

- **AMLA має перейти від контролю формального виконання вимог до оцінювання реальної ефективності систем ПВК/ФТ,** використовуючи ризик-орієнтований підхід FATF, оцінювання за безпосередніми результатами (Immediate Outcomes) та концентрацію на пріоритетних загрозах.
- **Європейському Союзу необхідно максимально гармонізувати процедури фінансового моніторингу,** насамперед стандартизувати формати SAR, CDD, KYC, інформацію про КБВ та вимоги до обміну інформацією, що суттєво підвищить якість транскордонного аналізу та зменшить адміністративне навантаження.
- **Створення централізованої AML/CFT Database та розвиток партнерств між державним і приватним секторами повинні стати основою нової інформаційної архітектури ЄС,** забезпечуючи інтегровану аналітику, оперативний обмін даними та ефективніше виявлення міжнародних злочинних мереж.
- **Для забезпечення довгострокової ефективності AMLA необхідно зміцнювати міжнародну координацію** з ПФР третіх країн, FATF, міжнародними організаціями та правоохоронними органами, приділяючи особливу увагу ризикам, пов'язаним із криптоактивами, штучним інтелектом, кіберзлочинністю, санкційними режимами та іншими новими транскордонними загрозами.

Окремий розділ документа присвячений ролі фінансової розвідки та інформаційного обміну. Автори підкреслюють, що сучасна боротьба з фінансовою злочинністю дедалі більше залежить від здатності компетентних органів швидко отримувати, аналізувати та передавати інформацію між різними державами, фінансовими установами та правоохоронними органами. Водночас існуючі законодавчі обмеження щодо захисту персональних даних, банківської таємниці, конфіденційності інформації та різних національних підходів до обробки даних

істотно ускладнюють ефективний міжнародний обмін інформацією. Документ аналізує останні зміни до Рекомендацій FATF щодо координації між компетентними органами та внутрішньогрупового обміну інформацією, відзначаючи, що вони створюють значно кращі передумови для розвитку інтегрованої системи фінансової розвідки. Однією з найважливіших ініціатив AMLA має стати створення централізованої бази даних AML/CFT Database, яка акумулюватиме інформацію про результати нагляду, оцінки ризиків, застосовані санкції, заходи впливу, результати перевірок та інші дані від компетентних органів держав-членів. Автори вважають, що ця база потенційно може стати одним із найпотужніших світових інформаційних ресурсів у сфері ПВК/ФТ, однак для реалізації цього потенціалу необхідно забезпечити її інтеграцію з діяльністю ПФР, міжнародних організацій та правоохоронних органів, а також створити ефективні механізми обміну інформацією з третіми країнами. Водночас значна увага приділяється розвитку партнерств між державним і приватним секторами (державно-приватні партнерства (PPP) та партнерства з обміну інформацією), які повинні стати важливим інструментом оперативного обміну інформацією про складні фінансові злочини, транскордонні мережі та нові типології відмивання коштів.

Підсумовуючи, автори доходять висновку, що AMLA має всі передумови для того, щоб стати центральною інституцією нової європейської системи ПВК/ФТ, однак успіх реформи визначатиметься не масштабом її повноважень, а здатністю забезпечити реальну ефективність функціонування всієї системи. Досягнення цієї мети потребуватиме послідовної реалізації ризик-орієнтованого підходу, переходу від формального контролю до оцінювання фактичних результатів, повної гармонізації правил фінансового моніторингу, розвитку сучасної інформаційної інфраструктури, активного використання фінансової розвідки, поглиблення міжнародного співробітництва та широкого залучення приватного сектору до спільної протидії відмиванню коштів, фінансуванню тероризму та іншим формам транскордонної фінансової злочинності. Саме ці елементи, на думку авторів, визначатимуть здатність AMLA суттєво підвищити ефективність системи ПВК/ФТ як у Європейському Союзі, так і в глобальному масштабі.

Від фінансового моніторингу до політичного контролю: нові виклики для системи FATF [7]

Документ присвячений комплексному дослідженню того, як міжнародна система протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ), сформована насамперед навколо стандартів FATF, дедалі частіше використовується окремими державами не лише для боротьби з фінансовою злочинністю, а й як інструмент політичного контролю над громадянським суспільством, незалежними медіа, правозахисниками та громадськими активістами. Автор наголошує, що проблема полягає не у самих стандартах FATF, які залишаються важливою складовою глобальної фінансової безпеки, а в їх політизованому та вибірковому застосуванні окремими урядами для легітимації репресивних заходів. Саме тому дослідження пропонує новий погляд на взаємозв'язок між міжнародними механізмами фінансового моніторингу, законами про «іноземних агентів», фінансовими обмеженнями щодо неурядових організацій та явищем транснаціональних репресій.

На початку документа автор окреслює загальний контекст сучасного демократичного регресу, зазначаючи, що в багатьох країнах світу дедалі активніше використовуються законодавчі механізми, спрямовані на обмеження діяльності громадянського суспільства під приводом захисту національної безпеки, боротьби з іноземним втручанням, корупцією або незаконними фінансовими потоками. Особливу увагу приділено тому, що такі аргументи дедалі частіше переплітаються із завданнями системи ПВК/ФТ, що створює хибне враження про відповідність подібних законів міжнародним стандартам FATF. У результаті боротьба з

[7] https://ecnl.org/sites/default/files/2026-06/ECNL%20FATF%20Long%20Shadow_0.pdf

відмиванням коштів починає використовуватися як політичний інструмент для виправдання значно ширших обмежень свободи асоціацій, свободи слова та діяльності громадських організацій. Документ підкреслює, що саме високий міжнародний авторитет FATF дозволяє окремим урядам посилювати легітимність власних репресивних заходів, хоча такі заходи часто не мають безпосереднього зв'язку із реальними ризиками відмивання коштів або фінансування тероризму.

Для підтвердження своїх висновків автор використовує емпіричний підхід, який поєднує аналіз законодавства, результати опитувань громадських організацій у країнах Центральної та Східної Європи, Західних Балкан, Центральної Азії та держав Східного партнерства, серію експертних інтерв'ю з представниками громадянського суспільства та юридичної спільноти, а також перевірку отриманих висновків під час тематичних міжнародних круглих столів. Така методологія дозволяє розглядати не окремі випадки, а системні тенденції, які проявляються одночасно у різних регіонах світу.

Окремий великий розділ документа присвячений законам про «іноземних агентів» та іншим заходам щодо обмеження іноземного фінансування громадських організацій. Автор зазначає, що сучасні версії подібних законів уже не обмежуються вимогами щодо реєстрації організацій, які отримують іноземне фінансування. Натомість вони поступово інтегрують механізми фінансового моніторингу у свою структуру, використовуючи аргументи про необхідність боротьби з відмиванням коштів, фінансуванням тероризму або незаконними фінансовими потоками. Таким чином відбувається своєрідне «запозичення легітимності» міжнародної системи ПВК/ФТ для обґрунтування заходів, які фактично спрямовані на політичний контроль над громадянським суспільством. Автор підкреслює, що навіть якщо в тексті закону прямо не згадується FATF, посилання на боротьбу з фінансовими злочинами нерідко виконують аналогічну функцію, формуючи суспільне уявлення про нібито міжнародну необхідність запровадження відповідних обмежень.

Дослідження детально аналізує низку конкретних законодавчих прикладів. У випадку Словаччини автор демонструє, що законопроєкт прямо обґрунтовувався необхідністю виконання рекомендацій FATF щодо неурядового сектору, хоча згодом був визнаний неконституційним. Аналогічні аргументи використовувалися під час розробки законодавства у Республіці Сербській, де громадські організації звертали увагу MONEYVAL на те, що запропоновані заходи значно перевищують вимоги міжнародних стандартів ПВК/ФТ. У Болгарії політичні сили, яким не вдалося ухвалити закон про «іноземних агентів», перейшли до створення парламентської комісії з перевірки фінансування громадських організацій, що свідчить про використання альтернативних механізмів досягнення аналогічних політичних цілей. Автор показує, що незалежно від конкретної законодавчої форми кінцева мета залишається однаковою – встановлення додаткового державного контролю за діяльністю громадянського суспільства через фінансові механізми.

Особливої уваги приділено прикладу Угорщини, який автор називає одним із найбільш показових випадків трансформації системи ПВК/ФТ у механізм політичного контролю. Законодавча ініціатива передбачала покладення на банки обов'язку перевіряти джерела фінансування громадських організацій на предмет можливого «іноземного впливу», а також фактично прирівнювала керівників громадських організацій до політично значущих осіб (PEPs). Це означало застосування до них процедур посиленої перевірки клієнта, хоча міжнародні стандарти FATF визначають статус PEP виключно для осіб, які через виконання державних функцій мають підвищений ризик корупції. Автор наголошує, що таке розширене трактування статусу PEP повністю суперечить ризик-орієнтованому підходу FATF та демонструє, як міжнародні стандарти можуть бути адаптовані до політичних потреб окремих урядів. Цікавим є й те, що найактивнішу критику відповідного законопроєкту висловили не лише правозахисники, а й сам банківський сектор, який звертав увагу на непропорційне зростання витрат на комплаєнс, репутаційні ризики та практичну неможливість реалізації окремих законодавчих вимог.

Не менш важливим є аналіз законодавства Киргизстану, де автор демонструє, що навіть після ухвалення закону його практична реалізація може залишатися обмеженою. Водночас саме існування такого нормативного акта створює постійну можливість для вибіркового застосування проти окремих організацій у майбутньому. Таким чином документ підкреслює, що небезпека полягає не лише у фактичному застосуванні законів, а й у самому створенні нормативних механізмів, які можуть бути використані у будь-який момент залежно від політичної ситуації.

На основі проведеного аналізу автор виділяє дві основні моделі використання системи ПВК/ФТ для підтримки законів про «іноземних агентів». Перша полягає у використанні посилань на FATF або боротьбу з фінансовими злочинами як політичного виправдання прийняття відповідного законодавства. Друга є значно небезпечнішою, оскільки передбачає безпосереднє використання інституцій ПВК/ФТ – підрозділів фінансової розвідки, процедур належної перевірки клієнтів, фінансових установ та інших елементів фінансової інфраструктури – для практичного виконання репресивних законодавчих положень. Автор наголошує, що саме ця тенденція свідчить про поступову інституціоналізацію політичного використання механізмів ПВК/ФТ.

Друга половина документа присвячена аналізу феномену фінансової транснаціональної репресії, під якою розуміється використання міжнародного співробітництва у сфері фінансового моніторингу та боротьби з фінансовими злочинами для переслідування політичних опонентів за межами країни їхнього походження. Автор зазначає, що останніми роками це питання дедалі активніше розглядається європейськими інституціями як окрема загроза верховенству права. Документ пропонує власну класифікацію фінансової транснаціональної репресії, яка включає три основні механізми: отримання фінансової інформації про дисидентів через міжнародний обмін між підрозділами фінансової розвідки, використання міжнародного поліцейського співробітництва для політично мотивованого переслідування та застосування процедур банківського комплаєнсу як інструменту фінансової ізоляції опонентів режиму.

Найбільш детально розглядається проблема міжнародного обміну фінансовою інформацією між підрозділами фінансової розвідки. Автор звертає увагу, що сама система Егмонтської групи побудована на високому рівні взаємної довіри між державами та передбачає активний обмін інформацією для боротьби з фінансовими злочинами. Однак саме ця довіра може використовуватися авторитарними державами для отримання конфіденційної фінансової інформації про політичних опонентів, які проживають за кордоном. Як приклад наведено справу білоруського правозахисника Алеся Бяляцького, інформація щодо рахунків якого була передана білоруській владі через міжнародні механізми співробітництва і використана як доказ у кримінальному переслідуванні. Автор зазначає, що подібні випадки демонструють необхідність суттєвого посилення перевірки міжнародних запитів на отримання фінансової інформації та запровадження ефективних гарантій від політично мотивованого використання механізмів співробітництва між підрозділами фінансової розвідки.

Окрему увагу приділено Грузії, де останні законодавчі зміни, на думку автора, можуть створити передумови для використання кримінальних проваджень щодо відмивання коштів проти громадських організацій, які працюють за межами країни, але займаються грузинською тематикою. Документ демонструє, як поєднання нових правил щодо іноземних грантів із внесенням змін до складу злочину з відмивання коштів може створити формальні підстави для направлення міжнародних запитів про надання фінансової інформації щодо громадських організацій, які фактично здійснюють легальну діяльність за кордоном. Таким чином система міжнародного співробітництва у сфері ПВК/ФТ може перетворюватися на інструмент політичного контролю далеко за межами національної юрисдикції.

Документ також аналізує використання міжнародних правоохоронних механізмів, насамперед червоних оповіщень Інтерполу (INTERPOL Red Notices) (INTERPOL Red Notice), для переслідування осіб під приводом фінансових злочинів. На прикладах російських та

білоруських справ автор демонструє, що обвинувачення у шахрайстві, привласненні коштів або ухиленні від сплати податків можуть використовуватися як формальна підстава для міжнародного переслідування політичних опонентів. При цьому навіть якщо повідомлення Інтерполу згодом скасовуються, сам факт їх існування вже створює серйозні негативні наслідки у вигляді затримань, обмеження пересування, блокування банківських рахунків та фінансової ізоляції. Окремо розглядаються нові срібні оповіщення Інтерполу (INTERPOL Silver Notice), призначені для міжнародного розшуку активів. Автор попереджає, що орієнтація цього механізму на швидкий міжнародний обмін інформацією може створити нові можливості для політично мотивованого блокування активів громадських діячів або дисидентів під приводом боротьби з фінансовою злочинністю.

Висновки:

- **Міжнародні стандарти FATF дедалі частіше використовуються окремими державами як політичне обґрунтування для запровадження законів про «іноземних агентів»,** хоча такі законодавчі ініціативи нерідко виходять далеко за межі вимог міжнародної системи ПВК/ФТ.
- **Найбільшим новим ризиком є використання міжнародних механізмів обміну фінансовою інформацією, співробітництва між підрозділами фінансової розвідки та інструментів Інтерполу** для політично мотивованого переслідування громадських активістів, правозахисників та інших представників громадянського суспільства за кордоном.
- **Для мінімізації ризиків необхідно** посилити гарантії захисту прав людини під час міжнародного обміну фінансовою інформацією, забезпечити ефективні механізми перевірки політично мотивованих запитів та не допустити використання інструментів ПВК/ФТ поза їх законною метою.
- **Громадянському суспільству доцільно будувати захист не лише на правозахисній аргументації, а й на технічних, економічних та комплаєнс-аргументах,** залучаючи до цього банківський сектор, міжнародні фінансові організації та самі інституції FATF, що суттєво підвищує шанси на перегляд надмірних або репресивних законодавчих ініціатив.

Завершальна частина дослідження містить практичні рекомендації щодо протидії зазначеним тенденціям. Автор переконаний, що громадянське суспільство повинно змінити традиційний підхід до адвокації та активніше використовувати можливості самої системи FATF для оскарження випадків зловживання міжнародними стандартами. Особлива увага приділяється необхідності формування широких коаліцій із банківським сектором, міжнародними фінансовими організаціями, професійними асоціаціями та міжнародними інституціями, які зацікавлені у збереженні довіри до глобальної системи ПВК/ФТ. Автор також підкреслює, що найбільш ефективною стратегією є не загальне заперечення законів про «іноземних агентів», а детальний аналіз конкретних положень, які виходять за межі міжнародних стандартів FATF, суперечать ризик-орієнтованому підходу або створюють непропорційні обмеження для діяльності громадянського суспільства. Саме такий підхід, на думку автора, дозволяє одночасно підтримувати ефективність міжнародної системи ПВК/ФТ та мінімізувати ризики її використання як інструменту політичних репресій.

Нерухомість як інструмент приховування активів: світові тенденції та регуляторні рішення [8]

Документ є комплексним міжнародним дослідженням стану прозорості власності на нерухоме майно та спроможності держав установлювати фізичних осіб, які фактично володіють нерухомістю, контролюють її або отримують від неї економічну вигоду. Документ охоплює 141 юрисдикцію та розглядає прозорість нерухомості як важливий елемент глобальної системи протидії відмиванню коштів, корупції, ухиленню від оподаткування, приховуванню активів, обходу міжнародних санкцій та іншим формам фінансової злочинності. Основна увага зосереджується не лише на формальному існуванні земельних кадастрів, реєстрів речових прав або реєстрів кінцевих бенефіціарних власників, а передусім на тому, чи дозволяє сукупність цих систем у практичному вимірі встановити конкретну фізичну особу, яка в кінцевому підсумку контролює нерухомий актив.

Автори виходять із того, що нерухомість є одним із найбільш привабливих інструментів для збереження, переміщення та легалізації незаконно одержаних коштів. Її привабливість для злочинців та корумпованих посадових осіб пояснюється високою вартістю активів, відносною стабільністю цін, можливістю накопичення капіталу протягом тривалого часу, а також складністю встановлення реальної ринкової вартості конкретного об’єкта. На відміну від фінансових активів, операції з нерухомістю можуть характеризуватися значною варіативністю цін залежно від місця розташування, стану об’єкта, умов договору та інших факторів, що створює можливості для штучного завищення або заниження вартості. Завищення ціни може використовуватися для формального пояснення походження значних сум коштів, тоді як заниження вартості дає змогу приховувати частину доходу, зменшувати податкові зобов’язання або здійснювати неофіційні розрахунки.

Особливі ризики виникають тоді, коли нерухомість реєструється не безпосередньо на фізичну особу, а на компанію, партнерство, фонд, приватну фундацію, траст або інше юридичне утворення. У такому випадку в реєстрі нерухомості зазвичай зазначається лише безпосередній юридичний власник, тоді як інформація про фізичну особу, яка контролює відповідну структуру, може бути відсутня або зберігатися в іншому реєстрі. Якщо структура власності включає декілька компаній у різних юрисдикціях, номінальних акціонерів, довірчих власників або інші посередницькі елементи, встановлення реального власника активу значно ускладнюється. Саме розрив між даними про юридичного власника нерухомості та інформацією про кінцевого бенефіціарного власника (КБВ) відповідної юридичної особи автори визначають як одну з головних системних вразливостей.

Документ наголошує, що прозорість нерухомості не повинна обмежуватися встановленням особи, ім’я якої формально зазначене в реєстрі прав власності. Для належного виявлення прихованих активів необхідно враховувати ширший спектр правових та економічних відносин із нерухомим майном. Фізична особа може не бути зареєстрованим власником, але фактично користуватися об’єктом, проживати в ньому без сплати орендної плати, отримувати доходи від його здавання в оренду, фінансувати його придбання, контролювати компанію-власника або мати інші права, які забезпечують їй економічну вигоду. Крім права власності, значення можуть мати права користування, узуфрукту, довгострокової оренди, іпотечні права, права на отримання доходу або інші обтяження. Кожне з таких прав також може належати юридичній особі або трасту, що створює додаткові рівні непрозорості. Тому ефективна система повинна дозволяти встановлювати не лише формального власника, а й усіх фізичних осіб, які прямо або опосередковано контролюють відповідні права та отримують від них вигоду.

Автори пояснюють, що історично земельні кадастри та реєстри нерухомості створювалися переважно для гарантування прав власності, оподаткування, планування територій та забезпечення безпеки цивільно-правових операцій. Їхнім основним завданням не було

[8] https://taxjustice.net/wp-content/uploads/2026/07/Beneficial-ownership-of-real-estate-around-the-world-2026-Tax-Justice-Network.pdf

виявлення відмивання коштів або встановлення КБВ. Через це такі реєстри зазвичай містять відомості про адресу, площу, межі земельної ділянки, кадастровий номер, вид права, іпотеку та безпосереднього юридичного власника, але не розкривають структуру контролю над компанією, якій належить майно. Реєстри бенефіціарної власності, навпаки, формувалися в межах політики у сфері протидії відмиванню коштів і фінансуванню тероризму та корпоративної прозорості. У багатьох державах обидві системи існують паралельно, управляються різними органами, використовують різні ідентифікатори та не мають автоматизованого обміну даними.

За такої моделі встановлення КБВ нерухомості потребує проведення декількох окремих етапів. Спочатку необхідно отримати інформацію про юридичного власника об'єкта з реєстру нерухомості, після чого знайти відповідну юридичну особу в корпоративному реєстрі, встановити її реєстраційні дані та лише потім звернутися до реєстру бенефіціарної власності. Навіть за наявності всіх необхідних реєстрів цей процес може бути ускладнений відсутністю єдиних ідентифікаторів, різними правилами доступу, платою за отримання інформації або неможливістю здійснювати пошук за іменем власника. Якщо юридичний власник зареєстрований в іншій державі, національний реєстр КБВ може взагалі не містити відомостей про нього, а встановлення фізичної особи залежатиме від доступності інформації в іноземній юрисдикції та ефективності міжнародного співробітництва.

Однією з центральних проблем, установлених у доповіді, є обмежене поширення вимог щодо розкриття бенефіціарної власності на іноземні юридичні особи та правові утворення, які володіють місцевою нерухомістю. Традиційно законодавство про реєстрацію КБВ застосовувалося передусім до компаній, створених відповідно до національного законодавства. Для трастів вирішальними могли бути місце проживання, місцезнаходження або податкове резидентство довірчого власника. У результаті іноземна компанія могла придбати нерухомість у певній державі, не маючи обов'язку повідомляти місцевим органам про свого КБВ. Аналогічна проблема виникала щодо іноземних трастів, якщо довірчий власник перебував за межами відповідної юрисдикції.

Ця прогалина може використовуватися не лише іноземними особами. Резидент держави може створити компанію в іншій юрисдикції та через неї придбати нерухомість у власній країні. Формально власником буде іноземна юридична особа, тому дані про фізичну особу, яка фактично контролює майно, можуть не потрапити до національного реєстру КБВ. Таким чином, використання іноземної структури створює додатковий рівень конфіденційності та дозволяє здійснювати повернення внутрішнього капіталу через зовнішню юридичну оболонку. Така практика ускладнює податковий контроль, застосування санкцій, конфіскацію активів і проведення фінансових розслідувань.

Дослідження демонструє значне глобальне поширення законодавства про бенефіціарну власність протягом останніх років. Кількість юрисдикцій, у яких були прийняті принаймні певні вимоги щодо реєстрації КБВ, зросла з приблизно 57 у 2018 році до 103 у 2022 році та до 117 станом на лютий 2026 року. Водночас автори застерігають, що прийняття законодавства ще не свідчить про реальне функціонування ефективного реєстру. У деяких державах нормативні положення можуть бути прийняті, але сам реєстр ще не запущений, функціонує частково або охоплює лише окремі види юридичних осіб. Крім того, формальна наявність реєстраційного обов'язку не гарантує точності даних, їхньої своєчасної актуалізації, незалежної перевірки або ефективного застосування санкцій за подання неправдивої інформації.

Найбільш показовим результатом є те, що лише 40 зі 117 юрисдикцій, які мають законодавство про реєстрацію бенефіціарної власності, поширюють відповідні вимоги хоча б на один вид іноземного юридичного утворення, що володіє або набуває нерухомість у цій державі. У 34 юрисдикціях вимоги охоплюють іноземні компанії та деякі інші юридичні утворення, тоді як у шести випадках вони застосовуються лише до трастів. Це означає, що в більшості досліджених держав іноземна компанія або інше іноземне утворення все ще може

використовуватися для володіння нерухомістю без повноцінного розкриття фізичних осіб, які здійснюють кінцевий контроль.

Документ аналізує вплив міжнародних стандартів на розвиток відповідного регулювання. Важливе значення має перегляд Рекомендації 24 FATF у 2022 році, відповідно до якого держави повинні враховувати іноземних юридичних осіб, що мають достатній зв'язок із юрисдикцією та становлять ризик відмивання коштів. Володіння нерухомістю прямо розглядається як один із можливих критеріїв такого зв'язку. Водночас стандарт не запроваджує абсолютного універсального обов'язку реєструвати КБВ кожної іноземної компанії, яка володіє нерухомістю, а залишає державам можливість визначати відповідний підхід на основі оцінки ризиків. Через це національні режими залишаються нерівномірними, а значна кількість юрисдикцій досі не встановила чітких правил для іноземних власників.

Окремо розглядається досвід Великої Британії, де Закон про економічну злочинність, корпоративну прозорість та правозастосування 2022 року запровадив спеціальний реєстр іноземних суб'єктів, які володіють нерухомістю. Іноземні юридичні особи, що набувають або утримують відповідні об'єкти, повинні зареєструватися в Companies House та розкрити інформацію про своїх бенефіціарних власників. Такий підхід демонструє можливість створення окремого правового механізму, орієнтованого саме на іноземні структури, без необхідності повністю перебудовувати загальну систему корпоративної реєстрації.

Значний вплив на регіональне поширення відповідних вимог має Європейський Союз. У межах нового пакета ЄС у сфері ПВК/ФТ вимоги щодо реєстрації бенефіціарної власності поширено на іноземних юридичних осіб та трасти, які набувають нерухомість на території Союзу. За певних умов охоплюється також майно, придбане раніше, зокрема після 2014 року. Автори вважають, що саме регіональне регулювання ЄС є основною причиною того, що європейські держави демонструють вищий рівень охоплення іноземних власників порівняно з іншими регіонами. Водночас членство в ОЕСР саме по собі не гарантує існування аналогічних вимог. У багатьох економічно розвинених державах система бенефіціарної прозорості може залишатися неповною, якщо немає регіонального або національного зобов'язання розкривати КБВ іноземних структур, пов'язаних із нерухомістю.

Автори звертають увагу і на ситуацію у Сполучених Штатах, яку вони розглядають як приклад відступу від загальної тенденції до розширення корпоративної прозорості. Після змін у застосуванні Закону США про корпоративну прозорість (Corporate Transparency Act) значна частина внутрішніх американських компаній була фактично виведена з-під вимог щодо подання відомостей про бенефіціарних власників, тоді як окремі зобов'язання збереглися для іноземних компаній, що здійснюють діяльність у США. Такий підхід, на думку авторів, суперечить глобальній тенденції до створення всеохопних реєстрів КБВ та може зберігати можливості для використання американських юридичних осіб у непрозорих структурах володіння активами.

Другий основний блок дослідження присвячений організації реєстрів нерухомості та практичній доступності інформації. Навіть якщо законодавство вимагає розкриття бенефіціарної власності, відповідні відомості можуть бути малокорисними, якщо інформація про нерухомість зберігається в децентралізованих місцевих або регіональних реєстрах, доступна лише в паперовому вигляді або потребує подання окремого запиту до кожного органу. Автори розглядають централізацію як наявність єдиного національного реєстру або центральної електронної платформи, яка забезпечує доступ до всіх регіональних систем. Централізація не обов'язково означає фізичне зберігання всіх даних в одному органі, однак користувач повинен мати можливість здійснювати пошук через єдиний інтерфейс.

Цифровізація також є принципово важливою. Наявність паперових документів або електронних зображень витягів не забезпечує можливості для автоматичного аналізу. Для ефективного фінансового моніторингу, розшуку активів і застосування санкцій дані повинні бути структурованими, машинозчитуваними та придатними для зіставлення з іншими інформаційними системами. Ідеальна модель передбачає можливість пошуку за адресою,

кадастровим номером, юридичним власником, реєстраційним номером компанії та КБВ. Особливе значення має зворотний пошук, який дозволяє встановити всі об'єкти нерухомості, пов'язані з конкретною фізичною або юридичною особою. Без такої функції компетентний орган може перевірити лише наперед відому адресу, але не здатний ефективно виявити невідомі активи особи.

За даними дослідження, 83 держави з централізованими системами надають в електронному вигляді принаймні певну інформацію про нерухомість. Проте така інформація не завжди включає відомості про власника. У багатьох випадках електронні кадастрові портали показують лише межі земельної ділянки, її площу, призначення, кадастровий номер або технічні характеристики. Лише приблизно 34 юрисдикції одночасно мають централізовану систему та дозволяють отримувати онлайн інформацію саме про власників. Отже, наявність електронного геопорталу або цифрового кадастру не може автоматично розглядатися як доказ належного рівня прозорості власності.

Навіть у тих державах, де інформація про власника доступна онлайн, доступ до неї може бути істотно обмежений. У деяких юрисдикціях заявник повинен довести законний інтерес, отримати дозвіл суду, згоду власника або підтвердження від державного органу. В інших випадках доступ надається лише нотаріусам, адвокатам, банкам, органам влади або іншим визначеним категоріям користувачів. Додатковою перешкодою може бути вимога мати місцеве громадянство, резидентство, національний ідентифікаційний номер або засіб електронної ідентифікації. Такі умови фактично унеможливлюють прямий доступ для іноземних компетентних органів, журналістів-розслідувачів, громадських організацій та дослідників.

Суттєвим бар'єром є плата за отримання інформації. Навіть якщо вартість одного витягу здається невисокою, необхідність перевірити сотні або тисячі об'єктів робить масовий аналіз надзвичайно дорогим. Автори умовно розглядають плату понад 12 євро за один запис як потенційно заборонну. Крім безпосередньої вартості, значення має складність здійснення транскордонних платежів, необхідність створення облікового запису, використання національних платіжних засобів або окремої оплати за кожний запит. Такі технічні та фінансові обмеження особливо негативно впливають на міжнародні розслідування та діяльність громадянського суспільства.

Лише сім держав відповідають визначеному авторами оптимальному сценарію, за якого інформація про власність централізована, доступна онлайн, відкрита для громадськості та надається безоплатно. До них належать Хорватія, Данія, Люксембург, Північна Македонія, Сербія, Словенія та Швеція. Велика Британія не включена до цієї групи через існування окремих систем для Англії та Уельсу, Шотландії й Північної Ірландії, хоча окремі британські реєстри можуть забезпечувати високий рівень доступності. Це свідчить, що методологія документа оцінює не лише відкритість відомостей, а й територіальну повноту та інституційну цілісність системи.

Автори визнають, що особистий доступ до реєстрів є кращим, ніж повна відсутність інформації, але значно поступається дистанційному електронному доступу. Необхідність фізично відвідувати державний орган створює значні часові та фінансові витрати, особливо для іноземних користувачів. Якщо реєстри децентралізовані, особа може бути змушена звертатися до десятків або сотень місцевих установ. Крім того, особистий доступ зазвичай не дозволяє здійснювати масове завантаження інформації або автоматизований аналіз.

У документі особливо підкреслюється значення реєстрових даних для підрозділів фінансової розвідки, правоохоронних органів, податкових адміністрацій, органів з повернення активів і санкційних органів. Централізований цифровий реєстр може використовуватися для зіставлення інформації про нерухомість із санкційними переліками, реєстрами юридичних осіб, даними про КБВ, податковими деклараціями, повідомленнями про підозрілі фінансові операції та іншими джерелами. Це дозволяє виявляти ситуації, коли особа з низькими офіційними доходами контролює значний обсяг нерухомості, коли одна адреса пов'язана з

великою кількістю компаній або коли нерухомість оформлена на структуру, пов'язану із санкційною особою чи високоризиковою юрисдикцією.

Транскордонний вимір прозорості нерухомості розглядається у зв'язку з новою системою ОЕСР для автоматичного обміну доступною інформацією про нерухоме майно – Immovable Property Information. Станом на грудень 2025 року 26 юрисдикцій зобов'язалися розпочати такий обмін у 2029 або 2030 році. Передбачається, що держави обмінюватимуться інформацією про нерухомість, якою володіють резиденти інших юрисдикцій, що може сприяти виявленню незадекларованих активів і випадків ухилення від оподаткування.

Водночас автори вказують на фундаментальне обмеження цього механізму. На відміну від Загального стандарту звітності щодо фінансових рахунків, система обміну інформацією про нерухомість не вимагає від держав створювати нові дані або змінювати національні реєстри. Обміну підлягатиме лише та інформація, яка вже є доступною в державі. Якщо національний реєстр містить лише дані про формального власника, не охоплює іноземні компанії, не включає інформацію про КБВ або функціонує лише на регіональному рівні, міжнародний обмін відтворюватиме ці прогалини. Отже, ефективність міжнародної системи безпосередньо залежить від якості та повноти національних реєстрів.

У завершальній частині доповіді автори формулюють комплексну модель реформування систем прозорості нерухомості. Насамперед державам рекомендується поширити вимоги щодо розкриття КБВ на всі місцеві та іноземні юридичні особи і правові утворення, які набувають або утримують права чи економічні інтереси щодо нерухомості. Тригером для реєстрації має бути не лише факт створення компанії відповідно до національного законодавства, а й сам факт володіння нерухомим майном у відповідній державі. Такі вимоги повинні охоплювати як нові придбання, так і вже наявні об'єкти, оскільки застосування правил лише до майбутніх операцій залишатиме значний масив старих активів поза системою прозорості.

Необхідною умовою є повна територіальна централізація або створення єдиного національного електронного шлюзу до всіх регіональних реєстрів. Дані повинні бути цифровими, структурованими та машинозчитуваними. Реєстр нерухомості має бути пов'язаний із корпоративним реєстром і реєстром КБВ за допомогою унікальних ідентифікаторів. Для компетентних органів необхідно передбачити прямий доступ, можливість масового завантаження даних та використання програмних інтерфейсів. Система повинна дозволяти здійснювати пошук не лише за конкретною адресою, а й за ім'ям фізичної особи, назвою юридичної особи, реєстраційним номером та КБВ.

Автори підтримують публічність інформації як найбільш ефективну модель, оскільки громадський доступ дозволяє журналістам, громадським організаціям, науковцям і приватному сектору виявляти невідповідності та доповнювати можливості державного контролю. Водночас допускаються індивідуальні винятки, якщо розкриття інформації створює доведену загрозу життю, здоров'ю або безпеці конкретної особи. Такі винятки не повинні бути автоматичними або поширюватися на широкі категорії власників.

Якщо держава застосовує вимогу щодо законного інтересу, законодавство повинно прямо визнавати такий інтерес за журналістами-розслідувачами, громадськими організаціями, науковими установами та іноземними компетентними органами. Власник не повинен автоматично отримувати повідомлення про кожний запит щодо його майна, оскільки це може створювати ризик приховування активів, перешкоджання розслідуванню або тиску на особу, яка проводить перевірку. Інформація про користувачів реєстру може розкриватися лише у виняткових випадках, наприклад за наявності доказів переслідування, шахрайства або іншого зловживання доступом.

Окремою рекомендацією є усунення надмірних фінансових бар'єрів. Інформація повинна бути безоплатною або принаймні надаватися безкоштовно компетентним органам, журналістам-розслідувачам, громадським організаціям та науковим установам. Плата за витяги не повинна

використовуватися як фактичний механізм обмеження доступу. Якщо держава потребує компенсації адміністративних витрат, вона може застосовувати помірну фіксовану плату або надавати пільгові умови для масового доступу, але не повинна створювати модель, за якої кожна перевірка окремого об'єкта потребує значних витрат.

Висновки:

- **Лише 40 зі 117 юрисдикцій, які мають законодавство про реєстрацію КБВ, поширюють його на іноземні структури, що володіють нерухомістю.** Це залишає значні можливості для приховування фактичних власників через іноземні компанії та трасти.
- **Наявність реєстру нерухомості не гарантує прозорості,** оскільки в багатьох країнах дані залишаються фрагментованими, або не містять інформації про юридичних осіб і КБВ.
- **Практичний доступ до інформації часто обмежують вимоги щодо** законного інтересу, місцевої електронної ідентифікації, професійного статусу заявника або сплати коштів за кожний витяг.
- **Міжнародний обмін інформацією про нерухомість буде ефективним лише за умови,** що національні реєстри міститимуть повні, актуальні та доступні дані про власників і КБВ.

Водночас документ містить низку методологічних застережень. Дослідження переважно оцінює формальну законодавчу та інституційну архітектуру, а не фактичну ефективність її застосування. Воно не проводить повної перевірки точності реєстрових даних, частоти їх оновлення, ефективності верифікації, практики застосування санкцій або спроможності компетентних органів використовувати відповідну інформацію. Юрисдикція може бути віднесена до категорії країн із реєстром КБВ навіть тоді, коли реєстр ще не функціонує повною мірою або охоплює лише окремі типи юридичних осіб. Аналогічно наявність електронного реєстру не означає, що він містить інформацію про власників або підтримує пошук за фізичною особою.

Таким чином, головний висновок доповіді полягає в тому, що глобальний прогрес у сфері прозорості бенефіціарної власності ще не призвів до створення цілісної системи прозорості нерухомості. У більшості держав реєстри нерухомості, юридичних осіб і КБВ залишаються фрагментованими, а іноземні структури часто не охоплюються національними вимогами. Навіть там, де інформація формально існує, вона може бути недоступною через децентралізацію, відсутність цифровізації, вимоги щодо законного інтересу, місцевої ідентифікації або високу плату. Тому ефективна протидія використанню нерухомості для відмивання коштів, корупції, обходу санкцій і приховування активів потребує не окремих формальних реєстрів, а інтегрованої системи, яка забезпечує встановлення фізичної особи – КБВ, дозволяє здійснювати автоматизований пошук і зіставлення даних та підтримує національний і міжнародний обмін повною, актуальною і придатною для аналізу інформацією.

Героїнові маршрути після заборони Талібану: трансформація незаконного обігу від Афганістану до Європи [9]

Документ Глобальної ініціативи проти транснаціональної організованої злочинності (GI-TOC) аналізує трансформацію міжнародних ланцюгів виробництва та постачання афганських опіатів після повернення Талібану до влади у 2021 році й запровадження у квітні 2022 року заборони на вирощування опійного маку, виробництво, транспортування та торгівлю наркотиками. Автори досліджують, наскільки різке скорочення виробництва опію вплинуло

[9] https://globalinitiative.net/wp-content/uploads/2026/07/Paddy-Ginn-and-Danial-Husain-Heroin-trafficking-along-the-northern-and-southern-routes-GI-TOC-July-2026.pdf

на доступність героїну в Центральній Азії, росії, Африці, Європі та Великій Британії, як злочинні мережі пристосувалися до нових умов і які ділянки маршрутів потребують першочергового міжнародного втручання. Основний висновок полягає в тому, що скорочення культивації в Афганістані не призвело до пропорційного зникнення героїну з міжнародних ринків. Натомість ринок став більш прихованим, географічно розосередженим, гнучким і тісніше пов'язаним із незаконним обігом синтетичних наркотиків.

Дослідження проводилося протягом шести місяців у 2025 році та на початку 2026 року й ґрунтувалося на польових даних, напівструктурованих інтерв'ю з учасниками наркотичної економіки, представниками правоохоронних органів, місцевою владою, експертами та членами громад. В Афганістані було проведено 39 інтерв'ю у шести провінціях, а отриману інформацію перевіряли шляхом зіставлення свідчень різних категорій респондентів. Водночас автори наголошують на обмеженнях дослідження, пов'язаних із закритістю Афганістану, обмеженням діяльності міжнародних організацій, послабленням системи моніторингу ООН, нестачею достовірних даних про вилучення наркотиків, контейнерні перевезення та діяльність іранських мереж.

Звіт демонструє суперечливість сучасного героїнового ринку. Якщо у 2017 році Афганістан забезпечував приблизно 86% світового виробництва опію, то після заборони Талібану обсяг виробництва афганських опіатів, за наведеними оцінками, скоротився приблизно на 97%. Площі вирощування маку зменшилися з 233 тис. гектарів у 2022 році до 10,8 тис. гектарів у 2023 році. Водночас героїн залишається доступним у Європі й Азії, а рівні споживання та пов'язаної з ним шкоди не скорочуються відповідно до падіння виробничих показників. Автори пояснюють це накопиченими запасами опію, залишковою культивацією, переміщенням виробництва до нових районів та здатністю злочинних мереж швидко змінювати маршрути й методи перевезення.

Значні запаси опію були сформовані ще до повного запровадження заборони. Опій може зберігатися протягом тривалого часу й використовується великими торговцями як засіб накопичення вартості та страхування від ринкових потрясінь. Частину таких запасів, за даними польових джерел, контролюють впливові учасники наркотичної економіки, пов'язані з представниками фактичної влади. Саме тому наслідки заборони можуть повністю проявитися лише після виснаження резервів. Нинішня відносна стабільність ринку не виключає майбутнього дефіциту, зниження чистоти героїну та його активнішого заміщення синтетичними речовинами.

Одночасно відбулася зміна географії виробництва. Якщо раніше основним центром опійної економіки був південний захід Афганістану, насамперед провінція Гільменд, то тепер особливого значення набули Бадахшан на північному сході країни та пакистанський Белуджистан. За оцінкою авторів, у 2025 році на Бадахшан припадало близько 40% регіонального виробництва опію, на Белуджистан – 25%, на Гільменд – 20%, на Фарах – 10%, а на східні та південно-східні райони Афганістану – близько 5%. Отже, заборона не ліквідувала виробничу базу, а частково перемістила її до районів, де контроль Талібану є слабшим, населення сильніше опирається знищенню посівів або виробництво відбувається вже за межами Афганістану.

Бадахшан перетворився на ключовий центр залишкового виробництва та початкову точку північного маршруту. Частина опію звідти безпосередньо переміщується через річки Пяндж та Амудар'ю до Таджикистану, а інша частина транспортується всередині Афганістану до Кабула, Кандагара, Гільменду, Німрозу і Фараху. Південно-західні провінції, навіть після скорочення місцевої культивації, зберегли значення як центри перероблення, зберігання, консолідації та підготовки вантажів до транскордонного переміщення. У цих районах продовжують діяти лабораторії, брокери, перевізники, склади й усталені корупційні зв'язки.

Внутрішня система незаконного обігу в Афганістані базується на племінних, сімейних та особистих зв'язках, патронаті, хабарництві й розподілі прибутку з представниками влади. Великі торговці закуповують опій у різних провінціях, використовують головних перевізників

і дрібних кур'єрів, передають вантажі брокерам у прикордонних районах, після чого продукцію отримують пакистанські та іранські белуджські мережі. Автори наводять приклади, коли місцеві представники Талібану нібито надавали захист торговцям, брали участь у перевезеннях або отримували частину прибутку. Застосування заборони описується як нерівномірне та вибіркове: відкриті ринки формально закриваються, але торгівля переміщується до приватних приміщень, одні лабораторії знищуються, тоді як інші продовжують роботу завдяки зв'язкам їхніх власників із впливовими особами.

Північний маршрут залишається дієвою, хоча й менш інтенсивною системою переміщення опіатів із північно-східного Афганістану через Таджикистан, Узбекистан, Киргизстан і Казахстан до росії та частково до Європи. Інша гілка може проходити через Туркменістан, Каспійське море, Азербайджан, Грузію, Туреччину та Балкани. Автори не вважають скорочення вилучень доказом занепаду маршруту, оскільки наркотики дедалі краще приховуються у великих потоках законної торгівлі, сільськогосподарських вантажах, автомобільних і залізничних перевезеннях. Таджикистан залишається головною точкою входу через протяжний і важкодоступний кордон з Афганістаном, Узбекистан і Киргизстан виконують функції альтернативних коридорів, Казахстан є основною транзитною магістраллю до росії, а Туркменістан забезпечує потенційний вихід до Кавказу через Каспійське море.

Однією з ключових змін на північному маршруті є зростання ролі синтетичних наркотиків. Героїн дедалі рідше перевозиться окремо, а змішані партії можуть містити метамфетамін, мефедрон, альфа-PVP, гашиш та інші нові психоактивні речовини. Частина синтетичних наркотиків виробляється безпосередньо в Афганістані, а частина – у державах Центральної Азії. У результаті героїн стає менш помітним для правоохоронних органів, які переорієнтовують ресурси на швидко зростаючий синтетичний ринок.

Південний маршрут є значно ширшим і складнішим та охоплює наземні потоки з Афганістану до Пакистану й Ірану, морські перевезення через Аравійське море та Індійський океан, контейнерні відправлення, традиційні судна доу, швидкі катери, морські схованки, повітряних кур'єрів і поштові відправлення. Пакистан виступає виробничою територією, транзитною державою, центром консолідації й морською платформою для експорту. У Белуджистані розширюється вирощування маку, а основні маршрути з'єднують афганський кордон із Кветтою, Карачі та узбережжям Макрану. Звідти наркотики прямують до держав Перської затоки, Східної Африки, Індії, Шрі-Ланки та Європи.

Іран залишається ключовим мостом між Афганістаном і Пакистаном, з одного боку, та Туреччиною, Кавказом, Балканами і Європою – з іншого. Великі партії дедалі частіше дробляться, тимчасово зберігаються, а потім повторно консолідуються. Наркотики приховують у вантажівках, приватному транспорті, легальних товарах і контейнерах. Частина маршрутів одночасно використовується для незаконного переправлення мігрантів, контрабанди товарів та інших злочинних операцій, що свідчить про багатофункціональність відповідної інфраструктури.

Східна та Південна Африка вже не є лише транзитними зонами. Кенія, Танзанія, Мозамбік, Мадагаскар, Маврикій і Південна Африка виконують функції приймання, зберігання, перепакування, розподілу та подальшого експорту наркотиків. Частина героїну залишається на місцевих ринках, посилюючи соціальні та медичні проблеми. Мадагаскар став важливим регіональним центром зберігання, Маврикій поєднує транзитну функцію зі значним внутрішнім споживанням, а Південна Африка є привабливою через великі контейнерні порти, міжнародні аеропорти, розвинену транспортну систему й фінансовий сектор.

Окрему увагу приділено посиленню Кавказького маршруту. Азербайджан набув стратегічного значення завдяки кордону з Іраном, виходу до Каспійського моря та сполученню через Нахічевань із Туреччиною. Вантажі можуть рухатися через Азербайджан і Грузію до Чорного моря або через Нахічевань до Туреччини, оминаючи найбільш контрольовані ділянки ірансько-турецького кордону. Російсько-українська війна змінила логістику Чорноморського регіону та сприяла перенаправленню частини потоків. Туреччина при цьому зберігає роль

головного вузла між азійськими джерелами постачання та європейськими ринками, зокрема через використання контейнерних перевезень до портів Італії, Хорватії та Словенії.

Європейський ринок героїну поки що не зіткнувся з різким дефіцитом завдяки запасам, залишковому виробництву та стійкості логістичних мереж. Водночас героїну надходить менше, його чистота знижується, а склад стає менш передбачуваним. Торговці компенсують обмежену пропозицію розведенням і змішуванням із синтетичними опіоїдами, зокрема нітазенами. У деяких випадках речовини, продані як героїн, можуть майже не містити самого героїну. Одночасно поширюється полінаркотичне вживання – поєднання героїну з кокаїном, креком, метадоном, бензодіазепінами та стимуляторами, що посилює ризики для здоров'я та ускладнює токсикологічний контроль.

У контексті України автори зазначають, що війна порушила частину традиційних поставок героїну з російського напрямку до Києва. Скорочення доступності героїну могло сприяти переходу частини споживачів до дешевих синтетичних катинонів місцевого виробництва. Це демонструє, що скорочення постачання традиційного наркотику не обов'язково зменшує шкоду, а може стимулювати його заміщення більш токсичними та непередбачуваними синтетичними речовинами.

Однією з наскрізних тем документа є перетворення Афганістану на значний центр виробництва метамфетаміну. Синтетичні наркотики використовують ті самі маршрути, транспортну інфраструктуру, корупційний захист і міжнародні контакти, що й героїн, а іноді повністю замінюють його у вантажах. Тому скорочення макових посівів не руйнує злочинні мережі, а підштовхує їх до багатотоварної моделі, у якій героїн є лише одним із видів незаконної продукції.

У підсумку автори наголошують, що сучасний героїновий ринок характеризується не стільки масштабом, скільки високою адаптивністю, непрозорістю та тісним переплетенням із синтетичними наркотиками. Для ефективного реагування необхідно відновлювати моніторинг наркотичних потоків у Центральній і Південній Азії, розвивати лабораторні можливості, удосконалювати контроль контейнерних і морських перевезень, посилювати міжнародний обмін інформацією та створювати системи раннього попередження про появу небезпечних синтетичних речовин. Заходи мають бути спрямовані не лише на окремі вилучення, а на всю

Висновки:

- **Необхідно відновити наскрізний моніторинг наркотичних потоків.** Необхідно поєднати дані про культивацію, вилучення, ціни, чистоту речовин, токсикологічні результати, контейнерні та пасажирські перевезення. Пріоритетними зонами мають бути афганські прикордонні райони, Таджикистан і Узбекистан, Кавказ, Пакистан та Іран, а також ключові порти Східної і Південної Африки.
- **Доцільно перенести акцент із вилучення окремих партій на руйнування всієї інфраструктури.** Практичні заходи мають охоплювати фінансові розслідування, виявлення брокерів, перевізників, експедиторів, корумпованих посадовців і власників підставних підприємств, аналіз вантажних документів та обмін інформацією про логістичні компанії.
- **Потрібно адаптувати контроль до змішаних партій і синтетизації ринку.** Прикордонним, митним і лабораторним органам потрібні сучасні засоби ідентифікації метамфетаміну, синтетичних речовин, а також механізми обміну хімічними профілями.
- **Необхідно поєднати правоохоронні заходи із системою раннього попередження та охороною здоров'я.** Необхідно розширити тестування речовин у спільнотах споживачів, токсикологічний моніторинг, попередження про небезпечні домішки, доступ до замісної підтримувальної терапії та програм зменшення шкоди.

інфраструктуру незаконного обігу – від виробництва й брокерів до фінансових потоків, логістичних компаній, корупційного захисту та наслідків для громадського здоров'я.

Глобальна організована злочинність в Океанії [10]

Океанія, регіон, який часто сприймається через призму своєї природної краси та географічної ізоляції, насправді є складним і суперечливим фронтом у глобальній боротьбі з організованою злочинністю. Як свідчить звіт Глобальної ініціативи проти транснаціональної організованої злочинності, цей континент демонструє парадоксальний профіль: його загальні показники злочинності є одними з найнижчих у світі, проте окремі види кримінальних ринків тут досягають загрозливих масштабів, а вразливість окремих субрегіонів створює поживне середовище для діяльності транснаціональних злочинних угруповань.

На перший погляд, Океанія демонструє відносну стабільність. Її сукупний показник злочинності, який у 2025 році становить 3.15 за 10-бальною шкалою, залишається найнижчим серед усіх континентів, значно поступаючись Азії (5.30), Африці (5.17) та навіть середньосвітовому рівню (5.08). Цей низький середній показник, однак, є оманливим, оскільки він маскує глибокі регіональні контрасти та приховує надзвичайно високі піки кримінальної активності в окремих сферах. Якщо заглибитися в структуру, стає зрозуміло, що Океанія не є епіцентром масової злочинності, як-от Азія, але вона є складним конгломератом кримінальних економік, де лише кілька ринків справляють непропорційно великий вплив завдяки глобальним потокам і місцевим вразливостям. Особливу тривогу викликає те, що за останні п'ять років, попри невелике зниження у 2025 році, загальний рівень злочинності в регіоні демонструє тенденцію до зростання, що свідчить про поступове, але стійке проникнення злочинних елементів у різні сфери життя.

Одним з найяскравіших і найбільш суперечливих аспектів регіону є його ринки кримінальних послуг та товарів. Незважаючи на те, що середній показник для всіх 15 кримінальних ринків є найнижчим у світі (3.06), Океанія водночас є домівкою для деяких з найбільш розвинених у світі ринків незаконного обігу фауни. Цей парадокс є ключем до розуміння ситуації.

Злочинність у сфері довкілля, зокрема незаконний вилов риби, є справжнім лихом для регіону, особливо для Меланезії та Мікронезії, які посідають друге та третє місця у світі за цим показником, поступаючись лише Південно-Східній Азії. Цей вид злочинності, що стрімко зріс на 0.68 пункту з 2021 року, живиться багатством морського біорізноманіття, яке приваблює промислові флоти, переважно з азійських країн, що діють без ліцензій, використовують руйнівні методи вилову та завдають колосальної шкоди морським екосистемам. Агентство рибальства Тихоокеанських островів оцінює щорічні збитки для країн регіону від рибальства приблизно в 600 мільйонів доларів США, що є відчутним ударом по їхніх крихких економіках, які часто є заручниками природних ресурсів. Торгівля дикими тваринами, зокрема птахами, рептиліями та морськими видами, додає ще один шар складності, живлячи азійські ринки та підриваючи зусилля зі збереження природи. Цей контраст підкреслює, що відносно низькі середні показники не повинні вводити в оману: злочинність у сфері фауни тут має руйнівний вплив, який не поступається впливу наркотрафіку в інших частинах світу.

Ринки наркотиків становлять ще один гострий кут океанійської кримінальної реальності. Синтетичні наркотики, зокрема метамфетамін, та канабіс є одними з п'яти найбільших кримінальних ринків континенту. Якщо канабіс демонструє певну стагнацію або навіть скорочення, то ринок синтетичних наркотиків неухильно зростає впродовж усіх трьох вимірів Індексу. Найбільш драматично ця тенденція проявляється в Австралії та Новій Зеландії, де аналізи стічних вод підтверджують домінування метамфетаміну, а ринкова вартість цієї речовини зростає з кожним роком. Цей регіон перетворився на один із глобальних вузлів наркоторгівлі, де попит на синтетику настільки високий, що тихоокеанські острови стали не лише транзитним пунктом, а й дедалі частіше – місцем дрібномасштабного виробництва. У

[10] https://globalinitiative.net/wp-content/uploads/2026/07/Global-Organized-Crime-Index_Continental-Overview_Oceania.pdf

Меланезії, особливо у Фіджі та Папуа-Новій Гвінеї, фіксуються випадки створення підпільних лабораторій та зростання споживання, що призвело до підвищення середнього показника для регіону, хоч він і залишається нижчим за світовий. Цей процес не є локальним явищем; він тісно переплетений з діяльністю транснаціональних мереж – від азійських синдикатів до мексиканських картелів, які постачають прекурсори з Китаю та кокаїн з Латинської Америки. Як наслідок, Океанія, незважаючи на відсутність значного ринку героїну, має найвищий у світі рівень споживання кокаїну на душу населення, що свідчить про глибоку інтеграцію регіону в глобальні наркотичні потоки та зміну структури споживання.

Структура кримінальних акторів в Океанії також є унікальною та відображає суперечливий характер регіону. На відміну від інших континентів, де домінують мафіозні групи або добре структуровані організації, океанійський ландшафт характеризується фрагментованою "мозаїкою" гравців, чия роль різко відрізняється залежно від субрегіону. Найпомітнішою та найвпливовішою силою є іноземні злочинці, чий вплив невпинно зростає з 2021 року. У країнах Меланезії, зокрема в Папуа-Новій Гвінеї та Соломонових Островах, їхня присутність є визначальною. Азійські синдикати, латиноамериканські картелі, а також іноземні компанії, що займаються вирубкою лісів або рибальством, проникають у всі сфери – від наркоторгівлі до екологічних злочинів та фінансових махінацій. Вони часто діють через корумповані місцеві еліти або утворюють альянси з політичними лідерами, фактично вбудовуючи злочинність у структури управління та ресурсні сектори. На противагу цьому, в Австралії та Новій Зеландії, де показники стійкості (resilience) є одними з найвищих у світі, домінують внутрішні структуровані групи, насамперед байкерські угруповання. Вони відомі своєю жорстокою репутацією, контролюють значну частину ринків метамфетаміну та канабісу, а також активно диверсифікуються у сфери шахрайства та відмивання грошей. Цікаво, що їхній вплив поширюється і на невеликі острівні держави через так званих "депортованих" злочинців, які повертаються на батьківщину та використовуються для створення нових осередків і налагодження кримінальних зв'язків, зокрема у Фіджі, Тонга та Французькій Полінезії.

Водночас, в Океанії спостерігається зростання ролі так званих "державно-вкорінених" акторів та кримінальних мереж. Останні набувають дедалі більшого значення в Австралії та Новій Зеландії, особливо у сфері кіберзлочинності та фінансових шахрайств, що відповідає світовим тенденціям. Однак найтривожнішим є посилення впливу державно-вкорінених акторів у Меланезії, де політичні та ділові лідери дедалі частіше використовують свої зв'язки та регуляторні прогалини для сприяння незаконній діяльності, від вирубки лісів до видобутку корисних копалин. Це явище не лише підриває верховенство права, але й створює ситуацію, за якої боротьба зі злочинністю стає неможливою без боротьби з корупцією на найвищих рівнях.

Аналіз стійкості (resilience) до організованої злочинності в Океанії виявляє ще один глибокий структурний розрив. Загальний показник стійкості континенту становить 5.44, що робить його другим найстійкішим регіоном у світі після Європи. Однак цей високий показник є, по суті, "ілюзією", створеною потужними системами Австралії та Нової Зеландії, які мають показники вище 7.0 завдяки сильним судовим системам, ефективній поліції та активній міжнародній співпраці. Вони демонструють значний прогрес у боротьбі з відмиванням грошей та кіберзлочинністю. На противагу цьому, більшість тихоокеанських острівних держав мають значно слабші та нерівномірні структури стійкості, з середніми показниками від 4.55 у Меланезії до 5.66 у Полінезії. Їхні правоохоронні органи потерпають від хронічного недофінансування, а судові системи завалені справами, що створює значні затримки в правосудді та підриває довіру до інституцій. Особливо проблемними є такі сфери, як підтримка жертв і свідків та превентивні заходи, які отримали найнижчі оцінки. У той час як Австралія та Нова Зеландія інвестують у громадські кампанії та комплексні стратегії запобігання, у більшості тихоокеанських країн ці показники рідко перевищують 4.0, що свідчить про значні ресурсні обмеження та відсутність захисних механізмів для найвразливіших груп населення, які стають легкою здобиччю для торговців людьми та експлуататорів.

На додачу до внутрішніх вразливостей, Океанія стикається з новими, екзистенційними викликами, що підживлюють організовану злочинність. Кліматична криза, яка тут проявляється з катастрофічною силою через підвищення рівня моря, часті циклони та посухи, вже сьогодні призводить до масового переміщення населення. За оцінками Всесвітньої метеорологічної організації, щонайменше 50 000 жителів Тихоокеанських островів ризикують бути переміщеними щороку. Це явище, відоме як "кліматична мобільність", створює безпрецедентні ризики. Люди, позбавлені домівок і традиційних засобів існування, стають надзвичайно вразливими до торгівлі людьми, примусової праці та експлуатації. Відсутність безпечних та легальних шляхів міграції, за винятком першого у світі "Шляху мобільності Фалепілі" за договором Австралії та Тувалу, змушує багатьох людей шукати нелегальні способи, що штовхає їх у тінь, де вони стають легкою мішенню для злочинців. Таким чином, кліматичні зміни не є віддаленою перспективою, а вже сьогодні діють як "каталізатор" злочинності, поглиблюючи існуючі соціально-економічні проблеми та створюючи нові вразливості, які організована злочинність не забариться використати.

Таким чином, звіт Глобальної ініціативи малює багатошарову та тривожну картину. Океанія не є «тихим куточком» планети в контексті організованої злочинності. Натомість, це арена гострих контрастів: низькі середні показники знаходяться поруч із висококонцентрованими кримінальними ринками, високий рівень інституційної стійкості в одних країнах різко дисонує з крихкістю та беззахисністю інших, а традиційні форми злочинності переплітаються з новими викликами, такими як кліматична міграція та стрімке зростання кіберзагроз.

Висновки:

- **Парадокс низьких середніх показників.** Океанія має найнижчий сукупний рівень організованої злочинності серед усіх континентів (3,15 із 10), однак цей показник оманливий: регіон є глобальним епіцентром злочинів проти довкілля, зокрема незаконного вилову риби, що завдає щорічних збитків тихоокеанським державам у ~$600.
- **Розрив у стійкості між регіонами.** Загалом високий рівень стійкості до організованої злочинності в Океанії (5,44 – другий у світі після Європи) є «ілюзією», створеною потужними інституціями Австралії та Нової Зеландії (понад 7,0). Натомість більшість острівних держав Меланезії та Мікронезії мають показники нижче 5,0, що свідчить про хронічну слабкість правоохоронних систем, судів і соціального захисту.
- **На відміну від інших континентів, де переважають локальні мафіозні структури, в Океанії визначальну роль відіграють іноземні кримінальні мережі** – азійські синдикати, латиноамериканські картелі та транснаціональні корпорації, які діють через корумпованих місцевих еліт. Це створює «вбудовану» злочинність у сектори управління ресурсами, особливо в Меланезії.

Перспективи для регіону не є оптимістичними. Якщо в Австралії та Новій Зеландії кримінальні ринки, такі як наркотики та кіберзлочинність, демонструють стійке зростання, що вимагає невпинного вдосконалення методів боротьби, то для тихоокеанських острівних держав ситуація є критичною. Їхня географічна ізоляція не є захистом, а слабкість інституцій та брак ресурсів роблять їх вразливими до експлуатації з боку іноземних кримінальних мереж, які використовують їхні морські простори, ресурси та навіть людей. Дисбаланс у стійкості між розвиненими країнами та острівними державами не просто зберігається, а й загрожує збільшуватися, створюючи «слабкі ланки» у всій системі безпеки континенту.

Якщо міжнародне співтовариство та регіональні лідери не зосередять зусиль на зміцненні інституційної спроможності, боротьбі з корупцією та створенні адаптивних механізмів реагування на нові загрози, Океанія ризикує стати не просто вразливим регіоном, а й значним

джерелом нестабільності в глобальному ландшафті організованої злочинності, де «тихий океан» перетвориться на арену кримінальних війн.

Парадокси управління та неформальні практики у лісовому господарстві Північної Кореї [11]

Публікація GI-TOC пропонує ґрунтовний аналітичний огляд сучасної політики КНДР у сфері лісового господарства, яка є яскравим прикладом того, як формальні інституційні реформи можуть вступати в суперечність із суворими реаліями виживання населення, створюючи складну та суперечливу динаміку.

На перший погляд, статистичні дані свідчать про відносно низький рівень злочинів у сфері флори в Північній Кореї, особливо у порівнянні з сусідніми країнами. Так, з 2021 року індекс злочинності у цій сфері коливається в межах від 1,00 до 3,00, що значно нижче за показники Південної Кореї (3,50–4,00) і особливо Китаю, який демонструє вражаючі 8,50 балів. Такі цифри створюють ілюзію відносного порядку та контролю, проте, як слушно зауважує автор, вони аж ніяк не є свідченням ефективного захисту лісів або відсутності проблем. Натомість, цей низький бал відображає іншу реальність – відсутність великих, незалежних кримінальних синдикатів та організованих ринків нелегальної деревини, що пояснюється тотальним державним контролем над усіма природними ресурсами, а не ефективністю природоохоронних заходів. Ключ до розуміння ситуації криється у показниках стійкості, зокрема в оцінках національної політики, законів та превентивних заходів, які залишаються стабільно низькими (2,0 та 1,0 з 10 відповідно), що вказує на глибоку структурну кризу, яку неможливо подолати лише адміністративними методами.

Історичне коріння цієї проблеми сягає трагічних часів «Важкого маршу» – масштабного голоду 1990-х років, коли крах державної системи постачання змусив мільйони корейців шукати будь-які засоби для виживання, і ліси стали головним джерелом палива, їжі та землі для сільськогосподарських угідь. Наслідки цього неконтрольованого використання були катастрофічними: суцільні вирубки та випалювання лісів, масове використання схилів під городи призвели до небаченої ерозії ґрунтів, зсувів та повеней, які у свою чергу завдали нищівного удару сільському господарству, замкнувши порочне коло залежності населення від лісових ресурсів. За підрахунками, між 1999 та 2008 роками площа деградованих лісів у країні збільшилася приблизно на 1,2 мільйона гектарів, що є колосальною цифрою для невеликої території. Однак важливо усвідомлювати, що сучасна лісова проблема КНДР – це не повернення до хаосу 1990-х, а зовсім інше явище, яке автори називають «дифузною та фрагментованою формою злочинності». Це не традиційний злочинний бізнес, а радше повсякденна практика виживання, вплетена у тканину державного управління, де інтереси окремих домогосподарств, місцевої влади та централізованих планів зіштовхуються у складний клубок неформальних угод, хабарів та адміністративних компромісів. Це сучасне обличчя лісової проблеми, де незаконні дії не є анархічними, а навпаки, структуровані через управлінські механізми, які самі ж їх і породжують.

У відповідь на цю кризу, за правління Кім Чен Ина, було розгорнуто безпрецедентну за своїми масштабами реформу лісового господарства, яка стала частиною ширшої державної політики. Два основоположні плани – «Національний план лісового будівництва» (2015–2044) та план «Чисан-Чису» (2021–2030) – проголосили лісовідновлення не просто екологічним завданням, а національною мобілізаційною кампанією, яка вимагає дисципліни, координації праці та ідеологічної пильності. Ці документи суттєво переформатували підхід до лісових ресурсів, розглядаючи їх не лише як об'єкт охорони, але й як інструмент місцевого економічного розвитку. Особливу увагу приділено так званим «економічним лісам», які призначені для

[11] https://insightcrime.org/news/nino-guerrero-is-dead-this-is-how-he-built-latin-americas-most-notorious-criminal-franchise/

постачання сировини для місцевої промисловості, а їхнє управління покладається на конкретні установи, підприємства та місцеві народні комітети. Це засвідчує перехід до децентралізованої, але жорстко контрольованої системи, де ліси інтегруються у регіональний розвиток, проте державна власність та нагляд залишаються непорушними. Відповідні зміни були внесені й до законодавства: Лісовий закон КНДР неодноразово переглядався та розширювався, включаючи нові положення щодо регулювання постачання, продажу та використання деревини, що мало на меті перетворити абстрактне право державної власності на чіткі юридичні категорії та адміністративні механізми розподілу.

Однак, незважаючи на цей потужний інституційний поштовх, фундаментальні вади системи залишилися невирішеними, що знаходить своє відображення у сталих низьких показниках стійкості. Превентивні заходи, такі як програми лісовідновлення, агролісівництво, боротьба з ерозією та створення спеціальних ділянок для заготівлі дров, є важливими, але вони спрямовані на лікування наслідків, а не на усунення першопричин. Вони не пропонують жодної реальної альтернативи для населення, яке продовжує покладатися на ліс як на основне джерело енергії для обігріву осель у суворі зими. Свідчення цьому – численні повідомлення з повіту Онджін про постійні конфлікти між селянами, які збирають дрова, та лісниками, змушеними посилювати репресії, щоб зберегти свої робочі місця.

Варто також врахувати вплив економічних змін епохи Кім Чен Ина, зокрема впровадження системи польової відповідальності, яка тісніше прив'язує добробут домогосподарств до доступу до землі, а також розширення ринкової діяльності. Ці фактори різко підвищили цінність деревини, дров та дикорослих рослин, перетворивши їх на цінний товар для отримання неформального доходу або для виконання численних зобов'язань перед трудовими колективами та місцевою владою. Таким чином, економічні стимули вступають у пряму суперечність із природоохоронними обмеженнями, посилюючи тиск на лісові масиви.

Висновки:

- **Низький рівень організованої лісової злочинності в КНДР є ілюзією контролю.** Він свідчить не про ефективну охорону природи, а про відсутність незалежних кримінальних ринків через тотальну державну монополію на ресурси; справжня проблема полягає у фрагментованій, повсякденній нелегальній діяльності населення, зумовленій потребами виживання.
- **Формальні інституційні реформи не працюють без усунення структурних причин залежності від лісу.** Попри потужну правову базу, плани лісовідновлення та посилення охорони, показники стійкості політики залишаються критично низькими, оскільки ці заходи не пропонують реальних альтернативних джерел енергії, їжі та доходу для населення.
- **Незаконні лісові практики в КНДР є не девіацією, а вбудованим елементом системи управління.** Вони структуруються через неформальні угоди, хабарі та компроміси між місцевою владою, лісниками та селянами, які одночасно є і виконавцями, і жертвами суворих державних приписів, що робить боротьбу з ними внутрішньо суперечливою.
- **Історична травма 1990-х років досі визначає екологічну та соціальну реальність.** Масштабна деградація лісів часів голоду створила порочне коло, де ерозія та повені підривають сільське господарство, а це, своєю чергою, змушує нові покоління знову звертатися до лісу як до єдиного рятівного ресурсу, попри всі сучасні заборони.

Саме цей дисонанс робить північнокорейський кейс унікальним для аналізу. Незаконне використання лісів тут не є ані класичним злочинним промислом, ані просто порушенням правил окремими громадянами. Воно являє собою складну, структуровану систему, що функціонує завдяки щільній інфраструктурі місцевих органів влади, установ, робочих

осередків, народних груп, лісників та самих мешканців. Саме через цих акторів лісові правила впроваджуються у повсякденне життя: вони організовують примусову працю на відновлювальних кампаніях, забезпечують виконання заборон, моніторять дотримання та передають центральні директиви на місця. Але ті ж самі виконавці, які мають забезпечувати виконання законів, самі ж і страждають від їхніх суворих вимог. Вони також залежать від лісових ресурсів для виживання, що створює нерозв'язну суперечність ролей.

На практиці цей конфлікт вирішується через неформальні механізми: хабарі, обмін товарами чи послугами, або навіть заміну примусової праці на грошову компенсацію. Такі практики дозволяють жителям уникнути покарань, отримати доступ до заборонених ресурсів або впоратися з непосильними зобов'язаннями. З іншого боку, посадовці, на яких покладено відповідальність за правозастосування, часто вимушено втягуються у ці обмінні операції, щоб виконати плани з відновлення та розвитку або ж просто показати керівництву видимість успішної роботи. Отже, посилення управління в даному випадку не пригнічує незаконні дії, а парадоксальним чином структурує умови, за яких відбуваються переговори між контролем, доступом та ухиленням.

Таким чином, розширення лісової політики КНДР не слід сприймати як поверхневий фасад або марну бюрократичну гру. Технічні реставраційні роботи, посилення охорони та вдосконалений моніторинг безсумнівно підвищують формальний потенціал держави, але вони неспроможні вирішити першопричини, які змушують людей і далі використовувати ліси. Це має надзвичайно важливе практичне значення для будь-якої міжнародної взаємодії з КНДР, особливо у сфері довкілля, яка часто вважається одним із найменш політично значущих напрямків для співпраці.

Якщо ж міжнародні партнери зосередяться виключно на цілях відновлення лісів та нарощуванні правоохоронного потенціалу, ігноруючи глибинні проблеми енергозабезпечення, продовольчої безпеки та місцевих інституційних тисків, їхні програми будуть приречені на провал. Реальний прогрес можливий лише за умови комплексного підходу, який визнає, що ліс у Північній Кореї – це не просто екологічний ресурс, а життєво важливий елемент складного соціально-економічного організму, де виживання населення, державний контроль та інституційні реформи переплетені в єдине, суперечливе й водночас стабільне ціле. Ігнорування цього факту означатиме продовження циклу неефективних заходів, які лише відтворюватимуть ті самі моделі неформальної поведінки, що їх вони намагаються подолати.

Рекомендовані матеріали

Роль національних судів у виконанні обмежувальних заходів ЄС [12]

У виданні European Law Review (2026, випуск 3, с. 432–446) опублікована стаття, присвячена зростаючій ролі звернень національних судів держав-членів ЄС до Суду справедливості (Суду ЄС) у справах щодо обмежувальних заходів (санкцій). Авторка констатує, що за період з 2006 року до завершення дослідження (15 березня 2026 року) до Суду ЄС надійшло 43 преюдиційні звернення щодо санкційного права, причому 23 з них – тобто більше половини – стосуються санкцій проти росії, переважно поданих після 2022 року. Показовою є й географічна диверсифікація: якщо перші звернення надходили здебільшого з Німеччини, Франції та Великої Британії, то після 2022 року до практики долучилися суди Австрії, Бельгії, Болгарії, Хорватії, Угорщини, Італії, Латвії, Литви, Румунії, Швеції та Нідерландів.

Стаття детально реконструює юриспруденційну еволюцію, унаслідок якої Суд ЄС узагалі отримав компетенцію розглядати преюдиційні звернення у сфері спільної зовнішньої та безпекової політики (СЗБП) – сфері, де за буквою договорів (стаття 24(1) ДЄС та перший абзац статті 275 ДФЄС) юрисдикція Суду ЄС у принципі виключена, за винятком прямого перегляду

[12] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7025258

законності обмежувальних заходів щодо фізичних чи юридичних осіб. Точкою відліку авторка визначає справи Segi та Gestoras Pro Amnistía (2007), далі – Peftiev (2014) і A and Others (2017), проте справжнім переломним моментом став Rosneft (2017), у якому Суд ЄС на основі системного тлумачення статей 19, 24 і 40 ДЄС, статті 275 ДФЄС та принципу ефективного судового захисту (стаття 47 Хартії) визнав за собою юрисдикцію розглядати в преюдиційному порядку питання дійсності (але не тлумачення) рішень СЗБП, якими запроваджуються обмежувальні заходи. Показово, що навіть після Rosneft ця юрисдикція залишається обмеженою: у справі Neves 77 (2024) Суд ЄС витлумачив положення рішення СЗБП лише тому, що Рада не встановила відповідне положення в регламенті, – тобто виключно через бездіяльність Ради, а не через визнання загальної компетенції тлумачити рішення СЗБП як такі.

Значну частину аналізу присвячено внеску преюдиційних звернень у визначення обсягу індивідуальних заморожень активів. Суд ЄС послідовно тлумачить ключові поняття розширено: «заморожування коштів» охоплює будь-яке використання коштів, що змінює їх призначення, навіть якщо це не призводить до вибуття активів з майна підсанкційної особи (Bank Sepah); заборона «надання коштів у розпорядження» застосовується незалежно від фактичного використання коштів для тероризму (Criminal proceedings E and F) та поширюється на вже укладені до дати внесення в санкційний список договори (Möllendorf), а також на ресурси, які на момент операції ще не готові до використання (Afrasiabi). Особливо показовою є справа EM System (2026), у якій Суд ЄС визнав, що частка володіння в 50% статутного капіталу компанії, не внесеної до санкційного переліку, породжує презумпцію контролю з боку підсанкційної особи, а отже кошти на рахунках такої компанії підлягають замороженню. Найгострішим із неврегульованих питань залишається справа T Trust (очікується рішення), у якій Генеральний адвокат уже висловився на користь поширення заморожування активів на майно, яким траст управляє в інтересах підсанкційної особи, навіть якщо право, що регулює траст, тимчасово позбавляє бенефіціара права розпоряджатися майном, – питання прямого практичного значення з огляду на масштаб трастових структур у європейському фінансовому секторі.

Не менш детально проаналізовано внесок преюдиційних звернень у делімітацію секторальних обмежувальних заходів проти росії. У справі Neves 77 Суд ЄС витлумачив заборону посередницьких послуг щодо військового обладнання розширено – вона застосовується навіть якщо обладнання фізично ніколи не потрапляло на територію ЄС. Натомість у справі W. GmbH (2024) щодо заборони імпорту деревини з М'янми Суд ЄС обрав несподівано вузьке тлумачення: посилаючись на статтю 24 Митного кодексу Союзу щодо суттєвої переробки товару, Суд визнав, що деревина, істотно перероблена в третій країні (у цій справі – на Тайвані), втрачає походження з М'янми і виходить за межі заборони, – висновок, який, на думку авторки, створює потенційну прогалину для обходу санкцій через переробку товарів у транзитних юрисдикціях і разюче контрастує з логікою протидії обходу, застосованою Судом в інших справах. У справі Jemerak (2024) Суд ЄС постановив, що заборона юридичних консультаційних послуг російським особам не поширюється на нотаріальне посвідчення угод з нерухомістю в Німеччині, аргументуючи це необхідністю уникнути розбіжностей у практичному ефекті заборони між державами-членами залежно від їхніх нотаріальних систем.

Окремий блок статті присвячено внеску преюдиційних звернень у тлумачення юридичних наслідків обмежувальних заходів для операторів і національних органів влади. У справі Afrasiabi (2011) Суд ЄС сформулював широкий, суб'єктивний за своєю природою тест обходу санкцій – достатньо, щоб особа свідомо прагнула мети чи наслідку обходу або усвідомлювала таку можливість і приймала її, – що створює операційну невизначеність для бізнесу, але водночас сигналізує про послідовно широке тлумачення заборони обходу в усіх санкційних режимах. У справах Peftiev (2014) та Russisch-Kirgizisch Ontwikkelingsfonds (2025) Суд ЄС обмежив дискрецію національних органів у наданні дозволів на розблокування коштів для покриття судових витрат підсанкційних осіб, визнавши, що стаття 47 Хартії про право на ефективний судовий захист унеможливлює відмову в доступі до коштів, необхідних для

оскарження власного включення до санкційного переліку, – включно з оплатою процесуального збору за подання позову. У справі Inter Rao Lietuva (очікується рішення) Генеральний адвокат висловився на користь права держав-членів самостійно визначати додаткові національні цілі понад перелік ЄС для цілей заморожування активів, оскільки перелік коштів і ресурсів, що підлягають замороженню, на відміну від переліку самих підсанкційних осіб, не є вичерпним за правом ЄС.

Одним із найцінніших методологічних спостережень статті є аналіз статусу «м'якого права» в санкційному правозастосуванні – зокрема консолідованих роз'яснень (FAQ) Європейської Комісії щодо виконання регламентів про санкції проти росії. Авторка підкреслює парадоксальність позиції Комісії: не будучи ані органом, відповідальним за виконання санкцій, ані стороною, яка захищає їх законність перед Судом ЄС, Комісія водночас є автором основного практичного інструменту тлумачення для операторів і національних органів. У справі Jemerak німецький суд прямо відхилив тлумачення Комісії з FAQ (яка вважала заборону юридичних послуг застосовною до нотаріальних дій), визнавши, що воно створює «такий рівень невизначеності», який унеможливлює покладання на нього судом держави-члена. Показово, що сам Суд ЄС у своєму рішенні жодного разу не згадав про статус FAQ Комісії, хоча фактично відхилив позицію, викладену в цьому документі, – авторка розцінює це мовчання Суду як втрачену нагоду дати чітку відповідь на питання про юридичну вагу консолідованих роз'яснень Комісії.

Не менш показовим є аналіз того, як преюдиційні звернення виявляють напругу між ефективністю санкцій та дотриманням основоположних прав. Посилаючись на Висновок Генерального адвоката Шарпстон у справі A and Others, авторка нагадує, що преюдиційні звернення відіграють особливо важливу роль саме для осіб, які постраждали від наслідків рішень СЗБП, але не мають права на пряме оскарження за статтею 275(2) ДФЄС, оскільки заходи не адресовані їм персонально, – для таких осіб преюдиційне звернення нерідко є єдиним доступним судовим засобом захисту. У справі Jemerak Генеральна адвокатка Медіна у своєму Висновку прямо обґрунтувала вузьке тлумачення заборони юридичних послуг через право власності (статті 17 і 52(1) Хартії), проте саме рішення Суду ЄС жодного разу не згадало ні право власності, ні відповідні статті Хартії, обмежившись аргументацією про єдність правового ефекту в межах Союзу, – авторка вважає це ще однією втраченою нагодою Суду закріпити роль основоположних прав як гарантії законності обмежувальних заходів.

Підсумовуючи, авторка доходить висновку, що зростання кількості преюдиційних звернень свідчить про поступову «нормалізацію» СЗБП як звичайної сфери правозастосування ЄС, підвладної судовому контролю, а національні суди виконують подвійну функцію – водночас ретранслятора практичних труднощів застосування санкцій і важеля нагляду за практикою національних органів влади. Авторка закликає Суд ЄС не обмежуватися виявленням порушень з боку держав-членів, а поширити таку ж прискіпливість на власну практику інституцій ЄС, зокрема на статус роз'яснень Комісії. Зважаючи на те, що Україна імплементує національний санкційний режим у тісній координації з санкційною політикою ЄС, а питання розшуку активів, пов'язаних з трастовими структурами, і використання заморожених активів рф для потреб відновлення України набуває дедалі більшої ваги, розглянута в статті практика Суду ЄС має пряме значення для формування української методології застосування та оскарження санкцій.

Інші новини

Глобальна операція INTERPOL: безпрецедентний удар по міжнародному шахрайству [13]

У липні 2026 року міжнародна спільнота отримала вагомі докази того, що боротьба з транснаціональною фінансовою злочинністю виходить на якісно новий рівень. Оприлюднені Інтерполом підсумки глобальної антишахрайської операції «First Light 2026» вражають не лише масштабами, а й глибиною аналітичної та оперативної роботи, що тривала понад три місяці за участі 97 країн та територій.

Ця скоординована акція, що відбувалася з 15 січня по 30 квітня 2026 року, стала черговим етапом у протистоянні правоохоронних органів усього світу злочинним синдикатам, які дедалі частіше використовують психологічні маніпуляції, цифрові технології та складні схеми відмивання грошей для досягнення своїх цілей. Результати операції красномовно свідчать про те, що загроза соціальної інженерії набула глобального характеру, зачіпаючи інтереси мільйонів пересічних громадян, приватних компаній і навіть державних установ.

За офіційними даними, у ході проведення «First Light 2026» правоохоронцям вдалося заарештувати 5811 осіб, причетних до організації або виконання шахрайських схем, а також перехопити незаконні активи на загальну суму, що сягає 293 мільйонів доларів США. Втім, ці цифри – лише верхівка айсберга, адже за кожним арештом та заблокованим рахунком стоїть ретельна робота з аналізу понад 152 тисяч кримінальних справ, виявлення понад 142 тисяч постраждалих осіб у різних куточках планети та блокування 31 тисячі банківських рахунків і віртуальних гаманців. Такі показники демонструють, що шахрайство, засноване на методах соціальної інженерії, перетворилося на один із найнебезпечніших видів транскордонної злочинності, який потребує негайного реагування не на національному, а на глобальному рівні. Прикметно, що операція стартувала після попереднього етапу збору та обміну розвідданими, що дозволило різним країнам узгодити свої дії та зосередитися на найбільш резонансних та фінансово потужних злочинних угрупованнях.

Однією з ключових технологічних новацій, що використовувалася під час операції, став механізм Інтерполу Global Rapid Intervention of Payments (I-GRIP), призначений для оперативного блокування незаконних фінансових потоків як у фіатних, так і у віртуальних активах. Завдяки цьому інструменту правоохоронці Сінгапуру та Оману зуміли перехопити транзакцію на суму 6,6 мільйона доларів, пов'язану з компрометацією корпоративної електронної пошти, коли зловмисники, видаючи себе за постачальника, ошукали сингапурську трейдингову компанію. Цей випадок яскраво ілюструє, як стрімкість реагування може буквально врятувати мільйонні статки, адже затримка навіть на кілька годин дозволила б шахраям вивести кошти через ланцюжок підставних рахунків. Крім того, I-GRIP було використано й в інших напрямках, що свідчить про поступовий перехід міжнародних органів від пасивного моніторингу до активного перехоплення фінансових операцій у режимі реального часу, що стає дедалі важливішим в епоху миттєвих переказів.

Незважаючи на значні успіхи в блокуванні активів, особливу увагу привертає різноманіття задокументованих злочинних схем, які свідчать про високу адаптивність та винахідливість сучасних шахрайських мереж. Наприклад, у Есватіні (колишньому Свазіленді) поліція не лише заарештувала 82 особи, але й повністю демонтувала злочинну організацію, яка поєднувала незаконний онлайн-гемблінг, відмивання грошей та складні імітаційні афери. Показово, що шахраї створили реалістичну копію бразильського поліцейського відділку з відповідною формою, вивісками та обладнанням, а потім, видаючи себе за співробітників федеральної поліції Бразилії, переконували жертв у необхідності перевести гроші на

[13] https://www.interpol.int/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust

«безпечне зберігання». Цей приклад демонструє не тільки технічну підготовку шахраїв, а й їхню здатність використовувати міжкультурні та міждержавні особливості: жертви, які довіряли «бразильським правоохоронцям», навіть не підозрювали, що спілкуються з угрупованням, що діє з африканської країни. Через складність цифрових доказів Інтерпол навіть направив на місце оперативну групу для криміналістичного аналізу вилучених пристроїв, що підкреслює критичну важливість міжнародної експертної підтримки під час розслідування подібних резонансних кейсів.

Не менш показовим є випадок у Таїланді, де поліція заарештувала двох осіб і розкрила схему відмивання коштів, отриманих від так званих романтичних шахрайств. Зловмисники конвертували викрадені гроші в різні криптовалюти для приховування слідів транзакцій. Цей метод ускладнює відстеження руху коштів через різні блокчейн-мережі, що ставить перед правоохоронцями нові виклики, адже традиційні методи фінансового моніторингу часто виявляються неефективними. Найбільше вражає, що цифровий гаманець одного з підозрюваних, якому виповнилося лише 20 років, за останні 10 місяців обробив понад 122,5 мільйона доларів США. Цей факт свідчить про те, що до організованої злочинності долучаються молоді люди, які мають глибокі знання в сфері цифрових активів, і що криптовалютна екосистема стає дедалі привабливішою для криміналітету через її відносну анонімність та швидкість проведення операцій.

Водночас операція «First Light 2026» виявила й важливість профілактичних заходів та роботи з населенням, адже найефективніший спосіб боротьби зі соціальною інженерією – це підвищення обізнаності потенційних жертв. Найяскравішим прикладом стала антишахрайська кампанія, проведена поліцією Макао в межах цієї ініціативи. Учасником одного з публічних заходів виявилася особа, яка на той момент перебувала під активним впливом злочинного синдикату. Шахраї, видаючи себе за державних службовців, переконали жертву нібито співпрацювати з ними в рамках вигаданого розслідування та переказати майже 372 тисячі доларів США. Завдяки тому, що поліцейські саме під час заходу виявили ознаки маніпуляції, вдалося втрутитися вчасно та запобігти непоправній фінансовій втраті. Цей випадок підтверджує, що активна комунікація з громадськістю, роз’яснення типових шахрайських патернів і пряме спілкування з громадянами можуть стати вирішальним фактором у порятунку людей від руйнівних фінансових рішень, прийнятих під впливом психологічного тиску.

Ще одним важливим напрямком роботи стало викриття так званих scam-центрів, які діють під прикриттям легальних бізнесів, зокрема готельного бізнесу. Влада Палау депортувала 22 іноземців, причетних до двох пов’язаних шахрайських центрів, що функціонували з готелів. Ці особи використовували криптовалюти та нелегальні гральні вебсайти для атак на іноземних громадян, оперуючи широким спектром онлайн-шахрайств. Цей випадок засвідчує, що географія організованої злочинності не обмежується традиційними «гарячими точками», а охоплює навіть такі віддалені локації, як тихоокеанські острови. Крім того, загалом у ході операції було видано 99 повідомлень Інтерполу (Notices and Diffusions), що дозволило розширити міжнародний розшук підозрюваних та обмежити їхню можливість перетинати кордони. Із 15 606 ідентифікованих підозрюваних та 23 715 розкритих справ випливає, що проблема має системний характер, а масштаби збитків, завданих шахрайськими синдикатами, обчислюються мільярдами доларів щороку.

Фінансування операції з боку Міністерства громадської безпеки Китаю, а також підтримка з боку трьох регіональних поліцейських організацій – ASEANAPOL, GCCPOL та Європолу – підкреслюють важливість колективних зусиль у боротьбі зі злочинністю, яка не визнає національних кордонів. Така широка коаліція свідчить про те, що проблема соціальної інженерії та пов’язаного з нею відмивання коштів є спільною для держав із різними рівнями економічного розвитку та політичними системами.

Таким чином, операція «First Light 2026» стала не лише масштабним поліцейським рейдом, а й важливим сигналом для міжнародної спільноти про те, що майбутнє безпеки у фінансовому секторі залежить від здатності до швидкого об’єднання зусиль, впровадження інноваційних

методів перехоплення платежів і постійного вдосконалення профілактичних заходів, спрямованих на захист найвразливіших верств населення від витончених психологічних маніпуляцій.

Індонезія відкриває канал легалізації активів сумнівного походження через імунітет облігацій Danantara [14]

Агентство Bloomberg повідомило про ухвалення в Індонезії 207-сторінкового закону про фінансовий сектор, який містить положення про безпрецедентний правовий імунітет для покупців облігацій державного інвестиційного фонду Danantara, що управляє активами на суму приблизно 900 млрд дол. США. Норма закону захищає покупки облігацій фонду від кримінальних, цивільних і податкових розслідувань, а також прямо забороняє використання записів про такі операції як доказ у судових провадженнях чи підставу для податкової оцінки. На відміну від попередніх програм податкової амністії – як індонезійських, так і, для порівняння, амністій в Аргентині, Італії та росії, – цей імунітет закріплений у законі без застереження щодо строку дії (sunset clause), що дозволило аналітику Control Risks Ахмаду Сукарсоно охарактеризувати механізм як «постійну угоду, замасковану під облігаційну схему».

Механізм слід розглядати в контексті ширшої політики президента Прабово Субіанто зі централізації державного контролю над ресурсами країни: за відносно низького співвідношення податкових надходжень до ВВП (близько 10%, за оцінкою МВФ, який рекомендував Джакарті пріоритизувати мобілізацію доходів), уряд дедалі більше покладається на Danantara для фінансування флагманських проєктів за умови стримування бюджетного дефіциту. Директор Vriens & Partners в Індонезії Брасукра Суджана прямо охарактеризував логіку норми як «quid pro quo, закріплене в юридичних термінах» – примус місцевих конгломератів купувати облігації Danantara в обмін на звільнення від відповідальності за минулі порушення. Міністр фінансів Пурбая Юдхі Садева намагався применшити ризики, заявивши, що імунітет поширюється виключно на кошти, безпосередньо інвестовані в боргові інструменти фонду, а не на інші активи чи бізнес інвесторів, що можуть залишатися предметом розслідувань.

Реакція профільних інституцій виявила суттєве розходження оцінок: PPATK (підрозділ фінансової розвідки Індонезії) публічно підтримав закон, заявивши, що не вбачає в ньому обмеження власних повноважень, підвищення ризиків відмивання коштів чи впливу на відповідність Індонезії міжнародним стандартам. Натомість Єнті Гарнасіх, одна з провідних індонезійських дослідниць у сфері протидії відмиванню коштів, застерегла, що норма відкриває канал для значно ширшого кола коштів сумнівного походження – включно з криптоактивами, злочинами на ринках капіталу та ухиленням від оподаткування – за обмеженого контролю. FATF у відповіді на запит Bloomberg утримався від коментарів щодо конкретної юрисдикції, проте послався на власні настанови, які прямо рекомендують не допускати винятків з вимог ПВК/ФТ у програмах податкової амністії та репатріації активів, зокрема звільнення фінансових установ від обов'язку проведення повної належної перевірки клієнтів (due diligence) і верифікації законного походження активів.

Історичний контекст підсилює методологічну цінність кейсу: попередня індонезійська амністія 2016–2017 років (з меншою повторною хвилею у 2022 році) задекларувала активи на суму близько 400 млрд дол. США, однак дала лише 14 млрд дол. США податкових надходжень і 12 млрд дол. США репатрійованих коштів – істотно гірше співвідношення декларованого до фактично повернутого капіталу, ніж за амністіями в Аргентині 2017 року (117 млрд дол. США задекларовано) чи Італії 2009 року (129 млрд дол. США). Індонезія вийшла із сірого списку FATF близько десятиліття тому; за оцінкою Гарнасіх, найгірший можливий наслідок нової

[14] https://www.bloomberg.com/news/articles/2026-06-25/indonesia-opens-door-to-dirty-money-to-fund-prabowo-s-plans

норми – не стільки повернення до сірого списку саме собою, скільки відлякування сумлінних інвесторів і посилення відпливу капіталу, тобто результат, протилежний заявленій меті закону.

Загалом кейс Danantara ілюструє типологію ризику, ширшу за традиційні неформальні канали відмивання коштів: законодавчо закріплений виняток з вимог належної перевірки клієнтів і верифікації джерела коштів, що діє безстроково і поширюється на державний інвестиційний інструмент. На відміну від точкових указів про амністію з обмеженим вікном дії, такий механізм створює структурний, постійний канал легалізації активів сумнівного походження через державні боргові інструменти, що суперечить логіці Рекомендації 34 FATF та накопиченому міжнародному досвіду впровадження програм репатріації капіталу.

Як росія перетворила медицину на зброю [15]

Документ, оприлюднений OCCRP та проєктом "Схеми" (Радіо Свобода), є ґрунтовним розслідуванням, яке викриває шокуючі факти систематичних тортур, медичної недбалості та приниження людської гідності, яких зазнають українські військовополонені в російських виправних установах. Фокус цього розслідування – колонія №7, розташована в невеликому селі Пакіно, приблизно за 230 кілометрів на північний схід від москви. Цей об'єкт став місцем невимовних страждань для десятків українців, які були захоплені в полон під час повномасштабного вторгнення.

В основі розслідування – свідчення майже п'ятдесяти колишніх в'язнів, включаючи військовослужбовців, цивільних осіб, журналіста та навіть колишнього мера Херсона. Їхні розповіді, зібрані у вигляді детальних інтерв'ю та листувань, малюють жахливу картину життя в колонії, де фізичне насильство, психологічний тиск і медична занедбаність стали буденністю. Особливе місце в цих свідченнях займає постать лікаря колонії, якого в'язні через його садистські нахили та знущальне ставлення прозвали "доктором Смерть". Жертви описують його не як медичного працівника, а як ката, який використовував своє службове становище для систематичного приниження та морального знищення полонених.

Одним із найяскравіших і водночас найтрагічніших прикладів є історія військовополоненого Ігоря Шишка. Під час спалаху корости в колонії влітку 2023 року, замість надання необхідної медичної допомоги, лікар використав зеленку не для лікування, а як інструмент сексуального приниження. Він намалював на обличчі Шишка непристойний напис після чого запросив інших дивитися на це. Цей випадок демонструє збочену логіку тортур, де медичний засіб перетворюється на зброю, а публічне приниження стає частиною "розваги" для наглядачів.

Свідчення інших колишніх в'язнів розкривають цілу низку знущань, які виходять далеко за межі індивідуальних випадків садизму. Вони свідчать про чітко вибудувану систему, спрямовану на дегуманізацію українських полонених. Серед описаних методів – примус до "плавання по-тюленячому", коли в'язнів змушували повзти по підлозі, використовуючи лише руки, дряпаючи ноги до крові; побиття ніг, що робило неможливим пересування; тривале перебування в холодних камерах без одягу (по місяць і більше); та систематичне недоїдання, коли добовий раціон іноді складався з кількох шматків запліснявілого хліба. Особливо цинічним було використання методів колективної відповідальності, коли за непослух одного карали всіх, позбавляючи їжі чи створюючи нестерпні умови, що штовхало в'язнів на зраду один одного чи виконання принизливих вимог лікаря, який отримував збочене задоволення.

Психологічний тиск і медична недбалість тісно переплітались. Журналіст Дмитро Хилюк, який провів у колонії понад два роки, описав, як лікар ігнорував спалах корости, не ізолюючи хворих, а навпаки, розміщуючи їх у камерах зі здоровими, що сприяло поширенню епідемії. Замість лікування в'язнів роздягали догола, пояснюючи це тим, що «кліщ повинен померти від холоду, бажано разом з вами». Інші свідки розповідають про те, як лікар відмовляв у

[15] https://www.occrp.org/en/investigation/for-ukrainians-in-a-russian-prison-colony-their-doctor-became-their-tormentor

знеболенні під час процедур (наприклад, видалення нігтя) або давав абсурдні поради: менше їсти та більше ходити. Виснажливі умови та знущання призвели до трагічних наслідків – 23-річний морпіх, не витримавши тортур, наклав на себе руки в травні 2023 року, а його тіло було повернуто в Україну лише через рік. Свідчення про те, що лікар погрожував зґвалтуванням, регулярно проводив принизливі огляди без медичних підстав, а також примушував в'язнів до танців та обіймів у оголеному вигляді, вказують на системний характер сексуалізованого насильства.

Розслідування не обмежується лише фіксацією свідчень, але й демонструє, як журналістам вдалося ідентифікувати особу лікаря-ката – В'ячеслава Черданцева. Використовуючи зіставлення інформації, отриманої від десятків колишніх полонених, аналіз відкритих баз даних та витоків інформації, а також за допомогою фотографій, знайдених у соціальних мережах його родичів, вдалося встановити особу 48-річного Черданцева. Його біографія виявилася примітною: народившись у Киргизстані, він працював у виправній колонії для неповнолітніх на батьківщині, займаючись профілактикою ВІЛ та лікуванням наркоманії, а пізніше переїхав до росії, отримав громадянство і влаштувався в дитячий будинок, перш ніж стати лікарем у колонії №7. Більше тридцяти колишніх в'язнів упізнали на наданих знімках лікаря-садиста, а Шишко заявив з абсолютною впевненістю, що впізнав його за очима, поглядом та особливо за руками, які запам'ятав дуже добре. Українські правоохоронці вже отримали ці докази та зафіксували свідчення потерпілих, що є частиною загальнонаціонального процесу притягнення до відповідальності за військові злочини.

Свідчення з колонії №7 є частиною ширшої, документованої картини систематичних зловживань щодо українських військовополонених у росії, на що неодноразово вказували місії ООН, ОБСЄ та Європейський суд з прав людини. Особливо показовим є епізод із візитом представників Міжнародного комітету Червоного Хреста в травні 2023 року. Колишні в'язні описали цей візит як "ганьбу" та "пародію", оскільки їх попередили про прихід гостей і погрожували розправою у разі скарг, а наглядачі з натільними камерами стояли поруч, коли представники організації запитували про умови утримання. Це свідчить про те, що міжнародні спостерігачі часто не мають доступу до справжньої картини, а їхні зусилля нівелюються залякуванням в'язнів.

Це розслідування виконує кілька ключових функцій. По-перше, воно дає голос жертвам і публічно документує воєнні злочини, які можуть бути використані в міжнародних судових інстанціях. По-друге, воно ідентифікує конкретних виконавців злочинів, що ускладнює їм можливість уникнути відповідальності. По-третє, воно демонструє, що знущання не є випадковими ексцесами окремих садистів, а мають системний характер, підтримуються адміністрацією установи та вищою владою росії. Відсутність жодної реакції з боку адміністрації колонії, Федеральної пенітенціарної служби та самого Черданцева лише підтверджує глибоку інституційну кризу та безкарність, яка панує в російській системі виконання покарань.

Поки тисячі українців залишаються в російському полоні, такі розслідування є критично важливими для привернення уваги світової громадськості до цих жахливих порушень прав людини та для майбутнього притягнення винних до справедливості.

Ваша думка важлива!

1. Які елементи моделі AMLA доцільно врахувати Україні під час реформування національної системи державного нагляду у сфері запобігання та протидії відмиванню коштів та фінансуванню тероризму?
2. Яку відповідальність має нести держатель реєстру КБВ за повноту, актуальність і технічну доступність інформації, необхідної для фінансових розслідувань та розшуку активів?
3. Як Україна може ефективно притягнути до відповідальності конкретних виконавців воєнних злочинів, враховуючи відсутність механізмів екстрадиції та юрисдикції на території росії, і наскільки міжнародні суди будуть достатнім інструментом справедливості?
4. В Україні, де значну частку економіки становлять аграрний, гірничо-металургійний та енергетичний сектори, які перебувають під пильною увагою іноземних інвесторів і водночас є об'єктами корупційних схем, – наскільки держава готова до системної протидії злочинності в цих секторах економіки, особливо в умовах післявоєнної відбудови?
5. Чому українські правоохоронні органи досі не демонструють системних результатів у викритті scam-центрів, хоча саме через територію України, за даними, проходять значні обсяги грошей із європейських шахрайських схем, і чи не означає це, що проблема свідомо недооцінюється?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-29

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].