Методологічний бюлетень

Серійний номер: МінФін-AML-2025-52

Грудень 2025

“Або ви керуєте вашим днем, або день управляє вами”

Джим Рон

Мета

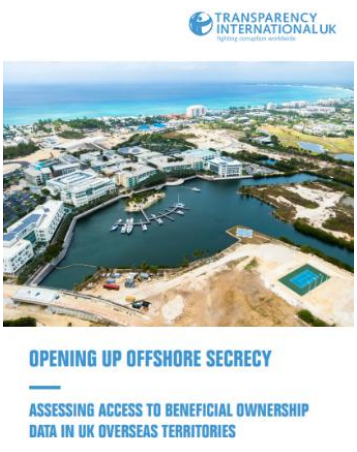
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

Мережа тіней: як офшорна секретність британських територій ставить під загрозу глобальну безпеку та фінансову цілісність [1]



У просторі глобальних фінансів існує паралельний всесвіт, побудований на секретності та анонімності. Після витоків «Panama Papers» у 2016 році цей світ вийшов із тіні, розкривши масштаби свого впливу: мільярди доларів, відмитих через корупцію, розкрадання держмайна та санкційні схеми, безкарно циркулюють по всьому світу.

Як показує дослідження Transparency International UK, Велика Британія та її мережа заморських територій і володінь залишаються системоутворюючим ядром цієї глобальної інфраструктури секретності. Проте навіть через сім років після історичної парламентської вимоги про прозорість, прогрес залишається болісно повільним, фрагментарним і, найчастіше,

[1] https://www.transparency.org.uk/sites/default/files/2025-12/Opening%20Up%20Offshore%20Secrecy.pdf

сфальсифікованим — замість справжньої відкритості, ключові фінансові центри пропонують складні бюрократичні моделі, які більше ховають, ніж відкривають.

Головна принада офшорів — це не лише низькі податки, а й гарантована конфіденційність. Саме вона перетворює ці юрисдикції на магніти для недобросовісних гравців: корупціонерів, що розкрадають бюджетні кошти своїх країн; організованих злочинних угруповань, які відмивають прибуток від наркоторгівлі; олігархів та політичних осіб, які прагнуть приховати активи та ухилитися від санкцій; фінансових шахраїв, що будують піраміди, тощо.

Transparency International UK ще у 2018 році документально підтвердила, що непрозорі структури, зареєстровані в британських заморських територіях, були задіяні у понад 273 випадках великомасштабної корупції та відмивання коштів на суму 250 мільярдів фунтів стерлінгів. Ці кошти були виведені з 79 країн через фіктивні держзакупівлі, хабарництво, привласнення майна. Британські Віргінські Острови фігурували у приголомшливих 92% цих справ, ставши епіцентром глобальної індустрії зловживань. Ці активи не лише відмивалися в офшорах — вони знаходили собі нове, легальне втілення: майже 6 мільярдів фунтів з цих коштів було інвестовано у нерухомість Великої Британії через ті самі фіктивні компанії, підриваючи цілісність фінансової системи країни та спотворюючи ринок житла.

У відповідь на міжнародне обурення та внутрішній тиск, британський парламент у 2018 році вніс історичну поправку до Закону про санкції та протидію відмиванню грошей. Вона зобов'язувала заморські території до кінця 2023 року (або пізніше за домовленістю) створити повністю публічні реєстри реальних (бенефіціарних) власників компаній. Це мало стати проривом: будь-яка людина в будь-якій точці світу змогла б безкоштовно перевірити, хто насправді стоїть за тією чи іншою зареєстрованою компанією. Проте шлях до прозорості виявився вкритим юридичними та політичними пастками. У 2022 році рішення Суду Європейського Союзу у справі щодо Люксембургу встановило, що повністю публічні реєстри можуть порушувати право на приватність. Хоча це рішення не має обов'язкової сили для британських територій, воно стало зручним інструментом саботажу. Багато юрисдикцій почали посилатися на це рішення, відступаючи від своїх обіцянок про публічність і зосереджуючись на більш обмеженій моделі, запропонованій шостою директивою ЄС проти відмивання грошей (6AMLD).

Ця модель, так званий доступ за «законним інтересом», передбачає, що дані отримують не всі, а лише ті, хто може довести свій прямий інтерес у боротьбі з відмиванням, фінансуванням тероризму та пов'язаними злочинами. В ідеалі, ЄС надає таким користувачам, як журналісти, дослідники та громадські організації, що спеціалізуються на антикорупції, статус «презумпційного законного інтересу», забезпечуючи їм широкий, повторюваний доступ до інформації. Проте, як показує оцінка чотирьох ключових територій — Бермуд, Британських Віргінських Островів, Каймановых Островів та Монтсеррату — на практиці її реалізація перетворюється на складний лабіринт з обмеженнями, які роблять дані майже марними для тих, хто на них покладається.

Основна проблема полягає в тому, що жодна з основних фінансових територій не впровадила доступ за «презумпційним інтересом» на зразок ЄС. Замість цього кожен запит на отримання даних про бенефіціарного власника розглядається окремо, на підставі конкретних, часто розмитих критеріїв. Бермуди, де централізований реєстр існує давно, але доступ для законних користувачів постійно відкладається (тепер очікується лише у 2026 році), пропонують неясний процес оцінки запитів. На Каймановых островах, де реєстр запрацював у лютому 2025 року, журналісту чи активісту потрібно для кожного окремого юридичного об'єкта подавати окрему заявку через спеціальний портал, прикріплювати документи та надавати детальне обґрунтування свого розслідування, доводячи, що саме ця інформація допоможе запобігти злочину. Після цього потрібно здійснити платіж через міжнародний банківський переказ

(картки не приймаються) у розмірі 36 доларів США за запит. Пошук можливий лише за назвою компанії, а не за іменем людини, що робить систему практично безкорисною для проактивного розслідування — адже щоб знайти компанію, потрібно спочатку точно знати про її існування та зв'язок з підозрюваним.

Найнебезпечніші механізми розроблені в Британських Віргінських Островах. Тут запропонована система містить так звані положення про «попередження» (tipping-off). Вони дозволяють бенефіціарному власнику отримати повідомлення про те, що хтось намагається отримати доступ до його даних, і навіть оскаржити це розкриття. Це — пряме викриття розслідування. Така практика не просто підриває антикорупційні зусилля; вона несе серйозну загрозу безпеці журналістів та активістів, які можуть стати об'єктами судових переслідувань чи залякування з боку впливових осіб, інтереси яких вони порушують. Крім того, у БВО відсутні будь-які захисти для користувачів: їхня ідентичність не захищена, а умови використання отриманих даних суворі та двозначні, обмежуючи можливості їх публікації чи аналізу.

Універсальною слабкістю всіх цих систем, окрім повністю публічного реєстру Монтсеррату, є трасти. Жодна юрисдикція не вимагає розкривати інформацію про осіб, які є засновниками або вигодонабувачами трастів, що, у свою чергу, контролюють компанії. Це критична лазівка, адже саме трасти часто є кінцевою ланкою в найскладніших схемах власності, призначених для максимального приховування. Компанія може належати іншій компанії, яка керується трастом, реальні засновники якого залишаються невидимими. Таким чином, навіть отримавши доступ до даних про бенефіціарного власника компанії, дослідник може натрапити на глухий кут у вигляді безособового трасту, що зводить нанівець усю ідею прозорості.

Висновки:

- **Обмежені моделі доступу за "законним інтересом", які впроваджують ключові британські офшори (Бермуди, БВО, Каймани), є неефективними та бюрократичними.** Вони не надають автоматичного доступу, вимагають окремих заявок на кожну компанію, часто містять механізми "попередження" злочинців і не розкривають інформацію про власників трастів, зберігаючи ключову лазівку для анонімності.
- **Публічні реєстри залишаються "золотим стандартом" прозорості.** Вони безкоштовні, доступні усім, прості в адмініструванні та створюють превентивний ефект, покращують якість даних через колективний нагляд і є найефективнішим інструментом для боротьби з відмиванням.
- **Британські офшори продовжують грати центральну роль** у глобальних корупційних та відмивних схемах.
- **Прогрес у боротьбі з офшорною секретністю блокується не технічними, а політичними та економічними інтересами** територій, які отримують вигоду від фінансової непрозорості.

На тлі цих складних і обмежених систем Монтсеррат, невелика територія з населенням менше 5 тисяч осіб та скромним корпоративним реєстром у 300 компаній, виглядає як надихаючий приклад. У жовтні 2024 року вона запустила повністю публічний, безкоштовний, онлайн-реєстр, доступний будь-кому без будь-яких запитів чи обґрунтувань. Це доказ того, що технічна та адміністративна реалізація публічної прозорості можлива навіть з обмеженими ресурсами, коли є політична воля. Цей приклад розвінчує міф про те, що тільки дорогі та бюрократичні системи «законного інтересу» можуть балансувати прозорість і приватність. Монтсеррат також запровадив механізм захисту вразливих осіб, який дозволяє приховувати дані за обґрунтованими винятками, що відповідає міжнародним стандартам. Його слабкістю залишається технічна сторона — відсутність можливості

масового завантаження даних у машинозчитуваному форматі, що ускладнює їх аналіз великими наборами, проте цю проблему порівняно легко вирішити.

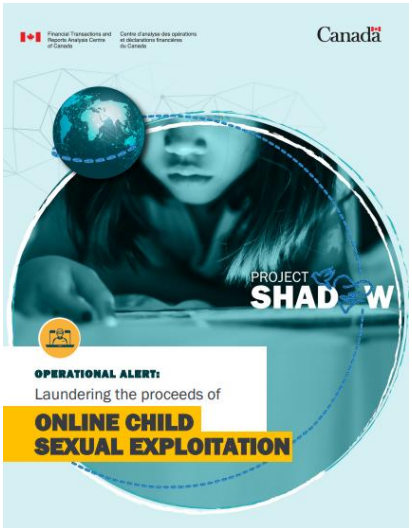
Сім років очікувань на прозорість британських офшорів демонструють не технічну складність, а політичну незгоду. Економіки таких територій, як БВО та Кайманові острови, критично залежать від фінансових послуг, а секретність була їх основною конкурентною перевагою. Тому їхній опір справжній відкритості є цілком закономірним з точки зору їхніх короткострокових економічних інтересів. Проте ці інтереси стикаються з національною безпекою та репутацією самої Великої Британії, а також з глобальною боротьбою проти корупції та організованої злочинності.

Досвід Монтсеррату та Гібралтару доводить, що публічний реєстр залишається найефективнішим, найпростішим та найдешевшим інструментом. Він створює превентивний ефект, підвищує якість даних за рахунок «колективної перевірки» (коли помилки можуть бути виявлені різними користувачами) та забезпечує миттєвий доступ для всіх стейкхолдерів: від місцевої правоохоронної системи до міжнародних журналістських розслідувань, від іноземних фінансових установ, які проводять перевірку клієнтів, до бізнес-партнерів, які хочуть переконатися в доброчесності контрагента.

Моделі «законного інтересу», у тому вигляді, в якому вони впроваджуються зараз, є непрактичними. Вони несуть витрати на створення складних систем контролю доступу, але при цьому не дають реальної прозорості.

Як зазначає Transparency International UK, безкарний потік злочинного капіталу через британські офшори триватиме доти, доки уряд Великої Британії не буде готовий перейти від дипломатичних закликів до рішучих дій, включно з використанням усіх своїх конституційних і законодавчих повноважень для забезпечення виконання домовленостей. Міжнародна спільнота, особливо на тлі санкційних війн та посилення боротьби з відмиванням, все менше готова терпіти юрисдикції, які свідомо залишають відкритими для кримінальних капіталів. Час для справжньої прозорості настав давно, і подальші затримки вже не можуть бути виправдані ні приватністю, ні технічними складностями — тільки відсутністю політичної волі.

Фінансові сліди зла: як грошові потоки допомагають розкривати мережі онлайн-експлуатації дітей [2]



У безмежному просторі цифрового світу, де інформація перетворюється на товар, а анонімність часто стає щитом, процвітає одна з найогидніших форм сучасного злочинності – онлайн-експлуатація дітей. Це не абстрактна загроза, а системна, глибоко вкорінена індустрія, що генерує значні прибутки та, відповідно, потребує складних механізмів легалізації цих доходів.

Центр аналізу фінансових операцій та звітності Канади (FINTRAC) у своєму проекті під кодовою назвою «Project Shadow» опублікував результати ґрунтовного дослідження, що висвітлює складну панораму фінансових потоків, які живлять цю індустрію, та надає фінансовому сектору безцінний інструментарій для її виявлення. Цей документ, створений у тісній співпраці з Scotiabank та Канадським центром захисту дітей, розкриває еволюцію злочину, де сексуальна вигода все частіше переплітається з чистою фінансовою

[2] https://fintrac-canafe.canada.ca/intel/operation/exploitation-eng.pdf

корисливістю, а анонімність темних ринків і криптовалют поєднується з буденними банківськими переказами.

Хоча психологічний профіль злочинця, що шукає сексуального задоволення, залишається ключовим, останні роки свідчать про тривожну комерціалізацію страждань дітей. Сексуальний шантаж, або сексторшн, перетворився з індивідуальних актів на відлагоджену схему, яку часто курують міжнародні організовані злочинні угруповання. Це вже не просто погрози – це чіткий бізнес-процес із стратегіями вербування через соціальні мережі, стандартизованими вимогами (готівка, подарункові картки, криптовалюта) та ескалацією вимог, що часто призводить до руйнування життя жертви. Фінансова складова стає каталізатором: доступ до ексклюзивного контенту, організація потокових трансляцій у реальному часі за запитом, навіть замовлення «ексклюзивних приватних матеріалів» – все це має свою ціну, що формує повноцінний ринок попиту та пропозиції.

Механізми оплати в цій індустрії диверсифіковані та адаптивні, відображаючи прагнення до балансу між доступністю, швидкістю та анонімністю.

Класичною схемою для фінансування живих злочинів, особливо в країнах Південно-Східної Азії та Латинської Америки, залишаються системи грошових переказів (MSB) та їхні цифрові платформи. Тут працює модель невеликих, але частих «стипендій» або «допомог». Чоловік, часто віком за 40 років, здійснює численні перекази у розмірі 50-200 CAD одній або кільком одержувачам у Філіппінах, Таїланді, Домініканській Республіці. Перекази відбуваються вночі або рано вранці за місцевим часом отримувача, що може вказувати на координацію для онлайн-сеансів. Ключовим індикатором є відсутність очевидного родинного чи соціального зв'язку з бенефіціаром, а також ігнорування економії на комісіях – злочинець готовий багаторазово платити комісії за дрібні суми, що суперечить логіці легальних трансферів на підтримку родини.

Окремої уваги заслуговує сфера криптовалют, яка стала стрижнем торгівлі матеріалами про сексуальне насильство над дітьми в даркнеті. Bitcoin довгий час був стандартом, але сьогодні зростає популярність приватних монет (privacy coins), таких як Monero або Zcash, чиї протоколи активно запобігають відстеженню. Аналіз показує типовий ланцюжок: покупець купує монети на біржі, переказує їх на особистий гаманець, а потім відправляє невелику суму (5-50 CAD) на публічну адресу продавця. Для додаткової анонімізації кошти часто проходять через криптоміксери (tumblers) або миттєві обмінники. Одним із найбільш виразних індикаторів є повторювані, нагадуючі передплату, платежі на одну й ту саму криптоадресу, яка, у свою чергу, може отримувати кошти від сотень різних джерел. Сленг у полі для нотаток (наприклад, «CP», «school girl», «loli») або навіть певні послідовності емодзі (піца, льодяник, соска) слугують кодом для позначення контенту.

Для менш технічно підготовлених злочинців, часто молодших, популярними є звичайні P2P-платіжні системи та електронні грошові перекази. Їхня привабливість – у простоті та швидкості. Підозру викликають численні низьковартісні перекази різним особам, часто з відсиланням у коментарях до соціальних мереж (Twitter, Telegram), файлообмінних платформ (Mega, Dropbox) або сайтів для дорослих із функцією контенту за передплатою.

Окрім прямих платежів, що безпосередньо фінансують злочин, існує цілий спектр опосередкованих фінансових поведінкових моделей, які, складаючись у мозаїку, формують профіль підозрюваного.

Одним з найважливіших контекстуальних індикаторів є активність, пов'язана з подорожами до високоризикових юрисдикцій. Це не просто бронювання готелю на відпочинок. Це ланцюжок витрат: купівля квитків у напрямку, наприклад, Філіппін, безпосередньо перед серією дрібних переказів місцевим одержувачам; оплата нетуристичного житла на тривалий період; численні зняття невеликих сум готівки в банкоматах на місці; або покупки, не характерні для туриста

(дитячий одяг, іграшки, ювелірні вироби). Такі патерни можуть вказувати на фізичні поїздки з метою скоєння злочинів, що особливо актуально в світлі канадського законодавства, яке дозволяє притягати до відповідальності громадян за такі злочини, скоєні за кордоном.

Прагнення до цифрової невидимості – ще одна визначальна риса. Окрім використання криптовалют, це регулярні витрати на послуги VPN, шифровані поштові сервіси (ProtonMail), програмне забезпечення для знищення цифрових слідів (віртуальні «подрібнювачі» файлів), послуги з анонімної реєстрації доменів або хостингу. Ці витрати, особливо коли вони не пов'язані з професійною діяльністю клієнта, є потужним сигналом.

Значна частина життя в інтернеті також знаходить своє фінансове відображення. Це можуть бути надмірні витрати на внутрішньоігрові покупки в онлайн-іграх, популярних серед неповнолітніх і оснащених чатом; численні підписки на платформи з дорослим контентом або вебкам-сайти; активна купівля подарункових карток різних номіналів (ідеальний інструмент для анонімних платежів); постійні платежі хостинг-провайдерам для великих обсягів даних.

FINTRAC чітко дає зрозуміти: жоден індикатор, взятий ізольовано, не може бути підставою для підозри. Купівля VPN – легальна практика. Переказ грошей родичам за кордоном – норма. Підписка на вебкам-сайт – особиста справа. Але коли ці елементи починають сходитися в одному фінансовому профілі, утворюючи «систему факторів», картина змінюється.

Уявіть клієнта: самотній чоловік похилого віку, зі скромним доходом. Його рахунок показує десятки низьковартісних P2P-переказів на Філіппіни в нічний час, регулярні платежі на криптобіржу з подальшим виведенням на приватні гаманці, передплату на кілька платформ дорослого контенту, разову велику витрату на послуги «очищення жорсткого диска», а також бронювання готелю в Манілі на наступний місяць. Кожна з цих операцій має потенційне невинне пояснення. Але їхня сукупність, конвергенція у часі та просторі, створює ту саму обґрунтовану підозру, яка вимагає подальшого розгляду та, ймовірно, подання детального звіту про підозрілу операцію (STR).

Висновки:

- **Фінансові транзакції є критично важливим індикатором онлайн-експлуатації дітей,** відображаючи як споживання, так і комерціалізацію цього злочину, включно з вимаганням та продажем матеріалів.
- **Злочинці використовують різноманітні канали легалізації коштів:** транскордонні перекази через MSB, криптовалюти (особливо приватні монети), P2P-платежі та інші інструменти, що поєднують доступність з анонімністю.
- **Контекст і сукупність індикаторів є ключем до виявлення:** окремі підозрілі операції можуть мати легальне пояснення, але їх поєднання з поведінковими та контекстуальними факторами формує обґрунтовану підозру.
- **Міжнародна співпраця та обмін інформацією між фінансовими установами, правоохоронцями та міжнародними організаціями** є життєво необхідними для ефективної боротьби з транснаціональним характером цієї злочинності.

Таким чином, звітні суб'єкти перетворюються з пасивних реєстраторів транзакцій на активних учасників системи національної безпеки. Їхня роль полягає в тому, щоб, ґрунтуючись на знанні свого клієнта (KYC) і аналізі його поведінки, вміти побачити за суворими колонками цифр та кодами операцій потенційну людську драму та злочин. Сила фінансової розвідки саме в цьому – у здатності зв'язати, на перший погляд, розрізнені фінансові події в єдину логічну (злочинну) послідовність.

Нове керівництво SFO щодо оцінки корпоративних програм комплаєнсу [3]

Керівництво опубліковане Управлінням боротьби з шахрайством Великої Британії (SFO) щодо оцінки корпоративних програм дотримання вимог (комплаєнсу) являє собою знаковий документ, що виходить далеко за рамки простого оновлення бюрократичних процедур.

Цей документ, що набув чинності для Англії, Уельсу та Північної Ірландії, можна розглядати як комплексну стратегічну доктрину, яка систематизує та підвищує стандарти взаємодії між державою та корпоративним сектором у сфері боротьби з найскладнішими економічними злочинами. У контексті глобального посилення фокусу на відмиванні коштів (AML), протидії корупції та шахрайству, а також у світлі останніх змін у британському законодавстві, зокрема прийняття Закону про економічні злочини та корпоративну прозорість 2023 року (ECCTA), керівництво SFO стає наріжним каменем у формуванні нової парадигми корпоративної відповідальності. Воно трансформує програму комплаєнсу з формального, часто реактивного, набору політик у живий, динамічний та стратегічно важливий актив, від ефективності якого може буквально залежати доля компанії – її фінансова стабільність, репутація та саме право на існування.

Документ детально описує, як саме SFO, використовуючи весь спектр своїх повноважень, буде аналізувати зусилля організацій у шести критично важливих процесуальних точках, що охоплюють повний життєвий цикл карного провадження: від початкового рішення про висунення обвинувачення, через альтернативні механізми врегулювання, такі як угоди про відстрочене судове переслідування (DPA), і аж до етапу визначення міри покарання. Ця всеосяжність підкреслює, що комплаєнс більше не є ізольованою функцією, якою займаються лише юристи та внутрішні аудитори; він стає центральним елементом доказової бази в діалозі компанії з державою.

Фундаментальна новизна керівництва полягає в його акценті на динамічній та контекстуальній оцінці. SFO не задовольнятиметься статичними даними щодо програми комплаєнсу на поточний момент. Навпаки, обвинувач буде ретельно досліджувати її стан та ефективність у різні часові відрізки, кожен з яких має вирішальне значення. Перш за все, це момент вчинення правопорушення. Була тоді програма комплаєнсу неефективною або відсутньою зовсім? Це стане вагомим публічно-правовим фактором на користь ініціювання судового переслідування, оскільки свідчитиме про системний недолік у корпоративній культурі.

Далі йде момент виявлення злочину та взаємодії з органом влади. Чи продемонструвало керівництво компанії справді проактивний підхід, негайно вживши виправних заходів, посиливши програму та повністю співпрацюючи з розслідуванням? Саме такі дії SFO визнає ключовими факторами проти обвинувачення.

Нарешті, оцінка проводиться на момент прийняття ключового рішення – чи то про пред'явлення звинувачення, чи то про укладення DPA. Таким чином, компанія змушена не просто мати комплаєнс-програму, а постійно її доопрацьовувати, адаптувати та, що найважливіше, вміти надати переконливі докази її реальної роботи, а не просто наявності на папері. Це вимагає ретельного документування всіх процесів: від протоколів оцінки ризиків та результатів внутрішніх аудитів до записів про навчання співробітників та аналізу інцидентів.

[3] https://www.gov.uk/government/publications/sfo-guidance-on-evaluating-a-corporate-compliance-programme/sfo-guidance-on-evaluating-a-corporate-compliance-programme

Особливо детально в керівництві розглядається роль комплаєнсу в контексті угод про відстрочене судове переслідування (DPA), які стали потужним інструментом альтернативного врегулювання у Великій Британії. Тут SFO встановлює дуже високу планку. Саме наявність «справді проактивної та ефективної корпоративної програми дотримання вимог» названа «важливим міркуванням» для укладення DPA. Іншими словами, належна програма комплаєнсу – це не лише запобіжний захід, а й квиток до столу переговорів, що дозволяє уникнути катастрофічних наслідків обвинувального вироку. Натомість відсутність такої програми на момент злочину та відсутність подальших «суттєвих покращень» робить отримання DPA майже неможливим, зміщуючи ваги на користь негайного кримінального переслідування.

Окремої уваги заслуговують роз'яснення щодо двох критично важливих законних елементів захисту: «адекватних процедур» проти звинувачення у недопущенні хабарництва (ст. 7 Закону про боротьбу з хабарництвом 2010) та «розумних процедур» проти звинувачення у недопущенні шахрайства (ст. 199 ECCTA 2023). SFO чітко вказує на концептуальні відмінності між ними. Захист за Законом про боротьбу з хабарництвом вимагає від компанії довести наявність саме «адекватних» процедур, тобто таких, що пропорційні ризикам та реально спрямовані на запобігання. Нова ж норма ECCTA, що стосується шахрайства, використовує більш гнучкий стандарт «розумних» процедур. Це не лише семантична різниця. ECCTA прямо передбачає, що в певних обставинах організація може навіть успішно стверджувати, що очікувати від неї наявності будь-яких запобіжних процедур було б «нерозумно». Це важлива зміна, яка враховує різноманіття бізнес-середовищ, особливо для невеликих підприємств.

Обидва режими базуються на структурі з шести принципів, що детально описані в окремих статутних керівництвах Міністерства юстиції та Міністерства внутрішніх справ. Порівняння цих принципів виявляє цікаві нюанси. Наприклад, принцип «оцінки ризиків» у керівництві щодо шахрайства повинен бути не просто періодичним, а «динамічним», що вимагає постійного оновлення. Принцип «зобов’язання вищого керівництва» у тому ж керівництві отримав посилення: керівники повинні не лише засуджувати шахрайство, але й активно «відкидати прибуток, отриманий на його основі або за його допомогою». Це прямий виклик короткостроковим фінансовим стимулам, які іноді можуть сприяти злочинній поведінці.

У контексті AML та фінансових злочинів надзвичайно важливим є розділ керівництва, присвячений призначенню покарання. SFO посилається на діючі рекомендації Судової ради щодо покарання корпорацій за шахрайство, хабарництво та відмивання коштів, які прямо пов’язують ступінь вини з ефективністю систем комплаєнсу. Так, ознакою «високої вини» визнається «культура свідомого ігнорування вчинення правопорушень співробітниками або агентами без жодних зусиль щодо створення ефективних систем». На противагу цьому, «менша вина» може бути встановлена, якщо були докладені «певні зусилля щодо впровадження заходів запобігання, яких, однак, виявилося недостатньо для повного захисту». Це створює чіткий градієнт відповідальності: від повного байдужості через неадекватні спроби до повноцінного захисту.

Найбільш інноваційним, однак, є положення про те, що як міра фінансової шкоди від злочину може розглядатися «ймовірна сума, недоотримана компанією через невжиття належних запобіжних заходів». Це радикальний підхід, який перетворює інвестиції в комплаєнс з витрат на стратегічне фінансове страхування. Невдача у створенні ефективної AML-програми, наприклад, може призвести не лише до штрафу за сам факт правопорушення, але й до конфіскації коштів, що могли б бути витрачені на її побудову.

SFO відверто визнає, що не існує єдиного шаблону «ефективної» програми комплаєнсу, який підходив би всім. Програма має бути пропорційною розміру, природі, масштабу та ризикам діяльності організації. Мале підприємство не повинно мати ту саму структуру, що й міжнародний банк, але воно повинно мати певні, реалізовані на практиці механізми контролю,

відповідні його операційним ризикам. Ключовим критерієм є практична результативність, а не формальне існування політик. SFO прямо застерігає, що ізольовані невдачі не обов'язково роблять всю програму неефективною; натомість обвинувач буде аналізувати, чи був в системі достатній рівень контролю для виявлення та запобігання обходу цих процедур. Для цього SFO буде використовувати повний арсенал своїх інструментів: від аналізу добровільно наданих даних та інтерв'ю до примусового витребування документів за ст. 2 Закону про кримінальне правосуддя 1987 року та допиту підозрюваних. Це означає, що інформація про комплаєнс може стати частиною основної доказової бази кримінальної справи.

Висновки:

- **Комплаєнс став динамічним доказовим фактором.** Ефективність програми оцінюється SFO не лише на момент злочину, а й на етапах виявлення, переговорів (DPA) та визначення покарання.
- **Наявність справді проактивної та ефективної програми комплаєнсу є критичною умовою для укладення угоди про відстрочене судове переслідування (DPA)**, що дозволяє уникнути руйнівного обвинувального вироку. Відсутність такої програми різко збільшує ймовірність кримінального переслідування.
- **Стандарти "адекватності" та "розумності" відрізняються.** Для захисту від звинувачень у недопущенні хабарництва потрібні "адекватні процедури", а для шахрайства — "розумні". Останній стандарт гнучкіший і навіть допускає те, що в певних обставинах наявність будь-яких процедур була б невиправданою.
- **Під час призначення покарання неефективність систем комплаєнсу може призвести до кваліфікації вини як "високої"**, а також до конфіскації гіпотетично "заощаджених" коштів, які компанія не витратила на належні запобіжні заходи.

Таким чином, керівництво SFO 2025 року – це набагато більше, ніж технічний документ. Це потужний сигнал ринку та корпоративним керівникам. Воно формалізує перехід від культури «галочки» в комплаєнсі до культури глибинної інтеграції та постійного вдосконалення. Інвестиції в якісну програму комплаєнсу, засновану на оцінці ризиків, підтриману згори та перевірену на практиці, тепер прямо конвертуються у відчутні юридичні та фінансові переваги: від можливості уникнути руйнівного судового процесу через DPA до суттєвого зменшення штрафів на етапі визначення покарання.

У світі, де AML, боротьба з шахрайством і корупцією стали питаннями національної безпеки та міжнародної репутації, компанії, здатні не просто мати, але й демонструвати свою проактивну та ефективну культуру дотримання вимог, отримують вирішальну конкурентну перевагу. Керівництво SFO чітко окреслює контур майбутнього: успішними будуть ті організації, які розуміють, що справжній комплаєнс – це не витрата, а стратегічний актив, що захищає саму основу їхнього бізнесу.

Від формальної звітності до інструменту фінансової розвідки: еволюція STOR [4]

Звіт ESMA є розгорнутим аналітичним дослідженням того, як у реальній практиці функціонує механізм Повідомлення про підозрілі операції та торговельні накази (STOR) у системі нагляду за ринками капіталу Європейського економічного простору, та якою мірою цей механізм здатен виконувати свою ключову роль — забезпечувати раннє виявлення та ефективне розслідування зловживань на ринку. Документ ґрунтується на даних, отриманих від усіх 30 національних

[4] https://www.esma.europa.eu/sites/default/files/2024-07/ESMA74-1103241886-992_Report_on_STORs_2024.pdf

компетентних органів (NCAs), що дозволяє говорити не про фрагментарну оцінку, а про повну європейську картину застосування STOR, доповнену ретроспективним аналізом багаторічних тенденцій

Концептуально звіт виходить з того, що STOR є не просто процедурною вимогою, а критично важливим елементом інформаційної інфраструктури ринкового нагляду. ESMA послідовно підкреслює, що жодна, навіть технічно розвинена, система регуляторного моніторингу не здатна замінити інформацію, якою володіють професійні учасники ринку на операційному рівні. Саме інвестиційні фірми, торговельні майданчики та інші особи, що професійно організовують або виконують операції, першими бачать аномальні торгові патерни, поведінкові відхилення, нетипові реакції ринку на інформаційні події або підозрілі зміни ордерів. STOR у цій логіці виступає механізмом трансляції цього первинного знання від приватного сектору до сектору публічного нагляду, і його ефективність визначається не формальною кількістю поданих повідомлень, а їх аналітичною глибиною, структурованістю та своєчасністю.

Емпірична частина звіту демонструє, що у 2023 році NCAs отримали 7 491 повідомлення, з яких 6 530 були кваліфіковані саме як STOR. Це зростання порівняно з попереднім роком не носить характеру різкого стрибка, а радше відображає поступове зміцнення культури повідомлення та стабілізацію STOR як стандартного інструменту ринкової поведінки. ESMA особливо наголошує, що динаміку показників необхідно інтерпретувати з урахуванням структурних факторів, зокрема виходу Великої Британії з ЄС. До 2018 року Управління з фінансового регулювання та нагляду Великої Британії (UK FCA) формувала надзвичайно значну частку STOR у загальноєвропейській статистиці, і саме її виключення з вибірки пояснює різке падіння абсолютних значень після 2019 року, а не зниження реального рівня виявлення зловживань.

Важливим змістовим елементом звіту є аналіз джерел STOR, який фактично підтверджує трансформацію інвестиційних фірм у центральних учасників системи раннього попередження про ринкові зловживання. Понад три чверті всіх STOR надходять саме від них, що означає, що якість функціонування ринкового нагляду прямо залежить від внутрішніх систем контролю цих суб'єктів. ESMA опосередковано підкреслює, що слабкі або формалізовані системи виявлення, орієнтовані лише на виконання нормативної вимоги, створюють системні ризики для всієї архітектури забезпечення дотримання законодавства у сфері протидії зловживанням на ринку. У цьому контексті STOR перестає бути індивідуальним комплаєнс-обов'язком окремої компанії й перетворюється на елемент колективної відповідальності ринку за його цілісність.

Аналіз розподілу STOR за типами фінансових інструментів дозволяє зробити висновок про стійку концентрацію ризиків у сегменті ринку акцій. Переважна більшість повідомлень стосується саме акцій, що відображає поєднання кількох факторів: високої ліквідності, швидкої реакції цін на інформацію, широкого кола учасників та значної асиметрії доступу до інсайдерської інформації. Водночас стабільна присутність деривативів і боргових фінансових інструментів у структурі STOR свідчить про те, що зловживання дедалі частіше мають складний, мультиінструментальний характер, а ризики можуть маскуватися через використання похідних або комбінованих торгових стратегій.

Особливу аналітичну вагу у звіті має розгляд типів підозрюваних порушень. Дані за 2023 рік демонструють повернення інсайдерської торгівлі як домінуючої категорії STOR після кількох років, коли переважали повідомлення про маніпулювання ринком. Така зміна не є лише статистичною флуктуацією, а відображає глибші структурні проблеми управління інформацією

всередині фінансових організацій. Вона вказує на вразливість механізмів контролю доступу до інсайдерської інформації, ефективності інформаційних бар'єрів, процедур допуску до інсайдерської інформації з обмеженим колом осіб, а також внутрішнього обміну чутливою інформацією. У ширшому контексті це означає, що, попри розвиток технологій моніторингу торгів, фундаментальний ризик зловживання інформаційною перевагою залишається центральним викликом для ринків капіталу.

Окремий і дедалі більш значущий вимір звіту стосується транскордонного обміну STOR між національними та іноземними компетентними органами. Зростання кількості STOR, що передаються між NCAs, а також до органів третіх країн, демонструє еволюцію STOR із суто національного інструменту у механізм міжнародної регуляторної взаємодії. ESMA фактично фіксує, що зловживання на ринках капіталу дедалі частіше мають транснаціональний характер, а ефективне розслідування неможливе без швидкого та структурованого обміну інформацією. У цьому сенсі STOR дедалі більше виконує роль тригера для спільних розслідувань і координації дій між регуляторами.

У підсумку звіт формує цілісне бачення STOR як динамічного інструменту, ефективність якого визначається рівнем зрілості ринку, якістю внутрішніх контролів та здатністю регуляторів і учасників ринку діяти в єдиній логіці захисту ринкової цілісності. ESMA не просто констатує статистичні показники, а фактично задає рамку для подальшого розвитку STOR як інструменту ризик-орієнтованого нагляду, що має бути інтегрований у ширшу систему фінансового регулювання, включно з ПВК/ФТ, санкційним комплаєнсом та, за необхідності, механізмами протидії фінансуванню розповсюдження зброї масового знищення.

Висновки:

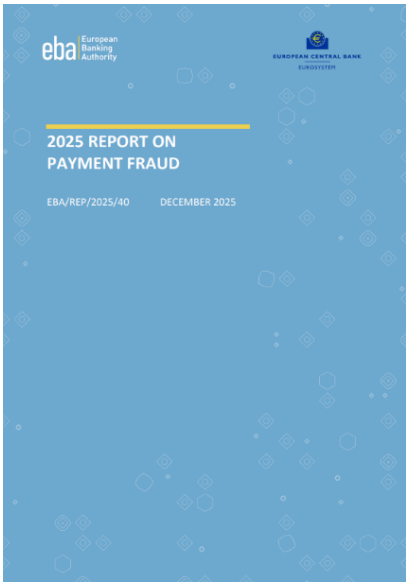
- **STOR є центральним елементом екосистеми виявлення ринкових зловживань, а не допоміжним звітним інструментом.** Домінування STOR у структурі сигналів для NCAs підтверджує, що саме професійні учасники ринку володіють критичною інформацією про потенційні зловживання. Ефективність нагляду безпосередньо залежить не від кількості STOR, а від їх аналітичної якості, своєчасності та здатності ініціювати розслідування.
- **Ключова роль інвестиційних фірм.** Інвестиційні фірми є першою лінією виявлення ринкових зловживань, а неефективність їхніх внутрішніх систем моніторингу безпосередньо формує прогалини регуляторного нагляду.
- **Вразливість контролю інсайдерської інформації.** Механізми управління інсайдерською інформацією та контролю доступу до чутливих даних є вразливими, що зумовлює необхідність їх тісної інтеграції з внутрішніми розслідуваннями та функціями протидії відмиванню коштів і фінансуванню тероризму.
- **Ринкові зловживання мають транскордонний характер.** Ринкові зловживання дедалі частіше мають транскордонний характер, що зумовлює необхідність системного міжнародного обміну інформацією та координації дій між компетентними органами.

Еволюція платіжного шахрайства в Європейському Союзі: аналітичні висновки зі звіту ЕВА та ЄЦБ за 2025 рік [5]

European Banking Authority, спільно з Європейським центральним банком, опублікували документ, який присвячений системному аналізу платіжного шахрайства в Європейському Союзі та Європейській економічній зоні. Його основною метою є надання регуляторам,

[5] https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf

наглядовим органам і фінансовому сектору цілісної картини масштабів, структури та еволюції шахрайства у сфері безготівкових платежів на основі гармонізованих статистичних даних, зібраних відповідно до вимог Директиви PSD2 та супровідних регуляторних стандартів і керівних принципів ЕВА.



Звіт охоплює всі ключові платіжні інструменти, що використовуються в ЄС: перекази (у тому числі миттєві), карткові платежі, прямі дебети, операції з електронними грошима та зняття готівки. Аналіз здійснюється за кількома вимірами одночасно — за вартістю та кількістю транзакцій, за типами шахрайства, каналами ініціювання платежів, застосуванням або незастосуванням автентифікації клієнта (SCA), а також за географічною ознакою (внутрішні, транскордонні в межах ЄЕЗ та операції поза ЄЕЗ). Такий підхід дозволяє не лише зафіксувати абсолютні обсяги втрат, а й виявити структурні вразливості платіжної екосистеми.

У звіті наголошується, що попри відносно низький загальний рівень шахрайства у відсотковому співвідношенні до сукупної вартості платіжних операцій, абсолютні фінансові втрати залишаються значними і демонструють стабільну тенденцію до зростання. Найбільша частка втрат припадає на кредитні перекази, що свідчить про зміщення фокусу шахраїв від традиційного карткового шахрайства до більш складних схем соціальної інженерії, зокрема шахрайство з авторизованими платіжними переказами (APP-шахрайство). Такі схеми ґрунтуються не на технічному зламі систем, а на маніпуляції поведінкою користувачів, що суттєво ускладнює їх виявлення та запобігання стандартними засобами автентифікації.

Документ детально показує, що абсолютна більшість шахрайських операцій здійснюється дистанційно, без фізичної присутності клієнта або платіжного інструменту. Це характерно практично для всіх платіжних інструментів, але особливо — для кредитних переказів та операцій з електронними грошима. У випадку карткових платежів спостерігається чіткий розрив між законним використанням карток, яке здебільшого залишається недистанційним, і шахрайством, яке концентрується саме в онлайн-каналах. Така асиметрія підтверджує, що цифровізація платежів без супровідного посилення контролів створює сприятливе середовище для зловживань.

Окрему увагу звіт приділяє ролі автентифікації клієнта як ключового інструменту регуляторного впливу на рівень шахрайства. Аналіз даних переконливо демонструє, що транзакції, до яких застосовується SCA, у середньому є значно менш уразливими до шахрайства, особливо у сфері карткових платежів та електронних грошей. Водночас підкреслюється, що сама по собі SCA не є панацеєю, оскільки у випадку кредитних переказів вона часто застосовується саме до операцій із підвищеним ризиком, що статистично спотворює порівняння. Це дозволяє авторам звіту зробити ширший висновок про необхідність поєднання автентифікації з поведінковою аналітикою, контекстними перевірками та додатковими превентивними механізмами.

Значний блок звіту присвячений транскордонному виміру платіжного шахрайства. Показано, що операції з контрагентами поза межами ЄЕЗ характеризуються кратно вищими рівнями шахрайства, особливо у картковому сегменті. Це прямо пов’язується з відсутністю обов’язкових вимог щодо SCA в третіх країнах та з обмеженою ефективністю координації між платіжними системами різних юрисдикцій. Таким чином, транскордонні платежі розглядаються як одна з ключових зон залишкового ризику навіть у високорегульованому середовищі ЄС.

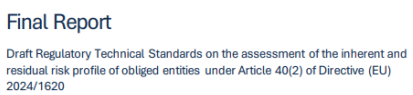
Важливим аспектом аналізу є розподіл фінансових втрат між платіжними установами та користувачами платіжних послуг. Звіт фіксує, що у випадку кредитних переказів переважна частка втрат покладається на клієнтів, тоді як у карткових платежах фінансове навантаження більш рівномірно розподілене або частіше лягає на платіжні установи. При цьому між державами-членами ЄС спостерігаються істотні відмінності, що вказує на різне тлумачення та застосування правил відповідальності, а також на неоднаковий рівень захисту споживачів у практичному вимірі.

У завершальній частині документа платіжне шахрайство розглядається не як ізольована проблема, а як динамічний ризик, тісно пов'язаний із розвитком миттєвих платежів, цифрових каналів обслуговування та трансформацією поведінки користувачів. Звіт чітко сигналізує, що подальше зниження рівня шахрайства можливе лише за умови системного підходу, який поєднує регуляторні вимоги, технологічні рішення, підвищення фінансової обізнаності клієнтів та більш тісну взаємодію між платіжними установами, наглядовими органами та органами фінансової розвідки.

Висновки:

- **APP-шахрайство є системним ризиком.** Необхідно перенести фокус контролів із технічної автентифікації на поведінкові та контекстні індикатори, включно з перевіркою отримувача платежу і затримками високоризикових платежів.
- **Винятки з SCA — ключова точка вразливості.** Надавачі платіжних послуг (PSP) мають переглянути політики застосування винятків автентифікації клієнта (SCA), особливо для дистанційних карткових операцій та операцій з електронними грошима.
- **Транскордонні операції поза ЄЕЗ — зона підвищеного ризику.** Потрібне посилення контролю платежів із контрагентами за межами ЄЕЗ, включно з обмеженнями та додатковою автентифікацією.
- **Нерівномірний розподіл втрат сигналізує про регуляторні прогалини.** Регуляторам доцільно гармонізувати підходи до відповідальності та відшкодування, оскільки нинішня практика перекладає основний тягар шахрайства на користувачів, що підвищує соціальні та репутаційні ризики.

Єдина європейська методологія оцінки ризиків відмивання коштів та фінансування тероризму: нові регуляторні технічні стандарти [6]


Final Report

Draft Regulatory Technical Standards on the assessment of the inherent and residual risk profile of obliged entities under Article 40(2) of Directive (EU) 2024/1620

Документ є фінальним звітом, що містить проєкт регуляторних технічних стандартів, розроблених Європейським органом з протидії відмиванню коштів відповідно до статті 40, пункту 2 Директиви (ЄС) 2024/1640, і спрямований на створення єдиної, обов'язкової для всіх держав-членів Європейського Союзу методології оцінки та класифікації ризику відмивання коштів і фінансування тероризму на рівні окремих зобов'язаних суб'єктів фінансового сектору.

Документ ґрунтується на визнанні того, що чинні національні підходи до оцінки ризиків є фрагментованими, непорівнюваними та такими, що призводять як до нерівномірності

[6] https://www.amla.europa.eu/document/download/c8782141-45bf-4ef9-9d66-33e2f90e607e_en?filename=1.1_20251216_FINAL%20REPORT%20RTS%2040%282%29%20AMLD%20financial%20only_Final.pdf

наглядових результатів, так і до надмірного регуляторного навантаження для суб'єктів, які здійснюють транскордонну діяльність, що в сукупності підриває ефективність загальноєвропейської системи протидії відмиванню коштів та фінансуванню тероризму. У цьому контексті документ розглядається не лише як технічний інструмент уніфікації наглядових практик, а як один із ключових елементів нової інституційної архітектури європейської системи протидії фінансовим злочинам, покликаної забезпечити єдине розуміння ризиків, однакову інтерпретацію наглядових сигналів та узгоджене застосування ресурсів нагляду в усіх державах-членах.

З цією метою у звіті запропоновано повністю гармонізовану ризик-орієнтовану методологію, яка встановлює спільний набір обов'язкових показників, єдині принципи їх зважування та стандартизований порядок формування підсумкових ризик профілів, що мають використовуватися всіма наглядовими органами без винятку. Такий підхід має усунути ситуації, за яких одна й та сама бізнес-модель або тип операцій оцінюється як високоризикова в одній державі та як помірно ризикова в іншій, а також мінімізувати можливості регуляторного арбітражу. Водночас документ наголошує, що гармонізація не означає механічної уніфікації, а має поєднувати стандартизацію з можливістю обмеженого врахування національних особливостей ризик-середовища за умови належного обґрунтування та документування таких рішень з боку наглядових органів.

Ключовою концептуальною основою документа є трирівнева модель оцінювання, яка передбачає послідовне визначення властивого ризику, оцінку якості системи внутрішніх заходів протидії відмиванню коштів та фінансуванню тероризму і, на цій основі, формування залишкового ризику, тобто того рівня ризику, який залишається після застосування відповідних політик, процедур, систем і контролів. Така логіка відповідає міжнародним стандартам і відображає розуміння того, що високий рівень властивого ризику сам по собі не є ознакою порушень, однак вимагає адекватно розвиненої та ефективної системи контролю. Властивий ризик визначається виходячи з об'єктивних характеристик діяльності установи, зокрема типів клієнтів, пропонованих продуктів і послуг, використовуваних каналів надання послуг, географічних зон діяльності та структури операцій, і розраховується переважно автоматизовано на основі кількісних даних, що покликано забезпечити масштабованість та порівнюваність оцінок у межах усього Європейського Союзу.

Оцінка якості контролю, навпаки, поєднує автоматизовані розрахунки з обґрунтованим професійним судженням наглядових органів, що базується на результатах інспекцій, тематичних перевірок, аналізу регуляторної звітності, матеріалів внутрішнього контролю та висновків внутрішнього або зовнішнього аудиту. Документ виходить з того, що ефективність системи протидії відмиванню коштів та фінансуванню тероризму не може бути адекватно оцінена виключно на основі формальних показників або наявності політик, а повинна відображати фактичну спроможність установи виявляти, аналізувати та своєчасно повідомляти про підозрілі фінансові операції, а також оперативно реагувати на санкційні обмеження. При цьому можливість коригування автоматично сформованих оцінок жорстко обмежена і допускається лише у виключних, належно обґрунтованих випадках, що покликано запобігти суб'єктивності та забезпечити цілісність методології.

Документ детально регламентує систему оцінювання, яка використовує чотирирівневу шкалу ризику для класифікації як властивого, так і залишкового ризику, а також окрему шкалу для оцінки якості заходів внутрішнього контролю, що дозволяє забезпечити порівнюваність результатів між державами-членами та різними секторами фінансового ринку. Водночас конкретні числові порогові значення та вагові коефіцієнти свідомо не закріплюються безпосередньо в регуляторних технічних стандартах, а підлягають визначенню та періодичному оновленню Європейським органом з протидії відмиванню коштів, що має забезпечити адаптивність методології до еволюції ризиків, появи нових фінансових продуктів, технологічних

змін і нових типологій відмивання коштів і фінансування тероризму. Такий підхід підкреслює динамічний характер ризиків і необхідність постійного коригування наглядових інструментів без внесення змін до базових нормативних актів.

Окремий акцент зроблено на принципі пропорційності, відповідно до якого стандартною є щорічна оцінка ризик-профілю підзвітних суб'єктів, однак для дуже малих або низькоризикових установ допускається перегляд один раз на три роки, за умови відсутності суттєвих змін у діяльності або системі управління ризиками. Водночас документ передбачає обов'язковість позапланових оцінок у разі виникнення істотних подій, таких як зміна бізнес-моделі, структури власності, виявлення серйозних недоліків у системі контролю або інших факторів, здатних суттєво вплинути на ризик-профіль установи, що посилює превентивну функцію нагляду.

Висновки:

- **Для наглядових органів:** документ фактично ліквідує національну дискрецію у методології оцінки ризиків — наглядові органи зобов'язані перейти на єдину модель уже до 2027 року.
- **Для фінансових установ:** фокус на кількісних показниках даних означає, що якість даних, їх агрегування та внутрішня аналітика ризиків стануть критичними — слабкі системи або фрагментовані дані безпосередньо підвищуватимуть ризик.
- **Для протидії відмиванню коштів та фінансуванню тероризму більше не працюватимуть формальні оцінки** — ефективність контролю буде оцінюватися через об'єктивні показники, що вимагає реального підвищення операційної спроможності, а не лише наявності політик.
- **Стратегічно для Європейського Союзу регуляторні технічні стандарти задають чіткий орієнтир для гармонізації наглядових практик** — національні системи протидії відмиванню коштів та фінансуванню тероризму, які не адаптують аналогічну ризик-орієнтовану модель, засновану на стандартизованих показниках даних, ризикують опинитися несумісними з європейською екосистемою фінансового моніторингу.

Невід'ємною складовою документа є додаток, який містить вичерпний і структурований перелік обов'язкових показників для оцінки як властивого ризику, так і якості заходів протидії відмиванню коштів та фінансуванню тероризму, з урахуванням секторальної специфіки банків, платіжних установ, інвестиційних фірм, емітентів електронних грошей, постачальників послуг, пов'язаних із віртуальними активами, та інших фінансових суб'єктів. Ці показники охоплюють клієнтські ризики, зокрема пов'язані з політично значущими особами та кінцевими бенефіціарними власниками, продуктові та операційні ризики, географічні фактори, використання посередників і дистанційних каналів, а також ефективність корпоративного управління, належної перевірки клієнтів, моніторингу операцій, подання повідомлень про підозрілі фінансові операції, дотримання режимів цільових фінансових санкцій і функціонування групових систем контролю. Така деталізація фактично переводить наглядову оцінку ризиків у площину системної роботи з даними та показниками результативності, змінюючи традиційний акцент із формальної відповідності вимогам на реальну ефективність.

Застосування цих регуляторних технічних стандартів передбачено поетапно, на першому етапі — виключно для фінансового сектору, із подальшою розробкою окремих стандартів для визначених нефінансових установ та професій, що дозволяє поступово та контрольовано впровадити нову модель нагляду з урахуванням різного рівня зрілості секторів. У підсумку документ формує нормативну основу для уніфікованого, прозорого та орієнтованого на дані підходу до наглядової оцінки ризиків у Європейському Союзі та водночас задає чіткий орієнтир

для держав-кандидатів, включно з Україною, у контексті гармонізації національних систем фінансового моніторингу з європейськими стандартами та поступової інтеграції до спільного європейського простору фінансового нагляду.

Антикорупційна стратегія Великої Британії 2025: від кримінального переслідування до управління ризиками та національної безпеки [7]

Документ є комплексною політичною рамкою, яка визначає підхід Сполученого Королівства до протидії корупції як системній загрозі економічному розвитку, національній безпеці та демократичному устрою.

Стратегія виходить із чіткого розуміння того, що корупція не обмежується окремими кримінальними правопорушеннями, а функціонує як транснаціональний механізм перерозподілу ресурсів, влади та впливу, тісно пов'язаний із відмиванням коштів, організованою злочинністю, клептократією та підривною діяльністю ворожих держав. У цьому контексті Велика Британія прямо визнає власну вразливість як глобального фінансового та професійного хабу, що робить її привабливою для інтеграції корупційних доходів у легальну економіку та суспільні інститути

Центральним концептуальним зрушенням документа є запровадження єдиного політичного визначення корупції, яке охоплює не лише незаконні дії, але й зловживання довіреною владою, що порушує стандарти доброчесності, регуляторні норми або професійну етику. Такий підхід дозволяє розглядати корупцію ширше за межі кримінального права і фокусуватися на її реальній шкоді — зниженні довіри до держави, спотворенні ринків, підриві інституцій та легалізації незаконно набутого впливу. Стратегія підкреслює, що традиційні індикатори, зокрема статистика вироків або сприйняття корупції, не відображають її реального масштабу, а тому ефективність державної політики має оцінюватися через зменшення шкоди та посилення стійкості системи

Аналітична частина документа детально описує економічний вимір корупції, наголошуючи, що вона є довгостроковим гальмом зростання. Корупційні практики руйнують конкуренцію, підвищують вартість ведення бізнесу, знижують інвестиційну привабливість та підривають репутацію країни як безпечної юрисдикції. Окремо підкреслюється масштаб проблеми легалізації корупційних доходів через британські фінансові та корпоративні структури, де, за оцінками Національного агентства з боротьби зі злочинністю, щороку можуть відмиватися суми, що обчислюються десятками мільярдів фунтів. Ці процеси безпосередньо впливають на ринок нерухомості, інфраструктурні проєкти та доступ громадян до базових послуг, формуючи соціальне невдоволення та нерівність

Безпековий вимір стратегії ґрунтується на тезі, що корупція є мультиплікатором загроз. Корумповані посадовці в поліції, прикордонній службі, міграційних органах чи пенітенціарній системі безпосередньо сприяють діяльності організованих злочинних угруповань, незаконному обігу наркотиків і зброї, а також обходу міграційних та санкційних режимів. На міжнародному рівні корупція розглядається як чинник дестабілізації, який сприяє державному захопленню, фінансуванню конфліктів і вимушеній міграції. Війна росії проти України у документі

[7] https://assets.publishing.service.gov.uk/media/6932caa7375aee4a15ee8c8c/36.37_HO_JACU-Strategy_v12b_FINAL_WEB.pdf

використовується як ключовий приклад того, як клептократичні режими трансформують корупцію на інструмент геополітичної агресії та підриву міжнародної безпеки.

Окрему увагу стратегія приділяє підриву демократичних процесів. Корупційний вплив на політичне фінансування, місцеве самоврядування, публічні закупівлі та суспільно значущі інституції розглядається як загроза довірі громадян до держави. Документ наголошує, що навіть поодинокі випадки недоброчесності у публічному секторі мають непропорційно високий репутаційний ефект, підриваючи легітимність влади та ефективність державної політики. Саме тому стратегія акцентує на посиленні стандартів доброчесності, інституційних механізмах нагляду та формуванні культури нульової толерантності до корупції

Функціонально стратегія вибудовує цілісний ланцюг реагування на корупцію — від раннього виявлення і повідомлення про підозрілі дії до розслідування, судового переслідування, конфіскації активів та міжнародної співпраці. Значний акцент зроблено на розвитку спеціалізованих правоохоронних і аналітичних спроможностей, зокрема через Domestic Corruption Unit, National Crime Agency, Serious Fraud Office та International Anti-Corruption Coordination Centre. Документ визнає структурні проблеми, пов'язані з тривалістю та складністю корупційних справ, дефіцитом фахових кадрів і навантаженням на судову систему, та пропонує інституційні й технологічні рішення для їх подолання, включно з активним використанням штучного інтелекту у фінансових розслідуваннях

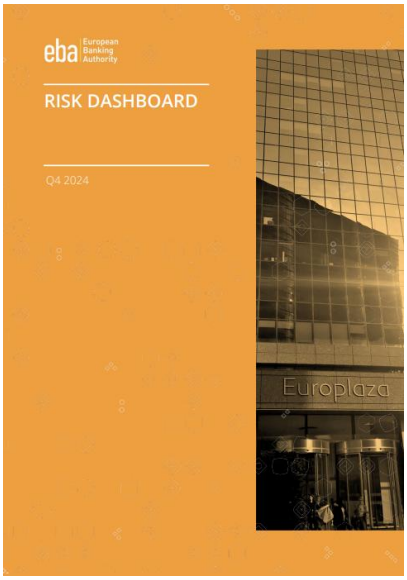
Висновки:

- **Корупція офіційно інтегрується в рамку національної безпеки та ПВК/ФТ,** що означає перехід від фрагментарних кримінальних розслідувань до системного управління ризиками, включно з фінансовою розвідкою, санкціями та контролем інсайдерських загроз.
- **Фінансова та професійна інфраструктура визнається ключовою «критичною ланкою»,** тому консолідація нагляду у сфері ПВК/ФТ і фокус на професійних посередниках фактично переносять центр ваги антикорупційної боротьби в сферу фінансового моніторингу та комплаєнсу.
- **Клептократія розглядається як окремий тип загрози,** що потребує спеціальних інструментів (санкції, імміграційні обмеження, прозорість активів), а не лише класичних механізмів протидії відмиванню коштів.
- **Використання штучного інтелекту та даних стає операційною необхідністю,** а не експериментом: прискорення розслідувань, пріоритизація кейсів і міжвідомча координація визначені як критичні фактори успіху антикорупційної діяльності.

Особливе місце у стратегії займає феномен клептократії, який описується як системна форма корупції, де незаконно набуте багатство легалізується через державні механізми країни походження, а потім інтегрується у західні економіки під виглядом легального капіталу. Документ детально аналізує роль професійних посередників, фінансових, юридичних, репутаційних та консалтингових сервісів у забезпеченні доступу клептократів до британських інституцій, політичних і культурних кіл. У відповідь пропонується поєднання санкцій, імміграційних обмежень, посилення прозорості бенефіціарної власності та перегляду ефективності чинного законодавства щодо боротьби з фінансовими злочинами

Наскрізною ідеєю документа є те, що успіх антикорупційної політики залежить не лише від законів чи окремих розслідувань, а від здатності держави вибудувати стійку екосистему доброчесності. Саме тому стратегія передбачає реформу системи нагляду у сфері ПВК/ФТ, консолідацію контролю за професійними секторами, посилення механізмів захисту викривачів, підвищення прозорості активів і системну міжнародну взаємодію.

Оцінка ризиків банківського сектору ЄС: ключові сигнали EBA у 2025 році [8]



Документ підготовлений European Banking Authority (EBA) є комплексним аналітичним оглядом стану та еволюції ризиків банківського сектору Європейського Союзу та Європейської економічної зони. Його зміст спрямований на систематичну фіксацію поточного профілю ризиків, їх динаміки у часі та ступеня концентрації в межах окремих країн, бізнес-моделей і розмірів банків, що робить документ ключовою аналітичною основою для наглядових рішень, макро-пруденційної політики та оцінки стійкості фінансової системи в цілому

В основі документа лежить уніфікована система показників ризику, яка охоплює чотири взаємопов'язані виміри: платоспроможність, кредитний ризик і якість активів, прибутковість, а також фінансування і ліквідність. Центральним інструментом візуалізації виступає теплова карта ризиків, що дозволяє одночасно оцінити абсолютні рівні показників і їхню динаміку у порівнянні з попередніми кварталами, а також ідентифікувати зони потенційного погіршення, навіть за відсутності різких змін у середніх значеннях по сектору.

Аналіз платоспроможності демонструє, що банківський сектор ЄС у цілому зберігає високий рівень капіталізації. Показники Tier 1 capital ratio, Total capital ratio та CET1 ratio залишаються стабільно вище регуляторних мінімумів і свідчать про значний запас міцності, накопичений у попередні роки внаслідок посилених регуляторних вимог, обмежень на розподіл прибутку та консервативної капітальної політики. Водночас детальний аналіз дисперсії показує істотну неоднорідність між країнами та групами банків, що означає, що середні агреговані значення маскують окремі сегменти з підвищеною вразливістю, особливо серед менших або структурно спеціалізованих установ.

У частині кредитного ризику та якості активів документ фіксує подальше зниження частки непрацюючих кредитів до історично низьких рівнів, що є результатом тривалого процесу очищення балансів, активного управління проблемною заборгованістю та впровадження стандартів IFRS 9. Разом з тим EBA звертає увагу на те, що позитивна динаміка супроводжується зниженням показників покриття та поступовим зростанням ризиків у новому кредитуванні, особливо в умовах високих відсоткових ставок і погіршення платоспроможності окремих секторів економіки. Це означає, що майбутні ризики можуть матеріалізуватися не через «спадщину минулих криз», а через нові кредитні портфелі, сформовані в умовах жорсткішої монетарної політики.

Показники реструктуризованих кредитів залишаються на відносно низькому рівні, що з одного боку свідчить про обмежене використання пом'якшувальних інструментів, а з іншого – може вказувати на ризик відкладеної проблемної заборгованості, якщо макроекономічні умови погіршаться. У цьому контексті документ підкреслює важливість раннього виявлення кредитних ускладнень і своєчасного коригування моделей оцінки ризику.

У блоці прибутковості EBA фіксує покращення фінансових результатів банків, зумовлене зростанням чистого процентного доходу на тлі підвищених ставок. Однак цей ефект розглядається як циклічний і потенційно тимчасовий, оскільки зростання витрат на ризик,

[8] https://www.eba.europa.eu/sites/default/files/2025-03/948020f4-c628-4698-87e9-3be7f21919c0/EBA%20Risk%20Dashboard%20-%20Q4%202024.pdf

операційних витрат і конкуренції за депозити поступово зменшує позитивний вплив процентного середовища. Документ акцентує увагу на структурних обмеженнях бізнес-моделей європейських банків і наголошує, що поточна прибутковість не повинна розглядатися як індикатор довгострокової стійкості без урахування профілю ризику.

Висновки:

- **Наглядовим органам доцільно зміщувати фокус із формального рівня капіталу на якість ризиків,** зокрема на структуру нових кредитних портфелів і концентрацію у вразливих секторах, оскільки високі показники не гарантують стійкості у разі шоків.
- **Банкам необхідно переглянути підходи до управління прибутковістю,** використовуючи поточне вікно підвищених процентних доходів для зміцнення резервів та інвестицій у управління ризиками, а не для короткострокової оптимізації фінансових результатів.
- **Політики ліквідності мають враховувати поведінкові ризики депозитів,** зокрема цифрові канали відтоку коштів, що потребує застосування більш стрес-орієнтованих сценаріїв та регулярного оновлення планів фінансування на випадок кризових ситуацій.
- **Для країн-кандидатів до ЄС та асоційованих юрисдикцій** цей документ може використовуватися як референтний показник для гармонізації наглядових підходів, калібрування пруденційних індикаторів та побудови власних національних оцінок ризиків за методологією EBA.

Аналіз фінансування і ліквідності показує, що більшість банків підтримують значні буфери ліквідності, а показники коефіцієнту покриття ліквідністю (LCR) та коефіцієнту чистого стабільного фондування (NSFR) залишаються на комфортних рівнях. Водночас EBA звертає увагу на зміну структури фондів, зростання чутливості депозитів до процентних ставок і поведінкові ризики, пов'язані з цифровізацією фінансових послуг. Це означає, що формальне дотримання нормативів ліквідності не завжди гарантує стійкість у разі швидких і нетрадиційних шоків, зокрема інформаційних або репутаційних.

У підсумку документ формує цілісну картину банківського сектору, який входить у фазу підвищеної макрофінансової невизначеності з відносно сильних позицій, але водночас накопичує низку прихованих і структурних ризиків. EBA чітко демонструє, що ключовим викликом для нагляду стає не рівень показників як таких, а їх якість, взаємозв'язок і здатність банків адаптуватися до швидких змін економічного та фінансового середовища.

Оновлені процедури FATF: нова архітектура взаємних оцінок, моніторингу та глобального нагляду у сфері ПВК/ФТ/ФР [9]

FATF випустила оновлену редакцію процедур, актуалізовану у грудні 2025 року, яка відображає зміни до стандартів і методології FATF, ухвалені у 2022 році, та встановлює єдині обов'язкові правила для проведення взаємних оцінок, подальшого моніторингу й процедур Групи з перегляду міжнародного співробітництва (ICRG) у межах п'ятого раунду оцінювання, що фактично розпочався з 2024 року.

Цей документ виконує роль процесуального «каркасу», який переводить стандарти FATF із рівня нормативних принципів у практично застосовуваний механізм глобального нагляду, взаємної

[9] https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/Assessment-Follow-Up-ICRG-Procedures-2022.pdf.coredownload.inline.pdf

підзвітності та системного тиску між державами з метою досягнення реальної ефективності систем ПВК/ФТ/ФР.

Документ виходить із фундаментального положення про те, що взаємна оцінка є не разовою перевіркою, а елементом безперервного циклу оцінювання, коригування та повторної перевірки національних систем ПВК/ФТ.

Центральним концептуальним ядром процедур є поєднання двох взаємопов'язаних вимірів — технічної відповідності та ефективності. Технічна відповідність трактується не як формальна наявність законів чи інституцій, а як їх реальна придатність до застосування, актуальність і узгодженість зі зміненими стандартами FATF. Ефективність оцінюється через досягнення одинадцяти безпосередніх результатів, які відображають фактичні результати функціонування системи: здатність держави ідентифікувати та розуміти ризики, забезпечувати міжвідомчу координацію, здійснювати результативні фінансові розслідування, застосовувати конфіскацію доходів і активів, а також ефективно співпрацювати на міжнародному рівні.

Процедури чітко закріплюють, що повний доказовий тягар покладається на державу, яка оцінюється. Саме вона зобов'язана надати вичерпні, актуальні та доказові матеріали, що підтверджують як формальну відповідність стандартам FATF, так і реальні результати їх застосування. Держава має не лише реагувати на запити оцінювачів, а й проактивно пояснювати власний ризик-профіль, національний контекст, особливості окремих секторів та логіку регуляторних і наглядових рішень. У такий спосіб взаємна оцінка вибудовується як глибокий аналітичний процес, у межах якого оцінюється не «наявність правил», а здатність системи працювати в умовах реальних ризиків.

Суттєвою рисою оновлених процедур є посилення ризик-орієнтованого підходу до визначення фокусу оцінювання. Ще до виїзної місії команда оцінювачів формує попереднє бачення ключових ризиків, сфер підвищеної уваги та напрямів можливого зниження інтенсивності аналізу. Це рішення ґрунтується на національній оцінці ризиків, матеріалах попередніх взаємних оцінок і звітів подальшого моніторингу, інформації з надійних зовнішніх джерел та відгуках інших юрисдикцій щодо практики міжнародної співпраці з оцінюваною державою. Такий підхід означає, що проблемні або структурно слабкі напрями автоматично стають центральними під час оцінки ефективності, незалежно від формальної відповідності законодавства.

Документ детально регламентує всі етапи оцінювального процесу — від підготовчої фази та збору інформації до проведення виїзної місії, підготовки проєкту звіту, його обговорення та ухвалення на Пленарному засіданні FATF. Особлива увага приділяється якості, узгодженості та об'єктивності звітів, що забезпечується через багаторівневі механізми внутрішнього та зовнішнього рецензування, участь незалежних експертів і активну координаційну роль Секретаріату FATF. Суворі часові межі для кожного етапу підкреслюють, що недотримання процедур або строків розглядається не як технічний збій, а як фактор, що впливає на довіру до держави та її готовність до співпраці.

Центральним інструментом, який поєднує взаємну оцінку з подальшим моніторингом, у документі виступає Дорожня карта ключових рекомендованих дій. Вона трансформує рекомендації взаємної оцінки у структуровану програму реформ із чітко визначеними очікуваними результатами та орієнтирами прогресу. Саме виконання або невиконання

ключових рекомендованих дій (KRA) стає основним критерієм оцінки в межах процедур подальшого моніторингу та діяльності ICRG, що фактично перетворює рекомендації FATF на інструмент постійного політико-регуляторного впливу на держави.

Окремі положення документа детально визначають ролі та відповідальність усіх учасників процесу — оцінюваних держав, оцінювачів, рецензентів, експертів подальшого моніторингу, спільних груп ICRG та Секретаріату. Особливий акцент зроблено на незалежності експертів, управлінні конфліктами інтересів і суворому режимі конфіденційності, що має на меті захист цілісності процесу та легітимності його результатів. Порушення цих принципів розглядається як серйозна загроза якості оцінювання та авторитету FATF.

Документ також враховує реалії наднаціонального регулювання, зокрема для держав, що входять до інтеграційних утворень. Він чітко закріплює, що навіть за наявності наднаціональних норм відповідальність за їх імплементацію та фактичну ефективність залишається на рівні окремої держави. Механізм визнання наднаціональної компетенції FATF визначається як винятковий і такий, що не звільняє державу від індивідуальної оцінки.

Важливою складовою оновлених процедур є інтеграція результатів взаємних оцінок FATF у ширший контекст глобального фінансового нагляду через взаємодію з МВФ і Світовим банком у межах Програми оцінки фінансового сектору (FSAP) та Звіту про дотримання стандартів і кодексів (ROSC). Це означає, що висновки FATF безпосередньо впливають не лише на статус держави у сфері ПВК/ФТ/ФР, а й на її загальну фінансову репутацію, інвестиційну привабливість і доступ до міжнародних фінансових ресурсів.

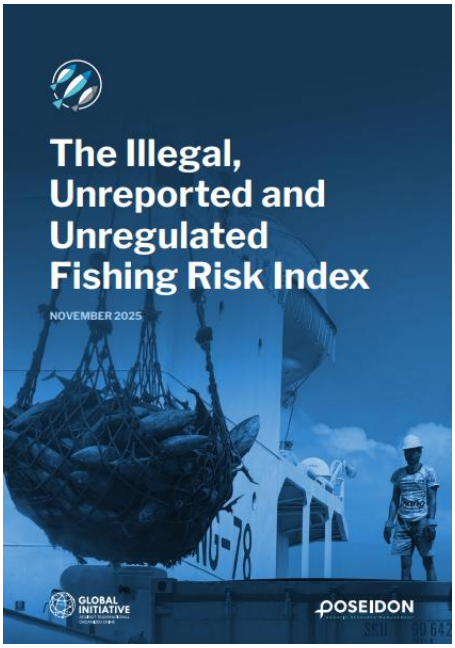
Висновки:

- **Підготовка до взаємної оцінки має бути безперервним процесом, а не реакцією на виїзну місію:** державам необхідно вибудовувати внутрішні механізми моніторингу ключових рекомендованих дій та безпосередніх результатів у режимі постійної готовності.
- **Ефективність домінує над формальною технічною відповідністю:** законодавчі та інституційні зміни без підтверджених практичних результатів більше не розглядаються як достатній прогрес.
- **Дорожня карта ключових рекомендованих дій стає інструментом політичної та інституційної відповідальності, а не технічним додатком до звіту:** її невиконання автоматично підвищує ризик переходу до процедур посиленого подальшого моніторингу або застосування механізмів Групи з перегляду міжнародного співробітництва.
- **Недотримання процедур і строків прирівнюється до браку співпраці,** що може мати прямі репутаційні та економічні наслідки, включно з публічними заявами FATF і впливом на оцінки МВФ / Світового банку.

У підсумку оновлений документ формує цілісну, жорстко структуровану та водночас ризик-орієнтовану модель глобального нагляду, у межах якої взаємна оцінка, подальший моніторинг і процедури ICRG є елементами єдиного безперервного процесу, спрямованого на досягнення не формальної, а доведеної та стійкої ефективності національних систем протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

Звіти окремих інституцій та експертів

Глобальний індекс ризику незаконного, нереєстрованого та нерегульованого вилову риби (IUU) 2025 [10]



У світі, де глобальні ланцюги поставок стають дедалі складнішими, а обсяги міжнародної торгівлі сягають трильйонів доларів, сектор риболовлі залишається одним з найбільш непрозорих та вразливих до зловживань. Незаконний, нереєстрований та нерегульований вилов (IUU) давно перестав бути виключно екологічною проблемою; це потужний, високоприбутковий вид транснаціональної злочинної діяльності, тісно переплетений з відмиванням коштів, корупцією, ухиленням від сплат податків та навіть фінансуванням збройних конфліктів.

Четверта ітерація Глобального індексу ризику IUU за 2025 рік, опублікована спільно Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC) та Poseidon Aquatic Resource Management, надає не просто черговий набір рейтингів. Вона пропонує комплексну, структуровані за методологією карту глобальних ризиків, яка є незамінним інструментом для аналітиків фінансової безпеки, правоохоронних органів, політиків та всіх, хто займається протидією відмиванню коштів (AML) у найширшому її розумінні.

Індекс, що охоплює 152 прибережні держави через призму 40 кількісних і якісних індикаторів, не вимірює безпосередні обсяги незаконного вилову — що залишається статистичною проблемою світового масштабу — але з неймовірною деталізацією оцінює інституційну спроможність, регуляторні прогалини та оперативну вразливість країн, створюючи уніфіковану метрику ризику, за якою можна порівнювати юрисдикції, відстежувати динаміку та вибудовувати профільні стратегії втручання.

Загальний глобальний бал у 2025 році, що становить 2.27, практично ідентичний показникам 2023 (2.28) та 2021 (2.24) років, ясно сигналізує про глобальну стагнацію. Ця цифра, що ледь зміщується впродовж шести років спостережень, є тривожним свідченням того, що міжнародні зусилля, ратифікація угод та публічні заяви поки що не призвели до якісного зменшення системних ризиків IUU.

За цією середньою величиною криється різка диференціація. Абсолютним аутсайдером, як і з моменту запуску індексу в 2019 році, залишається Китай з балом 3.60. Його вразливість оцінена в 4.36, поширеність — у 4.19, і навіть покращення у сфері реагування до 2.64 не змінюють загальної картини. Масштаби китайської флотилії далекого плавання, її присутність у всіх океанічних басейнах, а також складнощі в ефективному контролі за її діяльністю створюють безпрецедентний ризик. Для AML-режиму це прямий виклик: операції, пов'язані з китайськими риболовними суднами, компаніями, що їх фінансують, або трейдерами, що працюють з китайськими портами, мають розглядатися як такі, що мають підвищений ризик через високу ймовірність участі в нелегальних практиках, що потребують подальшої фінансової легалізації. Поруч із Китаєм у групі найбільш проблемних країн тривало перебувають Іран (3.01), Індонезія (3.00), росія (3.00) та Ємен (3.00). Цей список — готовий перелік юрисдикцій, присутність яких повинна запускати механізми посиленого нагляду в фінансових установах по всьому світу.

[10] https://globalinitiative.net/wp-content/uploads/2025/11/IUU-Report-2025.pdf

Регіональний аналіз підкреслює географічну концентрацію ризиків. Азія з загальним балом 2.55 посідає перше місце серед регіонів, демонструючи найвищі показники як за вразливістю (3.18), так і за поширеністю (2.38). Близький Схід (2.41) виділяється катастрофічно низькою ефективністю реагування (3.36), що свідчить про системну неспроможність або брак політичної волі в боротьбі з IUU. Для AML-фахівців це означає, що фінансові потоки, пов'язані з рибною промисловістю цих регіонів, особливо ті, що проходять через порти ОАЕ, Кувейту, Катару або Ємену, можуть бути частиною схем з легалізації коштів, отриманих від незаконного вилову.

Океанічні басейни демонструють ще більш виразну картину. Східний та Західний Індійський океан з балами 2.44 та 2.43 відповідно є найбільш проблемними акваторіями світу. Тут зосереджені не лише значні біологічні ресурси, а й часто слабкі прибережні держави з великими економічними зонами, що не мають ресурсів для їх належного контролю. Перехоплення риби, виловленої незаконно в водах Сомалі, Мозамбіку або Індонезії, та її подальша легалізація через порти сусідніх країн або через глобальні торгові хаби є класичною схемою, яка потребує від правоохоронних систем вміння відстежувати складні маршрути та виявляти розбіжності в документації.

Детальний розбір індексів за типами відповідальності розкриває механізми формування ризику. Прапорова відповідність залишається ключовою ланкою. Країни з великими флотами далекого плавання — Китай, Франція (3.84 за вразливість), Японія (4.28), Іспанія (3.52), Південна Корея (3.76) — природньо мають високі бали за вразливість. Однак проблема не у самому факті наявності флоту, а у ефективності контролю. Такі індикатори, як «Судна в IUU-списках RFMO», «Дані від спостерігачів про інциденти» та «Дотримання прапорових зобов'язань перед RFMO», викривають реальну картину. Погіршення багатьох з цих показників у 2025 році вказує на розширення практик ухилення. Для фінансових установ це прямий сигнал: судна під «зручними прапорами» або під прапорами країн зі слабким адмініструванням (наприклад, деяких острівних держав) є потенційними носіями не тільки екологічних, а й фінансових ризиків. Кредитування, страхування або обслуговування рахунків таких суден або пов'язаних із ними компаній може призвести до серйозних репутаційних втрат та правових наслідків.

Портова відповідальність, що регулюється Портовою угодою (PSMA), є іншим критичним бар'єром на шляху легалізації незаконного улову. Індекс фіксує, що ратифікація PSMA продовжує поширюватися, але її імплементація залишається нерівномірною. Близькосхідні порти, такі як Дубай, продовжують демонструвати критично низьку ефективність реагування. Водночас, зростання індикатора «Відвідування портів іноземними судами» у багатьох країнах вказує на збільшення трафіку, а отже, і на потенційні можливості для змішування легального та нелегального вилову. Для AML-процесів це означає необхідність глибшого аналізу контрактів, інвойсів та логістичних маршрутів, особливо коли риба проходить через транзитні порти в юрисдикціях зі слабким портовим контролем, перш ніж потрапити на ринки ЄС чи США.

Найбільш прямий зв'язок із традиційними AML-ризиками демонструють загальні індикатори. Такі фактори, як «Сприйняття рівня корупції» (за даними Transparency International), «Валовий національний дохід на душу населення» та «Торговий баланс рибної продукції», чітко корелюють із загальним балом IUU. Країни з низькими доходами, високою корупцією та значним імпортом риби (що часто свідчить про внутрішній попит, який перевищує легальні можливості) є надзвичайно вразливими. Наприклад, Коморські Острови (3.37), Еритрея (3.33) чи Демократична Республіка Конго (3.11) поєднують у собі всі ці ризики. У таких умовах незаконний вилов часто контролюється корумпованими елітами або організованими злочинними групами, а прибутки від нього інтегруються в економіку через нерухомість, банківські рахунки або розкішні товари. AML-підрозділи, що працюють у цих країнах або мають справу з клієнтами, які ведуть там бізнес, повинні включати IUU-ризики в свою загальну модель оцінки ризиків.

Важливим аспектом індексу є його динамічність. Між 2023 та 2025 роками 68 країн покращили свої показники, а 76 — погіршили. Різке просідання Брунею (-64 позиції), Сейшельських Островів (-62) та Малайзії (-59) є тривожним сигналом. Такі швидкі зміни можуть свідчити про послаблення регуляторного нагляду, зростання корупційного тиску або появу нових злочинних схем. Для міжнародних банків та компаній, що працюють у цих юрисдикціях, це вимагає негайного перегляду ризиків, пов'язаних із клієнтами з риболовного сектору. З іншого боку, значне покращення України (+63 позиції), Сент-Люсії (+70) та Куби (+49) показує, що цілеспрямовані реформи можуть давати результат, а отже, співпраця з фінансовими установами цих країн у сфері AML може стати більш ефективною.

Таким чином, Глобальний індекс ризику IUU за 2025 рік виступає не лише як довідник з екологічної безпеки, але як стратегічний навігаційний інструмент для всієї екосистеми фінансової безпеки. Він надає структуровані, порівнянні дані, які можуть бути інтегровані в системи оцінки ризиків клієнтів (Customer Risk Assessment), використані для таргетингу при проведенні трансакційного моніторингу (особливо для платежів, пов'язаних із логістикою, страхуванням суден або міжнародною торгівлею), а також для побудови регіональних профілів ризиків.

Висновки:

- **Загальний індекс ризику майже не змінився з 2021 року, що свідчить про недостатність зусиль на міжнародному рівні.** Китай, росія, Індонезія та низка країн Близького Сходу й далі залишаються «центрами ризику», де слабкий регуляторний контроль створює умови для легалізації прибутків від незаконної риболовлі.
- **Індекс чітко корелює високі ризики IUU з низькими доходами на душу населення, високою корупцією та слабкою портовою інфраструктурою.** Це робить IUU не просто екологічною проблемою, а каналом для відмивання коштів, ухилення від сплат податків та фінансування організованої злочинності.
- **Індекс можна використовувати для оцінки ризику клієнтів,** пов'язаних із риболовним сектором: від фінансування суден до торгівлі рибою.
- **Різке погіршення позицій деякими країнами може свідчити про появу нових шляхів легалізації незаконного улову.** Натомість покращення показників показує, що реформи можуть давати ефект навіть у складних умовах.

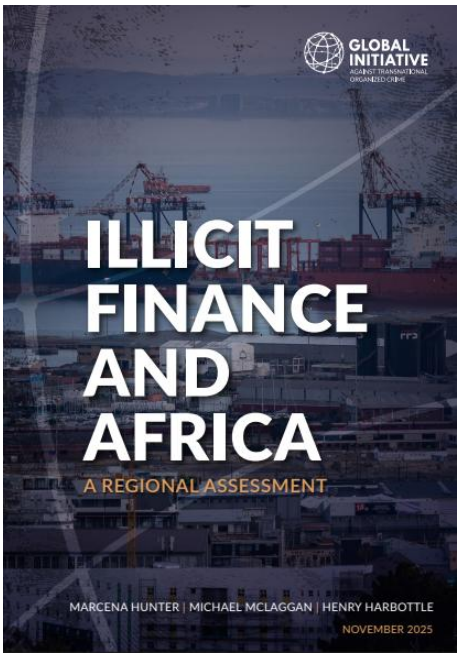
Учасники ринку, що ігнорують ці дані, ризикують не лише порушити принципи належної перевірки (Due Diligence), але й ненароком стати частиною складних схем відмивання коштів, що живляться від пограбування світового океану. Боротьба з IUU та боротьба з відмиванням коштів — це дві сторони однієї медалі, і Глобальний індекс ризику IUU 2025 року надає чіткий, кількісний мост між цими двома критично важливими фронтами захисту глобальної фінансової та екологічної стабільності.

Африка: комплексний аналіз нелегальних фінансових потоків як системного виклику для фінансової цілісності, безпеки та сталого розвитку [11]

Сучасний африканський континент перебуває на перехресті глобальних економічних трансформацій, політичних потрясінь та технологічних революцій, що робить його особливо вразливим до проникнення та зростання нелегальних фінансових потоків (НФП). Це явище, що визначається як незаконна генерація, переміщення та використання багатства і цінностей,

[11] https://globalinitiative.net/wp-content/uploads/2025/11/Marcena-Hunter-Michael-McLaggan-Henry-Harbottle-Illicit-finance-and-Africa-A-regional-assessment-GI-TOC-November-2025.v2.pdf

переросло з локальної проблеми в складну транснаціональну загрозу, яка системно руйнує інститути, підриває економічну стабільність і живить організовану злочинність.



Масштабний аналітичний звіт Global Initiative Against Transnational Organized Crime (GI-TOC) намагається розплутати цей клубок, пропонуючи не лише огляд типологій, а й концептуальну рамку для розуміння їх взаємозв'язків, визначаючи ключових суб'єктів, географічні вузли ризику та пропонуючи багаторівневу стратегію протидії.

В основі дослідження лежить ідея «піраміди НФП», яка служить потужним інструментом для візуалізації та аналізу. Ця піраміда не є просто ієрархією; це динамічна модель вертикальної інтеграції, де вразливості та спотворення на одному рівні неминуче посилюються та поширюються на інші.

Фундаментом цієї конструкції виступають неформальні потоки африканських економік, де готівка залишається абсолютним королем, а неформальні системи передачі цінностей (IVTS) створюють альтернативні артерії для переказу коштів. Серед останніх особливо виділяються традиційна система «хавала», глибоко вкорінена в ісламських громадах, та розгалужені китайські підпільні банківські схеми, такі як «фей-цянь». Ці системи, що базуються на довірі, родинних зв'язках та мережах діаспор, за своєю природою є непрозорими, залишаючи мінімальний цифровий слід, що робить їх ідеальним інструментом не лише для трудових мігрантів, які надсилають гроші додому, але й для фінансування терористичних груп на кшталт аш-Шабааб, оплати контрабанди наркотиків чи відмивання коштів від торгівлі людьми. Вони є сліпою плямою для більшості ПФР через брак лінгвістичних, технічних та культурних компетенцій для їх відстеження.

Наступний рівень піраміди – це сфера торгівлі, яка в африканському контексті перетворилася з двигуна зростання на один з наймасштабніших каналів для НФП. Відмивання коштів через торгівлю (TBML) набуло особливо загрозливих масштабів. Величезні порти, такі як Дурбан, Момбаса та Лагос, задіяні у мільйонах контейнерних перевезень на рік, стали вразливими точками через брак технологій, корупцію та складні логістичні ланцюги. Але справжніми розплідниками для гібридних схем, що поєднують формальну торгівлю, контрабанду та неформальні розрахунки, стали Особливі економічні зони (ОЕЗ) та Вільні торговельні зони (ВТЗ). Створені для залучення інвестицій через податкові пільги та спрощений адміністративний режим, вони часто перетворюються на оазиси регуляторної непрозорості. У цих зонах легко процвітають практики «кругових оборотів», коли капітал виводиться офшор лише для того, щоб повернутися під виглядом іноземних інвестицій, а товари, особливо такі як золото або коштовна деревина, можуть бути «перепаковані» з фіктивними документами для подальшого експорту. Так, наприклад, в Уганді 93% експорту з вільних зон у 2021 році припадало на золото, що викликало серйозні підозри щодо TBML.

Вершину піраміди займають формальна фінансова система та приватний сектор – інституції, які повинні бути основним бар'єром на шляху НФП, але часто стають їх головними співучасниками. Великі міжнародні та регіональні банки, через слабку внутрішню відповідність вимогам ПВК або пряме політичне втручання, неодноразово були втягнуті в гучні скандали. Однак справжнім «слабим місцем» виступають так звані DNFBPs (визначені нефінансові установи та професії) – юристи, бухгалтери, агентства з надання корпоративних послуг, ріелтори, забудовники та навіть дилери дорогоцінних металів. Ці професійні посередники володіють експертизою та легальним

прикриттям, необхідним для створення складних схем: реєстрації компаній, структурування офшорних холдингів, купівлі нерухомості на підставних осіб, проведення фіктивних судових процесів. Вони є тими архітекторами, які будують міцні мости між кримінальними ринками Африки та респектабельними фінансовими центрами світу, такими як Дубай, Лондон або Гонконг. При цьому нагляд за DNFBPs на континенті залишається мінімальним, показники подання звітів про підозрілі операції (STR) критично низькі, а професійні асоціації рідко притягають своїх членів до відповідальності.

Окремо в звіті розглядається найкритичніший з точки зору обсягів та політичних наслідків актив – золото. Африканський золотодобувний сектор перебуває в стані глибокої криміналізації та політизації. Від незаконного кустарного видобутку в ПАР та Лесото до захоплених державою копалень у Зімбабве та Малі, золото є валютою влади. Воно фінансує виборчі кампанії, живить політичні патронатні мережі, забезпечує ресурсами збройні групи в таких конфліктних регіонах, як Судан і ДР Конго.

Схеми контрабанди постійно вдосконалюються: від кур'єрів з золотом в ручній поклажі до масштабних перевезень приватною вантажною авіацією з приватних злітних смуг. Транзитними хабами слугують міста з розвиненою логістикою та слабким регулюванням – Бамако, Аккра, Кампала, Найробі, Йоганнесбург. Однак кінцевим пунктом призначення для більшості нелегального африканського золота, що часто не декларується, залишається Дубай (ОАЕ), звідки воно, вже переплавлене та «очищене», потрапляє на світові ринки. Це демонструє глибоко транснаціональний характер проблеми, де слабкість регулювання в африканських країнах-експортерах посилюється попитом та мінливими стандартами в країнах-імпортерах та переробниках.

Висновки:

- **Нелегальні фінансові потоки в Африці мають складну багаторівневу структуру,** де формальна фінансова система, торгівля та неформальні канали тісно взаємодіють, посилюючи один одного.
- **Технології одночасно є і рішенням для фінансової інклюзії, і новим викликом для безпеки.** Вони надають злочинцям швидкі, анонімні та крос-кордонні можливості, а регулювання в багатьох країнах відстає.
- **Нелегальні фінансові потоки — це не лише економічна проблема, але й загроза політичній стабільності та безпеці.** Вони живлять корупцію, фінансують збройні конфлікти, впливають на результати виборів і сприяють "захопленню держави" через контроль над ресурсами (золото, корисні копалини).
- **Ефективна боротьба вимагає комплексного підходу:** посилення прозорості, інвестицій в аналітику даних, міжнародної координації, публічно-приватного партнерства та балансу між контролем і фінансовою інклюзією.

Надзвичайно динамічною складовою ландшафту НФП став фінтех. Африка переживає справжню революцію мобільних грошей, яка надала доступ до фінансових послуг мільйонам громадян. Однак ця інклюзія має зворотний бік. Мобільні гроші, як-от M-Pesa в Кенії або MoMo в ЦАР, використовуються для дрібних, але масових платежів у нелегальній торгівлі дикими тваринами, для виплати викупів за викрадених чи для фінансування терористичних осередків.

Криптовалютна експансія, особливо в Нігерії, створила новий вимір для злочинності. Професійність кіберзлочинців, що постійно підвищується, діяльність таких транснаціональних мереж, як «Black Axe», та використання стейблкоїнів для анонімних міжнародних транзакцій значно випередили розвиток регуляторних рамок для постачальників послуг віртуальних активів (VASP) в більшості африканських країн.

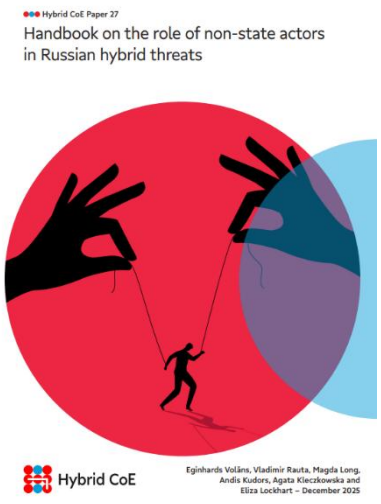
Реакція на ці загрози, як зазначається в звіті, залишається розрізненою, відсталою та неефективною. Традиційні режими ПВК/ФТ часто не враховують небанківські канали, такі як TBML або IVTS. Різниця в можливостях держав, втручання зовнішніх геополітичних суб'єктів (Китай, росія, ОАЕ) та присутність зловмисників у внутрішніх елітах підривають будь-які спроби узгодженої політики.

Тому автори закликають до радикальної зміни парадигми: від фрагментованих заходів до стратегії, цілісної та заснованої на типологіях. Серед ключових пропозицій – створення континентальної «Обсерваторії нелегальних фінансів» як центру знань і координації; капітальні інвестиції в аналітику даних та штучний інтелект для виявлення аномалій у торгівельних потоках; впровадження публічних реєстрів бенефіціарних власників; прямий тиск через підтримку незалежних журналістських розслідувань для демонстрації реальної шкоди від НФП; посилення нагляду за фінансуванням виборів; формування публічно-приватих партнерств для обміну інформацією про ризики; та гармонізація регіональних підходів до контролю за ОЕЗ, золотом та криптоактивами.

Надзвичайно важливо, що звіт підкреслює необхідність балансу: боротьба з НФП не повинна здійснюватися шляхом відключення цілих регіонів від фінансових послуг, що лише заглиблює вразливості. Регулювання цифрових грошей чи спроби формалізації IVTS мають бути чутливими, щоб не підрізати крихку основу фінансової інклюзії та легальних засобів існування мільйонів людей.

Таким чином, боротьба з нелегальними фінансовими потоками в Африці – це не просто технічне регуляторне завдання. Це комплексне, багатовимірне випробування для національної та міжнародної безпеки, тест на спроможність державних інститутів, виклик для міжнародної співпраці та моральний імператив для забезпечення справедливого розвитку. Успіх у протидії вимагає глибокого розуміння адаптивної природи злочинних мереж, готовності інвестувати в передові технології та аналітику, згуртованих дій на регіональному та глобальному рівнях та непохитної політичної волі, спрямованої на розвиток інституцій, а не на захист вузьких елітарних інтересів. Майбутнє фінансової цілісності та стабільності Африки залежить від того, наскільки ефективно буде реалізовано цю комплексну стратегію в наступні роки.

Симбіоз держави, олігархії та злочинності: як росія фінансує гібридну війну та обходить санкції [12]



Аналітичний звіт від Європейського центру з протидії гібридним загрозам (Hybrid CoE) про роль недержавних суб'єктів у російських гібридних загрозах, розкриває перед фахівцями безпрецедентну за складністю картину — фундаментальну трансформацію у відносинах між державою, капіталом і злочинністю в авторитарній системі, що веде тотальну гібридну війну.

Росія створила та вдосконалила гібридну фінансову екосистему, де традиційні межі між державою, приватним багатством олігархів, прибутками держкорпорацій, кримінальними надходженнями та фінансуванням спецоперацій розмиті навмисно та системно.

Ця екосистема призначена для досягнення двох головних цілей: фінансового виживання режиму в умовах безпрецедентних міжнародних санкцій та фінансування широкого спектру гібридних

[12] https://www.hybridcoe.fi/wp-content/uploads/2025/12/Hybrid-CoE-Paper-27-Handbook-on-the-role-of-non-state-actors-in-Russian-hybrid-threats.pdf

операцій — від кібератак і дезінформації, до роботи приватних військових компаній (ЧВК) та політичного впливу за кордоном. По суті, ми спостерігаємо за становленням воєнізованої клептократії, де ефективне управління тіньовими фінансами стало таким же важливим стратегічним ресурсом, як і військова сила.

Розуміння цієї екосистеми вимагає відходу від класичних AML-парадигм, зосереджених на окремих підозрілих операціях клієнтів. Загроза наразі носить системний та мережевий характер. Довідник наголошує, що основним оперативним простором для росії є «сіра зона» — спектр дій нижче порогу відкритої війни, що дозволяє уникати прямої відповідальності. У фінансовій площині ця «сіра зона» матеріалізується у вигляді складних, багаторівневих схем, що поєднують легальні та нелегальні елементи, внутрішніх та зовнішніх суб'єктів, криптовалютні операції та традиційні банківські перекази. Ключовим інструментом навігації в цій зоні для кремля виступають саме недержавні актори (НДА), які надають йому критично важливі ресурси: правдоподібне заперечення, оперативну гнучкість, доступ до закритих ринків та експертизу в обході регуляцій. Фінансування цих суб'єктів та їхня власна фінансова діяльність і становлять ядро нової фінансової загрози.

Основним каркасом цієї гібридної фінансової системи є симбіоз держави з олігархами та підконтрольними їм корпораціями. Проте після 2022 року характер цього симбіозу кардинально змінився. Якщо в попередні десятиліття олігархи виступали незалежними центрами сили та інструментами «м'якої сили» за кордоном (через інвестиції, лобіювання, медіа-власність), то після повномасштабного вторгнення їхня роль була жорстко реорганізована та націоналізована. Санкції Заходу, що фактично закрили для них доступ до глобальної фінансової системи, зробили їх повністю залежними від Кремля.

У новій реальності олігарх — це не володар капіталу, а довірений керуючий державними (або квазі-державними) активами, зобов'язаний виконувати політичне завдання зі збереження економічної стабільності та фінансування військових зусиль. Їхні інвестиційні рішення, розподіл ресурсів між підприємствами та навіть зовнішньоекономічна діяльність жорстко координуються через Адміністрацію президента та силові блоки. Наглядова рада чи рада директорів великої компанії тепер є не лише органом корпоративного управління, а й інструментом політичного контролю. Прибутки, які раніше виводилися в офшори або інвестувалися в західні активи, тепер змушені працювати на внутрішній ринок, поглинати інфляційні шоки через контрольовані ціни та фінансувати імпортозаміщення у ВПК. Лояльність стала єдиною валютою, що гарантує безпеку і збереження статусу. Це призвело до того, що великий бізнес в росії остаточно втратив будь-які ознаки автономності та перетворився на фінансове продовження державного апарату воєнного часу.

Державно-орієнтовані корпорації, особливо в енергетичному, сировинному та фінансовому секторах, перетворилися з комерційних підприємств на багатофункціональні інструменти гібридної війни. Вони одночасно виконують кілька ролей: генераторів валютної виручки (через «тіньовий флот» і перенаправлення експорту на східні ринки), каналів обходу санкцій на технології (через мережу дочірніх компаній і посередників у третіх країнах), інструментів політичного впливу (через медіа-активи та спонсорські програми) та навіть, як вказують деякі джерела, замовників послуг ЧВК.

Наприклад, «Газпром» як енергетичний гігант фінансує медіа-імперію для ведення інформаційної війни; його логістичні потужності можуть використовуватися для прикриття поставок санкційних товарів; а його структури, за даними розслідувачів, могли стояти біля витоків окремих приватних військових формувань. Для AML-фахівця це означає, що будь-яка транзакція, пов'язана з такою корпорацією, навіть якщо вона формально стосується, наприклад, купівлі обладнання для газовидобутку, потребує поглибленого аналізу на предмет можливого вторинного використання або участі в ланцюжку постачання для ВПК. Фінансові потоки цих

гігантів більше не є суто корпоративними — це кровоносна система режиму, що живе в умовах зовнішньої фінансової ізоляції.

Окремою та критично важливою ланкою в цій системі є транснаціональні злочинні мережі (ТЗМ) та кіберзлочинні угруповання. Їхня інтеграція в державну машину — не новий феномен, але після 2022 року вона набула характеру «мобілізації». Як зазначає експерт Марк Галеотті, держава перейшла в режим «мобілізації всіх елементів суспільства — легальних та нелегальних». ТЗМ, з їхніми налагодженими каналами контрабанди, відмивання коштів, створення фіктивних фірм та корупційними зв'язками в митних органах різних країн, стали незамінними для обходу санкцій. Вони забезпечують логістику для поставок товарів подвійного призначення (напівпровідників, мікроелектроніки, точних верстатів), організовуючи складні маршрути через країни Середньої Азії, Кавказу, Близького Сходу та Південно-Східної Азії. Їхня експертиза у створенні офшорних схем і роботі з підставними компаніями дозволяє приховувати кінцевого бенефіціара і призначення вантажів.

Крім того, ТЗМ традиційно є джерелом «чорної каси» для спецслужб — неврахованих готівкових коштів, що використовуються для фінансування таємних операцій, вербування агентів, підкупу іноземних чиновників та фінансової підтримки проросійських політичних сил за кордоном. Довідник наводить приклад спроби перевороту в Чорногорії у 2016 році, де фінансування через кримінальних посередників було ключовим елементом операції ГРУ.

Кіберзлочинний сегмент зазнав аналогічної трансформації. Російськомовні угруповання, що спеціалізуються на ransomware-атаках, викраденні криптовалют та промисловому шпигунстві, все менше розділяють власні кримінальні цілі та державні інтереси. Відбувається злиття мотивацій: фінансове збагачення та нанесення шкоди геополітичним супротивникам. Атаки на критичну інфраструктуру (енергетику, логістику, фінансові установи) країн, які підтримують Україну, одночасно приносять злочинцям викуп і послаблюють економічну стійкість супротивника. Держава, у свою чергу, демонструє «сприйнятливу терпимість» до цих груп, за умови, що вони не чіпають внутрішні цілі та спрямовують свою активність назовні. Іноді зв'язок набуває прямiших форм: кіберзлочинців вербують або шантажують для роботи на спецслужби, а їхні навички використовуються для проведення деструктивних атак або збору розвідданих. Високий статус цих суб’єктів у системі підтверджується фактами їх обміну на західних політв'язнів, як це сталося з Олександром Вінніком та Романом Селезньовим.

Глобальним механізмом, що забезпечує життєздатність усієї цієї системи, є архітектура обходу санкцій. Вона включає як внутрішні, так і зовнішні компоненти. Усередині країни це, перш за все, перебудова фінансової системи під управлінням ЦБ РФ, який розробив альтернативні платіжні шляхи, механізми контролю за валютними операціями та підтримки національної валюти. Зовні Росія створила масштабну мережу посередників. Ключову роль тут відіграють «професійні посередники» — адвокати, бухгалтери, управлінці активами, реєстратори компаній. Вони будують складні багаторівневі структури з використанням трастів, офшорних компаній, номінальних директорів і акціонерів, щоб приховати справжніх власників активів олігархів та джерела коштів. Вони ж допомагають перереєструвати бізнес, отримати альтернативне громадянство або дипломатичний паспорт для підсанкційних осіб. Їхня діяльність часто межує з так званою «правовою війною» (lawfare), коли західні судові системи використовуються для блокування заморожування активів, тиску на журналістів-розслідувачів та ведення довгих судових процесів, що витрачають ресурси правоохоронців.

Окремим феноменом став російський «тіньовий флот» — сотні старих, перереєстрованих танкерів з підставними власниками та підробленою страховкою, призначених для транспортування російської нафти в обхід санкцій та цінових обмежень G7. Цей флот не тільки забезпечує життєво важливий приплив валютної виручки в бюджет, але й являє собою масштабну логістично-фінансову операцію з використанням фіктивних контрактів, схем з

надуванням цін та відмиванням коштів через мережу компаній у різних країнах. Банки та фінансові установи в юрисдикціях, що сприяють таким операціям (наприклад, в ОАЕ, Гонконгу, Індії), свідомо (або ні) стають частиною цієї санкційно-митної архітектури.

Управління всією цією різноплановою системою фінансування гібридної війни здійснюється через складну та часто фрагментовану мережу державних інституцій. На чолі стоїть Адміністрація президента, що визначає стратегічні пріоритети та розподіл ресурсів. Безпосереднє управління різними категоріями НДА ведуть спецслужби: ФСБ зосереджена на ТЗМ, внутрішньому фінансовому контролі та роботі з частиною ЧВК; ГРУ управляє бойовими ЧВК (нащадками «Вагнера»), частиною кібероперацій та хакерами; СЗР відповідає за зовнішню розвідку, лобіювання та роботу з політичними силами за кордоном. Міністерство фінансів та ЦБ РФ керують макроекономічною політикою та створенням механізмів обходу санкцій. МЗС надає дипломатичне прикриття, а «Россотрудничество» використовує культурні та гуманітарні проекти як прикриття для вербування агентури та фінансування проросійських НДО. Важливо, що ця система не є монолітом — між різними «силовими корпораціями» іде постійна конкуренція за ресурси та вплив, що іноді призводить до неефективності або витоків інформації, але водночас ускладнює зовнішній аналіз та можливість атаки на систему в цілому.

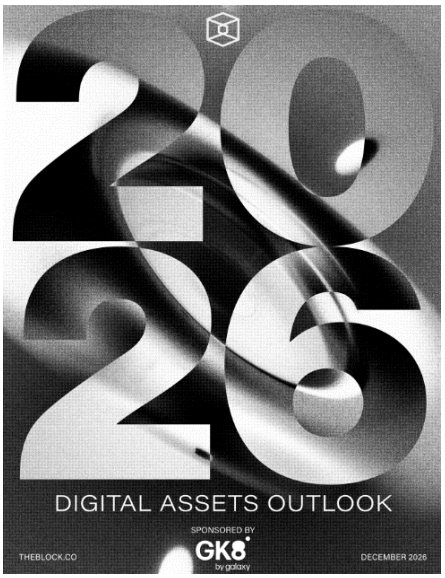
Висновки:

- **Росія створила цілісну гібридну фінансову екосистему**, де держава, олігархи, держкорпорації, транснаціональні злочинні мережі та кіберзлочинці діють у тісному симбіозі.
- **Роль олігархів і великого бізнесу кардинально змінилася після 2022 року:** з інструментів "м'якої сили" та міжнародного впливу вони перетворилися на підконтрольних державі "управителів активів", зобов'язаних фінансувати військові дії, стабілізувати економіку та забезпечувати імпортозаміщення для ВПК.
- **Транснаціональні злочинні мережі інституційно інтегровані в державну машину і виконують критичні функції:** обхід санкцій на товари подвійного призначення, логістика "тіньового флоту", створення "чорної каси" для спецоперацій, а також проведення кібератак.
- **Архітектура обходу санкцій є глобальною та багаторівневою, що включає внутрішні механізми** (альтернативні платежі, контроль ЦБ) та зовнішні ланки (професійні посередники в "дружніх" юрисдикціях, офшорні схеми, "тіньовий флот").

Для міжнародної AML-спільноти виклики, що постають з такої моделі, є екзистенційними. Вони вимагають радикального переосмислення підходів до фінансової безпеки. Недостатньо шукати окремі «червоні прапорці»; необхідно вчитися бачити та розплітати цілі мережі. Це означає тісну інтеграцію фінансової розвідки з даними кібербезпеки, зовнішньої розвідки, аналізу зовнішньої торгівлі та моніторингу судноплавства. Необхідно розвивати проактивні методи виявлення схем обходу санкцій, зосереджуючись не тільки на російських суб'єктах, але і на їхніх посередниках по всьому світу — на банках, юридичних фірмах, торгових компаніях у третіх країнах. Критично важливим стає застосування цілеспрямованих санкцій та кримінального переслідування саме професійних посередників, які роблять можливим існування всієї системи. Боротьба з «тіньовим флотом» вимагає координації між державами у сфері морського страхування, портового контролю та фінансового моніторингу операцій судновласників.

Документ Hybrid CoE чітко показує, що фінансова складова російської гібридної війни — це не допоміжний, а центральний фронт. Ефективна протидія їй вимагає глибокого розуміння політичної економії авторитарного режиму в умовах конфлікту, готовності до міждисциплінарної роботи та створення нових інструментів аналізу, здатних відстежувати не лінійні транзакції, а складні, адаптивні мережі, що живлять нову епоху гібридного протистояння.

Криптоіндустрія у фазі зрілості: ключові трансформації ринку цифрових активів у 2025 році [13]



Документ від GK8 є масштабним аналітичним оглядом, який комплексно підсумовує трансформації ринку цифрових активів у 2025 році та окреслює структурні тренди, що визначатимуть його розвиток у наступному році. Звіт вибудуваний як цілісна картина еволюції криптоекосистеми — від макроекономічного й політичного контексту до змін у технологічній архітектурі, ринковій структурі, поведінці користувачів, інституційній участі, безпеці та регулюванні.

У вступній частині документ фіксує ключову суперечність 2025 року: рекордне зростання загальної капіталізації крипторинку, яка досягла історичного максимуму близько 4,3 трлн доларів США, не супроводжувалося пропорційним зростанням більшості криптоактивів. Навпаки, значна частина ринку продемонструвала слабку або негативну цінову динаміку, що свідчить про перехід від спекулятивного, масового зростання до більш вибіркової, концентрованої та інституційно орієнтованої моделі розвитку. Автори наголошують, що 2025 рік став роком «конфліктних сигналів»: позитивні регуляторні та інституційні новини співіснували з млявими ринковими показниками, оголюючи структурну перебудову всієї галузі.

Макроекономічний блок звіту детально описує вплив політичних рішень США на глобальні фінансові ринки, включно з криптовалютним сегментом. Запровадження масштабних торговельних тарифів, короткострокові шоки на ринках капіталу та подальше відновлення котирувань створили нестабільне, але водночас сприятливе тло для цифрових активів. Вирішальним чинником стала поява найбільш про-криптовалютної адміністрації в історії США, яка не лише декларувала підтримку цифрових активів, а й реалізувала її через кадрові рішення та зміну регуляторної філософії. Перехід від жорсткого наглядово-карального підходу до формування спеціалізованих законодавчих рамок став фундаментом для активізації інституційних гравців.

Окремий акцент зроблено на різкому зростанні інституційної присутності в екосистемі. У 2025 році відбулася хвиля первинного публічного розміщення акцій (IPO) криптокомпаній, з’явився феномен компаній цифрових активів-скарбниць, а венчурне фінансування змістилося у бік зрілих, пізніх стадій проєктів. Паралельно відбулися рекордні угоди злиття та поглинання, які свідчать про інтеграцію криптосектору у традиційні фінансові ринки. Водночас звіт підкреслює, що інституційне прийняття не означає рівномірного зростання для всіх сегментів ринку, а навпаки — посилює конкуренцію та концентрацію.

У розділах, присвячених ринковій динаміці, простежується чітка еволюція тематичних циклів. Мемкоїни, які домінували у 2024 році, втратили свою роль як головного драйверу ліквідності, поступившись більш функціональним і масштабованим моделям. На перший план вийшли децентралізовані деривативи, ринки прогнозів, стейблкоїни та криптопродукти, орієнтовані на реальну економічну корисність. Особливо докладно розглядається вибухове зростання децентралізованих бірж (DEX), які змогли значно скоротити технологічний і ліквідний розрив із централізованими біржами, змінюючи баланс сил у торгівлі деривативами.

[13] https://www.tbstat.com/wp/uploads/2025/12/20251213_EOY_Report-1.pdf

Блокчейн-інфраструктура у звіті подається як система, що швидко набуває спеціалізації. Layer 1 мережі у 2025 році остаточно втратили універсальний характер і розділилися за функціональними ролями. Частина з них стала середовищем для високоризикової спекулятивної активності, тоді як Ethereum закріпився як базовий рівень розрахунків і доступності даних для ширшої екосистеми Layer 2. Водночас зростання стейблкоїнів і поява так званих стейблкоїн-орієнтованих блокчейн-мереж (stablechains) демонструють, що мережі дедалі частіше оптимізуються під вузькі, але економічно значущі сценарії використання, включно з комплаєнсом та інтеграцією у фінансову інфраструктуру.

Layer 2 сегмент у звіті описується як найбільш показовий приклад концентрації. Хоча кількість L2-рішень зростала, реальна економічна активність і ліквідність зосередилися на обмеженій кількості мереж, насамперед Base та Arbitrum. Автори підкреслюють, що ключовим чинником успіху стала не технічна інноваційність, а доступ до масштабних каналів дистрибуції через великі платформи та інституційних партнерів. При цьому питання централізації, контролю апгрейдів і безпеки L2 все ще залишаються критичними.

DeFi-сектор у документі представлений як такий, що входить у фазу зрілості. У 2025 році ончейн-кредитування пройшло повний цикл — від скорочення до відновлення, з чітким лідерством кількох протоколів і зростанням ролі токенізованих приватних кредитів. Водночас серія інцидентів із де-пегінгом стейблкоїнів і каскадними втратами продемонструвала, що зростаюча залежність створює системні ризики, здатні швидко поширюватися між протоколами та ринками.

Кульмінацією звіту є аналіз токенізації реальних активів, яку 2025 рік перетворив із експериментальної концепції на повноцінний інституційний інструмент. Токенізовані державні облігації, фонди та товарні активи стали інтегрованою частиною DeFi-екосистеми, створивши новий клас ончейн-фінансових продуктів, що поєднують традиційні ринки капіталу з публічними блокчейнами. Це, на думку авторів, закладає основу для формування цифрових ринків капіталу нового покоління.

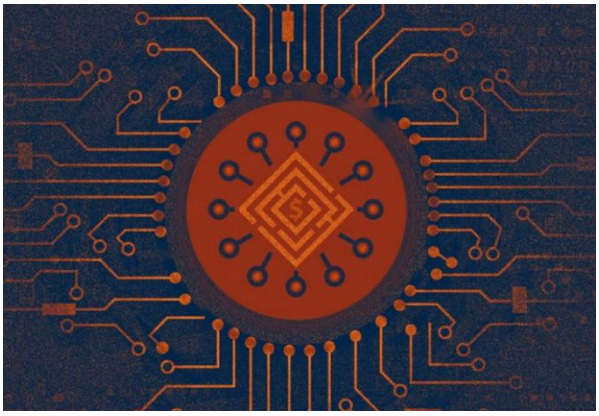
Завершальні частини документа присвячені безпековим і регуляторним викликам. Звіт підкреслює, що 2026 рік проходитиме в умовах зростання складних, адаптивних загроз, зокрема із використанням штучного інтелекту для соціальної інженерії та персоналізованих атак. Загалом документ формує цілісний висновок про те, що криптоіндустрія вступила у фазу структурної зрілості, де вирішальними стають не швидкість експериментів, а інституційна довіра, масштабованість, регуляторна сумісність і стійкість до системних ризиків.

Висновки:

- **Інституційна життєздатність стає головним критерієм успіху.** Проєкти, мережі та продукти, які не інтегруються у традиційні фінансові ланцюги вартості, втрачають економічне значення незалежно від технологічних інновацій.
- **Концентрація — нова норма крипторинку.** Ліквідність, користувачі та інновації концентруються навколо обмеженого кола мереж і протоколів. Для регуляторів і ПФР це означає можливість більш сфокусованого ризик-орієнтованого нагляду.
- **Токенізація реальних активів переходить у фазу масштабування.** Публічні блокчейни стають інфраструктурою для емісії та обігу інституційних фінансових інструментів. Це створює нові виклики для ПВК/ФТ, зокрема щодо прозорості бенефіціарів, транскордонного нагляду та сумісності з фінансовим моніторингом.
- **Безпека та комплаєнс мають бути закладені на етапі проєктування.** Зростання загроз, керованих штучним інтелектом і складних шахрайських схем означає, що архітектура цифрових активів у 2026 році має одразу закладати механізми контролю, аудиту та реагування, а не додавати їх постфактум.

Інші новини

Відмивання в промислових масштабах: як цифрові активи підживляють наркоторгівлю Мексики [14]



Сучасний ландшафт транснаціональної організованої злочинності зазнає глибинної технологічної трансформації, де традиційні методи відмивання коштів поступово витісняються високоефективними цифровими конвеєрами. Якщо ще на початку 2010-х років наркокартелі Мексики та Колумбії в основному покладалися на фізичну контрабанду готівки через кордони, створення мереж фіктивних підприємств для обґрунтування доходів або складні схеми TBML, то сьогодні ми спостерігаємо становлення справжньої індустрії з перетворення наркодоларів у цифрові активи. Цей перехід не є випадковим: він продиктований поєднанням технологічного прогресу, зміни регуляторного середовища та глобальних геополітичних факторів, що створили ідеальний час для впровадження криптовалютних інструментів.

Детальний аналіз сотень судових справ у Сполучених Штатах, даних провідних аналітичних компаній на кшталт Chainalysis та TRM Labs, а також закритих звітів правоохоронних органів демонструє не просто спорадичне використання біткоїнів для розрахунків, а системну, багаторівневу інфраструктуру, що функціонує за принципом конвеєра. Цей конвеєр забезпечує не тільки швидку та відносно безпечну легалізацію прибутків від торгівлі кокаїном, метамфетаміном та синтетичними опіоїдами, але й безпосередньо фінансує критичну ланку виробничого циклу — закупівлю прекурсорів у Китаї, без яких масове виробництво фентанілу на підпільних лабораторіях Мексики було б неможливим.

Історично криптовалютні транзакції асоціювалися з темними ринками типу Silk Road, де операції здійснювалися переважно біткоїнами та були відносно невеликими за обсягом. Проте, як зазначає Хелена Маргарідо, операційний директор FinTech School, після 2018 року ситуація кардинально змінилася. З'явився цілий арсенал інструментів, що різко знизили технічні та операційні бар'єри для кримінальних організацій.

Перш за все, це поява слаборегульованих peer-to-peer (P2P) бірж, які дозволяли обмінювати фіат на криптовалюту з мінімальною або відсутньою ідентифікацією користувача. По-друге, широке запровадження стейблкоїнів, прив'язаних до долара США, на кшталт Tether (USDT), усунуло головний ризик для кримінальних операцій — волатильність. Можливість утримувати вартість у стабільному цифровому активі під час багатоступінчастих транзакцій стала революційною. По-третє, розвиток сервісів обфускації — криптоміксерів (tumblers, mixers) і застосування техніки "chain-hopping" — дозволили ефективно розмивати слід коштів, переміщуючи їх через десятки або сотні проміжних гаманців на різних блокчейнах.

Результат не змусив себе чекати. За даними звіту Chainalysis за 2025 рік, обсяг незаконних потоків у криптовалюті з 2020 по 2024 рік виріс вчетверо, досягнувши оцінки в 40–51 мільярд доларів США. Приблизно чверть цієї суми, або понад 10 мільярдів доларів, безпосередньо

[14] https://insightcrime.org/news/us-court-cases-mexico-organized-crime-digital-money/

віднесено до транснаціональних злочинних організацій, серед яких мексиканські картелі Синалоа та Jalisco Nueva Generación (CJNG) є одними з найактивніших.

Однією з найважливіших ланок у цьому конвеєрі виявився стратегічний альянс між мексиканськими наркокартелами та китайськими підпільними фінансовими брокерами, які діють на території США. Цей симбіоз правоохоронці США називають "одною з найтривожніших загроз транснаціональної організованої злочинності". Його ефективність ґрунтується на взаємовигідному обміні.

Для китайських брокерів (часто об'єднаних у так звані "money transfer houses") співпраця з картелями забезпечує стабільний приплив доларів. Ці долари є надзвичайно ліквідним товаром на внутрішньому китайському ринку, де існують суворі валютні контролі (обмеження на вивіз у розмірі 50 тисяч доларів на людину на рік). Багаті китайські клієнти, які прагнуть інвестувати за кордоном, купують ці долари зі значною премією. Таким чином, брокер отримує подвійний прибуток: спочатку комісію за відмивання (яка, за свідченнями, становить всього 5-6%, що значно нижче традиційних для кримінального світу 10-15%), а потім — прибуток від перепродажу фізичних доларів у Китаї.

Для мексиканських картелів ця схема пропонує безпрецедентні переваги. Вона усуває необхідність ризикованого транспортування тонн готівки через кордон, значно прискорює оборот капіталу та робить процес дешевшим. Криза COVID-19, яка призвела до закриття кордонів та ускладнення логістики, лише прискорила перехід до цифрових каналів, змусивши картелі швидко масштабувати свої крипто-операції.

Операційна модель відмивання нагадує добре відлагоджений виробничий процес. Її можна розділити на п'ять чітких етапів.

1. **Збір та структурування (Collection & Structuring):** Кур'єри картелів збирають виручку від продажу наркотиків, часто в невеликих містах по всій території США. Готівка пакується в сумки, чемодани або навіть сміттєві пакети. Потім вона структурується — розбивається на суми, менші за поріг звітності (зазвичай $10,000), — і вноситься на рахунки через мережі банкоматів, або з використанням "грошових мулів", які роблять багаторазові внески. Ці рахунки контрольуються підставними особами або "відмивачами".
2. **Аггрегація та конвертація (Aggregation & Conversion):** Китайські брокери збирають кошти з численних рахунків на одні або кілька головних. Потім вони конвертують мільйони доларів у криптовалюту, переважно в стейблкоїни на кшталт USDT або USDC, через криптобіржі з слабкою KYC-політикою або через P2P-платформи.
3. **Обфускація та розшарування (Obfuscation & Layering):** Це ключовий технічний етап. Для того щоб розірвати зв'язок між наркодоларами і кінцевими отримувачами, застосовується низка методів. Криптоміксери, такі як Tornado Cash, "перемішують" кошти тисяч користувачів, роблячи відстеження практично неможливим. Техніка "chain-hopping" передбачає швидке переміщення активів між різними блокчейнами (наприклад, з Ethereum на Bitcoin, потім на Monero і знову на Ethereum). Кошти проходять через каскад проміжних гаманців ("hop-addresses"), кожен з яких використовується недовго.
4. **Маршрутизація (Routing)**: Очищені та анонімізовані криптоактиви направляються на гаманці, контрольовані картелями в Мексиці або на їхніх агентів у інших країнах.
5. **Фіналізація (Cash-Out or Direct Use):** На завершальному етапі картелі можуть або конвертувати криптовалюту назад у фіат через біржі в країнах з ліберальним регулюванням, або — що набагато важливіше — використати її безпосередньо для оплати.

Аналіз ланцюжків транзакцій показав, що значні обсяги коштів, які виходять з гаманців картелів, не йдуть на розкішні помешкання чи яхти, а прямують на конкретні криптоадреси, пов'язані з хімічними компаніями в Китаї. Це логічно: основним видом витрат для картелів, які контролюють виробництво, є закупівля сировини.

За оцінками TRM Labs, у 2023 році гаманці китайських постачальників прекурсорів отримали понад 26 мільйонів доларів у криптовалюті з адрес, пов'язаних із мексиканськими злочинними групами. Це було зростання на 600% порівняно з попереднім роком. До 2024 року цей потік збільшився ще вдвічі, досягнувши приблизно 64 мільйонів доларів.

Ця цифра не є абстрактною. Вона має пряме відображення у фізичному світі. Агенція DEA фіксує стрімке зростання вилучень прекурсорних хімікатів, необхідних для виробництва фентанілу: з 0,27 тонн у 2022 році до 23,5 тонн у 2023 році. Криптовалютні платежі буквально фінансують цей потік сировини.

Надзвичайною є стійкість цієї системи до спроб її дестабілізувати. Санкції, накладені Міністерством фінансів США на конкретних постачальників та їхні крипто-гаманці, часто дають зворотний ефект. Коли один гаманець блокують, злочинці негайно відкривають новий, використовуючи нові шаблони транзакцій.

Індустріалізація відмивання через віртуальні активи — це не тимчасова аномалія, а структурна зміна в економіці організованої злочинності. Це високотехнологічна інфраструктура, що живить одну з найбільш руйнівних криз сучасності. Перемога в цій боротьбі вимагатиме не меншої інноваційності, міжнародної координації та технологічної проникливості, ніж демонструє сам противник. Майбутнє AML лежить на перетині фінансової розвідки, кібер-кримінології та глобальної політичної волі.

Як страхування життя стало головним інструментом для приховування активів і обходу санкцій [15]

Світ високих фінансів та офшорних операцій постійно породжує нові, все більш витончені інструменти для приховування власності, ухилення від податків та обходу міжнародних санкцій. Останні масові витоки фінансових документів, серед яких особливо виділяються "Pandora Papers", надали безпрецедентне документальне підтвердження того, як саме ці інструменти втілюються в життя для служіння інтересам найзаможніших та найвпливовіших осіб, зокрема російських олігархів, тісно пов'язаних з кремлівським режимом. Центральне місце в цьому розслідуванні займає досить специфічний фінансовий продукт — приватне страхування життя (Private Placement Life Insurance, PPLI), який перетворився з нішевого інструменту майнового планування на могутній механізм створення фінансової непрозорості та захисту активів від будь-якого стороннього втручання.

Детальне вивчення документів, отриманих Міжнародним консорціумом журналістів-розслідувачів (ICIJ) та проаналізованих виданням Tax Notes, розкриває масштабну та тривалу діяльність швейцарського страхового гіганта Swiss Life Group. Ця компанія, яка сама у 2021 році уклала угоду про відстрочення судового переслідування з Міністерством юстиції США, сплативши штраф у розмірі понад 77 мільйонів доларів, активно створювала PPLI-структури для

[15] https://www.taxnotes.com/featured-news/how-do-russian-oligarchs-hide-money-wrap-it-insurance/2025/11/24/7t977

клієнтів з росії. Аналіз показує, що ці структури були далеко не дрібними схемами; вони впорядковували активи на сотні мільйонів доларів. Найбільш вражаючим прикладом є поліс, оформлений у 2011 році через люксембурзьку "дочку" Swiss Life, вартість інвестиційного портфеля якого перевищила 429 мільйонів доларів США. Ця сума не просто велика — вона перевершує вартість найбільшого публічно відомого страхового полісу в світі, що наочно демонструє потенційні обсяги офшорного ринку PPLI, який залишається малодослідженим та слаборегульованим.

Щоб зрозуміти, чому саме страхування життя стало таким привабливим інструментом, необхідно заглибитися в його архітектуру. Механізм дії PPLI як "обгортки" (wrapper) ґрунтується на унікальному поєднанні страхового права та трастового управління. Схема запускається з моменту коли, кінцевий бенефіціарний власник, який прагне залишитися в тіні, ініціює створення складного трастового утворення. Цей траст, часто зареєстрований у юрисдикції з жорсткими законами про конфіденційність, потім виступає в ролі власника договору страхування життя, укладеного зі спеціалізованою страховою компанією, що пропонує PPLI.

Наступним критичним кроком є переведення цільових активів — якими можуть бути акції приватних компаній, частки в хедж-фондах, пакети нерухомості або навіть боргові зобов'язання — на баланс цього страхового полісу. Юридично страхувальник, тобто траст, не володіє безпосередньо цими активами. Власником стає страхова компанія, яка керує ними в рамках інвестиційного портфеля полісу. Таким чином, траст володіє лише фінансовим інструментом (полісом), вартість якого прив'язана до результатів управління активами. Ця конструкція ефективно розриває прямий юридичний зв'язок між кінцевим бенефіціаром і його майном. З точки зору зовнішнього спостерігача чи навіть податкового органу, власником мільйонних статків є респектабельна європейська страхова компанія, а не громадянин росії, який може перебувати під санкціями. Крім того, такі поліси часто пропонують значні податкові переваги у деяких юрисдикціях, наприклад, відстрочку оподаткування доходів від інвестицій, що робить їх подвійно привабливими.

Розглянутий у документах приклад із залученням Євгена Новіцького та Кірілла Андросова є хрестоматійною ілюстрацією цієї схеми. Поліс, оформлений на Новіцького, був забезпечений активами Altera Investment Fund — складним конгломератом приватних інвестиційних фондів із залученням структур з росії, Кіпру, Люксембургу, Британських Віргінських Островів (БВО) та США. Формальним власником полісу виступала офшорна компанія Pharonic Investment Ltd. з БВО, а кінцевим бенефіціаром — Новіцький. У 2017 році, що характерно, відбулася заміна застрахованої особи: нею став Кірілл Андросов, колишній високопоставлений чиновник уряду росії. Цей факт не лише вказує на передачу контрольованих активів між особами, близькими до російської влади, але й демонструє гнучкість інструменту для реструктуризації володіння. Ще більш показовим є маніпулювання навколо декларування бенефіціарного володіння. Внутрішнє листування свідчить про спроби обґрунтувати, що контролюючою особою є не Андросов, а трастова компанія Asiaciti Trust, яка формально виконує функції управителя трасту. Ця майстерність у маніпулюванні юридичними категоріями для приховування істинного контролю — одна з ключових ознак використання PPLI в цілях, далеких від легального фінансового планування.

Окремої уваги заслуговує спроба використання механізму PPLI для активів, безпосередньо пов'язаних з олігархом Олегом Дерипаскою, що знаходиться під міжнародними санкціями. У 2017-2018 роках через ліхтенштейнську структуру Swiss Life розроблявся план створення полісу для компанії Saffron International Assets, яка, в свою чергу, володіла борговим зобов'язанням на 200 мільйонів доларів від іншої компанії Дерипаски. Для цього планувалося використати фіктивну компанію (shelf company) Maidenwells Ltd., створену заздалегідь в якості номінального власника полісу. Документи прямо вказують, що метою введення цієї додаткової ланки в ланцюжок володіння було "сегрегувати та захистити активи", а також забезпечити можливість

їх подальшого перерозподілу "без серйозних адміністративних перешкод". Іншими словами, структура була розроблена для того, щоб ізолювати санкційні активи, полегшити потенційні операції з ними та ускладнити правоохоронним органам їх ідентифікацію та арешт. Проте навіть у цьому світі обмеженого контролю знайшлися ліміти. Угода була згорнута після того, як приватний банк Bordier et Cie з Сінгапура, проводивши стандартну перевірку Due Diligence, виявив зв'язок з Дерипаскою та визнав операцію надмірно ризикованою. Цей епізод показує, що навіть найскладніші схеми можуть спіткнутися об елементарні процедури фінансової безпеки, якщо вони застосовуються належним чином.

Критично важливим контекстом, який робить подібні схеми можливими та успішними, є системні недоліки в національних та міжнародних системах фінансового нагляду. Дослідження Tax Notes вказує на глибоку проблему всередині самих правоохоронних органів США. Зокрема, відзначається, що агенти Подакового управління США (IRS) традиційно мають слабку підготовку для виявлення та аудиту PPLI-структур, що частково пов'язано з відсутністю чітких звітних вимог щодо цих продуктів. Більш того, інформаційні бар'єри всередині IRS перешкоджають ефективному обміну даними між підрозділами.

Не менш значущим є і міжнародний аспект контролю. Діяльність трастової компанії Asiaciti Trust з Сінгапура, яка керувала цими структурами, свідчить про прогалини в регулюванні навіть у таких розвинених фінансових центрах. Монетарне управління Сінгапуру визнало її системи протидії відмиванню коштів (AML) та фінансуванню тероризму (CFT) "слабкими" і наклало значний штраф. Документи показують, що компанія свідомо ігнорувала звіти, які вказували на ризикову репутацію осіб на кшталт Андросова. Це вказує на те, що боротьба з такими схемами вимагає не лише міцного національного законодавства, але й посилення нагляду за професійними посередниками — трастовими компаніями, юристами, бухгалтерами та страховими брокерами, які формують кістяк цієї тіньової інфраструктури.

Таким чином, викриті документи про використання PPLI російськими олігархами розкривають не просто окремі випадки порушень, а глибоку системну проблему. Вони демонструють, як інноваційні фінансові продукти можуть бути викривлені для створення непрозорості; як міжнародна мережа фінансових центрів (Люксембург, Ліхтенштейн, Сінгапур, БВО) може бути скоординована для обходу національних законів та санкцій; і як недостатній рівень ресурсів та політичної волі в ключових країнах, таких як США, може фактично легалізувати цю діяльність через бездіяльність.

Загроза, яку становлять такі схеми, виходить далеко за рамки втрати податкових надходжень. Вони безпосередньо пов'язані з фінансуванням авторитарних режимів, збереженням коштів, отриманих через корупцію, та підривом міжнародних зусиль щодо запобігання агресії через санкційні режими. Тому реакція повинна бути адекватною: посилення глобального автоматичного обміну фінансовою інформацією (CRS) з включенням даних про страхові продукти, введення жорстких зобов'язань щодо розкриття бенефіціарної власності для будь-якого страхового полісу вище певної суми, надання правоохоронним органам спеціалізованих ресурсів та повноважень, а також посилення відповідальності професійних посередників за їх роль у створенні шкідливих схем. Без таких комплексних заходів страхування залишатиметься надійним сейфом для тіньового капіталу, загрожуючи як фінансовій безпеці окремих країн, так і стабільності міжнародної системи в цілому.

Ваша думка важлива!

1. Як Україна може посилити нагляд за міжнародними фінансовими потоками, пов'язаними з російським капіталом? Чи достатньо механізмів для виявлення та блокування активів, прихованих у складних страхових або трастових структурах, і які законодавчі зміни могли б покращити цю роботу?
2. Як війна та пов'язані з нею гуманітарні кризи (внутрішньо переміщені особи, діти без нагляду) можуть підвищити ризики онлайн-експлуатації дітей в українському сегменті інтернету, і які профілактичні заходи мають вживати держава та громадянське суспільство для захисту вразливих груп?
3. Які механізми відмивання коштів через торгівлю (TBML) можуть бути найбільш актуальними для України, зважаючи на значення аграрного та металургійного експорту? Чи є ризики використання української логістичної інфраструктури для обходу санкцій?
4. Як Україна може системно протидіяти використанню російськими спецслужбами транснаціональних злочинних мереж для фінансування диверсійної діяльності, вербування агентури та впливу на політичні процеси в Україні та країнах-партнерах?
5. Як державним органам України вибудувати сталі механізми аналізу та оцінювання ризиків, щоб вони залишались актуальними у довгостроковій перспективі, а не потребували повного перегляду кожні кілька років? Які ризики для фінансового сектору можуть виникнути внаслідок надмірної стандартизації оцінювання?
6. Чи повинна держава розглядати блокчейн-інфраструктуру як критичну фінансову інфраструктуру, і якщо так — які наслідки це матиме для нагляду, кібербезпеки та міжнародної співпраці України?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-52

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

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