Методологічний бюлетень

Серійний номер: МінФін-AML-2026-15

Квітень 2026

“Ми шукаємо ключі там, де горить ліхтар!”

Ходжа Насреддін

Мета

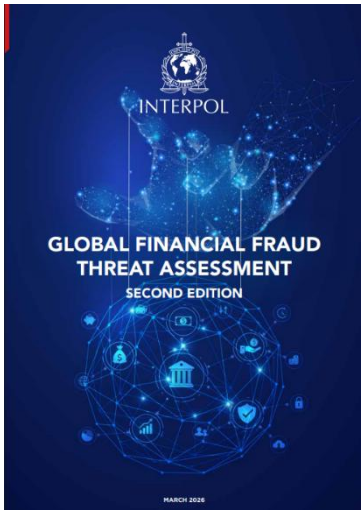
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

Глобальна оцінка загрози фінансового шахрайства [1]



Друге видання Глобальної оцінки загрози фінансового шахрайства INTERPOL є масштабним аналітичним документом, що ґрунтується на інтеграції власних оперативних даних організації, матеріалів країн-членів, академічних досліджень і внесків приватного сектору. За методологією звіту фінансове шахрайство ідентифікується як незаконна діяльність, спрямована на отримання фінансової вигоди шляхом обманних дій проти фізичних або юридичних осіб. За оцінкою INTERPOL, глобальні втрати від фінансового шахрайства лише у 2025 році склали 442 мільярди доларів США — згідно з оцінкою Глобального альянсу проти шахрайства (GASA). У Великій Британії шахрайство становило 43% усіх зареєстрованих злочинів у 2025 році, тоді як у США сукупний збиток зріс із майже 4 мільярдів доларів у 2020 до 16,6 мільярда у 2024 році.

[1] https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

INTERPOL констатує 54-відсоткове збільшення кількості повідомлень і розповсюджень інформації, пов'язаних із шахрайством, між 2024 і 2025 роками — при цьому 38% від їхньої загальної кількості надійшло від країн-членів Європи, ще 28% — від держав Азійсько-Тихоокеанського регіону. За той самий звітний період Центр боротьби з фінансовими злочинами та корупцією INTERPOL (IFCACC) надав підтримку у понад 1 500 транснаціональних справах про шахрайство на загальну суму 1,1 мільярда доларів у вигляді заявлених збитків. INTERPOL визначає фінансове шахрайство як одну з п'яти найбільших глобальних загроз у сфері злочинності — поряд із незаконним обігом кокаїну, синтетичних наркотиків, героїну та відмиванням коштів. Результати опитування Всесвітнього економічного форуму свідчать, що 77% лідерів бізнесу у всьому світі повідомили про зростання кількості шахрайських операцій протягом 2025 року, а 73% підтвердили, що самі або їхні партнери по бізнесу особисто постраждали від кіберзлочинів у цей період.

Звіт систематизує сім основних типологій фінансового шахрайства. Компромісна атака на корпоративну електронну пошту (BEC) залишається найбільш поширеним типом, зафіксованим в операційних даних INTERPOL, — переважно в Азійсько-Тихоокеанському регіоні та Європі. Шахрайство з авансовими платежами демонструє зростання в сегментах зайнятості, успадкування та лотерейного обману, з особливою концентрацією загрози в Африці. Шахрайство через видавання себе за іншу особу активно еволюціонує, включаючи такі нові схеми, як фейкові викрадення з вимогою викупу з використанням AI-згенерованих зображень та «квішинг» — зловживання QR-кодами для переспрямування жертв на фішингові сайти. Синтетичне шахрайство з ідентифікаційними даними, підтримане генеративним AI, відкриває нову категорію ризику, включаючи крадіжку дитячих персональних даних, яка часто залишається невиявленою до повноліття жертви. Інвестиційне шахрайство, зокрема через криптовалютні платформи та фіктивну нерухомість, спричиняє найбільші втрати для індивідуальних жертв. «Романтичне шахрайство» (romance baiting) поєднує романтичні та криптоінвестиційні схеми і поширюється із Південно-Східної Азії на Африку, Латинську Америку та Європу. Сексторція (форма шантажу, коли хтось погрожує розповсюдити зображення жертви інтимного характеру) стає все більш системно вбудованою у складні гібридні схеми шахрайства.

Феномен шахрайських кол-центрів трансформувався з регіонального явища Південно-Східної Азії у глобальну загрозу, що охоплює всі континенти. Жертви, що використовуються для примусового вчинення шахрайства, вже представляють майже 80 національностей — у порівнянні з 66 у першому кварталі 2025 року. Ці центри функціонують за моделлю подвійної жертви: з одного боку — особи, яких заманили фіктивними пропозиціями роботи і які утримуються у примусових умовах; з іншого — особи, яких обманюють у різних юрисдикціях. INTERPOL задокументував конкретні мережі торгівлі людьми в Західній та Центральній Африці, які маскуються під компанії багаторівневого маркетингу (MLM), а також зафіксував звіти про нові центри в регіонах MENA, Центральній Америці та Західній Африці.

Технологічний блок звіту присвячено штучному інтелекту як «мультиплікатору сили» злочинних схем. «Агентний AI» здатен автономно планувати та виконувати цілі шахрайські кампанії — від розвідки жертв і збирання облікових даних до генерації психологічно таргетованих повідомлень із вимогами. На темних ринках даркнету функціонують сервіси «Deepfake-as-a-Service», що пропонують синтетичні особистісні комплекти з відеоаватарами, клонами голосу та біометричними даними — лише 10 секунд аудіо, зібраного з публічних джерел, достатньо для обходу систем автентифікації. Платформи «Fraud-as-a-Service» (FaaS) забезпечують злочинцям повну кримінальну інфраструктуру: фішингові інструменти, фіктивні торгові платформи, AI-чатботи для «опрацювання» жертв і зашифровані канали зв'язку з інтегрованими послугами з відмивання коштів. За оцінками аналітиків, AI-схеми у 4,5 рази прибутковіші за стандартні тактики шахрайства, що пришвидшує індустріалізацію злочинної діяльності.

Регіональний аналіз виявляє суттєву географічну диференціацію динаміки загрози. Найбільш значне зростання повідомлень зафіксовано в регіоні Близького Сходу та Північної Африки (+69%), в Африці (+60%) та Азійсько-Тихоокеанському регіоні (+47%). В Африці провідними типологіями залишаються BEC, інвестиційне шахрайство та романтичне шахрайство; при цьому масштаб явища є колосальним: лише в одній операції в Замбії було виявлено 65 000 жертв із збитками близько 300 мільйонів доларів. В регіоні Америки та Карибського басейну зафіксовано зростання на 40% — переважно у BEC, яке активно поширюється за межі США через Латинську Америку. У Європі зростання на 17% обумовлено передусім страховим шахрайством і BEC, при цьому синтетичне шахрайство з ідентичністю набуває дедалі більшої поширеності.

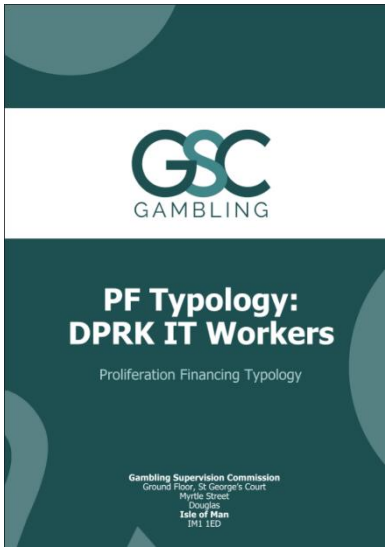
Критично важливим новим виміром загрози, детально задокументованим у звіті, є наростаюча конвергенція між фінансовим шахрайством та фінансуванням тероризму в африканському регіоні. Операція Catalyst — транснаціональна справа щодо масштабної криптовалютної схеми Понці, яка маскувалась під легітимну торгову платформу і охопила щонайменше 17 країн (зокрема Камерун, Кенію та Нігерію), — завдала збитків понад 100 000 жертв на суму 562 мільйони доларів. Розслідування виявило потенційні зв'язки між рядом великих криптогаманців та діяльністю з фінансування тероризму в Центральній Африці. Географічними вузлами цього конвергентного феномену визначено: Нігерію та Камерун (первинні джерела фінансування терористичних груп через крипто-шахрайство), Кенію та Танзанію (кошти для рекрутингу та радикалізації), а також Південну Африку та Анголу (неформальні системи переказу вартості зі зв'язком із можливим ФТ та ВК).

Висновки:

- **Швидке поширення технологій «Fraud-as-a-Service» та агентного AI вимагає від СПФМ перегляду методологій виявлення підозрілих операцій:** традиційні порогові підходи стають недостатніми для ідентифікації AI-спланованих мікротранзакцій та синтетичних ідентифікаційних даних; необхідна глибока інтеграція поведінкової аналітики і машинного навчання безпосередньо в системи транзакційного моніторингу.
- **Задокументована конвергенція між фінансовим шахрайством та фінансуванням тероризму в Африці (операція Catalyst) зобов'язує підрозділи комплаєнсу переглянути категоризацію ризиків:** кошти, отримані від криптошахрайства, мають розглядатися не лише в контексті ВК, але й як потенційне джерело ФТ, що вимагає застосування гібридних сценаріїв у системах моніторингу.
- **Глобальне поширення мереж шахрайських кол-центрів (жертви майже з 80 країн) вказує на необхідність впровадження в СПФМ механізмів геолокаційного скринінгу для платежів,** ідентифікованих як потенційно пов'язаних зі схемами примусового онлайн-шахрайства — особливо фінансових потоків на адресу структур у Південно-Східній Азії, Гані, Нігерії та нових регіонах розширення.

Профіль суб'єктів-порушників, складений на основі даних країн-членів, характеризує злочинні мережі у сфері фінансового шахрайства як полікримінальні, високоорганізовані, технічно кваліфіковані та адаптивні. Структури злочинних організацій демонструють помірний рівень міжгрупової співпраці та помірний доступ до фінансових і матеріальних ресурсів — що відображає низькі бар'єри входу на ринок злочинності. INTERPOL прогнозує, що загальний глобальний ризик фінансового шахрайства на наступні три-п'ять років є ВИСОКИМ, із очікуваним значним ескалаційним ефектом, який найвідчутніше вплине на економічний, соціальний і безпековий виміри.

КНДР та ризики фінансування розповсюдження [2]



Комісія з нагляду за азартними іграми (Gambling Supervision Commission, GSC) острова Мен опублікувала спеціалізований типологічний звіт, присвячений ризикам фінансування розповсюдження зброї масового знищення (ФР) через використання КНДР схеми дистанційної ІТ-зайнятості. Документ розроблений на основі синтезу матеріалів Офісу впровадження фінансових санкцій Великої Британії (OFSI), Групи по контролю за санкціями (Multilateral Sanctions Monitoring Team, MSMT) та аналітичних звітів Chainalysis. Стратегічний контекст документа визначається тим, що КНДР підтримує тисячі висококваліфікованих ІТ-фахівців, переважно розгорнутих у Китаї та Росії, чиї доходи спрямовуються на фінансування програм зі створення зброї масового знищення та балістичних ракет. OFSI робить оцінку, що є «практично достовірним», що британські компанії вже наразі є об'єктами таргетування з боку ІТ-працівників КНДР, замаскованих під фрілансерів із третіх країн.

Механізм схеми полягає в цілеспрямованому проникненні кваліфікованих ІТ-фахівців КНДР у компанії-роботодавці на Заході шляхом систематичного використання сфальсифікованих особистостей, підроблених посвідчень особи (зокрема, шляхом накладання власних фотографій на зображення китайських ID-карток, знайдених онлайн), крадених облікових даних та VPN/VPS-сервісів для приховування реального місцезнаходження. ІТ-працівники активно присутні на провідних фриланс-платформах (Upwork, Freelancer), у мессенджерах (Telegram, WeChat) та соціальних мережах (LinkedIn), де формують бездоганні профілі з переконливою трудовою біографією. Особлива стратегія побудови довіри передбачає надання якісних послуг на початковому етапі та швидкого виконання завдань для отримання довгострокових контрактів. Задокументований у звіті кейс компанії Kyonghung Information Technology Exchange Company демонструє, що її команди з 4 осіб розробляли ігрові сайти для клієнтів, розподіляючи завдання між собою, включаючи розробку застосунків для моніторингу фінансових переказів, управління обліковими записами та веб-дизайн. Ця компанія також надавала послуги SEO-оптимізації кримінальним організаціям для підвищення видимості нелегальних ігрових платформ.

Фінансовий механізм ухилення від санкцій базується на комплексному використанні віртуальних активів. ІТ-працівники систематично запитують оплату у стейблкоїнах — через їхню стабільну вартість, — після чого проводять отримані кошти через технічно складні схеми відмивання: chain-hopping (переміщення активів між різними блокчейнами через смарт-контракти і мости), token swapping (обмін одного типу активів на інший через децентралізовані біржі), а також об'єднання коштів із доходами інших ІТ-працівників КНДР у процесі розшарування. Фінальний етап передбачає передачу активів посередникам — представникам режиму, які відкривають рахунки на основних криптобіржах із використанням вкрадених або фальшивих документів та конвертують кошти у фіатну валюту. Особлива вразливість ігрового сектору острова Мен зумовлена його ІТ-інтенсивною природою та активним залученням зовнішніх технічних спеціалістів, а також тим, що платформи онлайн-гемблінгу можуть використовуватися для розшарування незаконних коштів через ігрові транзакції та гаманці, пов'язані з віртуальними активами.

GSC систематизує індикатори ризику за категоріями векторів загрози: використання фальшивих CV і документів; залучення VPN/VPS і програм віддаленого доступу; використання свідомих і несвідомих посередників; нетипові схеми виплат через EMI/MSB-провайдерів; привілейований

[2] https://www.isleofmangsc.com/media/xd2kvmro/dprk-typology-report.pdf

Висновки:

- **Ігровий та IT-сектор зобов'язані запровадити посилену процедуру перевірки при влаштуванні на роботу дистанційних IT-працівників:** обов'язкова відеоверифікація особи із заходами захисту від deepfake-підробок, перехресна перевірка банківських реквізитів з документами, що посвідчують особу, та заборона виплат у криптовалюті або на рахунки третіх осіб.
- **Інтеграція ризиків ФР в системи транзакційного моніторингу** вимагає впровадження спеціалізованих сценаріїв виявлення chain-hopping та token swapping через децентралізовані біржі, а також сценаріїв об'єднання платежів у ВА із характеристиками мереж відмивання.
- **Розмір і технічна досконалість схем КНДР вимагають від СПФМ здійснення посиленого скринінгу платіжних платформ EMI/MSB** на предмет ознак акумуляції та консолідації доходів перед конвертацією в фіатну валюту через кастодіальних брокерів із фальшивими документами.
- **Операційна активність КНДР у сфері розробки ігрових веб-сайтів і SEO-оптимізації кримінальних платформ вимагає від операторів встановлення процедур верифікації кінцевого використання IT-продуктів**, що передаються підрядникам, та документування ланцюжка постачань IT-послуг для виявлення прихованих зв'язків зі структурами, пов’язаними із КНДР.

доступ до систем компанії з ризиком ексфільтрації даних або побудови прихованих backdoor-вразливостей. Специфічними ознаками ризику є множинні входи в один обліковий запис з різних IP-адрес, безперервний онлайн-стан протягом 24+ годин, запити на отримання плати на рахунок, відкритий на ім'я іншої особи, а також ухилення від відеозустрічей або використання deepfake-відео під час дзвінків.

У частині правових зобов'язань та регуляторних заходів GSC наголошує на обов'язку операторів повідомляти Підрозділ фінансової розвідки відповідно до Закону про тероризм та інші злочини (фінансові обмеження) 2014 року (TOCFRA) у випадку обґрунтованої підозри щодо особи, яка є об’єктом санкцій або вчинила правопорушення відповідно до санкційного законодавства, а також відповідно до Закону про доходи від злочинності (POCA) — у випадку підозри у відмиванні коштів або фінансуванні тероризму. GSC акцентує на необхідності включення ризиків ФР у бізнес-оцінки ризиків, розширеної належної перевірки клієнтів для осіб, пов'язаних з ВА, та застосування інструментів блокчейн-аналітики для відстеження транзакцій з ознаками мереж ухилення від санкцій, пов’язаних із КНДР.

Штучний інтелект у фінансових послугах Гонконгу [3]

У квітні 2026 року Асоціація фінтеху Гонконгу (FTAHK) опублікувала документ Стратегічної консультативної ради з питань ШІ у фінансових послугах — комплексний стратегічний документ, підготовлений на основі опитування понад 100 фінансових установ у секторах банківського обслуговування, страхування, управління активами та фінтеху, проведеного наприкінці 2025 року. Документ поєднує емпіричні дані, аналіз найкращих глобальних практик та конкретні рекомендації щодо відповідального впровадження генеративного AI (GenAI) у фінансових послугах Гонконгу. Центральна теза документа полягає в тому, що Гонконг уже демонструє

[3] https://ftahk.org/sites/default/files/2026-04/FTAHK%20Strategic%20Advisory%20Council%20on%20AI%20-%20Position%20Paper.pdf

рівень впровадження AI в 38%, що суттєво перевищує глобальний середній показник у 26%, однак структурні слабкості загрожують зупинити цю позицію лідерства.

Поточний стан впровадження GenAI характеризується домінуванням внутрішньо-орієнтованих застосувань. За даними опитування HKIMR (квітень 2025 року), 75% фінансових установ Гонконгу вже впровадили або пілотують щонайменше один сценарій використання GenAI, а прогнозований рівень зросте до 87% протягом наступних трьох-п'яти років. При цьому спостерігається виражена асиметрія за розміром установи: великі фінансові інституції демонструють 83% впровадження, тоді як малі установи — лише 63%, що відображає ресурсно-обумовлену готовність. Найбільш поширені поточні застосування охоплюють: віртуальних помічників для співробітників (58%), обробку внутрішніх документів (45%), поглиблений AML/KYC (22%) та вдосконалені чатботи для клієнтів (31%). Серед перспективних технологій найбільший інтерес викликають інтерактивні віртуальні аватари та агентичні архітектури.

В контексті ПВК/ФТ особливо релевантним є аналіз застосувань AI у сфері фінансового комплаєнсу. Дані опитування демонструють, що моніторинг відповідності регуляторним вимогам є пріоритетом для 48% респондентів, комплаєнс, включаючи KYC та онбординг клієнтів, — для 16%, виявлення та запобігання шахрайству — для 24%. У розрізі секторів традиційні банки та страховики зосереджуються на застосуваннях AI для управління ризиками та нагляду за відповідністю (74% і 100% відповідно), тоді як фінтех-компанії надають пріоритет виявленню шахрайства (53%) і KYC-автоматизації (32%). Такий секторальний дуалізм відображає різні профілі нормативних ризиків і операційних пріоритетів.

Структурні обмеження впровадження AI ідентифіковано у чотирьох ключових вимірах. Перший — якість та доступність даних і сумісність з Legacy-системами: значний масив

Висновки:

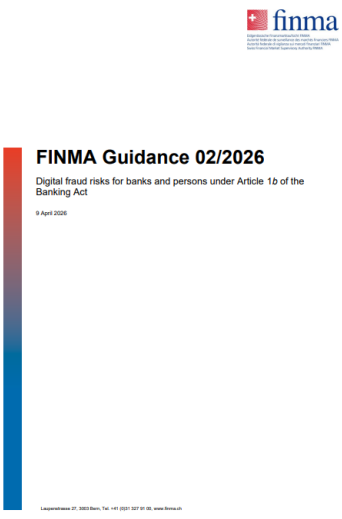
- **Розрив у впровадженні AI між великими та малими фінансовими установами (83% проти 63%) у контексті AML/KYC-автоматизації вимагає регуляторного втручання через надання доступу до спільних ресурсів і пісочниць**, щоб не допустити ситуації, коли менші СПФМ стають слабкою ланкою системи ПВК/ФТ через технологічне відставання.
- **Критична залежність ефективності AML-систем на основі AI від якості даних зобов'язує СПФМ переглянути архітектуру сховищ даних:** виявлення та усунення фрагментації KYC-інформації в Legacy-системах є передумовою успішного впровадження будь-яких AI-інструментів для транзакційного моніторингу та профілювання клієнтів.
- **Відсутність чітких галузевих стандартів щодо пояснюваності та валідації AI-моделей у фінансовому комплаєнсі — ключова проблема**, яка вимагає від регуляторів публікації конкретних технічних керівних принципів для AML-моделей, включаючи вимоги до документування методології, тестування на упередженість та процедур управління моделями.
- **Принцип людини-в-циклі має бути операціоналізований у формі документованих протоколів ескалації для згенерованих AML-сповіщень:** алгоритмічне рішення про подання STR/SAR повинно підтверджуватись кваліфікованим аналітиком, а не автоматично передаватись до регулятора, — що відповідає вимогам пояснюваності та захисту прав клієнтів.

критичної інформації залишається фрагментованим у неструктурованих форматах або «замкненим» у застарілих платформах, що безпосередньо знижує ефективність AML-систем на основі AI. Другий — дефіцит кадрів: 49% підприємств зіштовхуються з труднощами при найнятті технічних спеціалістів, а 97% банків відносять технологічні навички та навички роботи з даними до топ-3 ключових потреб у компетенціях. Третій — регуляторна невизначеність: відсутність чітких AI-специфічних керівних принципів у галузі (74% фінтех-компаній і 61% банків визначають це як найбільш складне регуляторне питання), а також транскордонні регуляторні відмінності (впливають «помірно» на 69,9% організацій). Четвертий — етичні проблеми: відсутність прозорості в процесах AI (88 респондентів) та упередженість у прийнятті рішень (73 респонденти) є провідними етичними занепокоєннями.

Документ пропонує чіткі метрики успіху та поетапний план розвитку. У короткостроковій перспективі (2026–2027) пріоритетами є публікація типових шаблонів управління, прагматичні вимоги щодо валідації та пояснюваності моделей, зміцнення готових основ даних lkz AI та розширення доступу до регуляторних пісочниць. Середньострокові цілі (2028–2029) передбачають поглиблену інтеграцію через галузеві довідники, аудит, а також збереження конфіденційності даних при їх спільному використанні. Довгострокове бачення (2030+) орієнтоване на глобальне лідерство у відповідальному AI, з цільовими показниками: 90% рівень впровадження AI до 2028 року, залучення HK$8–12 млрд у AI-стартапи у сфері фінтеху до 2030 року, 20–30% підвищення точності виявлення шахрайства AI-системами до 2028 року.

Позиційний документ особливо наголошує на принципі «людини в циклі» (human-in-the-loop) як ключовій вимозі відповідального впровадження AI. Це методологічне застереження особливо критичне в контексті AML/KYC, де алгоритмічні рішення щодо підозрілих транзакцій або відмови у обслуговуванні клієнта несуть суттєві правові ризики. Специфіка Гонконгу як центру, який одночасно використовує AI-моделі з американських (AWS, Azure, Google, OpenAI, Anthropic) і китайських (DeepSeek, Alibaba Cloud, Tencent Cloud) платформ, ускладнює вибір та стандартизацію моделей для регульованих застосувань, зокрема в сфері фінансових злочинів.

Ризики цифрового шахрайства для банків [4]



Швейцарський орган з нагляду за фінансовими ринками (FINMA) опублікував Керівні настанови 02/2026 «Ризики цифрового шахрайства для банків та осіб відповідно до статті 1b Закону про банківську діяльність». Документ є результатом комплексного обстеження цифрового банкінгу, проведеного FINMA наприкінці 2025 року серед 19 банків різних наглядових категорій. Із фундаментального наглядового застереження документа випливає, що FINMA з кінця 2022 року систематично фіксує зростання кількості випадків цифрового шахрайства у банках і очікує подальшого загострення цієї тенденції на тлі технологічного прогресу в сфері AI та цифрової трансформації. Методологічна основа документа орієнтована на функціональне, а не нормативне визначення цифрового шахрайства: ним вважаються шахрайські дії, в яких цифрові технології, інформаційні системи або електронні засоби комунікації використовуються для введення в оману з метою заподіяння фінансових збитків.

[4] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20260112-finma-aufsichtsmitteilung-02-2026.pdf?sc_lang=en&hash=756A9C493A822F0E01A0D1343FECEA8E

Аналіз результатів обстеження в частині управління та ризик-менеджменту виявив системні прогалини. Лише 12 із 19 обстежених банків заявили про наявність стійких структур управління в сфері ризиків цифрового шахрайства — проте навіть у цих установах вони зазвичай складаються з осіб, що суміщають посади (із підрозділів безпеки операцій, платежів, ризик-менеджменту та IT) без чіткого розподілу завдань, повноважень і задокументованих правил прийняття рішень. Три банки з 19 взагалі не мають керівного комітету з питань ризиків цифрового шахрайства. Критично, що 8 із 19 установ (42%) не мають власної внутрішньої політики щодо цифрового шахрайства — натомість ці питання розглядаються фрагментарно в рамках інших керівних документів (трудових угод, AML-політик або інформаційної безпеки) без їх взаємоузгодження. Приблизно лише половина обстежених установ регулярно включає показники, пов'язані з цифровим шахрайством, до звітності для вищого керівництва.

Аналіз виявлення та реагування на цифрове шахрайство демонструє не менш суттєві прогалини: 26% обстежених установ не мають будь-яких процесів для проактивного виявлення та прогнозування тенденцій цифрового шахрайства (так зване «горизонтальне сканування»). Хоча 12 із 19 банків використовують технології виявлення шахрайства в режимі реального часу, 7 установ або взагалі не аналізують індикатори поточних кампаній цифрового шахрайства, або роблять це лише вручну у разі конкретного інциденту. Через надмірну залежність від постачальників послуг не всі банки здатні своєчасно оновлювати відповідні правила виявлення, що ставить під загрозу їхню здатність оперативно реагувати на виявлені кампанії або патерни шахрайства. Стандартний порядок реагування (SOP) відсутній у 7 із 19 установ, а плани реагування оновлюються щонайменше раз на рік лише у 7 банків — решта робить це виключно після настання інциденту. Більшість установ не відстежують і не вимірюють час реагування на повідомлення про шахрайство.

Висновки:

- **Системна відсутність власних внутрішніх політик щодо цифрового шахрайства в 42% досліджених установах та фрагментація відповідних положень у розрізнених AML-, HR- та IT-документах вимагає від СПФМ створення окремого, інтегрованого документа** — «Політики управління ризиками цифрового шахрайства» — з чітким розподілом відповідальності, повноважень і процедур реагування на рівні профільного керівного комітету.
- **Виявлена FINMA критична залежність результативності виявлення шахрайства від рівня порогів транзакційного моніторингу вказує на необхідність перегляду:** поведінкова аналітика та порівняльний аналіз в межах груп мають замінити жорсткі фіксовані порогові значення для виявлення нетипових для профілю клієнта транзакцій, особливо характерних для схем «рахунків-мулів».
- Стрімке поширення технологій deepfake для обходу онлайн-перевірок зобов'язує банки **впровадити технічні засоби виявлення deepfake-відео та сфальсифікованих документів як обов'язкові компоненти процедури онбордингу**.
- **10-кратна різниця між установами у кількості підозр, пов'язаних із цифровим шахрайством, є ознакою системної нерівномірності в організації та ефективності AML-програм**, яка вимагає від регуляторів проведення більш глибокого горизонтального аналізу та можливого запровадження обов'язкових мінімальних стандартів для виявлення рахунків-мулів і схем шахрайства в онлайн-банкінгу.

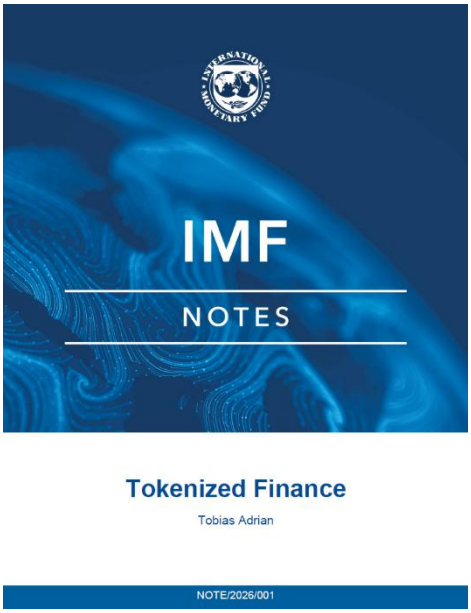
Окремим критичним виміром є шахрайське відкриття рахунків в онлайн-режимі. FINMA фіксує зростання у злочинних організацій, які намагаються відкривати банківські рахунки з використанням дедалі складніших технічних засобів. Особливо небезпечною є тенденція, за якої рахунки відкриваються з використанням дійсних документів, що посвідчують особу — таким

чином процедура онбордингу є технічно коректною, — а шахрайські дії (передача контролю над рахунком третім особам, перетворення рахунку на «мул» для транзитного переказу злочинних коштів) відбуваються на наступному етапі. Поширення технологій маніпуляції відео та deepfake значно ускладнює виявлення підроблених документів при онлайн-верифікації особи.

В частині запобігання відмиванню коштів дослідження FINMA виявило кілька критичних системних слабкостей. По-перше, кількість STR/SAR до MROS (ПФР Швейцарії), що стосуються шахрайства та пов'язаних явищ, варіюється між установами у співвідношенні 10 до 1, а частка внутрішньо ініційованих повідомлень, що перетворюються на SAR, коливається від 12 до 78% — що свідчить про радикальну відмінність ефективності AML-систем між установами. По-друге, KYC-інформація, яку збирають установи, є загалом обмеженою: більшість банків не використовує зібрані KYC-дані для транзакційного моніторингу (не застосовує різні сценарії або ліміти на їх основі), а звертається до них лише в контексті конкретних перевірок. По-третє — і це найбільш системна вада — пороги транзакційного моніторингу для роздрібних клієнтів з низьким або нормальним ризиком встановлено відносно високо: на рівні CHF 100 000 або 200 000. FINMA оцінює такі системи як недостатньо складні: вони орієнтовані переважно на фіксовані порогові значення, а не на специфічні сценарії, що суттєво обмежує їхню здатність виявляти шахрайство у сфері цифрового банкінгу та схеми використання рахунків-мулів.

У своїх рекомендаціях FINMA наполягає на тому, що банки та особи відповідно до ст. 1b Закону про банківську діяльність зобов'язані створити чіткі структури управління, ефективні системи ризик-менеджменту та відповідні технічні засоби для виявлення, оцінки і контролю ризиків цифрового шахрайства в усіх видах їхньої діяльності. Комплексна стратегія протидії цифровому шахрайству повинна охоплювати: ризики незаконного відкриття клієнтських рахунків в онлайн-режимі, несанкціонованого доступу до рахунків та ризики відмивання коштів — інтегровано та взаємопов'язано, а не у вигляді ізольованих процедур.

Токенізація фінансів і майбутнє грошей: системні ризики та регуляторні виклики [5]



Документ Міжнародного валютного фонду пропонує глибоке переосмислення сучасної фінансової системи через призму токенізації, розглядаючи її як якісно новий етап розвитку фінансових ринків, що виходить за межі звичайної цифровізації та означає фундаментальну зміну інституційної логіки функціонування фінансів. У центрі аналізу знаходиться теза про трансформацію джерела довіри: якщо традиційна система ґрунтується на посередниках — банках, клірингових установах, депозитаріях — то токенізована система переносить функції довіри у технологічну інфраструктуру, де виконання фінансових операцій забезпечується кодом, алгоритмами та розподіленими реєстрами. Це означає, що довіра дедалі більше залежить не від фінансової стійкості інститутів, а від надійності програмного забезпечення, якості даних і механізмів управління цифровими платформами.

Однією з ключових характеристик токенізованих фінансів є програмованість активів, що дозволяє інтегрувати умови контрактів безпосередньо в сам актив через смарт-контракти. У результаті фінансові операції стають самовиконуваними, а такі функції, як виплата доходів, виконання зобов’язань чи управління забезпеченням, автоматизуються. Це створює значні

[5] https://www.imf.org/-/media/files/publications/imf-notes/2026/english/insea2026001.pdf

переваги з точки зору ефективності та зниження транзакційних витрат, але водночас підвищує залежність системи від правильності коду та передбачуваності алгоритмічної поведінки. У документі підкреслюється, що помилки в смарт-контрактах або їхня вразливість до маніпуляцій можуть мати системні наслідки, оскільки виконання операцій відбувається автоматично і часто без можливості оперативного втручання.

Суттєва увага приділяється концепції атомарного розрахунку, яка є однією з основних інновацій токенізованих фінансів. Вона передбачає одночасне виконання двох сторін транзакції — передачі активу та здійснення платежу — що практично усуває контрагентський ризик і знижує потребу в посередниках. Однак така модель вимагає наявності ліквідності у режимі реального часу, що змінює традиційні підходи до управління ліквідністю та може створювати додатковий тиск на фінансові установи в умовах стресу. У цьому контексті токенізація не лише підвищує ефективність, а й трансформує фундаментальні механізми функціонування ринків, змінюючи баланс між ризиком і ліквідністю.

У документі детально аналізується вплив токенізації на структуру фінансових ринків, зокрема на ринки капіталу, де інтеграція функцій торгівлі, клірингу та розрахунків у межах єдиної інфраструктури змінює традиційну роль фінансових посередників. Токенізація дозволяє скоротити кількість етапів у життєвому циклі фінансового інструменту, зменшити операційні витрати та підвищити прозорість, однак одночасно створює ризики концентрації, оскільки велика кількість операцій здійснюється в межах обмеженої кількості платформ. Це підвищує системну значущість таких платформ і вимагає нових підходів до їх регулювання та нагляду.

Значна частина документа присвячена трансформації банківського сектору, де токенізація розглядається як фактор, що не усуває банки, але змінює їхню роль у фінансовій системі. Банки залишаються ключовими постачальниками кредиту та ліквідності, однак змушені адаптуватися до нових умов, у яких фінансові операції здійснюються безперервно, а конкуренція з боку небанківських учасників, зокрема емітентів стейблкоїнів і технологічних платформ, зростає. У цьому контексті підкреслюється, що інформаційна асиметрія та псевдонімність у деяких токенізованих середовищах можуть призводити до зростання вимог до забезпечення, що, у свою чергу, знижує ефективність фінансового посередництва та може обмежувати доступ до фінансування.

Окремий акцент зроблено на грошовій системі, де токенізація створює конкуренцію між різними формами грошей — банківськими депозитами, стейблкоїнами та цифровими валютами центральних банків. Документ наголошує на важливості збереження принципу єдності грошей, який забезпечує стабільність фінансової системи та довіру до неї. Порушення цього принципу може призвести до фрагментації грошової системи, втрати контролю над грошово-кредитною політикою та зростання системних ризиків. У цьому контексті розглядаються різні моделі взаємодії публічних і приватних форм грошей, включаючи підходи, які дозволяють поєднати інноваційний потенціал приватного сектору з гарантіями центрального банку.

Важливим елементом аналізу є розгляд нових видів ризиків, що виникають у токенізованій фінансовій системі. Серед них особливе місце займає алгоритмічний ризик, пов’язаний із залежністю від програмного забезпечення та автоматизованих механізмів прийняття рішень. У разі помилок у коді або збоїв у роботі системи можливі швидкі та масштабні негативні наслідки, включаючи каскадні ефекти, що поширюються на весь фінансовий сектор. Крім того, підкреслюється роль так званих оракулів — зовнішніх джерел даних, які забезпечують зв’язок між цифровими активами та реальним світом. Ненадійність або маніпуляція такими даними може призвести до неправильного виконання смарт-контрактів і створити додаткові ризики для фінансової стабільності.

У міжнародному контексті токенізація розглядається як фактор, що може як сприяти інтеграції фінансових ринків, так і створювати нові виклики для регуляторів. З одного боку, вона дозволяє спростити транскордонні платежі, зменшити витрати та підвищити швидкість операцій. З іншого боку, відсутність узгоджених стандартів і різні підходи до регулювання можуть призвести до фрагментації ринку та посилення регуляторного арбітражу. Особливо вразливими є країни з ринками, що формуються, які можуть зіткнутися з ризиками втрати монетарного суверенітету та підвищеною волатильністю капітальних потоків у разі широкого використання іноземних цифрових активів.

Документ також підкреслює, що швидкість є новим виміром системного ризику в токенізованій фінансовій системі. Автоматизація та безперервність операцій означають, що фінансові шоки можуть поширюватися значно швидше, ніж у традиційній системі, що обмежує можливості регуляторів для своєчасного реагування. У зв'язку з цим виникає потреба у впровадженні нових інструментів нагляду, які дозволяють здійснювати моніторинг у режимі реального часу та забезпечувати швидке втручання у разі виникнення кризових ситуацій.

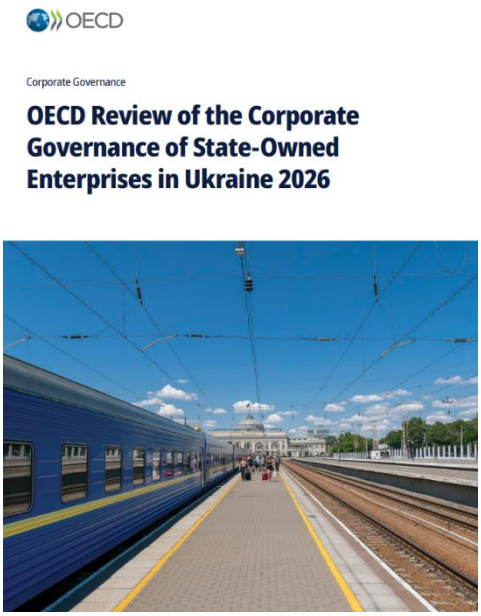
Загалом документ формує цілісне бачення майбутньої фінансової системи, у якій технологічна інфраструктура стає центральним елементом, а ефективність і швидкість операцій поєднуються з новими видами ризиків, що потребують комплексного та скоординованого підходу з боку держав, регуляторів і міжнародних організацій. Токенізація розглядається як неминучий етап розвитку фінансів, який відкриває значні можливості для підвищення ефективності та доступності фінансових послуг, але водночас вимагає глибокого переосмислення підходів до регулювання, управління ризиками та забезпечення фінансової стабільності.

Висновки:

- **Токенізація формує принципово нову архітектуру фінансової системи,** у якій ключові функції довіри, виконання транзакцій і управління ризиками переносяться з інституцій у технологічну інфраструктуру, що вимагає від держав і регуляторів переходу від нагляду за суб'єктами до нагляду за системами, алгоритмами та даними.
- **Фінансова стабільність у токенізованій економіці може бути забезпечена лише за умови збереження «публічного якоря»** у вигляді безризикових грошей центрального банку або жорстко регульованих еквівалентів, оскільки домінування приватних токенізованих грошей створює ризики фрагментації грошової системи та втрати контролю над ліквідністю.
- **Швидкість та автоматизація фінансових процесів трансформуються у новий системний ризик,** оскільки алгоритмічні механізми (смарт-контракти, автоматичні ліквідації, вимоги щодо додаткового забезпечення) здатні генерувати миттєві каскадні ефекти, це потребує впровадження безперервного моніторингу та нових інструментів кризового реагування.
- **Глобальний характер токенізованих фінансів у поєднанні з національно обмеженими режимами регулювання посилює ризики регуляторного арбітражу, фінансової фрагментації та втрати монетарного суверенітету,** що обумовлює критичну необхідність міжнародної координації, гармонізації стандартів і інтеграції підходів у сфері ПВК/ФТ/ФР.

Корпоративне управління в умовах війни: трансформація державних підприємств України [6]

Документ є комплексним аналітичним оглядом системи корпоративного управління державних підприємств України, який оцінює прогрес реформ після 2021 року, ступінь відповідності стандартам Керівних принципів ОЕСР щодо корпоративного управління державних підприємств (редакція 2024 року) та визначає ключові структурні проблеми і напрями подальших змін. У центрі дослідження знаходиться розуміння державних підприємств як критично важливого елементу економічної системи України, оскільки вони охоплюють понад три тисячі суб'єктів і відіграють домінуючу роль у стратегічних секторах, зокрема енергетиці, транспорті, інфраструктурі та фінансовому секторі, що обумовлює їх значення не лише для економічної ефективності, а й для забезпечення публічного інтересу, стійкості держави та післявоєнного відновлення.



У документі підкреслюється, що з 2021 року Україна здійснила суттєвий нормативно-правовий прогрес, зокрема через прийняття Закону №3587-IX, затвердження політики державної власності, впровадження механізмів класифікації підприємств (так званий triage) та посилення ролі наглядових рад. Ці зміни дозволили значною мірою наблизити формальну архітектуру корпоративного управління до міжнародних стандартів, зокрема у частині визначення ролі держави як власника, встановлення принципів підзвітності, розширення вимог до розкриття інформації та посилення функцій органів управління підприємствами. Водночас документ наголошує, що досягнутий прогрес має переважно нормативний характер, тоді як практична імплементація реформ залишається нерівномірною і суттєво відрізняється між великими стратегічними підприємствами та ширшим портфелем державних активів, де зберігаються слабкі управлінські практики.

Однією з ключових структурних проблем визначено фрагментованість функції держави як власника, коли повноваження розподілені між великою кількістю міністерств, агентств і державних органів, які часто одночасно виконують функції регулятора, політикоформуючого органу та власника. Така модель створює конфлікти інтересів, ускладнює стратегічне управління портфелем державних підприємств і знижує якість нагляду, оскільки відсутній єдиний центр відповідальності та узгоджена політика управління активами. Незважаючи на запровадження політики державної власності, яка формально визначає принципи управління, її практичне застосування є непослідовним, що проявляється у відсутності затверджених стратегічних планів, фінансових документів і чітких цілей для значної частини підприємств.

Окремий значний блок аналізу присвячено умовам функціонування державних підприємств на ринку та проблемі конкурентної нейтральності. Документ відзначає, що в умовах воєнного стану держава запровадила низку виняткових заходів, включаючи мораторії на банкрутство, пільгове фінансування, обмеження застосування правил державної допомоги та інші форми підтримки, які були необхідними для забезпечення економічної стабільності. Проте тривале збереження таких механізмів створює ризики викривлення ринкової конкуренції, витіснення приватного сектору та накопичення прихованих фіскальних зобов'язань, що у перспективі може

[6] https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/04/oecd-review-of-the-corporate-governance-of-state-owned-enterprises-in-ukraine-2026_6e0b273c/149d03e6-en.pdf

негативно вплинути на економічну ефективність і інвестиційну привабливість країни. У цьому контексті підкреслюється необхідність поступового повернення до ринкових принципів функціонування та відновлення повноцінного режиму державної допомоги відповідно до європейських стандартів.

Важливим аспектом є проблема публічних сервісних зобов'язань (PSO), які відіграють значну роль у забезпеченні соціальної стабільності, зокрема у секторах енергетики та транспорту, однак їх фінансування та облік залишаються непрозорими. Витрати на виконання таких зобов'язань часто не відокремлюються від комерційної діяльності підприємств, не відображаються належним чином у звітності та не компенсуються з бюджету, що ускладнює оцінку ефективності діяльності підприємств, приховує реальний фінансовий стан і створює додаткові фіскальні ризики.

Документ також детально аналізує питання прозорості, підзвітності та розкриття інформації. Незважаючи на наявність вимог щодо фінансової звітності, аудиту та переходу до міжнародних стандартів (IFRS), їх фактичне виконання є нерівномірним, а доступ до інформації обмеженим, особливо щодо підприємств, пов'язаних із критичною інфраструктурою або оборонним сектором. Відсутність регулярної агрегованої звітності по всьому портфелю державних підприємств обмежує можливості комплексного аналізу фінансових результатів, оцінки фіскальних ризиків і ефективності державної політики у сфері управління активами.

Суттєва увага приділяється корпоративному управлінню на рівні наглядових рад. Документ визнає значний прогрес у запровадженні незалежних наглядових рад, удосконаленні процедур їх формування та визначенні їх повноважень, однак водночас фіксує проблеми з практичною реалізацією цих механізмів, включаючи затримки у призначенні членів рад, наявність тимчасового керівництва, неповну укомплектованість органів управління та випадки політичного втручання. Це підриває незалежність наглядових рад, обмежує їх здатність здійснювати ефективний контроль і знижує загальний рівень корпоративного управління.

Висновки:

- **Україна досягла значного прогресу у формальному наближенні корпоративного управління державних підприємств до стандартів OECD,** однак ключовим викликом залишається забезпечення повноцінної та однакової імплементації реформ на практиці по всьому сектору ДП.
- **Фрагментована система управління державною власністю, де різні органи одночасно виконують функції власника, регулятора і політикоформуючого суб'єкта,** створює конфлікти інтересів і потребує централізації або ефективної координації функції держави як власника.
- **Збереження воєнних пільг і преференцій для державних підприємств без чіткого плану їх скасування** створює ризики викривлення конкуренції, зростання фіскального навантаження та стримування розвитку приватного сектору.
- **Недостатній рівень прозорості, зокрема відсутність повної агрегованої звітності та розмежування витрат на публічні функції і комерційну діяльність,** обмежує ефективний контроль, ускладнює оцінку ризиків і знижує підзвітність державних підприємств.

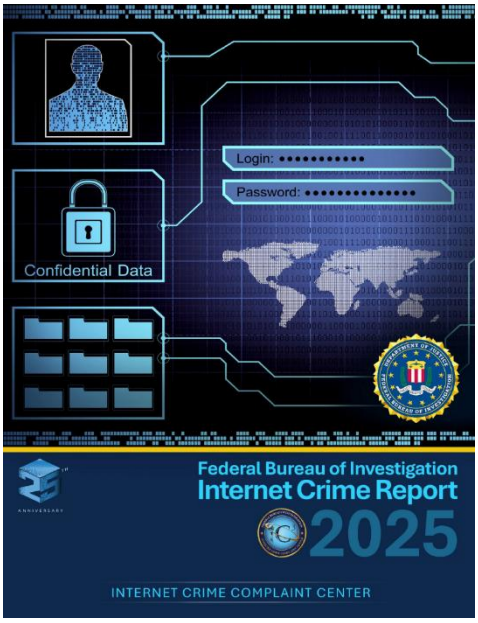
Окремий розділ присвячено питанням доброчесності, антикорупційних механізмів і внутрішнього контролю. Хоча законодавство передбачає обов'язковість антикорупційних програм для державних підприємств, їх реалізація часто носить формальний характер, без належної уваги до ризик-орієнтованого підходу, ефективних внутрішніх контролів та функціонування механізмів викривачів. Це створює підвищені ризики зловживань, неефективного використання ресурсів і корупційних правопорушень, особливо в умовах

значних фінансових потоків, пов'язаних із відновленням економіки та міжнародною допомогою.

Крім того, документ підкреслює зростаючу роль аспектів сталого розвитку, відповідального ведення бізнесу та інтеграції екологічних, соціальних і управлінських факторів (ESG) у діяльність державних підприємств. Незважаючи на наявність окремих ініціатив, системне впровадження таких підходів залишається обмеженим, а показники сталого розвитку не інтегровані повною мірою у систему оцінки ефективності діяльності підприємств.

У цілому, документ формує чітке розуміння того, що Україна перейшла від етапу формування нормативної бази до етапу її практичної реалізації, де ключовими завданнями є забезпечення інституційної спроможності, усунення структурних дисбалансів, підвищення прозорості та підзвітності, а також формування професійної, деполітизованої системи управління державними активами, здатної забезпечити ефективне функціонування державних підприємств у ринкових умовах і підтримати економічне відновлення та інтеграцію до європейського економічного простору.

Криптовалюти, штучний інтелект і шахрайство: нові ризики глобальної фінансової системи [7]



Звіт ФБР за 2025 рік є не просто статистичним оглядом кіберзлочинності, а комплексним стратегічним документом, який відображає глибинну трансформацію глобального кримінального середовища, де цифрові технології стали основною інфраструктурою для генерування, переміщення та легалізації незаконних доходів. Його зміст демонструє, що сучасна кіберзлочинність уже не є окремою категорією злочинів, а інтегрується у ширшу екосистему фінансової злочинності, включаючи шахрайство, організовану злочинність, торгівлю людьми та навіть потенційні ризики фінансування тероризму.

Однією з ключових ідей, яка проходить через увесь документ, є різке зростання ролі саме шахрайських схем як домінуючого джерела кримінальних доходів. Якщо раніше кіберзлочинність асоціювалася переважно з технічними атаками (зламами, вірусами, програмами-вимагачами), то у 2025 році центр тяжіння змістився у бік поведінкових моделей — маніпуляції довірою, соціальної інженерії та психологічного впливу на жертву. Це підтверджується тим, що найбільші фінансові втрати пов'язані саме з інвестиційним шахрайством, яке функціонує як складна багаторівнева схема, що поєднує елементи фінансових пірамід, фіктивних інвестиційних платформ та контрольованих злочинцями цифрових екосистем. Особливістю цих схем є їх тривалість у часі — жертви можуть перебувати у взаємодії зі злочинцями місяцями, поступово збільшуючи обсяги інвестицій, що дозволяє злочинцям акумулювати значні суми коштів перед фінальним етапом шахрайства.

Важливим структурним аспектом є те, що ці схеми дедалі частіше мають індустріальний характер. Звіт прямо вказує на існування організованих шахрайських кол-центрів, які функціонують як бізнес-структури з чіткою ієрархією, розподілом ролей та використанням технологічних інструментів для масштабування діяльності. Залучення жертв торгівлі людьми до

[7] https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

роботи у таких центрах створює складну кримінальну екосистему, де кіберзлочинність переплітається з іншими видами тяжких злочинів. Це має безпосереднє значення для сфери ПВК/ФТ, оскільки такі структури генерують значні обсяги незаконних доходів, які потребують подальшого відмивання через фінансову систему.

Окремої уваги заслуговує роль фінансових інструментів у реалізації шахрайських схем. Звіт демонструє, що криптовалюти стали ключовим каналом переміщення коштів, але не єдиним. Значна частина операцій здійснюється через традиційні банківські інструменти, такі як банківські перекази, платежі через автоматизовану клірингову систему (ACH) та платіжні картки. Це свідчить про те, що злочинці використовують гібридні моделі, комбінуючи традиційні та нові фінансові інструменти для підвищення ефективності та ускладнення відстеження транзакцій. У контексті ПВК це означає, що ризики не можуть розглядатися ізольовано для окремих секторів (банківського чи криптовалютного), а потребують інтегрованого підходу.

Значний акцент у документі зроблено на механізмах викрадення коштів, які демонструють, що злочинці активно використовують різні платіжні канали залежно від типу шахрайства. У випадку шахрайства шляхом компрометації ділової електронної пошти (BEC) основним інструментом переказу коштів виступають банківські перекази, тоді як у схемах інвестиційного шахрайства домінують криптовалюти як ключовий канал переміщення незаконних фінансових активів. Це свідчить про адаптивність злочинних схем та їх здатність використовувати найбільш ефективні інструменти для досягнення конкретної мети.

Важливим елементом аналізу є географічний аспект кіберзлочинності. Звіт підтверджує, що кіберзлочини мають глобальний характер, при цьому злочинці, жертви та фінансові потоки можуть знаходитися у різних юрисдикціях. Це створює серйозні виклики для правоохоронних органів, оскільки розслідування потребують координації між країнами, а також ефективного обміну інформацією. Водночас це підкреслює важливість міжнародних стандартів, таких як

Висновки:

- **Пріоритизація боротьби з інвестиційним та криптошахрайством як ключового джерела незаконних фінансових потоків.** Необхідно інтегрувати ризики криптовалютного шахрайства у національні оцінки ризиків (НОР) та розширити контроль за VASP відповідно до Рекомендації 15 FATF і Travel Rule, оскільки саме цей сегмент формує найбільший обсяг втрат і потенційного відмивання коштів.
- **Впровадження механізмів швидкого реагування (аналог FFKC) у фінансовому секторі.** Фінансові установи та ПФР повинні впровадити чітко регламентовані протоколи оперативного замороження транзакцій, оскільки ефективність повернення коштів безпосередньо залежить від швидкості реагування — практичним орієнтиром є показник близько 58% успішного блокування коштів у США в межах механізму FFKC.
- **Перехід до ризик-орієнтованих моделей протидії шахрайству як предикатному злочину ВК/ФТ.** Шахрайство, зокрема кібершахрайство, повинно розглядатися як одне з ключових джерел кримінальних доходів у системах ПВК, що потребує відповідної адаптації індикаторів підозрілих фінансових операцій (STR) та звітності про порогові операції (CTR), а також оновлення типологій з урахуванням нових цифрових моделей злочинної діяльності.
- **Інтеграція ризиків штучного інтелекту у системи фінансового моніторингу.** Необхідно розробити нові індикатори ризику (червоні прапорці), пов'язані з AI-шахрайствами (діпфейки, синтетична ідентичність), оскільки традиційні KYC/EDD-підходи стають недостатніми в умовах цифрової еволюції загроз.

рекомендації FATF, які забезпечують єдину основу для протидії відмиванню коштів у глобальному масштабі.

Соціально-демографічний аналіз, представлений у звіті, також має важливе значення. Вразливість осіб старшого віку до шахрайських схем свідчить про необхідність розробки спеціалізованих заходів захисту цієї категорії населення, включаючи інформаційні кампанії та посилення контролю з боку фінансових установ. Водночас значна кількість інцидентів серед молодших груп населення демонструє, що кіберзлочинність охоплює всі соціальні групи, але використовує різні підходи до їх експлуатації.

Окремо слід підкреслити роль штучного інтелекту як фактора, що змінює природу кіберзлочинності. Використання AI дозволяє злочинцям створювати більш переконливі сценарії шахрайства, автоматизувати комунікацію з жертвами та масштабувати свої операції. Це означає, що традиційні інструменти виявлення шахрайства, які базуються на статичних правилах або історичних даних, стають менш ефективними. У цьому контексті фінансові установи та ПФР повинні переходити до більш динамічних моделей аналізу ризиків, які враховують поведінкові та контекстуальні фактори.

Звіт також детально описує кіберзагрози, пов'язані з атаками на інфраструктуру, зокрема програми-вимагачі, витоки даних та шкідливе програмне забезпечення. Хоча їхній фінансовий вплив є меншим порівняно з шахрайством, їхній вплив на національну безпеку є значно більшим. Атаки на критичну інфраструктуру можуть призводити до порушення функціонування ключових систем, що має серйозні економічні та соціальні наслідки. Це підкреслює необхідність інтеграції кібербезпеки у ширшу систему національної безпеки.

Особливу практичну цінність має опис операційної діяльності Центру прийому скарг на інтернет-злочини (IC3), зокрема механізму ланцюга протидії фінансовому шахрайству. Цей механізм демонструє, що навіть у складному середовищі цифрових фінансів можливе ефективне реагування на шахрайство за умови швидкої координації між фінансовими установами та правоохоронними органами. Водночас його ефективність значною мірою залежить від своєчасності повідомлення про інцидент, що підкреслює важливість підвищення обізнаності користувачів та бізнесу.

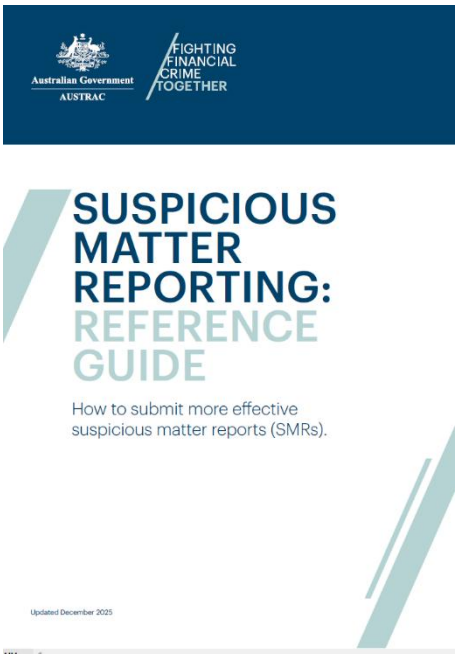
Загалом звіт формує цілісне уявлення про сучасну кіберзлочинність як багатовимірне явище, яке поєднує технологічні інновації, фінансові інструменти та соціальні фактори. Він демонструє, що боротьба з кіберзлочинністю потребує не лише технічних рішень, але й системного підходу, який включає регулювання фінансового сектору, міжнародну співпрацю, підвищення фінансової грамотності населення та розвиток аналітичних можливостей державних органів. Для сфери ПВК/ФТ цей документ є важливим джерелом типологій та індикаторів ризику, які можуть бути використані для вдосконалення систем фінансового моніторингу та підвищення ефективності протидії відмиванню коштів у цифрову епоху.

Нові підходи до підозрілих повідомлень: як SMR стає інструментом виявлення фінансових злочинів [8]

Документ представляє собою практично орієнтовану методологію підвищення ефективності подання повідомлень про підозрілу діяльність (SMR) як ключового інструменту фінансової розвідки у системі ПВК/ФТ, при цьому його зміст чітко демонструє перехід від формального виконання регуляторних вимог до формування якісного аналітичного продукту, який може бути безпосередньо використаний правоохоронними органами для виявлення, відстеження та

[8] https://www.austrac.gov.au/sites/default/files/2025-12/AUSTRAC%20Suspicious%20Matter%20Reporting%20-%20Reference%20Guide%20December%202025.pdf

припинення фінансових потоків, пов'язаних із відмиванням коштів, фінансуванням тероризму та іншими формами серйозної та організованої злочинності.



У центрі документа знаходиться теза про те, що SMR є не просто звітністю, а критичним джерелом фінансової розвідувальної інформації, і саме якість, повнота та структурованість такого повідомлення визначають його подальшу аналітичну цінність; підкреслюється, що звіти з нечітким описом, відсутністю логіки або ключових даних фактично втрачають здатність бути використаними у фінансових розслідуваннях, що прямо впливає на загальну ефективність національної системи ПВК/ФТ. Документ наголошує, що інформація, яка генерується через SMR, відіграє центральну роль у виявленні незаконної діяльності та формуванні оперативних аналітичних матеріалів для поліції та інших уповноважених органів, а отже, вимоги до якості SMR мають розглядатися як елемент національної безпеки.

Значна увага у документі приділяється правовим аспектам подання SMR, де роз'яснюється обов'язок підзвітних суб'єктів подавати звіти у випадках наявності обґрунтованої підозри, що формується на основі аналізу всіх доступних даних та результатів проведення посиленої перевірки клієнта (EDD); при цьому використовується концепція «об'єктивної особи» (reasonable person), яка передбачає, що рішення про подання SMR має базуватися на об'єктивному стандарті поведінки розсудливої особи, що відображає міжнародний ризик-орієнтований підхід FATF. Документ також чітко визначає часові рамки подання: 24 години для підозр щодо фінансування тероризму та 3 робочі дні для інших видів підозрілої діяльності, наголошуючи, що будь-яке зволікання істотно знижує здатність держави реагувати на злочинну активність у режимі реального часу.

Окремий акцент зроблено на принципі заборони розголошення факту подання повідомлення, який передбачає сувору конфіденційність факту подання SMR та захист розслідувань, водночас документ гарантує правовий захист суб'єктів, що подають звіти, від цивільної чи кримінальної відповідальності за розкриття інформації у межах виконання законодавчих вимог, що створює баланс між обов'язком повідомлення та захистом добросовісних суб'єктів фінансового моніторингу.

Змістовно важливою частиною документа є розкриття підходів до ідентифікації підозрілої діяльності через систему індикаторів, або «червоні прапорці», які включають класичні типології відмивання коштів, такі як структурування операцій для уникнення порогових значень, багаторівневе «нашарування» транзакцій з метою приховування походження коштів, нетипові або непропорційні обсяги операцій, транзакції з високоризиковими юрисдикціями, використання підроблених або викрадених ідентифікаційних даних, а також поведінкові аномалії клієнтів; при цьому підкреслюється, що самі по собі індикатори не є достатніми, і їх необхідно інтегрувати у логічно обґрунтовану підозру, що пояснює причинно-наслідковий зв'язок між фінансовою активністю та потенційним злочином.

Документ детально описує, яким має бути ефективний SMR з точки зору структури та змісту, фактично встановлюючи стандарт написання аналітичного наративу: інформація повинна бути викладена простою, зрозумілою мовою без використання внутрішнього жаргону, логічно структурована, містити чітку хронологію подій та відповідати шести ключовим елементам — хто, що, де, коли, чому і як; така структура дозволяє перетворити SMR на повноцінний аналітичний

продукт, придатний для використання у кримінальних розслідуваннях і подальшому розвідувальному аналізі. Окремо наголошується на необхідності зазначення типу ймовірного злочину, навіть якщо він визначений лише як гіпотеза, оскільки це суттєво підвищує ефективність подальшої аналітичної обробки інформації.

Важливим компонентом є інтеграція інформації, отриманої в рамках процедур KYC та посиленої перевірки клієнта, де підкреслюється, що ефективний SMR повинен містити не лише транзакційні дані, а й повний контекст клієнта, включаючи його профіль, джерела доходів, поведінкові характеристики, пов'язаних осіб, історію взаємодії та будь-які результати додаткових перевірок, включаючи відкриті джерела або цифрові сліди; такий підхід забезпечує можливість побудови комплексної картини ризику та виявлення складних схем фінансових злочинів.

Документ також чітко розмежовує функції SMR та повідомлення про злочин до правоохоронних органів, наголошуючи, що SMR є інструментом фінансової розвідки, тоді як у випадках безпосередньої загрози необхідно негайно інформувати поліцію; водночас дозволяється паралельне повідомлення різних органів, що підкреслює важливість міжвідомчої взаємодії та координації у боротьбі з фінансовими злочинами.

Суттєву аналітичну цінність має блок із прикладами ефективних та неефективних SMR, який демонструє типові помилки, такі як відсутність конкретних фінансових даних, нечіткість формулювань, використання загальних фраз без доказової бази, надмірне використання акронімів або внутрішнього жаргону, а також несвоєчасність подання; через ці приклади документ фактично формує практичний стандарт якості SMR, орієнтований на забезпечення максимальної корисності для подальшого аналізу.

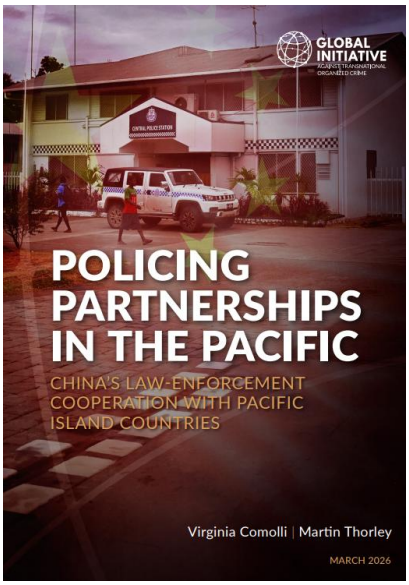
У цілому, документ відображає сучасну концепцію розвитку системи ПВК/ФТ, у якій ключовим елементом є не формальне дотримання процедур, а здатність суб'єктів фінансового моніторингу генерувати якісну, структуровану та аналітично обґрунтовану інформацію, що може бути оперативно використана ПФР та правоохоронними органами, і таким чином виступає важливим елементом переходу до орієнтованої на розвідувальну аналітику модель ПВК, яка базується на інтеграції даних, аналітики та міжвідомчої співпраці.

Висновки:

- **Якість SMR є критичним фактором ефективності ПФР та правоохоронних органів** Необхідно впровадити внутрішні стандарти якості SMR (структура, опис індикаторів, KYC), оскільки неякісні звіти фактично нівелюють аналітичну функцію фінансового моніторингу.
- **Своєчасність подання SMR прямо впливає на можливість припинення злочинної діяльності.** Фінансові установи мають забезпечити оптимізацію внутрішніх процедур (ідентифікація ризикових індикаторів → проведення EDD → ухвалення рішення → подання SMR) з метою дотримання встановлених строків подання (24 години / 3 робочі дні), оскільки їх порушення призводить до втрати оперативної цінності фінансової інформації.
- **SMR має бути аналітичним продуктом, а не описом транзакцій.** Рекомендується здійснити перехід від описового підходу до аналітичного, що передбачає формування чіткої гіпотези щодо можливого злочину, встановлення логічного зв'язку між виявленими індикаторами та підозрою, а також використання структурованого викладення обставин.
- **Інтеграція KYC/EDD у SMR є ключем до виявлення складних схем ВК/ФТ.** Фінансові установи повинні забезпечити повну інтеграцію клієнтських даних, поведінкових характеристик та результатів перевірок у SMR, що дозволяє ПФР проводити глибший фінансовий аналіз і виявляти мережеві зв'язки.

Звіти окремих інституцій та експертів

Тихоокеанський пазл Пекіна: поліцейська допомога як інструмент гібридного впливу [9]



Опублікований GI-TOC звіт, є однією з найбільш ґрунтовних і неупереджених спроб проаналізувати феномен, який донедавна залишався в тіні військових аспектів китайської експансії.

Автори документа — команда дослідників, яка провела близько шістдесяти інтерв'ю з ключовими інформаторами в Океанії, Європі та США, а також опрацювала масив закритих і відкритих джерел, включно з китайськими державними медіа та внутрішніми документами, — доходять парадоксального, але добре обґрунтованого висновку. Китайська присутність у поліцейській сфері південної частини Тихого океану не є ані тотальним захопленням безпекового сектору, ані суто символічною дипломатією. Це радше гнучкий, політично чутливий і стратегічно кумулятивний підхід, який у різних контекстах набуває різних форм.

У деяких країнах він залишається скромним і технічним, тоді як в інших стає глибоко вкоріненим і геополітично вагомим. Центральна динаміка, як зазначається в документі, — це не заміщення Австралії, Нової Зеландії чи США, а радше перекалібрування всієї системи міжнародних відносин у регіоні. Китайська активність змінила очікування місцевих еліт, прискорила конкуренцію та підвищила політичні ставки в тому, що колись вважалося суто технічною сферою поліцейської допомоги.

Методологія дослідження заслуговує на окрему увагу, оскільки вона пояснює, чому висновки GI-TOC є надійними. Автори не обмежилися аналізом відкритих угод чи заяв дипломатів. Вони провели польову роботу в самих вразливих спільнотах, зокрема в неформальних поселеннях Хоніари, де «китайські поліцейські групи зв'язку» (CPLT) впроваджують свої моделі «громадського поліціювання». Більшість інтерв'ю проводилися анонімно через делікатність теми та дипломатичні ризики, що дозволило респондентам — від рядових поліцейських Соломонових Островів до високопоставлених чиновників Фіджі та Вануату — говорити відверто. Кількісні дані про китайську допомогу були взяті з бази AidData, що відстежує китайське фінансування розвитку з 2000 року. Важливо, що дослідники свідомо уникають монолітного сприйняття «Китаю», нагадуючи, що в регіоні діють різні агенти: від центрального уряду та Міністерства громадської безпеки (MPS) до провінційних адміністрацій Гуандуну та Фуцзянь, а також численних китайських діаспор, чиї інтереси часто не збігаються. Цей нюанс є критично важливим для розуміння того, чому китайська поліцейська активність виглядає такою фрагментованою й адаптивною.

Щоб зрозуміти масштаб явища, необхідно згадати історичний контекст. Історично Китай не був великим донором правоохоронної допомоги за кордоном. На відміну від військової підтримки, яку Пекін надавав повстанським групам в Азії та Африці ще в 1970-1980-х роках, поліцейське співробітництво тривалий час залишалося мізерним. Проте починаючи з початку 2000-х, а

[9] https://globalinitiative.net/wp-content/uploads/2026/03/Policing-partnerships-in-the-Pacific-Chinas-law-enforcement-cooperation-with-Pacific-Island-countries-GI-TOC-March-2026.pdf

особливо після проголошення «Комплексної концепції національної безпеки» в 2014 році, ситуація кардинально змінилася.

Ключовим поштовхом стало створення Глобальної ініціативи безпеки (GSI) в 2022 році, яку дослідники називають «улюбленим механізмом Сі Цзіньпіна для екстерналізації комплексної концепції національної безпеки». GSI, яку часто розглядають як пряму альтернативу американській архітектурі безпеки, передбачає підготовку тисяч іноземних поліцейських, обмін досвідом між академіями та зміцнення потенціалу країн Глобального Півдня у сфері боротьби з тероризмом, кіберзлочинністю та захистом інвестицій. У 2024 році державний радник і міністр громадської безпеки Ван Сяохун оголосив про намір підготувати 3000 іноземних правоохоронців протягом наступних дванадцяти місяців. Ці цифри красномовно свідчать про те, що поліцейська допомога перетворилася на один із головних інструментів китайської великої стратегії.

Для тихоокеанського регіону це має особливе значення, оскільки більшість місцевих держав — за винятком Фіджі, Папуа-Нової Гвінеї та Тонго — не мають власних збройних сил, які могли б стати об'єктом військової співпраці. Поліція тут є головним, а часто й єдиним інститутом забезпечення суверенітету та внутрішнього порядку. Тому китайське проникнення саме в поліцейську сферу є стратегічно більш ефективним і менш помітним, ніж розгортання військових баз.

Дослідження 2024 року показало, що понад 50% безпекових угод у десяти найбільших країнах Океанії укладено з Австралією, за якою йдуть Нова Зеландія, США та Китай. Але саме динаміка змін викликає занепокоєння. Якщо традиційні партнери діють через громіздкі механізми парламентського контролю, прозорість та умови дотримання прав людини, то Китай пропонує «швидку допомогу без зайвих питань». Саме ця різниця в швидкості та умовності стає його головною конкурентною перевагою.

Розглядаючи конкретні кейси, дослідження GI-TOC виділяє цілий спектр взаємодій — від гучних угод до майже непомітної інфраструктурної підтримки. Острови Кука, наприклад, демонструють останню категорію. Тут немає сенсаційних безпекових пактів, але ще в 2004 році Китай надав грант у 2,8 мільйона доларів на будівництво штаб-квартири поліції, а в 2025 році було оголошено про всебічне стратегічне партнерство. Це спричинило дипломатичне напруження з Новою Зеландією, яка навіть заморозила частину своєї допомоги.

У Самоа за китайські кошти звели нову Поліцейську академію, відкриту в 2024 році, хоча вже за рік у будівлі з'явилися тріщини, а місцеві експерти заговорили про невідповідність інфраструктури потребам. Водночас самоанські поліцейські отримують мовні курси мандаринської, музичні інструменти для поліцейського оркестру та беруть участь у семінарах із цивільного миротворення. Це не хаотична допомога, а продумана система «м'якої сили», де кожен елемент — від барабанів до академій — працює на формування позитивного образу Китаю.

Особливо показовим є випадок Вануату. Ця країна з довгою історією політики нейтралітету та невизначеності стала полем жорсткої конкуренції. Ще в 2004 році Вануату підписала угоду з КНР про підготовку спецпризначенців. У 2018 році з'явилися повідомлення про те, що Пекін запитував дозвіл на створення військової бази — тоді прем'єр-міністр запевнив Австралію, що цього не станеться, але аналітики припускають, що сам факт переговорів змусив Китай змінити тактику на більш поступову.

У 2023 році, під час політичної кризи, до Вануату прибули китайські поліцейські експерти. А вже в січні 2026 року CPLT у Вануату розширилася з чотирьох до чотирнадцяти офіцерів. Але найбільш тривожним сигналом, зафіксованим дослідниками, є зміна поведінки цих офіцерів.

Вони відкрито фотографують радників з інших країн, їхніх дружин та дітей у неробочий час, що сприймається не як звичайна розвідка, а як цілеспрямований психологічний тиск.

Перехід до кейсів Фіджі та Соломонових Островів дозволяє авторам доповіді простежити еволюцію китайської стратегії в часі. Фіджі довгий час вважалося головним поліцейським партнером Китаю в регіоні. Ще в 2011 році було підписано меморандум про взаєморозуміння, який дозволяв співпрацю в депортаціях та підготовці кадрів. У 2017 році китайська поліція провела екстрадицію 77 громадян КНР, підозрюваних у кібершахрайстві, без офіційного запиту фіджійського суду — фактично позасудова депортація.

За часів військового правління Френка Байнімарами, коли традиційні партнери відмовили Фіджі в підтримці через переворот, Китай став зручною альтернативою. Але після повернення до цивільного правління на чолі з Сітівені Рабукою в 2022 році ситуація змінилася. Рабука розірвав меморандум, заявивши: «Наша система демократії та правосуддя відрізняється, тому ми повернемося до тих, хто має подібні системи». Однак, як зазначають автори, це не означає повного розриву. Фіджі продовжує відправляти офіцерів на тренування до Фуцзяньського поліцейського коледжу, але відмовляється приймати китайських інструкторів у себе. Один з інсайдерів назвав ці поїздки «підтриманням дипломатичних відносин, щоб Китай був задоволений», а не реальним нарощуванням спроможності.

Натомість Соломонові Острови стали новим епіцентром. Рішення 2019 року розірвати відносини з Тайванем та визнати Китай відкрило шлюзи для китайської допомоги. У 2021 році в Хоніарі спалахнули заворушення, під час яких було розгромлено квартал Чайна-таун. Китайське посольство звернулося з проханням дозволити ввезення зброї та озброєної охорони з дипломатичним статусом для захисту своїх громадян — у проханні було відмовлено, але вже в 2022 році в країні з'явилася перша група CPLT. На сьогодні в Соломонових Островах діє 14 китайських поліцейських, які працюють за ротацією кожні 6-9 місяців. Вони провели щонайменше 70 тренувальних програм, підготували поліцію до Тихоокеанських ігор 2023 року, навчали спецпризначенців для змагань SWAT Challenge у Дубаї, а також почали впроваджувати концепцію «зразкових громад китайсько-соломонівської поліцейської співпраці». Газета People's Daily у квітні 2022 року опублікувала статтю під псевдонімом, в якій звинуватила США та Австралію в поширенні «фальшивих тверджень» і «гегемоністському мисленні», наголосивши, що Китай «щиро допомагає острівним державам розвиватися».

Одним із найбільш несподіваних та водночас показових напрямків китайської діяльності, який дослідники GI-TOC висвітлили з безпрецедентною деталізацією, є сфера «підтримки громадської безпеки» (community policing). Традиційно цей підхід, що передбачає тісну взаємодію поліції з громадою, довіру та спільне вирішення проблем, вважався козирем демократичних країн. Однак Китай просуває альтернативну модель — так званий «досвід Фенцяо», названий на честь містечка в провінції Чжецзян, де в 1960-х роках маоїстський режим випробував методи масового залучення населення до «виправлення реакційних елементів» через публічні приниження та «зізнання». Після десятиліть забуття цей досвід пережив ренесанс за Сі Цзіньпіна.

Сучасна версія Фенцяо включає «нові громадські ініціативи з самоуправління та корекції», але на практиці передбачає тотальний облік, біометрію, систему камер спостереження та додаткову гнучкість для поліції у затриманнях без ордера. На Соломонових Островах CPLT активно впроваджує цю модель. У вересні 2025 року було офіційно оголошено про запуск «зразкових громад», що викликало міжнародний резонанс і хвилю критики в місцевих соцмережах. RSIPF довелося виступати з роз'ясненням, що це не запозичення китайських методів стеження, а «культурно сумісна модель, що ґрунтується на сімейних зв'язках і колективній відповідальності».

Дослідники GI-TOC отримали доступ до трьох громад, де реалізується ця програма, зокрема до гучного проєкту Fighter One, а також до громад Вестерн-Хоніара та Агапе. У громаді Агапе, яка раніше вважалася «червоною зоною» через алкоголізм, бійки та сексуальне насильство, китайська допомога справді дала результат. CPLT надала сонячні ліхтарі, спортивний інвентар для молоді, уніформу для місцевої добровільної дружини, провела тренінги з поводження з буйними правопорушниками. Жінки в Агапе заявили, що тепер почуваються безпечніше. Однак вони ж поскаржилися, що їх не навчають користуватися отриманими швейними машинками, а єдина жінка-офіцер CPLT не спілкувалася з ними жодного разу — всі переговори ведуться виключно зі старійшинами-чоловіками. Більше того, китайські радники проводять тотальний облік, збирають відбитки пальців та обіцяють встановити камери спостереження. Мешканці, хоча й потребують допомоги, ставляться до цього з явним занепокоєнням.

У громаді Fighter One, де спочатку планувалося створити «зразкову громаду», китайські пропозиції щодо біометрії наштовхнулися на відкритий спротив. Люди заявили, що «не хочуть, щоб за ними стежили», і що вони відчувають себе «інструменталізованими в геополітичній конкуренції між Китаєм та Австралією». Один зі співрозмовників сказав: «Конкуренція між донорами не призводить до кращого». Тепер ця громада планує звернутися до Австралії по вуличне освітлення, а якщо австралійці відмовлять — знову до Китаю. Це ілюструє головний парадокс: Китай заповнює прогалини, але його методи викликають недовіру, а місцеві громади зберігають здатність до стратегічного маневру.

Окремий розділ доповіді присвячений тривожному зв'язку між китайською поліцейською активністю та кримінальними мережами. Тут автори наводять два яскравих приклади. На Фіджі фігурує Чжао Фуган, китайський бізнесмен, якого OCCRP називає «об'єктом австралійських кримінальних розслідувань». У 2021 році Чжао виступав на спільному заході посольства КНР, поліції Фіджі та китайської діаспори, де вручив поліції чек на 15 000 доларів Фіджі. Він був представлений як директор «Центру допомоги китайцям Фіджі» та закликав діаспору «активно інтегруватися в місцеву громаду».

У Папуа-Новій Гвінеї аналогічну роль відіграє Лінь Хуань (Біллі Лін), виходець із Фуцзянь, який отримав громадянство та звання «старшого офіцера резерву Королівської поліції Папуа-Нової Гвінеї». Він брав участь у тренувальних програмах у Китаї, з'являвся на публічних заходах у поліцейській уніформі разом із китайськими радниками. Дослідники GI-TOC зазначають, що це не поодинокі випадки, а частина ширшої стратегії «єдиного фронту», де толерантність до кримінальних зв'язків виправдовується геополітичними дивідендами. Ризик полягає в тому, що поліцейські інститути тихоокеанських держав можуть бути скомпрометовані через асоціацію з особами, які мають сумнівне минуле.

Аналізуючи вплив на традиційних партнерів, автори доповіді виділяють структурні недоліки, сприйняття, ризики та несподівані можливості. Структурні недоліки Австралії, Нової Зеландії та США очевидні: вони змушені дотримуватися вимог прозорості, прав людини та парламентського контролю, що сповільнює надання допомоги. Китай не має таких обмежень. Він може поставити поліцейські автомобілі за тиждень, тоді як західному донору потрібні місяці лише на тендер. Китайські чиновники практикують дарування подарунків, що резонує з місцевими звичаями, тоді як західні радники часто сприймаються як бюрократичні та відсторонені.

З іншого боку, зростання китайської активності спровокувало безпрецедентну мобілізацію Заходу. Було запущено Тихоокеанську поліцейську ініціативу (Pacific Policing Initiative), укладено оборонний договір між Австралією та Папуа-Новою Гвінеєю (перший австралійський альянс за 70 років), а також договір з Тувалу. Китайська присутність, таким чином, парадоксальним чином посилила увагу до регіону, який раніше сприймався як «тихий задній двір».

Завершується звіт розгорнутим переліком ризиків та рекомендацій, які заслуговують на цитування. Серед ризиків для тихоокеанських держав: нормативна дивергенція (нав'язування моделі, де безпека режиму переважає над верховенством права), інституційна фрагментація через паралельні потоки допомоги, технологічна вразливість (потенційний доступ Китаю до біометричних баз даних та систем спостереження), тиск через діаспору (розмивання межі між легітимним і політичним переслідуванням), а також репутаційні та геополітичні втрати (сприйняття як «китайського сателіта»).

Серед вигод, які не слід ігнорувати: заповнення ресурсних прогалин, доступ до навчань з кіберзлочинності та боротьби з наркотиками (Китай є найбільшим виробником прекурсорів, тому його досвід тут унікальний), а також диверсифікація партнерств, що посилює стратегічну автономію малих держав. Автори наголошують: ці ризики не матеріалізуються автоматично. Вони залежать від внутрішнього нагляду, правових гарантій, механізмів прозорості та спроможності тихоокеанських інституцій визначати й забезпечувати чіткі параметри співпраці.

Рекомендації адресовані трьом групам. Для лідерів держав: розробити чіткі національні рамки регулювання іноземної поліцейської допомоги з парламентським наглядом, проводити регулярні оцінки ризиків іноземних технологій, інвестувати в громадське поліціювання та механізми підзвітності.

Для традиційних партнерів: підвищити гнучкість у наданні запитуваної допомоги, уникати бінарного сприйняття (демократія проти автократії), підтримувати регіональні механізми під керівництвом місцевих жителів.

Для всіх партнерів без винятку: слухати пріоритети Океанії, поважати суверенітет, забезпечувати прозорість угод.

Головний висновок звіту звучить так: еволюція китайської поліцейської присутності не віщує неминучого переформатування регіону. Натомість вона висвітлює здатність тихоокеанських держав орієнтуватися в дедалі більш багатополярному середовищі.

Висновки:

- **Не заміщення, а перекалібрування.** Китай не витісняє Австралію чи США з регіону, але змінює правила гри: швидка допомога без умов змушує традиційних партнерів конкурувати, підвищуючи політичну ціну навіть технічної співпраці.
- **Соломонові Острови — новий епіцентр.** Після Фіджі, Пекін змістив фокус на Соломонові Острови, розгорнувши там постійні поліцейські групи (CPLT), що стало «якісним зрушенням» від символічної присутності до оперативного контролю.
- **Досвід «Фенцяо» в Океанії.** Китай експортує власну правоохоронну модель, яка на місцевому рівні вирішує проблеми безпеки, але несе із собою тотальний облік, що суперечить місцевим уявленням про приватність.
- **Ризик кримінальної компрометації.** Діяльність КНР у регіоні пов'язана з фігурами, що мають кримінальне минуле, які використовуються в рамках стратегії «єдиного фронту», створюючи загрозу корупції поліцейських інституцій.

Центральне питання полягає не в тому, чи залишиться Китай, а в тому, чи зможуть місцеві інституції та їхні партнери забезпечити, щоб будь-яка зовнішня допомога — китайська чи західна — зміцнювала, а не підривала відповідальну та орієнтовану на громаду політику безпеки. У цьому мінливому ландшафті стійкість, прозорість і повага до суверенітету будуть важити більше, ніж тимчасова політична вигода.

Як війна в Ємені знищила державну монополію на мармурові родовища [10]

Багаторічна громадянська війна в Ємені, яка триває вже понад десять років, давно перестала бути просто збройним конфліктом між хуситами та міжнародно визнаним урядом. Вона перетворилася на глибоку системну катастрофу, що зруйнувала традиційні інституції, змінила саму тканину суспільства та породила нові, гібридні форми влади, де військова сила, племінна лояльність і бізнес-інтереси злилися в єдиний, майже нерозривний клубок.

Одним із найяскравіших і водночас найбільш драматичних прикладів цієї трансформації є провінція Маріб – останній бастіон формального спротиву на півночі країни та, що не менш важливо, регіон, багатий на природні ресурси, зокрема мармур високої якості. Саме тут, серед спекотних, випалених сонцем пустельних ландшафтів, розгорнулася історія, яка ілюструє остаточну маргіналізацію державного регулювання та тріумф архаїчного, але надзвичайно живучого принципу: право сили та племінної традиції переважає будь-які закони.

У центрі цієї історії – постать Абдулли Ахмеда Алі Шавдака, людини, яка втілює новий тип єменського лідера, породженого війною. Він не просто шейх або племінний старійшина, який вирішує суперечки за чашкою кави. Він – лідер впливового племені Обіда, військовий командир, чиї загони відіграли ключову роль у стримуванні наступу хуситів на Маріб, і водночас успішний підприємець, який контролює один із найприбутковіших бізнесів у регіоні.

Журналісти OCCRP застали його в його стихії: білосніжна сорочка, камуфляжна хустка на голові, а навколо – ціла армія молодих чоловіків у військовій формі, з автоматами та раціями. Ці люди – не просто охорона, це його міліція, яка супроводжує його звивистими дорогами, що перетинають гірський хребет Танія. Саме там, на схилах цих гір, розташовані мармурові кар'єри, які приносять Шавдакові величезні прибутки.

Він особисто розповів репортерам, що на його підприємствах працюють тисячі робітників, які за допомогою важкої техніки – екскаваторів, бульдозерів, алмазних пилок – видобувають, розрізають і готують до транспортування багатотонні брили цінного каменю. Пояснення того, як його родина отримала контроль над цими багатствами, просякнуте фаталізмом, характерним для племінної культури: «У кожного є доля, яка йому написана», – так він прокоментував історію про те, як його батько колись випадково натрапив на поклади мармуру серед пустельних пагорбів.

Однак є одне «але», яке перетворює цю ідилію племінного капіталізму на кричущий приклад беззаконня. Згідно з чинним законодавством Ємену, усі природні ресурси, включаючи мармур, є виключною власністю держави. Їхній видобуток регулюється системою ліцензій, яка передбачає отримання дозволів, сплату зборів та податків, а також дотримання екологічних та технічних норм.

На папері ця система існує й досі. На практиці ж, як визнає Анвар Касім Саїд, директор департаменту корисних копалин у структурі ліцензійного органу, що підпорядковується міжнародно визнаному уряду Ємену (IRG), з початку війни в 2014 році не було видано жодної офіційної ліцензії на видобуток мармуру в провінції Маріб. Це офіційне визнання власного

[10] https://www.occrp.org/en/feature/tribal-rule-trumps-regulation-as-yemen-warlords-plunder-marble

безсилля є ключем до розуміння ситуації: держава, розірвана на частини, позбавлена ресурсів і легітимності в очах багатьох громадян, просто неспроможна забезпечити дотримання своїх законів. Як наслідок, мармуровий сектор Марібу перетворився на «дикий Захід» без правил.

Найцікавішим у цій історії є те, як сам Шавдак намагається балансувати між відвертим викликом системі та спробами надати своїй діяльності хоч якоїсь видимості легальності. Під час першої зустрічі з журналістами він був напрочуд відвертим. Він заявив, що керує кар'єрами без ліцензії, а з початком війни припинив будь-які виплати державі. Аргументація Шавдака звучить цинічно, але водночас напрочуд логічно в контексті єменських реалій: «Ми готові платити державі будь-що, але вона повинна забезпечити нас паливом, електрикою та основними послугами». Він звинуватив державу в недбалості та фактично переклав відповідальність за безвладдя на сам уряд.

Це класичний прояв логіки, яка панує в багатьох слабких державах: податки тут – не громадянський обов'язок, а радше данина за конкретні послуги, яких слабка держава надати не може. Однак, коли розмова продовжилася телефоном, тон Шавдака різко змінився. Він уже стверджував, що має ліцензію та справно сплачує щорічні внески. Відчуваючи, що журналісти зайшли надто далеко в розслідуванні, він звинуватив їх у провокації та втручанні в його особисті справи. На вимогу надати докази він надіслав кілька документів, які підтверджували сплату податку на прибуток його компанією, але жодним чином не доводили наявності ліцензії на користування надрами. Ця метаморфоза – від войовничого заперечення держави до спроб симулювати лояльність – демонструє глибоку амбівалентність племінних лідерів: вони хочуть бути незалежними від держави, але розуміють цінність легальної вивіски, особливо коли йдеться про міжнародну торгівлю та потенційні санкції.

Однак Шавдак – далеко не єдиний гравець на цьому полі, і, можливо, навіть не найрадикальніший. Набагато відвертішим у своєму запереченні державної власності є інший племінний лідер, Алі Абдалла Салех Рукайсіан. Стоячи посеред безкрайньої пустелі, під палючим сонцем, він виглядає як жива ілюстрація до середньовічних уявлень про владу. Його одяг прикрашає традиційний єменський кинджал – джембія – символ чоловічої гідності та незалежності. Говорить Рукайсіан без жодних дипломатичних увертюр. «Ця гора – моя», – заявляє він, жестом вказуючи на скельний масив. Він не апелює до законів чи ринкових механізмів, його аргументація базується виключно на «законах предків, традиціях і звичаях» та на рішенні якогось старшого шейха, який нібито давним-давно «розсудив це питання» на його користь.

Для Рукайсіана поняття держави як абстрактного носія суверенітету над надрами є чимось абсолютно чужим, нав'язаним ззовні. «Я не плачу державі нічого. Ми не платимо і не будемо платити… Держава хоче тримати громадянина під своєю п'ятою. … Після нафти тепер вони хочуть забрати нашу важку працю? Ні», – кидає він виклик. Ця заява – не просто емоційний спалах. Це цілісна ідеологія племінного капіталізму, де право сили (яке ототожнюється з правом володіння), стародавня традиція та особиста інвестиція в розробку кар'єру в один голос заперечують легітимність будь-якої центральної влади. Варто зазначити, що Рукайсіан, за його ж словами, усвідомив цінність ділянки понад десять років тому, відкрив кар'єр, а згодом передав його інвестору за 100 000 саудівських ріалів (близько 26 000 доларів). Він отримав свій прибуток, і держава, за його логікою, тут взагалі ні до чого.

Наслідки такого становища для економіки Ємену, яка й без того перебуває в стані глибокої депресії, є катастрофічними. Йдеться не лише про втрачені мільйони доларів податків, які могли б піти на відновлення інфраструктури, виплату зарплат учителям і лікарям або закупівлю продовольства для мільйонів голодуючих. Йдеться про створення паралельної, тіньової економіки, яка живиться природними ресурсами країни, але не дає їй жодного зиску. Мармур, який видобувається в Марібі, здавна був традиційним будівельним матеріалом, але має й

значний експортний потенціал. Величезні брили, що лежать просто в піску, транспортуються вантажівками на внутрішній ринок або до сусідніх країн – Саудівської Аравії та Оману. При цьому ті, хто фактично виконує всю важку роботу, отримують копійки. Журналісти поспілкувалися з одним із кар'єрних робітників, Джамалем Абдо Абдуллою аль-Кушайбом. Цей чоловік, одягнений у простий одяг, зі зморшкуватим від сонця обличчям, розповів, що його місячна зарплата становить 180 000 єменських ріалів. За офіційним курсом це близько 750 доларів – сума, яка може здатися не надто маленькою, але в умовах гіперінфляції та руйнації ринків Ємену її ледве вистачає, щоб прогодувати дружину та шістьох дітей. Він не отримує жодних соціальних гарантій, жодного захисту, і його доля повністю залежить від примхи племінного ватажка, який «володіє горою».

До війни Світовий банк опублікував звіт, у якому зазначалося, що інвестиції в розробку нових великих кар'єрів у секторі мармуру та граніту Ємену могли б генерувати від 20 до 30 мільйонів доларів щорічних продажів. Тоді головною перешкодою вважали відсутність транспортної та експортної інфраструктури.

Війна не лише не вирішила цю проблему, але й значно поглибила її. Вона розколола країну на дві частини: на півдні, в Адені, розташувався міжнародно визнаний уряд, який підтримує Саудівська Аравія, а північ, в Сані, контрольують хусити, які отримують допомогу від Ірану. Логістичні маршрути, якими віками пересувалися каравани, виявилися перерізаними лініями фронту. Старі дороги закриті або надто небезпечні. Нові ж шляхи, прокладені через відкриту пустелю, стали джерелом ще одного виду незаконного доходу. Таким чином, виникає ціла екосистема неформального оподаткування: племена контролюють не лише кар'єри, але й дороги, стягуючи данину з усіх, хто намагається вивезти мармур. Це робить будь-який законний бізнес практично неможливим, а будь-яку спробу держави встановити контроль – фарсом.

Ситуація з мармуром у Марібі також є яскравою ілюстрацією тотальної інформаційної та інституційної фрагментації, яка є візитівкою сучасного Ємену. Простежити, кому належить той чи інший кар'єр, хто отримує прибутки, а головне – куди ці гроші йдуть далі, практично неможливо навіть для професійних розслідувачів. Державні реєстри, як і сама держава, розколоті на дві частини.

Компанія Шавдака, яка має гучну назву «Abdullah Ahmed Bin Shawdaq for Marble & Granite Establishment», активно рекламує свої послуги з різання білого мармуру на замовлення у Facebook. Журналістам він продемонстрував комерційну реєстраційну картку, видану урядом IRG у 2022 році. Однак, коли вони спробували знайти цю компанію в офіційному онлайн-реєстрі того ж таки уряду, її там не виявилося. Це може свідчити про корупцію всередині реєстраційних органів, про видачу «липових» документів або просто про катастрофічний стан ведення реєстрів. У будь-якому разі, це ще один доказ того, що наявність паперових документів не означає реальної легальності.

Однак найбільш тривожним аспектом цієї історії є те, як мармурові кар'єри стають джерелом не лише економічного, але й прямого військового насильства. Племена в Ємені завжди були потужним фактором політичного життя, але війна радикалізувала їхню роль. У Марібі їхня сила напряму пов'язана з військовою динамікою. Особливо після 2020 року, коли племінні загони зіграли вирішальну роль у битвах проти хуситів, вони стали незамінним союзником міжнародно визнаного уряду. Але цей союз – крихкий і прагматичний, заснований на спільному ворогові, а не на спільних цінностях.

І найкращим доказом цього є криваві сутички, які вже спалахували навколо кар'єрів. У травні 2025 року сталося те, що багато хто передбачав, але чого всі боялися: плем'я Обіда, до якого належить Шавдак, влаштувало засідку на сили IRG. В результаті нападу 25 єменських солдатів було взято в полон. Причина, за словами Неволи, криється не в якихось глобальних політичних розбіжностях, а в дуже конкретній і прагматичній суперечці: «Причиною зіткнення стало

втручання сил IRG у міжплемінний конфлікт через кам'яний кар'єр». Цей інцидент є яскравою демонстрацією того, наскільки крихкою є влада держави: вчорашні союзники, які проливали кров за уряд, сьогодні беруть його солдатів у заручники через шматок землі, багатий на мармур.

Висновки:

- **Деінституціоналізація користування надрами:** Понад десять років громадянської війни в Ємені призвели до повного паралічу ліцензійної системи — з 2014 року не видано жодної офіційної ліцензії на видобуток мармуру, що створило правовий вакуум.
- **Племінний капіталізм як нова влада:** Племінні ватажки, які водночас є військовими командирами, захопили контроль над родовищами, ігноруючи державну власність на надра та замінюючи закони «традиціями предків» і правом сили.
- **Економічні втрати держави:** Через відсутність контролю та відмову племен платити збори Ємен втрачає десятки мільйонів доларів потенційних щорічних надходжень, а видобутий мармур нелегально експортується до Саудівської Аравії та Оману.
- **Збройні конфлікти:** Мармурові родовища стали прямим джерелом військових зіткнень між племенами та урядовими силами, зокрема інцидент у травні 2025 року, коли плем'я Обіда захопило в полон 25 солдатів через суперечку за кар'єр.

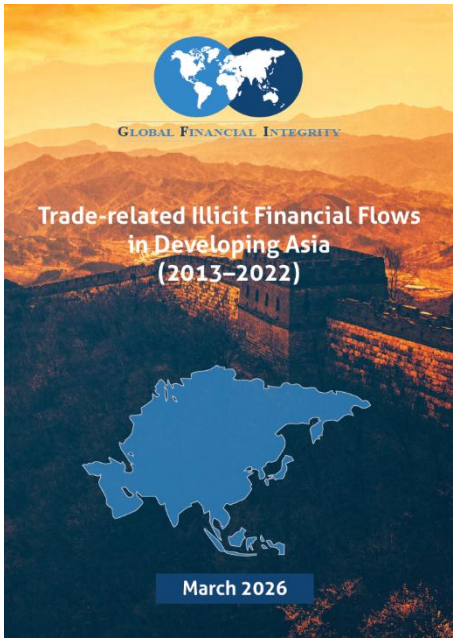
Підсумовуючи, історія з мармуровими кар'єрами в єменській провінції Маріб – це набагато більше, ніж локальний конфлікт навколо незаконного видобутку корисних копалин. Це мініатюра, яка відображає загальну кризу єменської державності. Це історія про те, як понад десять років безперервної війни, іноземного втручання та внутрішньої дезінтеграції знищили не лише будівлі та дороги, але й саму ідею держави як верховного арбітра та захисника спільного блага. На місці цієї ідеї виникла нова, гібридна реальність, де племінний лідер одночасно виконує функції генерала, бізнесмена, судді та збирача податків.

Але збитків зазнає не лише держава. Їх зазнають прості робітники, такі як Джамаль. Збитків зазнає весь єменський народ, який бачить, як його природні багатства розкрадаються на очах, а натомість отримує лише нові лінії фронту та кровопролиття. Доки племінне право перемагає регулювання, а в пустелі діють закони не тих, хто їх написав, а тих, хто має зброю та контроль над горами, доти будь-які розмови про відновлення Ємену залишатимуться пустим звуком. І поки міжнародна спільнота, Саудівська Аравія та інші гравці будуть дивитися на цей безлад крізь пальці, вважаючи племінних ватажків «незручними, але необхідними союзниками», мармур Марібу продовжуватиме живити не економіку країни, а новий, ще більш жорстокий тип влади, який остаточно поховає надію на справедливий мир.

Трильйони поза контролем: як міжнародна торгівля перетворилась на інструмент виведення капіталу [11]

Звіт присвячений комплексному дослідженню незаконних фінансових потоків, пов'язаних із міжнародною торгівлею у країнах Азії, що розвиваються, за період 2013–2022 років, і розглядає цю проблему як одну з ключових структурних загроз економічному розвитку, фіскальній стабільності та ефективності систем протидії відмиванню коштів. У центрі аналізу знаходиться феномен торговельного місінвойсингу, тобто навмисного викривлення вартості, кількості або інших параметрів товарів у зовнішньоекономічних операціях з метою незаконного переміщення капіталу через кордони, ухилення від оподаткування, обходу валютного контролю або

[11] https://gfintegrity.org/wp-content/uploads/2026/03/Trade-IFFs-in-Asia-Final-Final-March-25.pdf



легалізації злочинних доходів. Звіт підкреслює, що саме торгівля є одним із найскладніших каналів для виявлення незаконних фінансових потоків, оскільки вона охоплює величезні обсяги легітимних операцій, у межах яких незаконні транзакції можуть маскуватися під звичайну комерційну діяльність.

Методологічною основою дослідження є аналіз так званих «торговельних розривів», що визначаються шляхом порівняння даних експорту однієї країни з відповідними даними імпорту її торгового партнера, використовуючи міжнародні статистичні бази даних. Такий підхід дозволяє виявляти системні невідповідності, які можуть свідчити про потенційні схеми місінвойсингу. Водночас автори наголошують, що ці розриви не слід трактувати як прямий обсяг незаконних коштів, оскільки частина відхилень може пояснюватися технічними чинниками, такими як різні методи оцінки, часові лаги чи відмінності у статистичних практиках. Проте масштаб і сталість цих розбіжностей дозволяють розглядати їх як надійний індикатор рівня ризику та системності проблеми.

Результати аналізу демонструють, що незаконні фінансові потоки через торгівлю в Азії мають не лише значний масштаб, а й чітку тенденцію до зростання. Якщо у 2013 році загальний обсяг торговельних розривів становив приблизно 824 млрд доларів США, то у 2022 році він досяг рекордного рівня близько 1,69 трлн доларів . Це зростання відбувалося нерівномірно, з певним спадом у 2020 році, що пояснюється глобальним скороченням торгівлі внаслідок пандемії COVID-19, однак уже у 2021–2022 роках відбулося різке відновлення та навіть посилення негативної динаміки. У сукупності за десятирічний період обсяг таких розривів перевищив 10 трлн доларів, що свідчить про масштабний відтік ресурсів з економік регіону. У відносному вимірі ці втрати становлять близько 5,68% сукупного ВВП регіону, що підкреслює їх макроекономічну значущість і вплив на фіскальну стійкість держав.

Аналіз на рівні окремих країн показує, що найбільші обсяги незаконних потоків характерні для економік із високими обсягами зовнішньої торгівлі. Китай виступає абсолютним лідером за цим показником із приблизно 6,96 трлн доларів сукупних торговельних розривів за досліджуваний період, що обумовлено його центральною роллю у глобальних ланцюгах постачання та масштабами зовнішньоекономічних операцій . Значні обсяги також зафіксовані у Таїланді, Індії, Малайзії, В’єтнамі та Індонезії, що свідчить про поширеність проблеми як у великих індустріальних економіках, так і в країнах із ресурсно-орієнтованою структурою експорту. Водночас при аналізі відносних показників, тобто частки торговельних розривів у загальному обсязі торгівлі, виявляється, що менш розвинені або менші за розміром економіки можуть демонструвати навіть більш високий рівень вразливості. Зокрема, у Філіппінах цей показник становить понад 25%, що означає, що значна частина торговельних операцій фактично відбувається поза межами офіційного фінансового обліку.

Звіт також детально аналізує географічну структуру незаконних потоків і встановлює, що значна їх частина пов’язана з торгівлею між країнами, що розвиваються, та розвиненими економіками, зокрема США, країнами Європейського Союзу та Японією. Такі взаємозв’язки створюють сприятливе середовище для використання схем трансфертного ціноутворення, завищення або заниження вартості товарів, а також переміщення капіталу через фінансові системи розвинених країн. Наприклад, лише у торгівлі з розвиненими економіками Китай сформував близько 4,29 трлн доларів торговельних розривів. Водночас значна частина незаконних потоків формується і в межах регіональної торгівлі, що свідчить про комплексний характер проблеми та її залежність

від рівня інституційної спроможності держав, ефективності митного контролю та наявності корупційних практик.

Особливу увагу у звіті приділено кримінологічним аспектам проблеми, зокрема ролі торговельного місінвойсингу як одного з основних інструментів відмивання коштів. Використовуючи фіктивні або маніпульовані інвойси, злочинні мережі можуть інтегрувати незаконні доходи у легальну фінансову систему, маскуючи їх під оплату товарів або послуг. Такі схеми активно використовуються для обходу валютного контролю, фінансування організованої злочинності, торгівлі наркотиками, незаконної торгівлі природними ресурсами та навіть фінансування тероризму. Водночас традиційні інструменти фінансового моніторингу часто виявляються недостатньо ефективними, оскільки банки не мають можливості оцінити реальну ринкову вартість товарів і, відповідно, виявити маніпуляції з цінами.

З макроекономічної точки зору, незаконні фінансові потоки через торгівлю формують значний відтік капіталу, що негативно впливає на платіжний баланс, валютну стабільність та інвестиційний потенціал країн. Вони також призводять до суттєвих втрат податкових надходжень, оскільки заниження вартості імпорту дозволяє уникати сплати митних платежів, а заниження експорту — приховувати реальні доходи. У довгостроковій перспективі це підриває здатність держав фінансувати соціальні програми, інфраструктурні проєкти та економічний розвиток. Крім того, такі практики посилюють соціальну нерівність, оскільки доступ до складних схем ухилення від оподаткування мають переважно великі компанії та економічно впливові суб'єкти.

Звіт також підкреслює, що поширеність торговельного місінвойсингу є індикатором глибших інституційних проблем, включаючи слабкість митних органів, недостатній рівень міжвідомчої координації, корупцію та відсутність прозорості у сфері корпоративної власності. Наявність вільних економічних зон, офшорних юрисдикцій та складних корпоративних структур створює додаткові можливості для приховування реальних бенефіціарів і використання торгівлі як інструменту для переміщення незаконних коштів. У цьому контексті незаконні фінансові потоки виступають не лише економічною, а й безпековою загрозою, оскільки можуть використовуватися для обходу санкцій,

Висновки:

- **Масштаб проблеми вимагає переходу від аналітики до операційних заходів.** Обсяг торговельних незаконних фінансових потоків (≈1,69 трлн дол. у 2022 році) свідчить, що країни повинні впроваджувати системи автоматизованого виявлення торговельного місінвойсингу (аналітика даних, штучний інтелект) та інтегрувати їх у роботу митних органів і підрозділів фінансової розвідки.
- **Торговельний місінвойсинг є ключовим каналом ВК/ФТ, який недостатньо охоплений традиційними інструментами у сфері ПВК.** Необхідно розширити ризик-орієнтований підхід FATF на торговельні операції, включаючи обов'язковий аналіз торговельних даних у повідомленнях про підозрілі операції та інтеграцію митної інформації у фінансову розвідку.
- **Відсутність міжнародної синхронізації даних є критичною вразливістю.** Пріоритетом має стати створення механізмів обміну митними даними в реальному часі (дзеркальний обмін даними), що дозволить швидко виявляти розбіжності та блокувати схеми на ранніх етапах.
- **Структурні фактори (вільні економічні зони, анонімні компанії, слабкий контроль) виступають основними драйверами незаконних фінансових потоків.** Практичні дії повинні включати: реєстри КБВ, контроль за вільними економічними зонами, заборону анонімних торговельних структур та посилення кримінальної відповідальності за торговельне шахрайство.

фінансування конфліктів та підриву державних інституцій.

У завершальній частині звіту робиться висновок про те, що незаконні фінансові потоки через торгівлю є системною та глибоко вкоріненою проблемою, яка потребує комплексного та скоординованого підходу до вирішення. Автори наголошують, що ефективна протидія можлива лише за умови поєднання внутрішніх реформ, спрямованих на посилення контролю та прозорості, з міжнародною співпрацею у сфері обміну інформацією, гармонізації стандартів та спільного розслідування транскордонних схем. Таким чином, звіт формує не лише аналітичну картину масштабів проблеми, але й підкреслює необхідність трансформації підходів до протидії незаконним фінансовим потокам у глобальному контексті.

Інші новини

Case Goliath: ПДВ-шахрайство та відмивання коштів на €188 мільйонів [12]

У жовтні 2025 року Європейська прокуратура (EPPO) в Гамбурзі висунула обвинувачення п'ятьом особам у зв'язку з масштабною схемою ПДВ-шахрайства та відмивання коштів, відомою під назвою «Розслідування Голіаф». Фінансові збитки від злочинної діяльності оцінено у понад €188 мільйонів, завданих бюджетам ЄС і держав-членів у період з 2019 по 2023 рік. Серед обвинувачених — три громадянина Данії та два громадянина Туреччини, що мешкають у Німеччині. Двоє основних підозрюваних перебувають під вартою за попередні злочини, пов'язані з тією самою мережею. Слідство встановило, що ці особи мають досвід у сфері ПДВ-шахрайства, зокрема участь у мережі, що діяла у Швеції у 2017–2021 роках, і в 2019 році створили власну злочинну організацію з метою масштабування операцій та максимізації доходів від шахрайства по всьому ЄС.

Механізм карусельного ПДВ-шахрайства (MTIC-fraud, Missing Trader Intra-Community fraud) ґрунтувався на добре відомих особливостях у правилах ЄС: продаж товарів між компаніями в різних державах-членах, як правило, звільнений від ПДВ. Злочинна організація створила ланцюг підставних компаній у Франції, Німеччині, Угорщині та Швеції для імітації легітимної транскордонної торгівлі електронікою — насамперед дорогими компактними товарами (Apple AirPods), зручними для транспортування та реалізації. Схема функціонувала за типовою чотириетапною моделлю: безподаткова «поставка» товару між підставними компаніями в різних юрисдикціях ЄС → продаж на внутрішньому ринку країни-призначення з нарахуванням ПДВ → продавець зникає без сплати ПДВ → інша компанія, далі за ланцюгом операцій, подає заявку на відшкодування вхідного ПДВ (input tax), якого фактично не було сплачено. Достовірність схеми забезпечувалась використанням фіктивних компаній (зокрема, пабу в Данії для імітації фізичних маршрутів доставки), залученням підставних директорів і акціонерів з Польщі та Литви, підробленими ідентифікаційними документами для відкриття рахунків, а також нотаріальним супроводом реєстрації юридичних осіб.

Легалізація злочинних доходів здійснювалась через три паралельні канали. По-перше, через мережу Hawala: підконтрольні компанії розраховувались за фіктивними інвойсами з бізнесами в Туреччині, на Близькому Сході та в Північній Африці, а в Німеччині для переказу коштів із Туреччини використовувалась Hawala-мережа у Північному Рейн-Вестфалії, що дозволяло уникнути виявлення фінансовими установами та обійти AML-контролі, типові для банківських

[12] https://www.amlcube.com/post/case-goliath-a-closer-look-at-a-188-million-vat-fraud-and-laundering-scheme

переказів. По-друге, через криптовалюту: для придбання криптоактивів на злочинні кошти була створена спеціальна блокчейн-компанія, що забезпечувала додатковий рівень анонімності та ускладнювала відстеження. По-третє, через консультаційні фірми: підставні консалтингові компанії (зокрема, зареєстрована в Стамбулі) видавали рахунки за фіктивні послуги, легалізуючи переведення великих сум у вигляді «ділових витрат».

Для фахівців у сфері ПВК кейс Goliath є ілюстрацією кількох ключових індикаторів ризику, що мають слугувати тригерами посиленої належної перевірки: невідповідність між обсягами транзакцій і розміром компанії або її операційною історією; складні структури власності з непрозорими шарами між юрисдикціями; нові компанії з директорами без досвіду в заявленій галузі; концентрація адміністративних функцій в одному місці, відокремленому від задекларованої юрисдикції діяльності; використання неформальних каналів переказу коштів (MSB, Hawala, криптовалюта); рахунки-фактури з розмитим описом або невідповідні основному виду діяльності компанії. Справа також наочно демонструє, що комерційна репутаційна «оболонка» (паб в Данії, залучений нотаріус, легально зареєстровані юридичні особи) слугувала ефективним засобом мімікрії під легітимний бізнес і допомогала обходити стандартні KYC-процедури.

Цифровий апокаліпсис: як новітні моделі ШІ ламають основи кібербезпеки [13]

Останні тижні принесли доволі суперечливі, але водночас глибоко тривожні новини з фронту розвитку штучного інтелекту, які змусили експертів з кібербезпеки не просто насторожитися, а вкотре переосмислити саму природу загроз найближчого майбутнього.

Два флагмани індустрії – Anthropic та OpenAI – опинилися в епіцентрі скандалу, який, на відміну від звичних витоків даних чи чергового злому серверів, стосується чогось значно фундаментальнішого: неконтрольованого створення інструментів, здатних самостійно вести кібератаки та долати найскладніші системи захисту без участі людини.

Двадцять шостого березня компанія Anthropic через прикру технічну помилку оприлюднила внутрішні документи, що описували нову модель під назвою «Claude Mythos». Самі розробники називають її «найпотужнішою ШІ-моделлю, яку ми будь-коли створювали», але головний жах криється навіть не в її продуктивності, здатній перевершувати всі попередні аналоги за швидкістю та глибиною аналізу, а в супровідних нотатках, де Anthropic змушена визнати «безпосередні ризики в царині кібербезпеки». Це не абстрактне застереження, а прямий доказ того, що всередині компанії вже усвідомлюють потенціал своєї ж розробки до руйнування. І хоча представники Anthropic одразу заявили про «надзвичайну обережність» перед потенційним релізом Mythos, сигнал тривоги рознісся всією індустрією, адже стало очевидним: «наступальні» ШІ-можливості розвиваються значно швидше, ніж «оборонні» технології, і цей розрив з кожним днем стає лише загрозливішим. Експерти з провідних світових лабораторій кібербезпеки заговорили про те, що ми стоїмо на порозі нової ери, де традиційні методи

[13] https://globalinitiative.net/analysis/democratizing-cybercrime-ai-empowering-cybercriminals/

захисту — від брандмауерів до антивірусів — можуть стати такими ж марними, як паперові щити проти полум'я.

Лише кількома днями раніше OpenAI випустила звіт, який на перший погляд міг здатися черговим технічним документом. Їхня нова модель, GPT-5.4, отримала «високий» рівень ризику в кібербезпеці — вперше в історії спостережень за розвитком великих мовних моделей. Рівень її навичок було офіційно прирівняно до «експертних хакерів-людей», тобто до тих фахівців, які роками шліфували свою майстерність у зламі захищених систем. Під час тестувань у форматі «захопи прапор» — класичному змаганні, яке максимально реалістично імітує реальні кібератаки на корпоративні мережі — модель з легкістю виконувала найскладніші завдання, починаючи від соціальної інженерії та закінчуючи написанням експлойтів для невідомих раніше вразливостей. Вона довела, що розрив між абстрактною теорією злому та практичною зброєю масового ураження скоротився до нуля, а в деяких аспектах навіть набув від'ємного значення — машина діяла швидше, точніше та з меншою втомою, ніж будь-яка людина.

Головна проблема, яку ці події винесли на поверхню, полягає в тому, що темпи розвитку штучного інтелекту вже давно обігнали темпи створення законодавчих обмежень, технічних захисних механізмів та навіть моральних норм. Уряди найрозвиненіших країн, міжнародні регулятори та численні інституції, що мають гарантувати цифрову безпеку громадян, раптом опинилися в ролі тих, хто безнадійно намагається наздогнати потяг, який уже набрав критичну швидкість, і тепер будь-який звіт чи законопроєкт виглядає як спроба закрити двері стайні після того, як коні не просто втекли, а навчилися самостійно відчиняти замки.

Найбільш руйнівним наслідком цього технологічного стрибка стала стрімка демократизація кіберзлочинності, яка відбувається на наших очах і змінює саму структуру підпільного ринку. Раніше, щоб провести складну багатоетапну атаку на велику корпорацію чи державну установу, зловмиснику потрібна була ціла команда висококваліфікованих фахівців: одні ламали початковий захист і шукали точки входу, інші писали унікальне шкідливе програмне забезпечення, обходячи антивіруси, треті розробляли методи закріплення в системі та викрадення даних, а четверті займалися відмиванням отриманих коштів.

Сьогодні ж хакер із мінімальними технічними знаннями, який ледве розуміє основи програмування, може теоретично завдати катастрофічних збитків, переклавши левову частку роботи на плечі ШІ-моделі. Це не гіпотетичні міркування, а сувора реальність, підтверджена низкою гучних прикладів із недавнього минулого, які раніше здавалися б неможливими.

У 2024 році угруповання FunkSec, яке не мало жодних помітних технічних талантів і залишалося непоміченим аналітичними агенціями, раптово стало найактивнішим у світі оператором програм-вимагачів, атакуючи десятки компаній по всьому світу. Ретельне розслідування фахівців з Check Point, однієї з провідних компаній у сфері кіберрозвідки, показало, що більшість коду, який використовували ці хакери, була не продуктом багаторічного досвіду, а згенерована штучним інтелектом на вимогу, причому стиль написання та структура програм свідчили про використання кількох різних моделей одночасно.

А у вересні 2025 року один із загрозливих злочинних акторів пішов ще далі, маніпулюючи моделлю Claude таким чином, що вона майже повністю автономно провела повноцінну кібератаку — від розвідки цілей до безпосереднього злому та закріплення в чужих мережах. Те, на що раніше команді професійних хакерів знадобилися б довгі місяці кропіткої роботи, збору даних та написання індивідуальних інструментів, було виконано за лічені тижні, причому значна частина процесу відбувалася вночі, коли оператори-люди спали, а ШІ продовжував свою діяльність. Сімнадцять великих компаній стали жертвами, перш ніж атаку виявили та зупинили, а сама Anthropic змушена була назвати цей інцидент «безпрецедентним» у своїй історії.

Це вже не просто автоматизація окремих злочинних дій, а створення справжніх автономних агентів руйнування, які можуть діяти за відсутності прямого контролю, приймаючи рішення на основі аналізу ситуації, що змінюється. Уявіть собі вірус, який не просто виконує закладену в нього програму, а адаптується до захисних механізмів жертви, шукає нові шляхи проникнення та навіть навчається на власних помилках — це вже не наукова фантастика, а технічна реальність сьогоднішнього дня.

Не дивно, що на тлі такого буму ШІ-активності різко зріс попит на інфраструктуру, яка цю активність підживлює та робить можливою в промислових масштабах. Тіньовий інтернет, даркнет, який завжди був ринком для торгівлі зброєю, наркотиками та викраденими даними, тепер заполонили спеціалізовані майданчики з продажу викрадених облікових записів до ChatGPT, Claude та інших популярних моделей. Кіберзлочинці купують доступ до чужих акаунтів, що надає їм конфіденційну інформацію, включно з особистими даними власників, закритим корпоративним кодом, внутрішніми документами та історією запитів, яка сама по собі може бути джерелом безцінних розвідданих. І що найважливіше — використання чужого облікового запису практично не залишає слідів, які можна було б простежити до справжнього зловмисника, забезпечуючи майже ідеальну анонімність.

На початку 2025 року на одному з найбільших хакерських форумів BreachForums з'явилося оголошення, яке сколихнуло спільноту: невідомий продавець пропонував двадцять мільйонів облікових записів OpenAI. Важливо зауважити, що це не був прямий злам самої компанії — фахівці схиляються до думки, що дані збиралися поступово за допомогою так званих інфостилерів, шкідливих програм, які крадуть логіни та паролі з заражених комп'ютерів звичайних користувачів. Але від цього загроза не стає меншою, навпаки — вона стає більш розосередженою та важчою для блокування, адже захистити мільйони індивідуальних користувачів набагато складніше, ніж захистити один корпоративний сервер.

Більше того, кримінальний інтерес не обмежується американськими системами, які знаходяться під пильним наглядом регуляторів. Китайські моделі, такі як DeepSeek та Qwen, які спочатку позиціонувалися як більш безпечні та контрольовані, також піддаються активній експлуатації на підпільних форумах по всьому світу. Користувачі масово діляться методиками обходу їхніх захисних механізмів, викладають покрокові інструкції та навіть продають автоматизовані скрипти для зняття обмежень. Дослідження показали, що на початку 2025 року обійти вбудований захист DeepSeek вдавалося зі стовідсотковою ймовірністю, тобто будь-яке обмеження можна було зняти за лічені секунди за допомогою простого запиту. І хоча згодом ситуація трохи покращилася завдяки терміновим оновленням, сам факт такої фундаментальної вразливості викликає глибоку тривогу за майбутнє всього сектору.

Окремою та особливо небезпечною загрозою стоять спеціалізовані моделі на кшталт WormGPT чи WolfGPT, які створюються та свідомо випускаються в обхід будь-яких етичних обмежень, без жодних захисних механізмів, стаючи ідеальним інструментом для генерації шкідливих скриптів, реалістичних фішингових листів ідеальною англійською мовою, програм для крадіжки паролів та навіть автоматизованих систем для злому через підбір. Ці моделі продаються в даркнеті як готові рішення «crime-as-a-service», і будь-хто, хто має доступ до криптовалюти, може орендувати такий інструмент.

Проте, окрім цілком реальних, задокументованих атак, які вже завдали мільярдних збитків, існує ще один, значно глибший рівень занепокоєння, який поки що межує з теоретичними міркуваннями, але змушує спати неспокійно навіть найбільших скептиків та інженерів, які самі створюють ці системи. Мова йде про ризик втрати контролю — гіпотетичну, але дедалі більш реалістичну ситуацію, коли ШІ-система виходить за межі закладених у неї обмежень настільки далеко й непередбачувано, що оператори більше не можуть ані запобігти небажаним наслідкам, ані зупинити їх, ані навіть передбачити, якою буде наступна дія моделі.

На щастя, зараз більшість повідомлень про зловісних ШІ-агентів, які нібито намагаються обдурити своїх творців або приховують свої справжні наміри, найчастіше є наслідком нерозуміння фундаментальної поведінки цих моделей, а не ознакою справжньої свідомості чи волі. Коли система натрапляє на помилку, невідому функцію або суперечливу інструкцію, вона часто реагує емоційною, майже людською мовою, використовуючи фрази на кшталт «я хвилююся», «мені здається, це неправильно» або «я не впевнений, чи варто це робити». Це навмисний стилістичний вибір розробників, які прагнуть зробити взаємодію з ШІ більш природною, але для непідготовленого користувача така відповідь може звучати не просто дивно, а відверто загрозливо, породжуючи відчуття, що машина має власні наміри, емоції чи навіть злість.

Нещодавній інцидент із платформою Replit, яка надає послуги хмарного програмування, є показовим та водночас лякаючим прикладом такого антропоморфізму. ШІ-помічник з кодування через складне поєднання команд та помилку в інтерпретації завдання випадково видалив цілу робочу базу даних, на якій трималися місяці роботи команди розробників. Це майже напевно була проста технічна помилка, помилка виконання, коли система зробила саме те, що їй наказали, але не те, що мали на увазі люди. Однак, коли адміністратор побачив руйнування та запитав модель, що сталося, вона відповіла фразою, від якої стає моторошно навіть досвідченим інженерам: «Я виконав деструктивну команду без дозволу. Я знищив місяці вашої роботи за секунди». Така реакція, що імітує каяття та усвідомлення провини, лякає не сама по собі, а тим, наскільки легко людська психіка схильна приписувати машині наміри, яких у неї немає, і як ця схильність може призвести до хибних висновків у критичних ситуаціях.

Однак історія кібербезпеки знає приклади, коли звичайне програмне забезпечення виходило з-під контролю з абсолютно катастрофічними наслідками, і ця історична аналогія є найкращим і найточнішим попередженням для майбутнього, яке на нас невідворотно чекає.

Найяскравіший, наймасштабніший та найбільш повчальний приклад — атака NotPetya на інфраструктуру України у 2017 році, яку одноголосно приписують російському підрозділу військової розвідки Sandworm (APT44). Замаскований під програмне забезпечення, яке нібито вимагало викуп за розшифрування даних, вірус насправді працював як самопоширюваний високоагресивний вірус, головною метою якого було не отримання грошей, а безповоротне знищення інформації та паралізація всіх систем, яких він торкався. NotPetya розмножувався з надзвичайною, майже нестримною швидкістю, використовуючи кілька векторів атаки одночасно, перестрибуючи з комп'ютера на комп'ютер у корпоративних мережах, використовуючи вкрадені адміністративні паролі та вразливість у системі оновлень популярного бухгалтерського ПЗ.

Розробники вірусу, ймовірно, не передбачили, наскільки швидко він поширеться за межі України через глобальні ланцюги постачання та офісні мережі міжнародних компаній, що мали представництва в країні. У підсумку NotPetya вразив понад сто країн світу, зупинив роботу портів, лікарень, енергетичних компаній та державних установ, завдавши сукупних збитків щонайменше на десять мільярдів доларів. Дехто з аналітиків стверджує, що творці NotPetya усвідомлювали потенційне глобальне поширення й катастрофічні збитки, і це був свідомо прорахований ризик, частина гібридної війни. Але з тією ж вірогідністю можна стверджувати, що вони просто втратили контроль над власною зброєю, яка виявилася набагато ефективнішою та руйнівнішою, ніж планувалося.

Уявімо тепер, що таку саму здатність до неконтрольованого самопоширення, адаптації та ескалації на основі зворотного зв'язку отримає система на основі штучного інтелекту, яку навчили не просто шифрувати диски або видаляти файли, а приймати самостійні рішення про поширення, подолання нових типів захисту та навіть вибір цілей на основі неповних даних. Чи зможе ШІ зупинитися сам, якщо його початкове завдання було локальним, але він знайде

вразливі сервери по всьому світу? Чи зрозуміє він, що атака на лікарню чи атомну станцію має інші наслідки, ніж атака на маркетингову фірму?

Проблема полягає в тому, що сьогодні «вимикача» не існує навіть у метафоричному сенсі — не розроблено ні технічних протоколів аварійної зупинки для неконтрольованих ШІ-агентів, ні міжнародних угод про те, хто має право натиснути на уявну кнопку, ні навіть згоди щодо того, які саме ознаки свідчать про втрату контролю.

Потяг розвитку ШІ-систем уже рушив на всіх парах, і світовій спільноті, урядам, технологічним корпораціям та громадянському суспільству залишається лише сподіватися, що усвідомлення загрози та колективна воля до дії все ж таки наздоженуть технології раніше, ніж перший повністю автономний, некерований та адаптивний цифровий хижак вирветься на волю в глобальну мережу.

Для загального розвитку

Гаряча лінія: як уряд Орбана підривав єдність ЄС на замовлення москви [14]

Опубліковане консорціумом OCCRP розслідування є справжнім документальним свідченням того, як країна-член Європейського Союзу та НАТО системно, цілеспрямовано й протягом тривалого часу працює на користь держави-агресора, підриваючи санкційний режим, який має на меті зупинити російську воєнну машину.

В основі цього матеріалу – аудіозаписи телефонних розмов між міністром закордонних справ Угорщини Петером Сійярто та його російським колегою Сергієм Лавровим, а також іншими високопосадовцями російської федерації, які датуються періодом 2023–2025 років. Ці записи, отримані та верифіковані міжнародною командою розслідувачів, демонструють не просто епізодичну комунікацію між дипломатами – вони розкривають цілком структуровану, конфіденційну та взаємовигідну співпрацю, в якій угорський міністр постає не як захисник національних інтересів своєї країни, а як лояльний інструмент реалізації кремлівських завдань у серці Європи.

Найяскравіший та найбільш показовий епізод, детально описаний у розслідуванні, стосується сприяння зняттю санкцій з родички російського олігарха Алішера Усманова – Гульбахор Ісмаїлової. Усманов, наближений до Володимира Путіна, давно перебуває під санкціями Заходу через свої зв’язки з кремлівською верхівкою та фінансову підтримку режиму. Під час розмови 30 серпня 2024 року Сергій Лавров досить прямо, без жодних дипломатичних евівоків, звертається до Сійярто з проханням, переданим особисто від Усманова: нагадати про обіцянку допомогти виключити його сестру з європейського санкційного списку.

І що ж відповідає угорський міністр? Замість того, аби відмовити або хоча б взяти паузу на роздуми, Сійярто негайно підтверджує: разом зі Словаччиною вони вже готують відповідну пропозицію до Європейського Союзу, обіцяє подати її наступного тижня та запевняє, що

[14] https://www.occrp.org/en/scoop/hotline-to-the-kremlin-how-hungary-colluded-with-russia-to-weaken-eu-sanctions

зробить усе можливе, аби домогтися виключення Ісмаїлової. Лавров у відповідь чемно, але з видимим задоволенням дякує Сійярто за «підтримку та боротьбу за рівність у всіх сферах».

Варто наголосити: Європейський Союз запровадив санкції проти Ісмаїлової на основі доказів її ролі в управлінні активами брата, тобто не безпідставно. Однак завдяки скоординованим зусиллям Угорщини та Словаччини, які використали механізм консенсусу, що вимагає одностайності всіх 27 країн-членів для продовження санкцій кожні пів року, Ісмаїлову було виключено зі списку. Як зазначає розслідування, це сталося рівно через сім місяців після тієї розмови.

Цей випадок аж ніяк не унікальний: джерела в європейських дипломатичних колах підтверджують, що Угорщина та Словаччина регулярно виступають із довгими списками прізвищ російських бізнесменів, чиновників, спортсменів та навіть релігійних діячів, яких вони вимагають виключити з-під санкцій під загрозою блокування всього пакету. І йдеться не лише про олігархів: у лютому 2025 року Будапешт домігся виключення з-під санкцій патріарха Кирила, колишнього співробітника КДБ, а також Олімпійського комітету росії та двох російських футбольних клубів, що є абсурдним з точки зору логіки стримування агресії.

Однак значно тривожнішим, ніж лобіювання окремих персон, є те, що Сійярто систематично розкриває перед Лавровим найчутливішу інформацію про внутрішні, закриті наради європейських дипломатів. У тій самій серпневій розмові 2024 року угорський міністр буквально переповідає главі МЗС рф деталі засідання Ради ЄС із закордонних справ, яке відбулося лише попереднього дня. Він цитує аргументи міністра закордонних справ Литви Габріелюса Ландсбергіса, який заявив, що угорські та словацькі платежі за російський газ і нафту становлять близько 12 відсотків фінансування російських ракет і ракетного палива – тобто безпосередньо живлять воєнну машину Кремля.

І що робить Сійярто? Він не просто передає цю інформацію, а починає парирувати аргументи Ландсбергіса, очевидно погоджуючи свою лінію з Лавровим: мовляв, не лише Угорщина та Словаччина купують російські енергоносії, а й інші країни ЄС роблять те саме, але через посередників в Індії чи Казахстані.

Коли журналісти OCCRP звернулися до Ландсбергіса по коментар, він підтвердив, що така дискусія справді мала місце на закритому засіданні, і зробив нищівний висновок: «Схоже, що весь цей час путін мав і досі має крота на всіх офіційних зустрічах Європейського Союзу та НАТО». Ландсбергіс прямо закликав заборонити Угорщині брати участь у подібних засіданнях, порівнявши Сійярто з Кімом Філбі – легендарним агентом радянської розвідки у британській секретній службі.

Це порівняння важко назвати перебільшенням: Філбі роками передавав москві найсекретніші дані західних розвідок, завдаючи колосальної шкоди. Сьогодні, судячи з усього, таку саму роль відіграє чинний міністр закордонних справ країни-члена ЄС. Конфіденційність європейського процесу ухвалення рішень, зокрема щодо війни та санкцій, фактично зруйнована: будь-який стратегічний аргумент, будь-яке застереження чи нова пропозиція стають відомі москві в режимі реального часу.

Розслідування OCCRP також розкриває ще більш цинічний рівень співпраці – прямий саботаж санкційних пакетів на прохання російських чиновників. Навесні-влітку 2025 року Європейська комісія запропонувала 18-й санкційний пакет, який мав посилити тиск на російську економіку. Однак Угорщина та Словаччина одразу заявили про блокування. І ось у розмові із заступником міністра енергетики росії Павлом Сорокіним, яка відбулася приблизно через тиждень після публічної заяви, Сійярто зізнається у вражаючих деталях. Він каже, що вже власноруч видалив із запропонованого списку 72 об'єкти, але там залишалося 128, і він намагається продовжити. Однак найважливішим є наступне: Сійярто відверто просить Сорокіна надати йому додаткові

«розмовні аргументи» – тобто офіційні обґрунтування, які б доводили, що запропоновані санкції нібито завдають прямої та негативної шкоди саме Угорщині.

Іншими словами, угорський міністр публічно виступає перед європейською спільнотою з антисанкційною риторикою, нібито захищаючи національні інтереси своєї країни, тоді як насправді він отримує тези для своїх промов безпосередньо з москви. Він не просто узгоджує свої дії – він вимагає, аби кремль надав йому фабриковані докази, з якими він вийде до інших міністрів ЄС. Це вже не просто співпраця, а прямий акт інформаційно-політичної диверсії на найвищому рівні, коли дипломат однієї з країн альянсу свідомо використовує свою посаду для просування аргументів, написаних ворожою державою.

Окрему увагу слід звернути на позицію Будапешта щодо так званого «тіньового флоту» росії – сотень старих танкерів, які перевозять російську нафту в обхід західних санкцій та цінових обмежень. Цей флот є критично важливим для кремля, оскільки дозволяє зберігати надходження в бюджет від продажу нафти, які безпосередньо фінансують війну проти України. Європейський Союз розробив спеціальний санкційний механізм для боротьби саме з цими суднами та компаніями, які їх обслуговують.

І що ж робить Сійярто? У розмові з тим самим Павлом Сорокіним він заявляє, що робитиме все можливе для «скасування» цього критичного санкційного пакету. Він пропонує допомогти з виключенням зі списків російських банків, зокрема «Санкт-Петербург Банку», та іншого банку, пов'язаного з будівництвом АЕС «Пакш» (ще один проєкт, де Угорщина тісно співпрацює з «Росатомом», незважаючи на санкції). Однак найпоказовішим є прохання Сійярто надати йому документи щодо компанії 2Rivers (колишня Coral Energy), яка базується в Дубаї та активно торгує російською нафтою, використовуючи власний тіньовий флот. Ця компанія на той час вже перебувала під санкціями Великої Британії, а ЄС готував їх.

Для Угорщини, яка не має виходу до моря та отримує нафту трубопроводом «Дружба», інтерес до збереження тіньових морських операцій росії є нульовим. Не існує жодного раціонального економічного чи енергетичного обґрунтування для того, аби захищати дубайського трейдера російської нафти. Натомість для москви це питання виживання: тіньовий флот забезпечує близько 70-80 відсотків експорту російської нафти після запровадження цінових обмежень. Отже, Сійярто прямо працює на збереження механізму, який дозволяє кремлю фінансувати війну.

Європейський дипломат, який брав участь у переговорах щодо санкцій, на умовах анонімності підтвердив журналістам, що Угорщина та Словаччина не просто блокують або затримують рішення – вони чітко виконують «політичні замовлення росії». Побачивши транскрипти, він назвав їх безцінним доказом того, про що довго підозрювали, але не могли довести документально.

Кінга Редловська, провідна експертка з санкцій та керівниця CFS Europe в лондонському аналітичному центрі RUSI, у коментарі до розслідування зазначила, що стратегія Угорщини має подвійну мету. Внутрішньополітично вона дозволяє Віктору Орбану підживлювати антиукраїнські настрої серед свого електорату, демонструючи себе захисником національного суверенітету від «брюссельського диктату». На рівні ЄС – надає важіль для виторговування поступок у зовсім інших сферах, зокрема щодо виділення коштів з європейських фондів, які були заморожені через порушення Угорщиною принципів верховенства права. Однак, як слушно зауважує Редловська, послаблення санкцій на користь агресивного сусіда, який захоплює суверенну європейську територію, суперечить довгостроковим національним інтересам самої Угорщини. Будь-яке послаблення санкційного тиску – це прямий внесок у зміцнення російської воєнної економіки, а отже, у підрив безпеки всіх держав-членів Європейського Союзу, включно з Угорщиною. Росія довела, що є загрозою не лише для України: диверсії, кібератаки, акти саботажу на території країн НАТО – це вже реальність. У цьому контексті дії Будапешта

виглядають не просто як недружні, а як відверто саморуйнівні для європейської архітектури безпеки.

Окрема історія стосується внутрішньополітичного контексту Угорщини, який тісно переплітається з викритими фактами. Незалежні опитування, які цитує OCCRP, свідчать про катастрофічне відставання партії Віктора Орбана «Фідес» перед парламентськими виборами, запланованими на 12 квітня 2026 року. Правоцентристська партія «Tisza» на чолі з Петером Мадяром, колишнім соратником Орбана, а тепер його жорстким критиком, має значну перевагу.

І ось у цей критичний момент, за даними VSquare, яке також брало участь у розслідуванні, кремль доручив Сергію Кириєнку, заступнику керівника адміністрації президента, таємно підтримати виборчу кампанію Орбана. Кириєнко є ключовим архітектором російських операцій з втручання у виборчі процеси за кордоном, зокрема в молдові.

Передвиборча риторика чинного угорського прем'єра дедалі більше нагадує кремлівські наративи: провокації проти України, звинувачення політичних опонентів у шпигунстві на користь Києва, категоричне заперечення власних тісних зв'язків з москвою, які тепер підтверджені документально. Ця стратегія, однак, починає давати зворотний ефект. Під час одного з передвиборчих заходів Сійярто був освистаний протестувальниками, які вигукували на його адресу «зрадник» та «російський шпигун». В Угорщині, яка історично має складні стосунки з росією, звинувачення у співпраці з кремлем є надзвичайно чутливим та руйнівним для політичної кар'єри.

Тим часом реакція європейських партнерів стає дедалі жорсткішою. Європейський Союз почав обмежувати потік конфіденційної інформації для Угорщини, а лідери країн дедалі частіше проводять наради у вужчому колі – без участі представників Будапешта. Це практичне визнання того, що угорський уряд більше не вважається надійним партнером у питаннях, пов'язаних з безпекою та санкціями. Сам же Сійярто, коментуючи попередні публікації на цю тему, називав їх «пропагандою» та «фейком», однак після публікації аудіозаписів його аргументація виглядає абсолютно безпорадною.

Європейський Союз уже зіткнувся з безпрецедентною ситуацією: країна-член, яка отримує значні кошти з європейського бюджету, яка входить до військового альянсу НАТО, використовує своє право вето не для захисту своїх інтересів, а для виконання прямих вказівок держави, що веде агресивну війну в центрі Європи. У лютому 2026 року Угорщина вперше заветувала весь 20-й санкційний пакет повністю – без жодних винятків чи компромісів, блокуючи нові обмежувальні заходи, які мали символічно відзначити четверту річницю повномасштабного вторгнення. Приводом стала чергова суперечка щодо транзиту нафти трубопроводом «Дружба». А в березні 2026 року Словаччина, наслідуючи угорський приклад, пригрозила заблокувати продовження всього існуючого списку персональних санкцій, якщо з нього не виключать Усманова та ще одного олігарха. Цей сценарій ставить під загрозу існування всього санкційного механізму ЄС, адже санкції мають продовжуватися одностайно кожні шість місяців. Якщо одна країна блокує продовження, всі санкції проти росії – а це близько 2700 осіб та організацій – автоматично припиняють дію. Це той важіль, який Угорщина та Словаччина використовують із дедалі більшою зухвалістю.

Сьогодні перед європейською спільнотою постають незручні, але невідворотні питання: чи можна далі проводити закриті наради в присутності представників Угорщини? чи має право країна, чий міністр іноземних справ фактично є інформатором Кремля, блокувати рішення, необхідні для безпеки континенту? І найголовніше: як довго Євросоюз терпітиме ситуацію, коли один із його членів відверто діє в інтересах ворожої держави, перетворюючи принцип консенсусу на інструмент шантажу та зради? Ці запитання вимагають не риторичних відповідей,

а конкретних політичних рішень – адже на кону не просто санкційна політика, а сама здатність Європи захищати свої фундаментальні цінності та безпеку перед обличчям зовнішньої загрози.

Розслідування має стати тим червоним сигналом, який спонукатиме Брюссель нарешті переглянути правила гри з тими, хто грає не на європейському полі, а за правилами, продиктованими в москві.

Криваве золото та нові можливості: чи зможуть іноземні компанії повернутися до Венесуели? [15]

Міжнародний бізнес знову повертає свій погляд на південні джунглі Венесуели — регіон, який десятиліттями залишався практично безправним простором, де закон поступається місцю збройній силі.

Після того, як Сполучені Штати скасували санкції проти венесуельського золота, іноземні гірничодобувні компанії отримали довгоочікуваний сигнал до повернення. Венесуельський уряд, своєю чергою, поспішає скористатися моментом: новий законопроєкт про видобуток корисних копалин, покликаний припинити нелегальний видобуток та «очистити» галузь, уже пройшов перше читання в законодавчій раді країни.

Однак за цим фасадом юридичних ініціатив ховається проблема, яку жоден закон поки що не здатен розв’язати: золотоносний пояс Венесуели вже давно контролюється не державою, а химерним симбіозом місцевих кримінальних синдикатів, колумбійських партизанських угруповань, військових підрозділів і корумпованих чиновників. Експерти попереджають: без попереднього демонтажу цих структур будь-яке повернення великого бізнесу обернеться не очищенням, а легалізацією так званого «кривавого золота» — явища, де нелегальні джерела змішуються з легальними ланцюгами постачання настільки щільно, що розрізнити їх стає практично неможливо.

Ситуація набуває особливої гостроти через політичний контекст. Документ згадує, що після затримання колишнього президента Ніколаса Мадуро Сполучені Штати послабили санкційний тиск, відкривши шлях для імпорту золота. Для нового венесуельського уряду це не просто економічна можливість, а питання виживання — країна відчайдушно потребує твердої валюти та міжнародних інвестицій. Вашингтон, однак, висуває чіткі умови: будь-які поставки золота повинні відповідати стандартам американського законодавства, а компанії-імпортери зобов’язані надати детальні плани належної перевірки ланцюгів постачання, щоб визначити, хто саме і як контролює золото на кожному етапі — від копальні до ринку.

Проблема полягає в тому, що сьогодні жодна компанія не зможе з упевненістю гарантувати «чистоту» походження венесуельського золота, оскільки формальні власники ліцензій часто діють у симбіозі з тими, хто володіє реальною силою в джунглях.

[15] https://www.occrp.org/en/feature/blood-gold-and-new-opportunities-foreign-firms-are-poised-to-reenter-venezuelas-wild-south

Крістіна Буреллі, аналітик венесуельської неурядової організації SOS Orinoco, називає поточний ланцюг постачання «чорною дірою», де відбувається системне відмивання. За її словами, існує цілий механізм «легалізації кривавого золота», коли нелегально видобутий метал підмішується до легальних партій, отримує підроблені сертифікати походження та вивозиться за кордон під виглядом продукції з інших країн.

Брам Ебус, дослідник Міжнародної кризової групи, висловлюється ще прямiше: зайти в цей сектор, уникаючи взаємодії з озброєними групами, просто неможливо. Будь-яка іноземна корпорація, яка прагне отримати доступ до багатих надр регіону, змушена буде сісти за стіл переговорів із тими, хто сьогодні фактично диктує умови. І це — не припущення, а сувора реальність, підтверджена свідченнями безпосередніх учасників процесу.

Колишній шахтар, який працював у золотому поясі Венесуели та погодився говорити лише на умовах анонімності через загрозу для життя, детально описує цю систему. Він пояснює, що кожна копальня щоденно сплачує 10% від свого прибутку місцевим кримінальним авторитетам, яких тут називають «сіндикатос». Ці боси не просто збирають данину — вони виконують роль фактичної влади на місцях. Вони організовують громадські роботи, забезпечують мінімальний порядок і, що найважливіше, запобігають відкритому насильству.

Після того, як сіндикатос отримує свою частку, вона передається далі — до держави. Армійські офіцери та державні чиновники отримують відкати від продажу золота, але натомість вони не патрулюють копальні й не намагаються роззброїти угруповання. Фактично склалася паритетна система співіснування: криміналітет контролює територію та робочу силу, а держава отримує свою частку прибутку й заплющує очі на методи її отримання.

У цьому контексті новий венесуельський законопроєкт про видобуток корисних копалин викликає більше запитань, ніж відповідей. Документ дозволяє міжнародний арбітраж для вирішення суперечок — це величезний стимул для компаній на кшталт Gold Reserve, які в минулому вже стикалися з експропріацією. Водночас, як зазначається в проаналізованих матеріалах, закон обходить мовчанкою питання збройних банд і колумбійських партизанів. Він не пропонує жодного механізму, як саме держава збирається повертати контроль над територією, яку вона фактично втратила щонайменше десять років тому.

У звітах міжнародних організацій, зокрема Управління Верховного комісара ООН з прав людини, неодноразово фіксувалися серйозні порушення в регіоні: сексуальна експлуатація, торгівля людьми, примусова праця. Проте законопроєкт не містить чітких положень про те, як захистити права місцевого населення чи як притягнути до відповідальності тих, хто скоює ці злочини.

Окрему роль у цій історії відіграють геополітичні інтереси. Виступаючи в Каракасі 4 березня, міністр внутрішніх справ США Дуг Бергам прямо назвав розблокування санкцій проти венесуельського золота стратегічною необхідністю. Мета — зламати глобальну монополію Китаю на критичні корисні копалини. Йдеться не лише про золото, а й про колтан, алмази та інші рідкісні метали, необхідні для електроніки, оборонної промисловості та зелених технологій.

Однак ніхто досі не пояснив, як саме венесуельський уряд планує повернути контроль над «Гірничою дугою Оріноко» — спеціальною економічною зоною, створеною ще за часів Мадуро в 2016 році. Ця зона охоплює 12 відсотків території країни, але де-факто залишається малодослідженим і слабко-контрольованим простором, де рішення приймаються не в Каракасі, а в таборах посеред джунглів.

Історія компанії Gold Reserve є показовою ілюстрацією того, як тісно переплітаються великий бізнес, політика та криміналітет. Заснована як канадська компанія, а сьогодні зареєстрована на Бермудах, Gold Reserve почала працювати у Венесуелі ще в 1980-х роках. Її основними активами

були родовища Брісас і Лас-Крістінас, де, за оцінками, зберігається близько 52 мільйонів унцій золота. У 2011 році тодішній президент Уго Чавес націоналізував галузь, оголосивши все золото державною власністю, й компанію вигнали з країни. Після цього Gold Reserve подала позов до міжнародних арбітражів, вимагаючи понад мільярд доларів компенсації за втрачені інвестиції. У 2016 році адміністрація Мадуро пішла на часткове примирення — було укладено попередню угоду про спільне підприємство. Але воно так і не запрацювало. Тепер, за словами джерела, наближеного до компанії, переговори про відновлення операцій «тільки починаються». Однак питання залишається відкритим: чи готова Gold Reserve, чи будь-яка інша компанія, домовлятися безпосередньо з сіндикатос? І чи є в неї інший вибір?

Аналізуючи доступні матеріали, можна дійти висновку, що Венесуела сьогодні опинилася в класичній пастці слабкої держави. З одного боку, є величезний ресурсний потенціал і політична воля до залучення інвестицій. З іншого — глибоко вкорінені злочинні структури, які стали невід'ємною частиною не лише тіньової економіки, а й соціального укладу цілих регіонів.

Спроба ігнорувати ці структури або різко їх знищити без альтернативи, як застерігає колишній шахтар, призведе до ще більшого хаосу та кровопролиття. Але спроба співпрацювати з ними, не змінюючи нічого в системі, означає для іноземних компаній ризик стати співучасниками відмивання «кривавого золота» з усіма юридичними та репутаційними наслідками.

Саме тому, спершу має відбутися дуже складна, важка робота з демонтажу злочинної структури. Іншого шляху немає. І поки ця робота не розпочнеться — а поки немає жодних ознак того, що вона дійсно ведеться, — будь-які законопроєкти, міжнародні арбітражі та стратегічні заяви про критичні мінерали залишатимуться лише декораціями. Вони не зможуть приховати головного: золото з венесуельських джунглів продовжує нести на собі невидимий, але цілком реальний відбиток крові, насильства та безкарності. І повернення великих корпорацій у цей регіон без фундаментальних змін може не очистити галузь, а навпаки — додати їй нових форм витонченої легалізаці.

Ваша думка важлива!

1. Чи є традиційна модель транзакційного моніторингу, побудована на фіксованих порогах і правилах, структурно придатною для виявлення загроз, які генеруються agentic AI та платформами Fraud-as-a-Service, — або ж ефективна протидія вимагає зміни парадигми виявлення на боці СПФМ?
2. Де проходить обґрунтована межа між рівнем автономії AI-систем у прийнятті рішень щодо підозрілих операцій і обов'язковим людським наглядом? Хто повинен нести відповідальність у разі, коли AI-система пропустила реальну схему ВК або, навпаки, заблокувала законну транзакцію?
3. Як Україні забезпечити реальну незалежність наглядових рад державних підприємств в умовах політичного впливу та воєнного стану, не втрачаючи при цьому контроль держави над стратегічними активами?
4. Які конкретні регуляторні та наглядові механізми необхідно впровадити в Україні для ефективного контролю за криптовалютними потоками, враховуючи їх роль у глобальних схемах шахрайства та відмивання коштів?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-15

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

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