Методологічний бюлетень

Серійний номер: МінФін-AML-2026-23

Червень 2026

“Той, хто пересуває гори, починає з того, що відносить маленькі камінці!”

давньокитайська мудрість

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

Аналіз структурних дефіцитів системи управління ризиками ВК у швейцарських фінансових установах [1]

Наглядове керівництво FINMA 04/2026 від 4 червня 2026 року, що доповнює Керівництво 05/2023 щодо аналізу ризиків відмивання коштів відповідно до статті 25(2) AMLO-FINMA, ґрунтується на масштабному аналітичному огляді практики близько 30 банків, перевірених навесні 2023 року, а також численних постанов відповідно до Закону про фінансові установи (FinIA) – управляючих активами, фірм з управління колективними інвестиціями, портфельних менеджерів та керуючих трастами. Документ не є ситуативною реакцією на конкретне порушення, а є методичним інструментом системного удосконалення: регулятор каталогізує стійкі дефіцити за трьома рубриками (визначення допустимого рівня ризику, аналіз ризику ВК та моніторинг дотримання стратегії), зосереджуючись виключно на ситуаціях, де практика установ залишається незадовільною, та надаючи конкретні позитивні приклади. FINMA констатує: незважаючи на прогрес порівняно зі станом 2023 року, у більшості установ зберігаються структурні прогалини, що не дозволяють аналізу ризику ВК виконувати роль справжнього центрального управлінського інструменту протидії ВК/ФТ.

[1] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20260604-finma-aufsichtsmitteilung-04-2026.pdf?sc_lang=en&hash=DC357BD566F8BABF8C3D8C54735EBB72

Перший і найбільш концептуально значимий дефіцит стосується визначення допустимого рівня ризику відмивання коштів (risk tolerance). FINMA виявила характерну патологію: установи схильні описувати лише заходи зниження ризику там, де методологічно правильним є чіткі виключення – категоричне виведення певних країн, клієнтських сегментів, продуктів або послуг зі сфери ділової активності установи. Регулятор наводить конкретні приклади належних виключень: відмова від відносин з іноземними PEP, від складних корпоративних структур, від криптосервісів, від торговельного фінансування, від клієнтів із певних галузей. Підкреслюється принципова різниця між «ми не обслуговуємо певних клієнтів» та «ми обслуговуємо їх, але з посиленими заходами контролю»: друге – це управління ризиком у рамках допустимого рівня. Формальне виключення лише тих ризиків, що і так виключені за законом (КНДР, Іран, невелике коло клієнтів, причетних до наркоторгівлі), FINMA кваліфікує як явно недостатнє.

Суттєвою системною проблемою є виявлений FINMA провал процесу «Exception to Policy» (ETP). Регулятор зафіксував установи, де ETP-процес застосовувався настільки широко, що фактично нівелював встановлений рівень допустимого ризику: виняткова одинична операція ставала правилом, а кількість схвалених ETP, не підтверджених документально та не консолідованих у централізованому реєстрі, вказувала на системний обхід регуляторного периметру – а не на управління ним. FINMA формулює принцип: якщо установа систематично дозволяє ETP для певної категорії ризику, це є сигналом необхідності формального перегляду самого визначення допустимого рівня ризику через рішення ради директорів, а не ознакою гнучкості управлінського процесу. Крім того, FINMA окремо відзначає позитивно ті нечисленні установи, які повністю забороняють ETP і суворо дотримуються визначеного рівня ризику. Ключовими вимогами є: централізований реєстр ETP-кейсів, моніторинг кількості, обсягу та тенденцій, а також регулярна звітність перед радою директорів.

Третьою проблемною зоною є відсутність або неналежна конфігурація ключових показників ризику (Key Risk Indicators – KRI). FINMA виявила, що більшість установ не визначили KRI, достатніх для регулярного моніторингу дотримання рівня допустимого ризику правлінням і радою директорів. Особливо грубими методологічними помилками є: використання відносних показників у вигляді змін порівняно з попереднім роком (що автоматично нормалізує поступове підвищення ризику без формального перегляду; FINMA зазначає, що це фактично призводить до «повзучого» розширення толерантності); агрегування клієнтів різних рівнів ризику в єдиний показник без розбиття за критичністю; визначення KRI виключно для control risk без охоплення inherent risk. Регулятор уточнює принципову відмінність: KRI і «ліміти ризику» – не тотожні поняття, KRI мають відображати ключові ризики (числові показники: кількість відносин з підвищеним ризиком, кількість PEP, кількість схвалених ETP, позиції в країнах підвищеного ризику поза цільовими ринками), а не автоматично дублювати кожен ліміт ризику.

У сфері власне методології аналізу ризиків ВК FINMA виявила системну проблему неповноти охоплення категорій ризику, прямо перелічених у статті 25(2) AMLO-FINMA – клієнтські сегменти, юрисдикція реєстрації/місця проживання, продукти та послуги. Критично важливим є і питання гранулярності: деякі банки агрегували клієнтів різних рівнів заможності (retail, affluent, HNWI) в один рядок аналізу або групували країни різного рівня ризику без розбивки за критичністю, що унеможливлює адекватну оцінку притаманного ризику. Зафіксовані грубі помилки в класифікації: привласнення рейтингу «medium» для складних корпоративних структур, для PEP або для криптосервісів замість обов'язкового «high». Для деяких банків, які займаються управлінням активів, з високим або дуже високим рівнем risk tolerance FINMA констатує, що ризик за країнами реєстрації клієнтів агрегується замість звітування на рівні окремих країн, що є неприпустимим з огляду на специфіку бізнес-моделі.

Окрема методологічна проблема – неправильне обчислення залишкового ризику. Установи схильні враховувати заходи зниження ризику на етапі притаманного ризику, або враховувати risk tolerance в контексті притаманного ризику. FINMA наголошує на нормі Додатку 3 Наглядового аудиторського регламенту FINMA від 31 жовтня 2024 року: дуже високий

притаманний ризик не може бути знижений нижче рівня «high» навіть за умови реалізації найефективніших контрольних заходів – принцип, що залишається маловідомим у практиці ринку. Аналіз опису control risk показав: більшість установ описують заходи контролю загальними посиланнями на внутрішні директиви, не надаючи показників ефективності. FINMA наводить прийнятний приклад: «Під час щомісячних перевірок підрозділу комплаєнсу у 5% випадків виявлені недоліки в документації, проте в жодному з них не встановлено порушення вимог щодо звітування».

На рівні моніторингу відповідності стратегії та ризик-політики FINMA фіксує відсутність у більшості установ конкретних числових лімітів для ризикових показників, порушення яких ініціювало б коригувальні заходи. Виявлено також нетривіальний управлінський патерн: деякі установи застосовували авторизацію ETP у випадках перевищення встановлених лімітів ризику, що є регуляторним нонсенсом – порушення ліміту ризику, що «вирішується» через ETP, означає повне розмивання управлінських функцій самого ліміту. Нарешті, більшість установ не агрегують залишковий ризик по всьому портфелю для порівняння із загальним рівнем допустимості: вони обчислюють залишковий ризик для окремих критеріїв, але не формують загальну картину і не ухвалюють заходів у разі виходу за рамки відповідного порогу, що є порушенням статті 25(2) AMLO-FINMA.

Розділ щодо установ FinIA встановлює принцип пропорційності: рівень деталізації аналізу ризику і кількість KRI визначаються природою, масштабом, складністю та ризик-профілем бізнесу. Установа з низьким рівнем притаманного ризику не зобов'язана розбивати ризик за окремими країнами або секторами – послуги можна групувати у широкі категорії за критичністю. Натомість установи з вищим ризиком зобов'язані забезпечувати більш детальну гранулярність. Принципово важливим є роз'яснення FINMA щодо методологічної відмінності між аналізом ризику ВК (ризик використання установи для ВК/ФТ – «ризик зловживання») та аналізом комплаєнс-ризику (ризик недотримання регуляторних вимог – «ризик невідповідності»): ці два документи мають різні методологічні підходи, різні притаманні ризики, що ідентифікуються, і різні заходи управління. Їх змішування або взаємна заміна є методологічною помилкою, що свідчить про нерозуміння природи ризику ВК.

Висновки:

- **Вимога FINMA чітко розмежовувати повні виключення з risk tolerance та заходи пом'якшення для допустимих категорій ризику вимагає від установ перегляду наявних документів з прийняття ризику:** якщо замість виключень у них перелічені лише «заходи EDD», аналіз ризику є юридично вразливим з точки зору FINMA і підлягає невідкладному переопрацюванню з безпосереднім залученням ради директорів до формального затвердження змін.
- Системна вимога FINMA до централізованої реєстрації та моніторингу ETP-кейсів (за кількістю, обсягом, тенденціями та якістю обґрунтування) означає, що **процес «виняток з правила» повинен управлятися через спеціалізоване IT-рішення або ретельно структуровану автоматизовану звітність – а не через ad hoc рішення правління без сукупного аналізу наслідків для профілю ризику установи.**
- **Методологічна вимога визначати KRI для притаманних ризиків вимагає перекалібрування внутрішніх аналітичних дашбордів правління та ради директорів:** ці органи повинні отримувати звітність, що дозволяє оцінювати позиціонування притаманного ризику установи, а не лише операційну ефективність заходів з пом'якшення.
- **Принцип неможливості зниження «дуже високого» притаманного ризику нижче «високого» через пом'якшувальні заходи є нормою прямої дії, що впливає на оцінку складних структур, PEP та криптовалютних послуг.** Установи, що систематично присвоювали цим категоріям «середній» рівень, ризикують мати дефектний підрахунок залишкового ризику і повинні терміново переглянути відповідні розрахунки.

Стейблкоїни в очікуванні регулювання [2]

Доповідь Комітету Палати лордів з регулювання фінансових послуг є першим масштабним законодавчим документом британського парламенту, що системно оцінює регуляторні пропозиції Банку Англії та FCA щодо стейблкоїнів виражених у фунтах стерлінгів (далі - стерлінгових стейблкоїнів), сформульовані у листопаді 2025 року у відповідних консультаційних документах. Комітет, очолюваний баронесою Ноакс, провів поглиблену роботу з аналітичною базою від провідних учасників ринку – Mastercard, Revolut, NatWest, Coinbase – та фінансових асоціацій, зокрема UK Finance. Доповідь концептуально окреслює рамки, у яких Велика Британія прагне сформувати конкурентоспроможний ринок стерлінгових стейблкоїнів на тлі вже функціонуючих американської (GENIUS Act, 2025) та європейської (MiCA, 2024) регуляторних систем, і застерігає від будь-яких затримок.

Відправна позиція доповіді поєднує стратегічний оптимізм щодо потенціалу стейблкоїнів з конкретною критикою окремих параметрів пропонованого регулювання. Комітет визнає переваги стерлінгових стейблкоїнів: швидкість та здешевлення переказів, ефективність розрахунків, програмованість платежів. Водночас підкреслюється чіткий ризик: значні затримки у прийнятті регуляторного режиму здатні закріпити глобальне домінування доларових стейблкоїнів (насамперед USDT та USDC) і виштовхнути британські фінтех-компанії на нестерлінгові платіжні рейки. Доповідь особливо акцентує потенційний ефект для сегменту послуг з переказу коштів: програмовані стерлінгові токени можуть автоматизувати виплати та усунути додаткові валютні і посередницькі витрати – однак лише за умови відповідної регуляторної ясності, яка наразі відсутня.

Центральний предмет критики – вимога Банку Англії до системних емітентів стейблкоїнів тримати щонайменше 40% резервних активів у безвідсоткових депозитах безпосередньо у Банку Англії. Комітет, спираючись на позицію більшості респондентів, встановлює, що ця вимога: (а) робить Велику Британію «міжнародним аутсайдером» порівняно з MiCA та GENIUS Act, де аналогічні жорсткі вимоги відсутні; (б) суттєво погіршує бізнес-модель емітентів, оскільки безвідсоткові депозити є прямим операційним збитком; (в) підриває загальну конкурентоспроможність майбутнього британського стерлінгового ринку на тлі регуляторно більш сприятливих юрисдикцій. Комітет рекомендує Банку Англії перейти до менш директивного підходу до структури резервних активів та розглянути питання про нарахування базової відсоткової ставки на депозити, що зберігаються в ньому як резерви.

Другим вектором критики є пропоновані ліміти на утримання стейблкоїнів: £20 000 для фізичних осіб та £10 млн для юридичних осіб. Комітет вважає ці обмеження передчасними і такими, що «необґрунтовано гальмують зростання стерлінгових стейблкоїнів», оскільки вони запроваджуються ще до того, як ринок продемонстрував реальні задокументовані системні ризики фінансової стабільності. Підкреслюється, що ці ліміти надзвичайно складно технічно реалізувати: одна особа може утримувати стейблкоїни через різних емітентів без можливості агрегованого моніторингу між різними емітентами, що робить таке обмеження не лише обтяжливим, але й неефективним. Комітет рекомендує відстрочити введення будь-яких лімітів до моменту, коли фінансово-стабілізаційні ризики чітко виявляться і обґрунтують відповідні заходи у формі конкретних ринкових даних.

Третя критична ділянка – вимоги до компаній, що прагнуть емітувати стейблкоїни: вони зобов'язані робити це під окремим брендом і через insolvency-remote entity (відокремлену структуру із захистом від банкрутства). Комітет оцінює цю вимогу як «надмірно обмежувальну та таку, що ризикує непотрібно стримувати інновації» – вона фактично унеможливлює для великих комерційних банків (Barclays, NatWest, Lloyds) пряму інтеграцію стерлінгових стейблкоїнів у свій основний бренд і продуктовий ряд. Комітет рекомендує переглянути цю вимогу, беручи до уваги, що присутність сильних брендів традиційних банків

[2] https://publications.parliament.uk/pa/ld5902/ldselect/ldfsrc/6/6.pdf

на ринку стейблкоїнів підвищуватиме рівень довіри споживачів і прискорюватиме ринкове прийняття технології, а не загрожуватиме фінансовій стабільності.

У сфері ПВК/ФТ та ризиків незаконного фінансування доповідь займає виважену, але аналітично чітку позицію. Визнається, що стейблкоїни можуть використовуватися для фінансової злочинності та відмивання коштів. Проте доповідь наводить протилежний аргумент: ці ризики можуть бути пом'якшені в такий самий спосіб, яким вони вже пом'якшуються стосовно інших форм грошей – через KYC, AML-процедури та моніторинг транзакцій. Комітет застерігає регуляторів від застосування «більш суворого ризикового підходу до стейблкоїнів, ніж до інших форм платежів», оскільки це нерівноважно порівняно з ризиками, що вже приймаються стосовно карткових мереж, SWIFT-переказів та кореспондентського банкінгу. Підкреслюється необхідність «нейтральності до варіантів використання» регуляторного режиму.

Найбільш значимою з точки зору ПВК/ФТ є рекомендація щодо некастодіальних гаманців (unhosted wallets). Комітет закликає Казначейство у взаємодії з Банком Англії та FCA оцінити достатність чинного правового поля Великої Британії для виявлення та запобігання зловживанням з некастодіальними гаманцями, при цьому явно запрошуючи уряд до законодавчого обмеження їх використання, якщо наявне регулювання виявиться недостатнім. Це є значним зрушенням у тональності: Комітет, загалом схильний до підтримки інновацій, у цьому конкретному питанні чітко сигналізує про готовність підтримати обмежувальне законодавство щодо некастодіальних гаманців – у відповідь на занепокоєння, що проявилися у США та ЄС у зв'язку з підходом адміністрації Трампа до крипторинку та відповідними ризиками переміщення незаконних коштів до менш регульованих юрисдикцій.

Висновки:

- **Рекомендація Комітету Палати лордів про юридичну оцінку достатності чинного законодавства Великобританії щодо некастодіальних гаманців та потенційне законодавче обмеження їх використання** є прямим сигналом для VASP та провайдерів для інфраструктури: необхідно готуватися до посилення вимог Travel Rule та розширення KYC-стандартів для транзакцій з некастодіальними гаманцями у найближчій перспективі.
- **Відмова від передчасного введення лімітів на суму утримуваних стейблкоїнів однією особою означає, що регулятори, вірогідно, компенсуватимуть це посиленням вимог до реєстрації та звітності щодо обсягів утримання стейблкоїнів з боку емітентів** – СПФМ повинні закладати відповідні вимоги до звітування в архітектуру своїх комплаєнс-систем заздалегідь.
- **Критика вимоги до зберігання 40% резервів у безвідсоткових депозитах у Банку Англії є суттєвим тиском на конфігурацію вимог ліквідності для майбутніх системних стейблкоїн-емітентів**. Якщо Банк Англії не пом'якшить цю вимогу, ринок стерлінгових стейблкоїнів, вірогідно, залишатиметься нішевим, а СПФМ, що очікують транзакцій у стерлінгових стейблкоїнах, повинні закладати обмежений попит на такі інструменти в поточному регуляторному середовищі.

Ширший конкурентний контекст, що пронизує всю доповідь, полягає у наступному: глобальний ринок стейблкоїнів домінується доларовими токенами, а США і ЄС вже сформували відносно стабільні регуляторні рамки. Якщо Велика Британія не завершить регуляторний процес у найближчі строки, британські фінтехи та платіжні компанії, що розробляють стейблкоїн-рішення, із великою ймовірністю переорієнтуються на доларовий або євро-ринок – стандартний сценарій регуляторного арбітражу, що вже неодноразово спостерігався у британській фінтех-екосистемі. Баронеса Ноакс підсумовує ключову дилему: «Регулювання повинне дозволяти інновації, водночас забезпечуючи ефективне пом'якшення ризиків. Форма майбутнього британського ринку стейблкоїнів буде сильно визначатися напрямом регуляторного режиму – і тому регулятори повинні правильно скалібрувати баланс».

Цифрова трансформація платіжних систем країн Балтії та нові виклики у сфері ПВК/ФТ [3]

Документ є спільним стратегічним дослідженням підрозділів фінансової розвідки (ПФР) Естонії, Латвії та Литви за підтримки Банку Литви, присвяченим аналізу трансформації платіжного сектору Балтійського регіону та її впливу на ризики відмивання коштів і фінансування тероризму у період 2021 – першого півріччя 2024. Дослідження має комплексний міждержавний характер і поєднує аналіз фінансової статистики, даних платіжних сервісів, інформації ПФР, повідомлення про підозрілі операції (STRs), національних оцінок ризиків (НОР), а також міжнародних звітів IMF, EBA, ECB та інших джерел. Основною метою документа є оцінка того, як стрімка цифровізація фінансових послуг, розвиток фінтех-сектору та зростання транскордонного використання платіжних сервісів змінюють архітектуру ризиків ВК/ФТ у Балтійському регіоні.

Документ виходить із того, що Балтійські держави за останні роки пройшли одночасно два взаємопов'язані процеси: масштабне посилення системи ПВК/ФТ після великих фінансових скандалів кінця 2010-х років та швидку цифрову трансформацію фінансового сектору. Усі три країни значно посилили ризик-орієнтований нагляд, міжвідомчу координацію, співпрацю між ПФР, правоохоронними органами та наглядовими органами, удосконалили механізми забезпечення прозорості бенефіціарної власності, а також активізували державно-приватне партнерство. Водночас цифровізація фінансового сектору, дистанційне встановлення ділових відносин, розвиток фінтех-моделей та інтеграція до фінансового ринку ЄС створили принципово нові вразливості у сфері ПВК/ФТ, пов'язані зі швидким транскордонним переміщенням коштів, ускладненням відстеження фінансових потоків та появою нових цифрових фінансових посередників.

Дослідження демонструє, що хоча Естонія, Латвія та Литва мають формально схожі регуляторні системи ПВК/ФТ, фактична структура їхніх фінансових ринків та ризикові профілі суттєво відрізняються. Естонія та Латвія характеризуються банкоцентричними моделями фінансового сектору з переважно внутрішньою клієнтською базою та відносно обмеженою міжнародною активністю фінтех-сектору. Після проведення масштабних реформ обидві країни реалізували політику цілеспрямованого зниження ризиків шляхом скорочення експозиції до високоризикових клієнтів-нерезидентів та посилення заходів контролю у сфері ПВК/ФТ. Це сприяло підвищенню стійкості фінансових систем і зменшенню залежності від ризикових транскордонних потоків капіталу. Разом із тим наслідком такої політики стало широке застосування практик де-ріскінгу та припинення ділових відносин із частиною клієнтів, які оцінювалися як такі, що мають підвищений ризик ВК/ФТ.

Литва, на відміну від Естонії та Латвії, свідомо обрала стратегію розвитку як регіонального центру фінансових технологій. Банк Литви проводив активну політику залучення фінтех-компаній через формування сприятливого регуляторного середовища, розвиток сучасної платіжної інфраструктури, інтеграцію до сервісів TARGET Євросистеми, підтримку відкритого банкінгу та спрощення процедур ліцензування. Це дозволило країні стати однією з провідних фінтех-юрисдикцій ЄС, насамперед у сегменті платіжних установ та установ електронних грошей. Дослідження показує, що масштаби розвитку цього сектору в Литві є непропорційно високими порівняно з розміром економіки країни та суттєво перевищують відповідні показники інших держав Балтії.

Водночас автори прямо зазначають, що саме така модель розвитку сформувала нові структурні ризики ВК/ФТ. IMF та НОР Литви визначають сектор платіжних установ та установ електронних грошей як найбільш ризиковий сегмент фінансової системи через високу частку клієнтів-нерезидентів, широке використання механізмів дистанційного встановлення ділових відносин, значні обсяги транскордонних операцій, проведення транзитних платежів та

[3] https://fiu.ee/sites/default/files/documents/2026-05/Evolving%20Payment%20Landscape%20and%20AML%20Challenges%20in%20the%20Baltic%20States.pdf

обслуговування високоризикових видів економічної діяльності. Документ наголошує, що стрімке зростання цифрових фінансових сервісів у багатьох випадках випереджає наглядові та аналітичні спроможності компетентних органів, що створює ризик виникнення прогалин у системі контролю у сфері ПВК/ФТ.

Одним із ключових аспектів дослідження є аналіз клієнтської структури та обсягів операцій постачальників платіжних послуг у країнах Балтії. Дослідження показує, що кредитні установи залишаються основними учасниками фінансового ринку за кількістю клієнтів і обсягами операцій. Водночас у Литві сектор платіжних установ та установ електронних грошей відіграє значно важливішу роль, ніж в Естонії та Латвії. Якщо в останніх його частка становить близько 0,2% від обсягів операцій кредитних установ, то у Литві вона сягає близько 11%, що свідчить про високий рівень розвитку та інтеграції фінтех-сектору у фінансову систему країни.

Документ також досліджує структуру клієнтської бази у розрізі фізичних та юридичних осіб. Хоча в усіх країнах переважають клієнти-фізичні особи, основна частина фінансових операцій генерується юридичними особами. Особливо це характерно для Литви, де середні обсяги операцій юридичних осіб у секторі платіжних установ та установ електронних грошей обчислюються сотнями тисяч євро. Така концентрація значних фінансових потоків підвищує притаманний ризик ВК/ФТ та ускладнює застосування ефективних заходів моніторингу. Автори підкреслюють, що великі обсяги транзакцій у цифрових платіжних установах створюють додаткові виклики для систем ПВК/ФТ, особливо коли йдеться про складні транскордонні фінансові та корпоративні структури.

Значну увагу в дослідженні приділено географічному розподілу клієнтів та масштабам транскордонного використання платіжних послуг у Балтійському регіоні. Якщо фінансові установи Естонії та Латвії переважно зосереджені на обслуговуванні внутрішніх клієнтів, то Литва демонструє значно вищий рівень міжнародної інтеграції. За даними дослідження, у 2024 році приблизно 72% клієнтів литовських постачальників платіжних послуг становили резиденти інших держав-членів ЄС. Така структура клієнтської бази свідчить про формування в Литві регіонального центру транскордонних платіжних послуг та фінансових технологій, що забезпечує її глибоку інтеграцію до європейського фінансового простору, але водночас підвищує ризики, пов’язані з транскордонними фінансовими потоками та ПВК/ФТ.

Дослідження наголошує на тому, що політика зниження ризиків, реалізована в Латвії та Естонії після посилення режиму ПВК/ФТ, мала не лише позитивні, а й побічні ефекти. Масове припинення ділових відносин із клієнтами, які оцінювалися як високоризикові, сприяло їхньому переміщенню до інших фінансових установ регіону, насамперед до литовських фінтех-компаній, платіжних установ та установ електронних грошей. Автори доходять висновку, що в багатьох випадках відбулося не зниження ризиків, а їхнє перенесення між секторами та країнами. Це особливо характерно для латвійсько-литовського фінансового коридору, де спостерігалася найбільша міграція клієнтів. На думку авторів, невибірковий підхід до зниження ризиків може створювати нові вразливості у сфері ПВК/ФТ, коли клієнти з підвищеним ризиком переходять до установ із менш розвиненими системами контролю та управління ризиками.

Одним із найважливіших аналітичних напрямів дослідження є аналіз типологій ВК/ФТ на основі повідомлень про підозрілі фінансові операції та інформації, отриманої підрозділами фінансової розвідки. Результати свідчать про формування в Балтійському регіоні стійких транскордонних схем, пов’язаних із шахрайством, шахрайством у сфері ПДВ, ухиленням від сплати податків, обходом санкційних обмежень, діяльністю організованої злочинності та використанням криптоактивів. Дослідження показує, що в багатьох випадках ключову роль у таких схемах відіграють рахунки, відкриті у литовських фінтех-компаніях, які використовуються для оперативного переміщення коштів між країнами та ускладнення встановлення маршруту їхнього руху і походження.

Дослідження наголошує, що організовані злочинні мережі дедалі частіше використовують цифрові банки, установи електронних грошей, постачальників послуг, пов'язаних з віртуальними активами, а також екосистеми вбудованих фінансових послуг для реалізації складних багаторівневих схем ВК/ФТ. Серед найпоширеніших типологій виокремлюються компанії-оболонки, використання підставних осіб, транзитних рахунків та структур на основі віртуальних міжнародних банківських рахунків. Такі інструменти дають змогу приховувати інформацію про кінцевих бенефіціарних власників, маскувати справжню економічну сутність операцій та значно ускладнювати виявлення і відстеження незаконних фінансових потоків.

Дослідження окремо акцентує увагу на ризиках, пов'язаних із моделями «банкінг як послуга» та вбудованих фінансових послуг. На думку авторів, поширення таких моделей формує нові вразливості у сфері ПВК/ФТ, оскільки фінансові послуги дедалі частіше надаються через цифрові платформи та технологічні екосистеми, а межі між фінансовими установами та технологічними провайдерами стають менш чіткими. За таких умов банки та установи електронних грошей можуть надавати платіжну інфраструктуру, віртуальні міжнародні банківські рахунки та кореспондентські послуги широкому колу посередників, включаючи криптовалютні платформи та фінтех-компанії. Це підвищує складність встановлення походження коштів, ідентифікації учасників операцій та забезпечення належної прозорості транскордонних фінансових потоків.

Дослідження наголошує на стрімкому зростанні кіберзалежної фінансової злочинності як наслідку прискореної цифрової трансформації фінансового сектору. Пандемія COVID-19 стала каталізатором розвитку дистанційного банківського обслуговування, цифрової ідентифікації клієнтів та транскордонних цифрових фінансових послуг, що забезпечило суттєві переваги для споживачів, але одночасно розширило можливості для шахрайства, кіберзлочинності та використання цифрових каналів для відмивання коштів. Автори підкреслюють, що швидкість розвитку фінтех-сектору дедалі більше випереджає можливості традиційного нагляду, що вимагає модернізації підходів до фінансової розвідки, моніторингу транзакцій та виявлення підозрілих фінансових операцій.

Однією з ключових проблем, на які звертає увагу дослідження, є фрагментація даних та недостатній рівень гармонізації фінансової статистики в Балтійському регіоні. Автори наголошують, що відсутність єдиних підходів до збору, класифікації та аналізу інформації про клієнтів платіжних установ і установ електронних грошей, транскордонні платіжні потоки та структуру клієнтських баз істотно ускладнює проведення комплексної регіональної оцінки ризиків ВК/ФТ. На думку авторів, в умовах високої інтеграції фінансових ринків традиційний аналіз ризиків на рівні окремих держав уже не дозволяє повною мірою виявляти транскордонні загрози. У зв'язку з цим виникає потреба у створенні спільних регіональних аналітичних механізмів, гармонізованих підходів до оцінки ризиків та постійного обміну інформацією між ПФР, наглядовими та правоохоронними органами.

Дослідження показує, що цифрова платіжна екосистема Балтійського регіону фактично функціонує як єдиний високоінтегрований транскордонний фінансовий простір, у якому ризики ВК/ФТ швидко перетікають між країнами, фінансовими секторами та різними категоріями фінансових посередників. Автори наголошують, що навіть суттєве посилення національних систем ПВК/ФТ не гарантує автоматичного зниження системних ризиків, оскільки вони можуть переноситися між юрисдикціями внаслідок транскордонної міграції клієнтів, фінансових потоків та бізнес-моделей. Це свідчить про необхідність розглядати ризики ВК/ФТ не лише на національному, а й на регіональному рівні.

У рекомендаційній частині документа автори наголошують на необхідності формування комплексної системи регіональної взаємодії у сфері ПВК/ФТ. Серед ключових пропозицій – розроблення спільних регіональних індикаторів ризику для виявлення підозрілих операцій, пов'язаних із постачальниками платіжних послуг, гармонізація підходів до звітності, регулярний обмін результатами досліджень типологій ВК/ФТ та впровадження спільних програм підготовки для наглядових органів, ПФР і суб'єктів первинного фінансового моніторингу. Автори також підкреслюють важливість зміцнення аналітичних спроможностей компетентних органів, використання сучасних технологій моніторингу транзакцій та посилення нагляду за фінтех-компаніями, цифровими банками й інфраструктурою вбудованих фінансових послуг, які дедалі більше впливають на ризиковий профіль фінансової системи.

У підсумку автори доходять висновку, що Балтійський регіон є одним із найяскравіших прикладів впливу цифрової трансформації фінансового сектору на ризики ВК/ФТ. Дослідження показує, що стрімкий розвиток фінансових технологій, цифрових платіжних сервісів та транскордонної інтеграції поступово змінює традиційну архітектуру фінансового сектору і водночас створює нові виклики для систем ПВК/ФТ. За таких умов моделі нагляду та контролю, побудовані навколо традиційного банківського сектору, втрачають свою достатність. Балтійський кейс демонструє, що ефективне управління ризиками ВК/ФТ у сучасній цифровій економіці потребує поглибленої міжнародної співпраці, гармонізації наглядових підходів, активного обміну інформацією та створення інтегрованих регіональних механізмів фінансової розвідки.

Висновки:

- **Документ демонструє, що агресивна політика зниження ризиків у банківському секторі не усуває ризики ВК/ФТ, а часто переміщує їх до фінтех-компаній, платіжних установ та установ електронних грошей.** Це підкреслює необхідність ризик-орієнтованого управління ризиками замість механічного закриття рахунків.
- **Документ демонструє, що поширення нових цифрових платіжних моделей підвищує ризики ВК/ФТ, шахрайства та обходу санкцій.** Це вимагає посилення нагляду за фінтех-компаніями та іншими учасниками цифрової платіжної екосистеми.
- **Документ демонструє, що поширення нових цифрових платіжних моделей підвищує ризики ВК/ФТ, шахрайства та обходу санкцій.** Це вимагає посилення нагляду за фінтех-компаніями та іншими учасниками цифрової платіжної екосистеми.
- **Документ демонструє, що поширення нових цифрових платіжних моделей створює додаткові вразливості для ВК/ФТ, шахрайства та обходу санкцій.** Практичний висновок полягає у необхідності адаптації систем ПВК/ФТ до цифрового фінансового середовища та посилення контролю за небанківськими фінансовими посередниками.

Трансформація міжнародних платежів у добу токенізації фінансових активів [4]

Документ є результатом масштабної спільної ініціативи центральних банків, міжнародних фінансових інституцій та провідних комерційних банків, спрямованої на дослідження можливостей трансформації сучасної системи транскордонних платежів за допомогою токенізації та програмованих фінансів. У центрі дослідження знаходиться проблема структурної неефективності чинної міжнародної платіжної архітектури, яка базується на мережі кореспондентських банківських відносин. Автори зазначають, що така модель, незважаючи на свою надійність та багаторічне функціонування, залишається складною, фрагментованою та витратною через необхідність залучення численних посередників, проведення багатоетапних перевірок, використання різних платіжних систем і виконання

[4] https://www.bis.org/publ/othp110.pdf

розрахунків через декілька юрисдикцій. У результаті транскордонні платежі часто супроводжуються високими операційними витратами, затримками, обмеженою прозорістю та складними процесами управління ліквідністю.

Проєкт Agorá пропонує принципово новий підхід до організації міжнародних розрахунків через створення спільної програмованої платформи, на якій можуть взаємодіяти токенізовані резерви центральних банків та токенізовані депозити комерційних банків. При цьому автори наголошують, що метою проєкту не є заміна існуючої дворівневої банківської системи або створення нової форми грошей. Навпаки, дослідження виходить із необхідності збереження поточної ролі центральних та комерційних банків, але із перенесенням їхніх зобов'язань у токенізоване середовище, що дозволяє використовувати переваги програмованих фінансів та технологій розподілених реєстрів. В основі проєкту лежить концепція Єдиного реєстру, відповідно до якої різні форми фінансових активів можуть існувати в спільному цифровому середовищі, де правила взаємодії визначаються програмним кодом і виконуються автоматично.

Значна увага у документі приділяється архітектурі майбутньої платформи. Автори описують модель, яка складається з двох взаємопов'язаних рівнів. Перший рівень являє собою спільний міжнародний реєстр, у межах якого здійснюється координація транскордонних платежів і циркуляція токенізованих депозитів комерційних банків. Другий рівень представлений окремими національними реєстрами центральних банків, у яких обліковуються токенізовані резерви відповідної юрисдикції. Такий підхід дозволяє поєднати глобальну інтеграцію платіжних процесів із збереженням монетарного суверенітету кожної держави. Центральні банки продовжують повністю контролювати власні резерви, визначати правила доступу до них та забезпечувати дотримання національних нормативних вимог, тоді як міжнародна платформа виконує функцію координації та синхронізації транскордонних операцій.

Окремим предметом аналізу є життєвий цикл транскордонного платежу в межах нової архітектури. Документ демонструє відхід від традиційної послідовної моделі виконання операцій, коли кожний учасник проводить власні перевірки та здійснює дії незалежно від інших сторін процесу. Натомість пропонується модель попередньої координації всіх елементів платежу ще до початку розрахунків. На першому етапі здійснюється підтвердження отримувача коштів для мінімізації ризику помилкових платежів. Далі система автоматично визначає оптимальний маршрут проведення операції через мережу фінансових установ. Після цього всі учасники виконують необхідні перевірки щодо відповідності вимогам ПВК/ФТ, санкційного законодавства, внутрішніх процедур управління ризиками та інших регуляторних вимог. Наступним етапом є резервування ліквідності всіма сторонами операції. Лише після виконання всіх попередніх умов запускається фінальний етап розрахунку, який відбувається одночасно для всіх учасників.

Ключовою технологічною особливістю проєкту є використання механізму атомарного розрахунку. Документ детально пояснює, що всі зміни балансів між учасниками здійснюються як єдина неподільна операція. Це означає, що транзакція або виконується повністю для всіх сторін, або не виконується взагалі. Такий підхід дозволяє практично усунути класичний розрахунковий ризик, який виникає у випадках, коли одна сторона вже виконала свої зобов'язання, тоді як інша ще не завершила відповідну частину операції. Автори підкреслюють, що під час експерименту вдалося підтвердити технічну можливість реалізації такого механізму одночасно для кількох валют та юрисдикцій, що є одним із найбільш значущих результатів проєкту.

Суттєве місце у дослідженні займають питання комплаєнсу та фінансової безпеки. Документ розглядає можливість інтеграції процедур ПВК/ФТ, санкційного скринінгу, протидії шахрайству та інших контрольних механізмів безпосередньо в процес виконання транскордонних платежів. При цьому автори свідомо відмовляються від моделі централізації конфіденційних даних на спільній платформі. Кожна фінансова установа зберігає відповідальність за проведення власних перевірок клієнтів і транзакцій, а на платформу

передаються лише результати таких перевірок, необхідні для продовження операції. Такий підхід дозволяє поєднати вимоги щодо фінансової прозорості та контролю з дотриманням вимог щодо захисту інформації, банківської таємниці та конфіденційності клієнтів. Автори також звертають увагу на перспективи скорочення дублювання перевірок між фінансовими установами та підвищення ефективності міжнародної взаємодії у сфері ПВК/ФТ.

Важливим напрямом дослідження є правовий аналіз токенізованих форм грошей. Документ доходить висновку, що токенізація сама по собі не змінює юридичної природи фінансових активів. Токенізовані резерви продовжують залишатися зобов'язаннями центральних банків, а токенізовані депозити – зобов'язаннями комерційних банків. Це дозволяє використовувати більшість існуючих правових конструкцій без необхідності фундаментального перегляду чинного законодавства. Водночас автори визнають, що для повноцінного впровадження подібної інфраструктури необхідно додатково врегулювати питання остаточності розрахунків, відповідальності учасників, управління платформою та розподілу повноважень між національними регуляторами.

Окремо розглядаються питання операційної стійкості, кібербезпеки та управління ліквідністю. Автори наголошують, що майбутні токенізовані платіжні системи повинні функціонувати в режимі безперервної доступності та забезпечувати високий рівень захисту від технологічних збоїв і кіберзагроз. Також значна увага приділяється можливості автоматизації процесів управління ліквідністю через використання програмованих механізмів резервування коштів та оптимізації міжбанківських розрахунків.

У підсумку документ формує бачення майбутньої міжнародної платіжної інфраструктури як єдиного програмованого середовища, у якому транскордонні платежі виконуються практично в режимі реального часу, із попередньою автоматизованою перевіркою всіх умов операції, інтегрованими механізмами ПВК/ФТ та мінімізацією розрахункових ризиків. Проєкт Agorá демонструє, що токенізація поступово переходить із концептуальної площини до стадії практичного тестування на рівні провідних центральних банків та найбільших міжнародних фінансових установ, формуючи потенційну основу для наступного покоління глобальної платіжної інфраструктури.

Висновки:

- **Документ демонструє, що майбутня архітектура транскордонних платежів поступово зміщується від обміну фінансовими повідомленнями до моделі спільних програмованих платформ із використанням токенізованих грошей центральних та комерційних банків.** Це створює передумови для суттєвої трансформації глобальної платіжної інфраструктури.
- **Дослідження показує, що механізми атомарного розрахунку та попередньої координації всіх учасників платежу здатні значно зменшити операційні, кредитні та розрахункові ризики.** Це вимагає від фінансових установ адаптації процесів управління ліквідністю та підготовки до роботи у середовищі програмованих фінансів.
- **Автори наголошують, що контроль у сфері ПВК/ФТ може бути інтегрований безпосередньо у процес виконання транскордонних платежів із використанням автоматизованих перевірок та підтвердження результатів комплаєнс-процедур між учасниками.** Для сфери ПВК/ФТ це відкриває можливості для підвищення ефективності контролю та скорочення дублювання перевірок.
- **Проєкт підтверджує, що токенізація фінансової інфраструктури вже переходить із концептуальної стадії до практичного тестування за участю провідних центральних банків і глобальних фінансових установ.** Це свідчить про необхідність для регуляторів та учасників фінансового сектору враховувати такі моделі під час розробки майбутніх стратегій цифрової трансформації фінансових ринків.

Управління корупційними ризиками у лісовій галузі: практичні підходи країн Латинської Америки [5]

Документ підготовлений Базельським інститутом управління на основі практичного досвіду реалізації програми Green Corruption у Болівії, Еквадорі та Перу й присвячений розробці та впровадженню механізмів управління корупційними ризиками у ланцюгу створення вартості деревини. Центральна ідея дослідження полягає в тому, що незаконна вирубка лісів, нелегальна торгівля деревиною та деградація лісових екосистем не можуть розглядатися виключно як екологічні або природоохоронні проблеми. На думку авторів, одним із головних структурних чинників цих явищ є корупція, яка створює умови для обходу законодавства, маніпуляцій із дозвільними процедурами, легалізації незаконно заготовленої деревини та уникнення відповідальності за порушення. Саме тому документ пропонує перейти від переважно реактивної моделі боротьби з порушеннями до системної моделі попередження корупції шляхом виявлення та усунення корупційних ризиків ще до того, як вони реалізуються на практиці.

У вступній частині дослідження детально описується ситуація з лісовими ресурсами в Амазонському регіоні. Автори наголошують, що Болівія, Еквадор і Перу продовжують втрачати значні площі природних лісів через поєднання таких факторів, як комерційна заготівля деревини, розширення сільськогосподарських угідь, лісові пожежі та незаконний видобуток корисних копалин. Додатковим каталізатором цих процесів виступає корупція, яка послаблює ефективність державного контролю та сприяє проникненню незаконно добутої деревини до легальних ринків. У цьому контексті автори використовують поняття «зелена корупція», під яким розуміються корупційні практики, що прямо або опосередковано призводять до виснаження природних ресурсів, руйнування екосистем та погіршення екологічного управління. Документ підкреслює, що корупція в екологічному секторі має не лише економічні наслідки, але й безпосередньо впливає на сталий розвиток, права місцевих громад та досягнення Цілей сталого розвитку ООН.

Значна частина документа присвячена концепції управління корупційними ризиками. Автори виходять із того, що ризик корупції не означає наявність уже вчиненого правопорушення, а характеризує можливість виникнення ситуації, за якої посадова особа може використати свої повноваження в особистих інтересах або в інтересах третіх осіб. Управління такими ризиками розглядається як безперервний цикл, що включає ідентифікацію ризиків, оцінку їх імовірності та наслідків, визначення заходів реагування, моніторинг та постійне вдосконалення системи контролю. При цьому особлива увага приділяється не лише індивідуальній поведінці посадових осіб, а й організаційним умовам, які можуть сприяти виникненню корупції. До таких умов віднесено нечітке нормативне регулювання, надмірну дискрецію посадовців, недостатню прозорість процедур, слабкі механізми контролю та низький рівень підзвітності. Автори підкреслюють, що ефективна антикорупційна політика повинна бути інтегрована в повсякденну діяльність організації та стати елементом її інституційної культури.

Для практичного застосування цього підходу було проведено аналіз усіх основних етапів ланцюга створення вартості деревини. У документі описується, що такий ланцюг охоплює заготівлю лісових ресурсів, транспортування деревини, первинну та вторинну переробку, а також реалізацію продукції на внутрішньому й міжнародному ринках. У кожному з цих сегментів діють різні групи учасників: власники лісових ділянок, користувачі лісових ресурсів, лісові менеджери, перевізники, посередники, власники складів та пилорам, деревообробні підприємства, експортери та торговельні структури. Аналіз показав, що найбільш вразливими до корупції є ті етапи, де державні органи наділені повноваженнями приймати рішення щодо доступу до ресурсів, контролювати діяльність суб'єктів господарювання або застосовувати санкції. Саме тому дослідження зосереджується на трьох

[5] https://baselgovernance.org/sites/default/files/2026-04/260401_Preventing-corruption-in-the-timber-value-chain_Latam.pdf

ключових ризикових контекстах: наданні лісокористувальних прав, видачі та використанні транспортних накладних на перевезення деревини, а також здійсненні наглядових і контрольних функцій державними органами.

У межах першого ризикового контексту особливу увагу приділено процедурі надання прав на заготівлю деревини. Документ показує, що саме цей етап фактично визначає легальність подальшої діяльності в ланцюгу створення вартості деревини. Найбільш поширеним ризиком визнається змова між посадовими особами та заявниками, за якої дозволи можуть видаватися на основі недостовірної інформації, фальсифікованих лісогосподарських планів або без належної перевірки дотримання встановлених вимог. Особливу небезпеку становлять спеціальні дозволи на видалення лісового покриву, де економічна цінність отриманої деревини створює додаткові стимули для зловживань. Іншим важливим ризиком визначено зловживання владою з боку посадових осіб, яке може проявлятися у навмисному затягуванні процедур, створенні штучних адміністративних бар'єрів або вимаганні неправомірної вигоди за прискорення процесу. Автори наголошують, що особливо вразливими до таких практик є громадянське суспільство та сільські громади, які часто мають обмежений доступ до інформації та стикаються з мовними або географічними бар'єрами.

Другим великим блоком дослідження є аналіз корупційних ризиків, пов'язаних із транспортними накладними на перевезення деревини. Саме ці документи забезпечують простежуваність походження деревини та є ключовим інструментом запобігання проникненню незаконно заготовленої продукції до легального обігу. Документ демонструє, що фальсифікація інформації у транспортних документах, завищення обсягів деревини, використання порожніх або повторно використаних накладних, а також оформлення документів на деревину невідомого походження є одними з основних механізмів легалізації незаконної деревини. Водночас існують ризики, коли посадові особи навмисно вводять заявників в оману щодо вимог до оформлення документів або використовують технічні проблеми інформаційних систем як привід для вимагання неправомірної вигоди. Як відповідь на ці виклики документ акцентує увагу на необхідності автоматизації процесів, використання електронних систем оформлення документів та максимального усунення людського фактора із процедур ухвалення рішень.

Особливе місце в дослідженні займає аналіз фізичних інспекцій та контрольних заходів. Автори наголошують, що навіть за наявності формально належно оформлених документів ефективність системи залежить від здатності державних органів здійснювати перевірки безпосередньо на місцях. Разом із тим саме інспекційна діяльність створює широкі можливості для корупційних зловживань. Посадові особи можуть свідомо не проводити перевірки, погоджуватися на фіктивне підтвердження даних, приховувати порушення або фальсифікувати результати інспекцій в обмін на хабарі. Документ детально описує ризики як на етапі попередніх перевірок перед наданням прав на заготівлю деревини, так і під час контролю фактичного використання лісових ресурсів, перевірок на стаціонарних та мобільних контрольних постах, а також аудитів підприємств із переробки та реалізації деревини. Важливою проблемою визначається обмеженість ресурсів природоохоронних органів, які через нестачу персоналу та фінансування не здатні перевіряти всі об'єкти, що створює ризики вибіркового контролю та непрозорого визначення пріоритетів для інспекцій.

Окремий розділ присвячено адміністративним санкційним процедурам. Автори підкреслюють, що навіть ефективне виявлення порушень не гарантує результативності системи, якщо рішення про притягнення винних до відповідальності можуть блокуватися або спотворюватися через корупційний вплив. Особливу увагу приділено ризику тиску з боку керівництва на працівників, відповідальних за розгляд справ, а також можливості змови між посадовими особами та порушниками для приховування фактів правопорушень або пом'якшення санкцій. Такі практики створюють атмосферу безкарності, підривають довіру до державних інституцій та знижують превентивний ефект контролю. Документ наголошує на важливості цифровізації матеріалів справ, створення механізмів простежуваності всіх

процесуальних дій, проведення вибіркових перевірок завершених проваджень та забезпечення максимальної прозорості санкційних рішень.

Завершуючи аналіз, автори переходять до питання формування культури доброчесності як фундаментальної умови довгострокового зниження корупційних ризиків. Документ виходить із того, що навіть найкращі процедури контролю не можуть повністю усунути ризики, якщо працівники не поділяють принципів етичної поведінки та служіння суспільним інтересам. Саме тому значна увага приділяється проведенню навчальних програм з питань доброчесності, управління ризиками, антикорупційного законодавства та професійної етики. Додатково рекомендується проводити інформаційні кампанії, посилювати взаємодію з правоохоронними органами, здійснювати перевірки доброчесності персоналу та розвивати механізми співпраці з громадянським суспільством і місцевими громадами. Одним із головних висновків дослідження є те, що управління корупційними ризиками повинно стати невід'ємною частиною інституційного управління природними ресурсами, а не розглядатися як окремий антикорупційний проєкт. Досвід Болівії, Еквадору та Перу демонструє, що системне поєднання організаційних реформ, цифровізації, міжвідомчої взаємодії та розвитку культури доброчесності здатне суттєво знизити ризики корупції та зміцнити управління лісовими ресурсами у країнах Латинської Америки.

Висновки:

- **Документ демонструє, що найбільші корупційні ризики у лісовому секторі виникають на етапах надання лісокористувальних прав, видачі транспортних документів та здійснення контрольних функцій.** Є необхідність у концентрації антикорупційних ресурсів саме на цих критичних точках, а не розпорошувати їх по всьому ланцюгу створення вартості деревини.
- **Досвід Болівії, Еквадору та Перу показує, що цифровізація процедур, створення систем простежуваності документів, автоматичні сповіщення, електронні журнали дій та цифрові контрольні листи** є одними з найефективніших інструментів зниження дискреції посадових осіб та запобігання корупції.
- **Автори підкреслюють, що боротьба з корупцією у природоохоронній сфері повинна поєднувати організаційні реформи з формуванням культури доброчесності.** Це вимагає постійних програм навчання, етичного лідерства, перевірок доброчесності персоналу та інституціоналізації управління корупційними ризиками як складової щоденної діяльності органів влади.
- **Документ показує, що ефективне запобігання незаконній заготівлі деревини неможливе без міжвідомчої координації.** Необхідне створення спільних протоколів взаємодії між природоохоронними органами, поліцією, прокуратурою, митними та податковими органами, а також активне залучення місцевих громад і корінних народів до системи контролю та моніторингу.

30 років міжнародного обміну фінансовою розвідкою: історія та майбутнє Егмонтської групи [6]

Щорічний звіт Егмонтської групи є комплексним оглядом діяльності глобальної мережі підрозділів фінансової розвідки (ПФР) та водночас підсумком тридцятирічного розвитку міжнародної системи співробітництва у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Центральною темою документа є відзначення 30-річчя Егмонтської групи, яка за цей час трансформувалася з неформального об'єднання 13 ПФР, створеного у 1995 році в Брюсселі, у найбільшу світову мережу фінансової розвідки, що об'єднує 182 ПФР у восьми регіонах світу та виступає ключовим міжнародним механізмом оперативного обміну фінансовою інформацією. Звіт

[6] https://egmontgroup.org/wp-content/uploads/2026/05/Egmont_Group_Annual_Report_2024-2025.pdf

демонструє, що міжнародна архітектура ПВК/ФТ дедалі більше спирається саме на ПФР як на центральний елемент збору, аналізу та обміну фінансовою розвідкою, а сама Егмонтська група поступово перетворюється на глобальний центр координації, стандартизації та розвитку професійних спроможностей ПФР.

Документ детально описує організаційну структуру Егмонтської групи, яка складається з голів ПФР, Комітету Егмонтської групи, чотирьох робочих груп, восьми регіональних груп, Секретаріату Егмонтської групи та Центру досконалості та лідерства ПФР (ECOFEL). Така структура забезпечує поєднання стратегічного управління, оперативної діяльності, регіональної координації та розвитку професійної експертизи. Особливе місце займає Egmont Secure Web (ESW) – захищена система обміну інформацією між ПФР, яка залишається фундаментом усієї мережі та ключовим інструментом міжнародної співпраці. Звіт підкреслює, що саме можливість швидкого та безпечного обміну інформацією між юрисдикціями є головною конкурентною перевагою Егмонтської групи та основою її внеску у глобальну систему ПВК/ФТ.

Важливою частиною звіту є статистичний аналіз діяльності ПФР у світі. Дані за 2024 рік демонструють безпрецедентний масштаб фінансової розвідки. ПФР-члени Егмонтської групи отримали понад 22,6 млн повідомлень про підозрілі операції, понад 305 млн звітів про великі готівкові операції, понад 852 млн порогових звітів щодо фінансових транзакцій, понад 6,7 млн повідомлень про транскордонне переміщення готівки та оборотних інструментів на пред'явника, а також понад 88 тис. повідомлень від інших державних органів. На міжнародному рівні було направлено понад 22 тис. запитів між ПФР та здійснено понад 106 тис. спонтанних розкриттів інформації іноземним партнерам. Наведені цифри демонструють, що сучасні ПФР функціонують не просто як аналітичні підрозділи, а як глобальна мережа обробки величезних масивів фінансових даних, необхідних для виявлення складних транскордонних схем ВК/ФТ, корупції, кіберзлочинності, шахрайства, екологічних злочинів та інших форм організованої злочинності.

Значний інтерес становить аналіз моделей організації ПФР. Звіт показує, що адміністративна модель залишається домінуючою у світі: із 139 ПФР, які взяли участь в опитуванні, 102 функціонують як адміністративні органи, тоді як правоохоронна модель використовується лише у 18 випадках, а судова – лише у двох. Водночас багато ПФР виконують додаткові функції, що виходять за межі класичного фінансового аналізу. Частина з них здійснює регулювання та нагляд за суб'єктами первинного фінансового моніторингу, має повноваження щодо призупинення підозрілих операцій, заморожування чи арешту активів, а окремі ПФР навіть залучені до кримінальних розслідувань та процесуального супроводу справ. Таким чином документ демонструє відсутність універсальної моделі ПФР та підтверджує, що інституційна архітектура фінансової розвідки формується відповідно до особливостей національних правових систем.

Одним із ключових напрямів діяльності Егмонтської групи у звітному періоді стало посилення міжнародного інформаційного обміну. Документ описує розвиток низки проєктів, спрямованих на цифровізацію та автоматизацію діяльності ПФР. Особливу увагу приділено розвитку ESW Matching System, яка має автоматизувати процес пошуку зв'язків між запитами та інформацією, що знаходиться у розпорядженні різних ПФР. Водночас реалізується проєкт Проєкт автоматизованої інтеграції даних для анкет та опитувальників ПФР (SDIFQ), який дозволяє автоматизувати збір та аналіз структурованих даних, а на наступному етапі передбачає використання великих мовних моделей для аналізу неструктурованої інформації. Це свідчить про поступовий перехід міжнародної системи фінансової розвідки до використання штучного інтелекту, автоматизованого аналізу та технологій великих даних для підвищення швидкості та якості виявлення фінансових злочинів.

Важливим досягненням року стало завершення кількох міжнародних проєктів за участю FATF, INTERPOL та UNODC. Найбільш значущим серед них є підготовка комплексного посібника з неформальної міжнародної співпраці у розслідуваннях відмивання коштів та

пов'язаних злочинів. Додатково були підготовлені спеціалізовані практичні матеріали для ПФР, правоохоронних органів та прокуратури. Документ наголошує, що швидкість міжнародної взаємодії стає критичним фактором успіху фінансових розслідувань, а тому розвиток механізмів неформального співробітництва між компетентними органами розглядається як один із пріоритетних напрямів розвитку глобальної системи ПВК/ФТ.

Окремий великий блок звіту присвячений реалізації Стратегічного плану Егмонтської групи на 2022–2027 роки. Документ визначає чотири основні стратегічні напрями: удосконалення механізмів обміну інформацією між ПФР, розвиток співпраці з міжнародними партнерами, формування нових знань щодо сучасних ризиків та типологій ВК/ФТ, а також підтримка членів і кандидатів на вступ до Егмонтської групи. У межах цих напрямів організація реалізує численні проєкти, спрямовані на розвиток методології, підготовку аналітичних матеріалів, проведення тренінгів, підтримку ПФР із нижчим рівнем спроможностей та вдосконалення міжнародних стандартів співробітництва. Звіт демонструє, що стратегія Егмонтської групи поступово зміщується від ролі платформи обміну інформацією до ролі глобального центру формування професійних стандартів та знань у сфері фінансової розвідки.

Значне місце у документі займає діяльність ECOFEL, який перетворюється на міжнародний центр професійного розвитку ПФР. Протягом року було проведено 18 навчальних заходів, підготовлено сотні спеціалістів та розширено онлайн-платформу навчання до 9400 користувачів. Особливу увагу приділено створенню міжнародної сертифікаційної програми для працівників ПФР. У звіті прямо зазначається, що відсутність єдиних стандартів підготовки фахівців фінансової розвідки залишається серйозною проблемою глобальної системи ПВК/ФТ, а тому створення сертифікаційної програми може стати переломним моментом для професіоналізації діяльності ПФР у світі.

Висновки:

- **Документ демонструє, що міжнародний обмін фінансовою розвідувальною інформацією переходить від моделі двосторонніх запитів до технологічно інтегрованої системи з використанням автоматизації, цифрових платформ та елементів штучного інтелекту.** ПФР необхідно інвестувати у цифрову трансформацію, аналітичні інструменти та сумісність інформаційних систем.
- **Егмонтська група фактично формує новий міжнародний стандарт незалежності ПФР, підвищуючи вимоги щодо операційної автономії до рівня обов'язкових критеріїв членства.** Це означає, що держави повинні забезпечувати належні законодавчі та інституційні гарантії незалежності своїх ПФР.
- **Розвиток ECOFEL та майбутньої сертифікаційної програми свідчить про перехід до глобальної стандартизації професійної підготовки працівників ПФР.** Для національних систем ПВК/ФТ це означає необхідність системного розвитку компетенцій, аналітичних навичок та безперервного навчання персоналу.
- **Звіт підтверджує, що ефективна протидія ВК/ФТ дедалі більше залежить від багатосторонньої співпраці між ПФР, правоохоронними органами, міжнародними організаціями та приватним сектором.** Необхідне розширення механізмів міжнародного інформаційного обміну, міжвідомчої взаємодії та державно-приватних партнерств у сфері ПВК/ФТ.

Суттєвим напрямом діяльності Егмонтської групи залишається підтримка членів та кандидатів на вступ до організації. Протягом звітного періоду було прийнято п'ять нових членів, а ще шість кандидатів продовжували проходити процедури вступу. Водночас реалізовувалися численні проєкти технічної допомоги, програми стажувань між ПФР, спеціалізовані тренінги та регіональні ініціативи з розвитку спроможностей. Особливу увагу приділено оновленню Процесу підтримки та забезпечення відповідності (Support and Compliance Process) – механізму моніторингу відповідності членів вимогам Егмонтської групи. Новий підхід базується на принципі «support first», тобто передбачає першочергове надання підтримки ПФР для усунення недоліків та досягнення відповідності

стандартам, а не застосування каральних заходів.

Окремо звіт висвітлює результати 31-го Пленарного засідання Егмонтської групи у Люксембурзі, яке стало найбільшим за всю історію організації та було присвячене 30-річному ювілею мережі. Під час пленарного засідання було схвалено низку стратегічно важливих рішень, серед яких підвищення вимог щодо операційної незалежності та автономії ПФР до рівня базових умов членства, підтримка нових проєктів у сфері повернення активів, екологічних злочинів та інтеграції даних, розвиток ESW та затвердження нової моделі фінансування ECOFEL. Фактично Егмонтська група офіційно закріпила курс на посилення інституційної незалежності ПФР як одну з ключових умов ефективності системи фінансової розвідки.

У завершальній частині документа окреслюються майбутні пріоритети розвитку Егмонтської групи. Організація планує посилювати використання штучного інтелекту, машинного навчання та аналітики великих даних у діяльності ПФР, розвивати механізми спільного аналізу між юрисдикціями, удосконалювати цифрову інфраструктуру міжнародного обміну інформацією, підтримувати фінансову стійкість ПФР та розширювати співпрацю з FATF, INTERPOL, UNODC, МВФ, Світовим банком та іншими міжнародними організаціями. Звіт демонструє, що в умовах зростання обсягів транскордонних фінансових потоків, цифровізації фінансових послуг та ускладнення злочинних схем майбутнє глобальної системи ПВК/ФТ дедалі більше залежатиме від здатності ПФР ефективно обмінюватися інформацією, використовувати сучасні технології та підтримувати високий рівень міжнародної координації.

Регулювання

Виконавчий наказ Білого дому: AI, кібербезпека та фінансова злочинність у системі «America First» [7]

Виконавчий наказ Президента США «Просування інновацій та безпеки у сфері штучного інтелекту», підписаний 2 червня 2026 року, є наступним документом у ланцюжку регуляторних дій адміністрації Трампа, що встановлює архітектуру управління AI в умовах «America First». На відміну від попередніх стратегічних документів рівня політики, цей наказ вводить конкретні нормативні приписи з чіткою хронологічною структурою виконання – більшість ключових заходів мають бути реалізовані протягом 30 або 60 днів з дати підписання. Це свідчить про наміри адміністрації здійснити оперативну операціоналізацію кіберзахисної інфраструктури на базі AI, не вдаючись до тривалих консультацій і нормотворчих процедур.

Структурна логіка документу будується навколо чотирьох операційних кластерів. Перший – кіберзахист федеральних систем: протягом 30 днів Комітет з систем національної безпеки, Міністерство війни та Агентство з кібербезпеки та захисту інфраструктури США (CISA) зобов'язані пріоритизувати захист відповідних інформаційних систем і випустити Обов'язкові операційні директиви. Особливо значимим є доручення CISA розширити програми кіберзахисту, що надають доступ до AI-інструментів не лише федеральним органам, але й місцевим органам влади та операторам критичної інфраструктури – у переліку прямо названі сільські лікарні, регіональні банки та комунальні підприємства. Цей елемент виходить за межі традиційного федерального кіберзахисту і фактично встановлює нову модель каскадного поширення державних можливостей з AI-захисту на нижчі рівні критичної інфраструктури, включаючи малих та середніх суб'єктів фінансового сектору.

Другий і найбільш значимий кластер з точки зору AML/CFT - доручення Міністерству фінансів протягом 30 днів сформувати Координаційний центр кібербезпеки у сфері AI (AI cybersecurity clearinghouse). Участь у цьому механізмі є добровільною – у рамках партнерства

[7] https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/

з AI-індустрією та операторами критичної інфраструктури. Центр матиме функції координації сканування програмних вразливостей, їх верифікації та пріоритизації усунення. Позиціонування Міністерства фінансів як координатора цього механізму – не нейтральний вибір: фінансова розвідка (FinCEN) і кібербезпекові функції Казначейства формують єдину інституційну платформу для синтезу даних про кіберзагрози і фінансові ризики. Це є принципово новим архітектурним рішенням, що закладає підвалини для майбутньої інтеграції кіберрозвідки та AML-аналітики в рамках єдиної федеральної структури.

Третій кластер – концепція «covered frontier models». У межах 60 днів Національне агентство з безпеки (NSA) у консультації з іншими агентствами повинне розробити класифікований процес для оцінки просунутих кіберможливостей AI-моделей та визначення порогу, при досягненні якого модель отримує статус «covered frontier model». Паралельно формується добровільна рамка взаємодії з розробниками AI, яка надає їм можливість дізнатися, чи відповідає їхня модель цьому порогу; надати уряду доступ до таких моделей на строк до 30 днів до їх публічного релізу; та співпрацювати у виборі «довірених партнерів» для раннього доступу. Критично важливим є положення Розділу 3(c): ніщо в цьому розділі не може тлумачитися як дозвіл на встановлення обов'язкового ліцензування, попередньої перевірки або дозвільного режиму – чітке нормативне відмежування від потенційного сповзання до моделі регулювання, де тлумачення «безпеки» стає підставою для de facto контролю над AI.

Четвертий кластер – правозастосовний. Генеральний прокурор США зобов'язаний пріоритизувати виконання статутів 18 U.S.C. 1028 (крадіжка ідентифікаційних даних та шахрайство), 18 U.S.C. 1030 (комп'ютерне шахрайство та зловживання) і 18 U.S.C. 1343 (телекомунікаційне шахрайство) – зокрема проти тих, хто використовує AI для незаконного доступу до комп'ютерних систем або застосовує отримані таким чином дані для подальших злочинів. Формулювання є технологічно нейтральним: AI виступає не як ознака злочину, а як інструмент-підсилювач предикатних злочинів, що входять до стандартних типологій предикатних злочинів для відмивання коштів у рамках FATF. Цей мандат поєднує кримінальне переслідування за AI-злочини з правозастосуванням у сфері фінансових злочинів, що є значним методологічним зрушенням у підходах до визначення предикатних злочинів.

В ширшому регуляторному контексті, цей наказ є третьою ключовою ланкою в ланцюжку AI-регуляторних дій адміністрації, слідом за скасуванням попереднього наказу Байдена (2025) і підписанням наказу про AI-освіту (квітень 2025). Архітектура документу формує чіткий інституційний дизайн: пріоритет інновацій + добровільне партнерство з промисловістю + нарощування виконавчих можливостей AI у сфері безпеки + кримінальне переслідування зловживань – без обов'язкового ліцензування або нормативного попереднього затвердження моделей. Для міжнародних СПФМ, що здійснюють операції на

Висновки:

- **Утворення Координаційного центру кібербезпеки у сфері AI під егідою Міністерства фінансів США відкриває нову модель обміну розвідданими про кіберзагрози** між федеральними органами та операторами критичної інфраструктури. Фінансові установи, що долучаться до clearinghouse, отримають доступ до верифікованих даних про вразливості систем і можливість превентивного патчингу задовго до поширення загроз на широкий ринок.
- **Мандат Генерального прокурора розширює застосування положень 18 U.S.C. 1028/1030/1343 на AI-опосередковані злочини і фактично визнає їх як новий клас предикатних злочинів для цілей ПВК**. СПФМ повинні переглянути типологічні моделі моніторингу транзакцій, включивши індикатори AI-enabled computer fraud та AI-assisted identity theft як самостійні сценарії виявлення підозрілих операцій.
- **Розширення доступу до AI-інструментів кіберзахисту для місцевих банків є прямим регуляторним сигналом для дрібних та середніх фінансових установ США**: CISA-програми технологічної модернізації стануть доступними для широкого кола СПФМ, що може суттєво вплинути на конкурентну динаміку ринку AML/CFT-технологій у сегменті середніх банків.

американському ринку або є операторами критичної інфраструктури, виникає стратегічне питання щодо позиціонування по відношенню до clearinghouse та можливості отримання раннього доступу до covered frontier models – що може стати конкурентним інструментом у розвитку AI-рішень для фінансового комплаєнсу.

Звіти окремих інституцій та експертів

Прихована політика стейблкоїнів: як резерви та нагляд змінюють фінансову систему [8]

Документ є комплексним порівняльним дослідженням регуляторних режимів стейблкоїнів у семи провідних юрисдикціях світу – Європейському Союзі, Сполучених Штатах Америки, Великій Британії, Гонконзі, Сінгапурі, Японії та Об'єднаних Арабських Еміратах. Центральна ідея роботи полягає у тому, що глобальна хвиля регулювання стейблкоїнів призвела до зовнішньої конвергенції правил, однак на практиці між юрисдикціями формуються суттєво відмінні регуляторні режими, які по-різному впливають на фінансові ринки, конкуренцію, міжнародні платежі та майбутню архітектуру цифрових фінансів. Автор наголошує, що сьогодні більшість держав уже досягли консенсусу щодо базових принципів регулювання стейблкоїнів: резерви повинні повністю або майже повністю покривати зобов'язання емітента, активи резервного забезпечення мають бути ліквідними та відокремленими від власних активів емітента, алгоритмічні моделі повинні бути виключені з регульованого середовища, а виплата доходу власникам стейблкоїнів має бути заборонена. Проте за однаковими нормативними формулюваннями приховуються різні політичні цілі, наглядові підходи та економічні наслідки.

Дослідження виходить із того, що масштаби ринку стейблкоїнів уже роблять його системно значущим елементом глобальної фінансової екосистеми. Наприкінці 2025 року загальна капіталізація стейблкоїнів перевищила 317 млрд доларів США, а прогнози розвитку ринку до 2030 року коливаються від 500 млрд до 3,7 трлн доларів. При цьому значення мають не лише обсяги капіталізації, а й транзакційна активність, оскільки річні обсяги переказів у стейблкоїнах уже вимірюються багатьма трильйонами доларів. Автор підкреслює, що вперше в історії використання стейблкоїнів неторговельні сценарії застосування – міжнародні платежі, транскордонні перекази, розрахунки та корпоративне управління ліквідністю – починають зростати швидше, ніж використання стейблкоїнів для операцій із криптоактивами. Це означає, що стейблкоїни поступово перетворюються із допоміжного інструменту крипторинку на окремий сегмент глобальної платіжної інфраструктури.

Значна частина документа присвячена аналізу самого поняття «стейблкоїн». Автор демонструє, що цей термін використовується для опису широкого спектра цифрових активів, які суттєво відрізняються між собою за механізмом підтримання стабільності вартості, структурою резервів, моделями управління та рівнем ризику. У роботі запропоновано систематизацію стейблкоїнів за шістьма основними категоріями: забезпечені фіатними валютами токени з прив'язкою до однієї валюти, забезпечені кошиком активів токени, товарно-забезпечені стейблкоїни, криптозабезпечені моделі, алгоритмічні конструкції та гібридні механізми. При цьому автор зазначає, що більшість сучасних регуляторних режимів фактично регулюють лише одну категорію – централізовані стейблкоїни, забезпечені резервами у традиційній фінансовій системі та прив'язані до однієї офіційної валюти. Саме цей сегмент представлений найбільшими світовими проєктами, такими як USDT та USDC, які разом контролюють приблизно 85 % глобального ринку.

Окремий аспект дослідження стосується вибору регуляторної архітектури. Автор порівнює підходи, за яких стейблкоїни інтегруються до вже існуючих правових категорій, із підходами, де для них створюються нові спеціалізовані режими. Європейський Союз обрав модель

[8] https://www.ecri.eu/sites/default/files/stablecoins_formatted_cover_pages.pdf

інтеграції через категорію токенів електронних грошей (EMT), фактично поширивши на стейблкоїни логіку регулювання електронних грошей. Одночасно для інших категорій стабільних цифрових активів було створено окрему категорію токенів, прив'язаних до активів (ART). Японія також інтегрувала стейблкоїни до традиційної системи платіжних інструментів. Натомість США у межах GENIUS Act створили нову окрему категорію авторизованих платіжних стейблкоїнів, яка не має прямого аналога у попередньому законодавстві. Велика Британія та Гонконг зайняли проміжну позицію, створивши нові категорії активів, але використовуючи існуючу регуляторну інфраструктуру для їх нагляду. На думку автора, цей вибір відображає фундаментальне бачення державою природи стейблкоїнів: чи розглядаються вони як еволюція існуючих форм грошей, чи як принципово новий фінансовий інструмент.

Найбільш детально у документі досліджується питання регулювання іноземних стейблкоїнів. Автор стверджує, що саме цей аспект є головним джерелом практичних розбіжностей між формально схожими режимами регулювання. Якщо раніше держави обирали між повною забороною або повним допуском іноземних цифрових активів, то зараз формується значно складніша модель багаторівневого доступу. У Великій Британії обговорюється можливість дозволити використання іноземних стейблкоїнів для міжнародних операцій, але обмежити їх застосування у внутрішніх платежах. Сінгапур дозволяє обіг іноземних токенів, але не надає їм статусу регульованих стейблкоїнів, які прив'язані до однієї валюти. США створюють механізм допуску через оцінку еквівалентності іноземного регулювання та вимогу локалізації резервів на території США. Гонконг, Японія та федеральний режим ОАЕ займають більш закриту позицію. Особливо цікавим є висновок автора щодо Європейського Союзу: попри те, що текст MiCA формально допускає модель множинного випуску стейблкоїнів, тобто існування глобального стейблкоїна через локально ліцензованих емітентів у різних юрисдикціях, інституційна позиція окремих органів ЄС може фактично призвести до виключення глобальних стейблкоїнів із європейського ринку. У результаті ЄС ризикує стати найбільш обмежувальною юрисдикцією серед усіх розглянутих режимів, незважаючи на формально більш гнучкі законодавчі положення.

Другим ключовим напрямом аналізу є резервне забезпечення стейблкоїнів. Автор наполягає, що структура резервів є не технічним питанням фінансової стабільності, а важливим елементом політичної економії. Вибір

Висновки:

- **Документ демонструє, що глобальне регулювання стейблкоїнів уже досягло високого рівня формальної гармонізації, однак практичні результати дедалі більше визначаються не текстом законів, а підходами регуляторів до їх застосування.** Є необхідність у розвитку механізмів взаємного визнання та еквівалентності режимів регулювання, щоб уникнути фрагментації глобального ринку цифрових активів.
- **Автор показує, що політика щодо резервного забезпечення стейблкоїнів фактично є інструментом перерозподілу фінансових ресурсів між банками, державою, центральними банками та емітентами.** Це означає, що регулятори повинні оцінювати резервні вимоги не лише з точки зору фінансової стабільності, але й через їх вплив на банківське фінансування, ринки державного боргу та монетарну політику.
- **Дослідження свідчить про поступовий перехід від моделі повної заборони або повного допуску іноземних стейблкоїнів до багаторівневих режимів доступу, де права токена залежать від конкретного сценарію використання.** Доцільне впровадження ризик-орієнтованих обмежень для окремих видів використання стейблкоїнів замість повної ізоляції іноземних проєктів.
- **Документ підкреслює, що заборона виплати доходу власникам стейблкоїнів є не технічним, а фундаментальним політичним рішенням щодо природи цих активів.** Для регуляторів це означає необхідність чіткого визначення, чи розглядаються стейблкоїни як цифрова форма грошей, чи як інвестиційний інструмент, оскільки від цього залежатиме майбутня модель регулювання, нагляду та інтеграції стейблкоїнів у фінансову систему.

активів, у яких повинні зберігатися резерви стейблкоїнів, визначає розподіл значних фінансових потоків між банківською системою, урядами, центральними банками та приватними емітентами. У Європейському Союзі значна частина резервів повинна утримуватися у формі банківських депозитів, що підтримує ресурсну базу кредитних установ та зменшує ризик відтоку коштів із банківської системи. У США акцент зроблено на короткострокових державних цінних паперах, що створює додатковий попит на державний борг та сприяє фінансуванню федерального бюджету. Велика Британія поєднує інвестиції у державні облігації із зберіганням частини резервів на рахунках центрального банку. Японія використовує трастову модель, яка обмежує можливість емітентів отримувати дохід від резервів. Автор наголошує, що всі ці підходи мають однаковий зовнішній вигляд з точки зору пруденційного регулювання, але фактично визначають, хто отримуватиме економічні вигоди від майбутнього багатотрильйонного ринку стейблкоїнів.

Значна увага приділяється також питанню доходності стейблкоїнів. Усі сім розглянутих режимів прямо або опосередковано забороняють виплату відсотків власникам токенів. Однак автор вважає, що ця заборона приховує значно глибшу концептуальну дискусію. Якщо стейблкоїн розглядається як аналог готівкових грошей або платіжного інструменту, то відсутність доходності є логічною. Якщо ж він ближчий до інвестиційного продукту або паю фонду грошового ринку, то отримання доходу власником виглядає цілком природним. Автор зазначає, що наразі більшість регуляторів фактично обрали модель «цифрових грошей», але зробили це не через відкриту політичну дискусію, а через технічні регуляторні рішення. Це створює ризики регуляторного арбітражу та появи конкурентних переваг для окремих юрисдикцій або посередників.

На завершення автор формулює три стратегічні рекомендації. По-перше, необхідно створити міжнародну систему взаємного визнання та пропорційного допуску іноземних стейблкоїнів замість політики повної ізоляції. По-друге, регулятори повинні відкрито визнавати політичні та перерозподільчі наслідки вимог до резервного забезпечення та враховувати їх під час формування політики. По-третє, міжнародні організації та регулятори мають винести питання доходності стейблкоїнів на рівень окремої політичної дискусії та виробити узгоджений підхід до визначення природи цих активів. Загальний висновок дослідження полягає в тому, що перший глобальний цикл регулювання стейблкоїнів уже сформував основу майбутньої архітектури цифрових фінансів. Саме підходи до міжнародного допуску стейблкоїнів, розподілу резервів та визначення їхньої економічної природи значною мірою визначатимуть розвиток міжнародної валютної системи, токенізованих фінансових ринків та цифрових платежів протягом наступного десятиліття.

Штучний інтелект у боротьбі з екологічними злочинами [9]

Звіт, підготовлений Global Initiative Against Transnational Organized Crime за результатами Бангкокського семінару, пропонує огляд технологічних новинок у сфері застосування штучного інтелекту (ШІ) для захисту довкілля. Автори звіту послідовно доводять, що ШІ може бути або потужним підсилювачем правосуддя, або черговою дорогою ілюзією – що залежить виключно від того, в яке середовище його вміщують.

Екологічна злочинність сьогодні – це не поодинокі випадки браконьєрства, а високоорганізований, транснаціональний бізнес, що за масштабами шкоди поступається хіба що торгівлі наркотиками та зброєю. Незаконний видобуток золота в Амазонії, вирубка лісів у басейні Конго, контрабанда рідкісних видів птахів з Південно-Східної Азії, нелегальне скидання токсичних відходів до океану – всі ці діяння об'єднує одне: вони відбуваються на величезних територіях, генерують колосальні обсяги даних (супутникові знімки, трекінгові

[9] https://globalinitiative.net/wp-content/uploads/2026/05/Artificial-intelligence-for-environmental-crime-enforcement-GI-TOC-May-2026.pdf

записи, фінансові транзакції, соціальні медіа) та водночас відбуваються в юрисдикціях, де державний контроль традиційно слабкий.

Саме тут уявний потенціал ШІ здається безмежним. Алгоритми здатні обробляти терабайти зображень, виявляти аномалії в русі суден за даними Automatic Identification Systems (AIS), відстежувати підозрілі патерни в митних деклараціях або навіть аналізувати оголошення про продаж екзотичних тварин на інтернет-майданчиках. Однак практика, як невпинно наголошується у звіті, виявляє жорстоку закономірність: там, де немає оцифрованих архівів, де бази даних розрізнені, де суди не визнають електронні докази, а чиновники бояться втратити робочі місця через автоматизацію – найкращий алгоритм перетворюється на дорогий генератор шуму.

Одним із найбільш інтригуючих концептуальних внесків звіту є поняття «парадоксу впровадження». Суть його полягає в тому, що ШІ є найбільш необхідним саме в найменш сприятливих умовах. «Гарячі точки» екологічних злочинів – це, як правило, регіони з низькою щільністю населення, слабкою присутністю держави, хронічним недофінансуванням правоохоронних органів, а головне – з катастрофічним станом даних. Більшість інформації там досі існує на папері, дані польових інспекцій не оцифровані, супутникові знімки не мають верифікованої інформації про те, що насправді відбувається на місці. Але ж саме там, у глибині джунглів Амазонки або в дельтах річок Південно-Східної Азії, відбуваються наймасштабніші злочини проти природи. Натомість у країнах з високим інституційним потенціалом, де дані вже давно оцифровані, а суди мають досвід роботи з електронними доказами, потреба в революційних ШІ-рішеннях значно нижча. Таким чином, створюється ситуація, коли технологія, розроблена в комфортних умовах, потрапляє в середовище, де вона апріорі не може працювати на повну потужність, і звіт фіксує це як фундаментальне протиріччя, яке не долається додатковими інвестиціями в софт, а вимагає системної перебудови всіх ланок правозастосування.

Автори наводять яскраві приклади з різних куточків світу, які демонструють як успішні моделі, так і приховані ризики. Федеральна поліція Бразилії, безсумнівно, є флагманом у цій сфері з двома масштабними ініціативами. Перша з них, програма Ouro Alvo (TraceForGold), започаткована 2019 року, являє собою елегантне поєднання класичної криміналістики та сучасних алгоритмів. Справа в тому, що незаконне золото, видобуте на території індіанських резервацій або національних парків, потрапляє до легальних ювелірних магазинів через складні схеми відмивання. Система Ouro Alvo накопичує бібліотеку хімічних та ізотопних профілів золота з різних родовищ – як легальних, так і нелегальних. Коли поліція вилучає партію золота, ШІ зіставляє її хімічний відбиток з цією бібліотекою та, паралельно, аналізує супутні документи: чи сходяться обсяги видобутку з офіційними деклараціями, чи не виникають аномалії в ланцюжку постачання. Це не просто технологія – це зміна філософії розслідування, де ШІ виступає не самостійним агентом, а радше розумним асистентом, що підсвічує суперечності, на які людське око могло б не звернути уваги.

Паралельно бразильська поліція розгорнула систему Brasil MAIS, яка є ще більш амбітною за масштабом. Цей проєкт аналізує супутникові знімки високої роздільної здатності для виявлення змін ландшафту, пов'язаних із вирубкою лісів, незаконним видобутком корисних копалин та іншими порушеннями. Щомісяця система генерує десятки тисяч автоматичних сповіщень, які надходять до єдиної платформи. Вражає не стільки технологічна досконаліть, скільки організаційна архітектура: до платформи приєднано майже 730 установ та близько 130 000 користувачів. Це не ізольований інструмент поліції, а спільний інформаційний простір для різних агентств, які отримують можливість координувати свої дії на основі єдиної картини.

Важливо, що стратегічний нагляд залишається за Федеральною поліцією, тоді як технічну розробку та обслуговування передано приватному підряднику – це зразок ефективної публічно-приватної співпраці, який демонструє, що ШІ не обов'язково має бути повністю внутрішньою розробкою, але контроль не може бути аутсорсований. Результати вражають: за

період від запуску до квітня 2025 року рівень вирубок суттєво знизився, а проєкт приніс мільярди доларів штрафів, конфіскацій та заморожених активів.

Однак звіт застерігає: успіхи Бразилії не повинні створювати ілюзію легкої масштабованості. Умови там є унікальними – наявність сильної централізованої поліції, політичної волі, технічних кадрів та, що важливо, супутникової інфраструктури, якою володіє країна. Перенесення цього досвіду до, скажімо, країн Західної Африки з їхньою фрагментованою владою та слабкою цифровізацією було б наївним.

Інший показовий кейс – Чеська Республіка. Поліція Чехії розробила систему AIDA (AI Digital Assistant), яка інтегрована безпосередньо в роботу слідчих. Цікаво, що спочатку система створювалася для боротьби з кіберзлочинністю, але її логіка виявилася універсальною. AIDA бере на себе рутинну, але критично важливу роботу: вона обробляє тексти інтерв'ю зі свідками, автоматично структурує їх у формат, придатний для подальшого розслідування, ідентифікує ключові сутності (підозрюваних, жертв, місця подій), готує стандартні запити до банків для блокування рахунків або отримання виписок, складає клопотання до прокуратури. У звіті наголошується, що час розслідування скорочується на 40–70 відсотків, а кількість помилок – через те, що система автоматично перевіряє суперечності – також знижується. Але ключовим є не прискорення, а те, що слідчі звільняються від паперової роботи й можуть зосередитися на змістовному аналізі. І знову ж таки, AIDA працює лише тому, що чеська правоохоронна система вже була досить стандартизована: банки надають дані в однаковому форматі, прокуратура має чіткі вимоги до документів, а самі слідчі пройшли навчання роботи з системою.

Переходячи до прикладів із громадянського суспільства, автори звіту звертають увагу на проєкти, які намагаються заповнити прогалини там, де держава не справляється. Ганська ініціатива EcoScan AI від The Academic Success Foundation є особливо натхненною, оскільки вона спирається не на дорогі супутники, а на найпоширеніший у світі месенджер – WhatsApp. Місцеві мешканці можуть анонімно надіслати повідомлення, фото або аудіо про підозрілу діяльність (наприклад, незаконне звалище або вирубку). ШІ аналізує це неструктуроване повідомлення, виокремлює з нього геодані, опис загрози, тип активності, після чого інформація потрапляє до навчених місцевих аналітиків. Вони фільтрують хибні спрацювання, додають контекст (наприклад, що певна діяльність є традиційною для цієї пори року і не є злочином) і лише тоді передають узагальнені дані правоохоронцям. Під час пілотної фази платформа створила понад сто звітів. Цей приклад демонструє, як ШІ може демократизувати моніторинг довкілля, долучаючи громади до захисту власних ресурсів – але за умови, що існує «людина в циклі прийняття рішень», яка розуміє локальну специфіку.

Ще одним потужним прикладом є платформа PERIVALLON, розроблена грецьким Центром досліджень та технологій Hellas. Вона відома своїм мультимодальним підходом: система об'єднує геопросторову інтелектуальну інформацію (супутникові та аерознімки), дані з безпілотників, сенсорів, систем автоматичної ідентифікації суден (AIS) та навіть контент з онлайн-майданчиків. Шукаючи незаконні сміттєзвалища, PERIVALLON накладає супутниковий знімок на дані про рух вантажівок із датчиків, аналізує текстові оголошення про вивіз сміття – і на основі кореляцій робить висновок про ймовірність порушення. Це перехід від «розумної камери» до справжнього аналітичного центру, який бачить картину цілісно. Втім, і тут автори звіту нагадують про обмеження: чим складніша система, тим більше даних їй потрібно, тим чутливішою вона стає до прогалин у вхідних масивах, і тим важче її обслуговувати в умовах обмежених ресурсів.

Американська некомерційна організація Wildlife Protection Solutions розробила систему wpsWatch, яка поєднує мережі датчиків (фотопасток) з алгоритмами розпізнавання зображень. Камери в національних парках фіксують появу людей чи транспортних засобів, знімки передаються через супутник або стільниковий зв'язок у центр, де ШІ спочатку виокремлює зображення, що містять людей або машини (відкидаючи тисячі фото з тваринами), а потім більш точний класифікатор визначає, чи є це браконьєром. Система обробляє близько 40 000

зображень на день, і на момент написання звіту спричинила понад тисячу детекцій, що призвели до реальних арештів. Це наочний доказ того, що навіть відносно прості ШІ-рішення (wpsWatch використовує відкритий алгоритм MegaDetector) можуть мати величезний вплив, якщо вони вбудовані в чіткий операційний ланцюжок від камери до патруля.

Однак, читаючи ці історії успіху, не можна ігнорувати тривожні тренди, які звіт виносить на поверхню. По-перше, це проблема «нерівномірної видимості». Алгоритми надзвичайно добре знаходять те, що можна легко виміряти: площу знелісненої землі, кількість рибальських човнів у забороненій зоні, підозрілу активність на окремій золотій копальні. Але екологічна злочинність має складну структуру: часто за лаштунками стоять фінансові посередники, корумповані чиновники, транснаціональні трейдери, які ніколи не з'являються на супутникових знімках. В результаті ШІ може створювати хибне враження прогресу, спрямовуючи обмежені ресурси поліції на «легкі цілі» – дрібних лісорубів або старателів-одинаків, – у той час як великі гравці залишаються в тіні. Це не технічна вада, а структурна упередженість, закладена в самому підході до збору даних. Автори звіту прямо закликають: розробляючи ШІ для моніторингу довкілля, завжди питайте, кого робить видимим ваша система, а кого – ні, і чи не підсилюєте ви цим існуючу нерівність.

По-друге, звіт акцентує увагу на тому, що ШІ – це не нейтральний інструмент, а поле геополітичної боротьби. Переважна більшість систем розробляється установами «Глобальної Півночі», часто без змістовної участі країн, які найбільше страждають від екологічних злочинів. Це створює ризик «колоніалізму даних», коли технологічне рішення нав'язується ззовні, не враховуючи місцевих правових реалій, культурних особливостей або навіть банальної відсутності інтернету. Крім того, залежність від пропрієтарних рішень великих технологічних корпорацій несе в собі загрозу «блокування вендором»: система може бути встановлена на грантові кошти, але через два-три роки ліцензія закінчується, спеціалісти, які її налаштовували, їдуть, і правоохоронний орган залишається з «чорною скринькою», яку він не може ні підтримувати, ні адаптувати, ні навіть пояснити судді, як вона працює. Альтернативою, яку пропонує звіт, є відкриті платформи, спільні бази даних (на зразок Global Fishing Watch) та інвестиції в місцевий інжиніринг, щоб технологія стала органічною частиною місцевої інфраструктури.

Третій аспект, який часто ігнорується, – це те, що кримінальні мережі самі активно опановують ШІ. У звіті з посиланням на дослідження Інституту Тьюрінга зазначається, що злочинці вже використовують генеративні моделі для створення підроблених дозволів на видобуток, адаптують оголошення про продаж нелегальної деревини на онлайн-платформах так, щоб вони обходили автоматичні фільтри, або навіть аналізують патрульні маршрути, щоб уникати зустрічі з рейнджерами. Це означає, що ШІ-системи для захисту довкілля не можуть бути статичними; вони мають бути стійкими до адаптивних супротивників, що вимагає постійного оновлення та моніторингу зворотного зв'язку – ресурсу, якого в багатьох агенціях просто немає.

На завершення, звіт пропонує низку принципів, які радикально зміщують фокус із «впровадження ШІ» на «управління системами, що уможливлюють ШІ». Головний із них – починати з проблеми, а не з технології. Це звучить банально, але на практиці донори часто шукають «інноваційне рішення», а правоохоронці – грант на «цифровізацію», в результаті чого купується черговий софт, тоді як реальна проблема полягає в тому, що два відомства в одній країні не можуть обмінятися паперовими документами.

Другий принцип – будувати ШІ як публічне благо. Це означає підтримку відкритого коду, створення спільних навчальних наборів даних (анонімізованих та безпечних), інвестиції в довгострокове навчання кадрів та створення незалежних механізмів аудиту алгоритмів.

Третій – визнати, що людський нагляд не є перепоною на шляху до ефективності, а є єдиною гарантією того, що система не вийде з-під контролю. Суддя або слідчий мають не просто право, а обов'язок ставити під сумнів висновки алгоритму, і система має бути спроєктована так, щоб цей скепсис був можливий технічно.

Для донорів рекомендації звучать особливо жорстко: припиніть фінансувати короткострокові проекти заради галочки. Фінансуйте інфраструктуру даних – оцифровування архівів, стандартизацію форматів, юридичне врегулювання питань обміну даними через кордони. Без цього ШІ буде не більш ніж блискучою іграшкою.

Для правоохоронців у країнах, що розвиваються, порада парадоксальна: не поспішайте впроваджувати ШІ. Спочатку оцифруйте те, що маєте, навчіть людей аналізувати, створіть прості ручні процеси. І лише тоді – автоматизовуйте їх.

Для міжнародних НУО заклик не менш радикальний: перестаньте бути «імпортерами рішень» і станьте «посередниками». Допомагайте місцевим установам формулювати їхні власні технічні завдання, перекладайте технічну мову на мову права, створюйте довіру там, де є скепсис.

Висновки:

- **Головний бар'єр – не технологія, а структури.** Ефективність ШІ в боротьбі з екологічними злочинами визначається не складністю алгоритмів, а якістю даних, інституційною спроможністю та правовими рамками.
- **Парадокс впровадження.** ШІ найнеобхідніший у слабко керованих, бідних на дані регіонах, але саме там його відповідальне та ефективне застосування є найскладнішим через відсутність спроможностей.
- **Людина залишається в циклі ухвалення рішень.** Успішні кейси доводять, що ШІ має підсилювати людське судження, а не замінювати його. Автоматизовані сповіщення обов'язково повинні проходити верифікацію аналітиком, який враховує локальний контекст та юридичні нюанси.
- **ШІ має бути публічним благом, а не корпоративним продуктом.** Залежність від закритих систем створює ризики «колоніалізму даних», блокування та непрозорості.

Отже, підсумовуючи цей глибокий аналіз, можна сказати: майбутнє боротьби з екологічними злочинами за допомогою ШІ залежить не від швидкості процесорів або досконалості нейромереж. Воно залежить від здатності суспільства побудувати три наступні речі: по-перше, надійний інституційний каркас (закони, стандарти, підготовлені судді), по-друге, чесну цифрову інфраструктуру (спільні бази даних, протоколи обміну, відкриті формати), і по-третє, політичну волю не перекладати відповідальність на алгоритми, а використовувати їх як підсилення для людського судження.

ШІ не є панацеєю, і він ніколи не замінить рейнджера в лісі або слідчого, який розуміє місцеві звичаї. Але він може стати тим самим ліхтарем, який дозволить побачити злочин там, де раніше була лише темрява невідомості.

Між розривом і стійкістю: чому голоси громадянського суспільства є вирішальними для боротьби з організованою злочинністю на глобальному рівні [10]

У час, коли геополітична нестабільність стає нормою, а злочинні ринки лише розширюють свій вплив, питання участі громадянського суспільства в багатосторонніх процесах набуває не лише технічного, але й фундаментального політичного значення.

Публікація GI-TOC фіксує тривожну тенденцію: участь неурядових організацій у роботі ключових органів ООН, зокрема Комісії з питань запобігання злочинності та кримінального правосуддя (CCPCJ), неухильно знижується протягом останніх двох десятиліть.

У центрі уваги – діяльність Resilience Fund, який протягом останніх п'яти років виступає своєрідним містком між локальними спільнотами та віденськими залами для переговорів,

[10] https://globalinitiative.net/analysis/why-un-engagement-matters-for-strengthening-state-resilience-to-organized-crime/

доводячи, що глобальна стійкість до організованої злочинності неможлива без інтеграції голосів тих, хто щоденно протистоїть їй на передовій.

Ключовим меседжем документа є попередження про системну кризу легітимності багатосторонніх форумів. Починаючи з 2015 року, коли держави-члени розпочали практику попереднього узгодження підсумкових документів Конгресів ООН з питань злочинності (починаючи з Дохи, а потім і в Кіото під час пандемії), громадянське суспільство було фактично усунуто від змістовного діалогу. Це не просто технічне рішення про порядок роботи – це політичне рішення, яке створює небезпечний когнітивний розрив. Коли політики обговорюють заходи протидії торгівлі людьми чи наркотрафіку, покладаючись виключно на офіційні звіти та узагальнену статистику, вони ризикують створювати ситуацію, де складні локальні контексти редукуються до спрощених індикаторів.

Як слушно зазначається в тексті, саме неурядові організації, що діють на рівні вулиць та громад, володіють унікальними знаннями про механізми вербування молоді до злочинних угруповань, про корумповані практики на місцях чи про неочікувані наслідки репресивних законів. Їхнє виключення робить міжнародні зобов'язання не лише менш ефективними, але й часто неможливими для імплементації, оскільки вони не враховують реальної динаміки влади та ресурсів на місцях.

Найбільш тривожним висновком, який посилює терміновість залученості громадянського суспільства, є дані Глобального індексу організованої злочинності 2025 року. Цей індекс фіксує парадоксальну, але небезпечну ситуацію: на тлі розширення кримінальних ринків (наркотики, незаконний видобуток корисних копалин, торгівля людьми) показники стійкості держав – тобто їхньої спроможності протистояти цьому тиску – або стагнують, або знижуються.

Зростання глобальної конфліктності, безперечно, відіграє тут роль каталізатора: вона послаблює інституції, створює зони правового вакууму та перетворює організовану злочинність на інструмент виживання для цілих громад. І саме в цьому контексті стає очевидним, що заклики до міжнародної співпраці втрачають свою дієвість. Коли країни не співпрацюють через політичні суперечки чи взаємні підозри, єдиними суб'єктами, які продовжують тримати «лінію оборони», стають локальні організації.

Однак парадокс полягає в тому, що саме ці організації, через брак ресурсів і візові обмеження, першими виключаються з багатосторонніх процесів. Resilience Fund, про який ідеться в документі, демонструє іншу логіку: за останні п'ять років він забезпечив участь понад двох десятків представників саме таких місцевих організацій у заходах ООН, поступово нормалізуючи їхню присутність і доводячи, що їхній досвід є не маргінальним доповненням, а центральним елементом ефективної політики.

Показовим моментом, детально описаним у статті, стала поява семи партнерів Resilience Fund у Відні у вересні 2025 року, під час початку переговорів щодо підсумкового документа майбутнього Конгресу. Їхні свідчення розкривають глибинні структурні проблеми, які зазвичай залишаються поза рамками дипломатичного дискурсу. Наприклад, представниця Парагваю говорила про те, що, незважаючи на колосальні перешкоди та звуження демократичного простору, саме довіра громади дозволяє її організації виживати. Ще більш промовистим є застереження про масовий характер захоплення держави (state capture) злочинними структурами, що унеможливлює роботу в правовому полі. Учасники наголосили на нагальній потребі в юридичних рамкових механізмах для захисту громадянського суспільства, без яких будь-яка діяльність стає небезпечною. Це не просто прохання про фінансування або доступ – це вимога переглянути саму філософію безпекової політики, де організації низового рівня визнаються не просто бенефіціарами, але рівноправними творцями стратегій.

Особливої ваги надають особисті історії та досвід конкретних людей, які прибули до Відня на 35-ту сесію CCPCJ у червні 2026 року. Ці сім історій – з Мексики, Гондурасу, Гаїті, України,

Судану, Індонезії та Камбоджі – не є випадковим набором географічних точок. Кожна з них репрезентує унікальний перетин організованої злочинності з іншими формами кризи.

Ксенія Ткачук з українського фонду LEAD приносить у віденські зали досвід роботи з посттравматичним відновленням ветеранів, де організована злочинність часто використовує незахищеність і зброю, що вільно ходить у зонах конфлікту. Марлен Леон Фонтес з ініціативи Sinaloa в Мексикці демонструє, як боротьба з корупцією на кордонах потребує адвокаційних стратегій, які неможливо виробити без доступу до даних та судових механізмів. Хуан Енаморадо з Гондурасу, лідер руху Warriors Zulu Nation, через призму хіп-хопу та вуличних мистецтв розповідає про профілактику насильства та запобігання примусовому рекрутингу молоді до банд, тоді як Срейкев Ім з Камбоджі – про захист дітей від сексуальної експлуатації в онлайн-просторі. І хоча географічні та тематичні контексти цих кейсів різняться, їх об'єднує спільний знаменник: міжнародні політики, які сидять за столом переговорів, мають надто далеке уявлення про те, як саме організована злочинність проникає в тканину повсякденного життя, і надто слабко розуміють, які саме локальні практики підтримки є дієвими.

Кульмінацією аналітичної статті є заклик, який лунає від Стівена Очієнга Оквані з Talanta Africa: «Не продовжуйте організовувати все в нарадчих кімнатах. Дія краще перетворюється на реальність на передовій. Нехай міжнародна спільнота прийде на рівень громад. Нехай вони прийдуть до нас. І нехай вони сприймають мову громад, наративи громад, їхні прожиті реалії». Це набагато глибше за звичайне прохання про фінансову підтримку. Це вимога справедливості – визнання того, що знання, народжені в умовах кризи, є не менш цінними, ніж академічні моделі або дипломатичні компроміси.

З огляду на те, що Конгрес ООН з питань злочинності в Абу-Дабі, спочатку запланований на 2026 рік, було перенесено на вересень на тлі регіональної нестабільності, існує реальна загроза того, що розрив між політиками та практиками лише зросте. Саме тому 35-та CCPCJ у Відні розглядається не як черговий захід, а як критичне вікно можливостей. Резолюції та декларації, ухвалені сьогодні, безпосередньо впливатимуть на порядок денний вересневого Конгресу. Якщо міжнародне співтовариство дозволить виключити голоси громадянського суспільства зараз, воно ризикує узаконити цю практику на наступні роки.

Тільки визнавши, що глобальний вплив починається локально, ми зможемо перетворити урочисті зобов'язання на реальну стійкість, захист і довгоочікувані зміни.

Висновки:

- **Криза участі:** За останні два десятиліття участь громадянського суспільства в профільних форумах ООН (CCPCJ, Конгреси ООН) системно скоротилася, а підсумкові документи держави почали узгоджувати заздалегідь без змістовного внеску НУО.
- **Розрив між політикою та реаліями:** Виключення громадських організацій із міжнародних переговорів призводить до того, що політичні зобов'язання втрачають зв'язок із реаліями спільнот, які щоденно стикаються з організованою злочинністю.
- **Зростання злочинності при стагнації стійкості:** Згідно з Global Organized Crime Index 2025, кримінальні ринки розширюються водночас із стагнацією стійкості державних інституцій, а міжнародна співпраця (індикатор стійкості) майже не прогресує.
- **Брак правового захисту для активістів:** Громадянське суспільство на місцях стикається з масовим захопленням держави (state capture) злочинними структурами та звуженням демократичного простору, що робить критично необхідним створення міжнародних юридичних рамок для їхнього захисту.

Інші новини

FCA попереджає футбольні клуби: спонсорство неавторизованих криптовалютних фірм - ризик [11]

Лист Управління з фінансового регулювання та нагляду Великобританії (FCA) до футбольних клубів, підписаний Фіоною Маккіннон-Міллер, керівником Департаменту боротьби з шахрайством, просуванням фінансових послуг, взаємодії з учасниками ринку та регуляторним периметром, є класичним зразком превентивного регуляторного сигналу на перетині спортивного та фінансового секторів. FCA фіксує зростаючу кількість партнерств між футбольними клубами та неавторизованими фірмами, що надають послуги в галузі криптовалютних бірж і торговельних платформ без відповідної авторизації FCA. Регулятор прямо вказує, що такі спонсорські домовленості ризикують «надати легітимності» цим фірмам у сприйнятті широкої аудиторії уболівальників, перетворюючи клуб на канал просування потенційно небезпечних фінансових продуктів до кінцевих споживачів. Цей документ є публічним попередженням, але водночас і встановленням стандартів належної перевірки, відступ від яких у майбутніх виконавчих провадженнях FCA матиме наслідки.Юридична конструкція листа будується на двох взаємопов'язаних нормативних базах. По-перше, неавторизована фінансова діяльність є кримінальним правопорушенням відповідно до статті 19 Закону про фінансові ринки і послуги 2000 року (FSMA), а несанкціоноване фінансове просування – відповідно до статті 21 FSMA. По-друге – і це є ключовим аспектом – кошти, отримані від таких фірм у вигляді спонсорства, можуть кваліфікуватися як «кримінальне майно» у розумінні Закону про доходи від злочинів 2002 року (POCA), що потенційно перетворює клуб, який отримав таке фінансування, на суб'єкта відповідальності за відмивання коштів або прийняття злочинних доходів. FCA окремо застерігає: власний промоційний контент клубу стосовно продуктів або послуг спонсора може самостійно кваліфікуватися як несанкціоноване фінансове просування за статтею 21 FSMA – тобто клуб стає не лише пасивним, але й активним суб'єктом потенційного порушення незалежно від наявності комерційного умислу.

Базові вимоги до належної перевірки (due diligence), встановлені FCA як обов'язкові базові кроки перед укладанням будь-яких спонсорських угод із фінансовими компаніями, включають: підтвердження регуляторного статусу спонсора (авторизація FCA або наявність звільнення від неї); оцінку природи запропонованих послуг (чи є вони регульованою діяльністю за британським законодавством); перевірку наявності контрольних заходів для запобігання доступу британських споживачів (геоблокування, застереження, перевірки при онбордингу); перевірку FCA Firm Checker та Warning List, при цьому регулятор особливо підкреслює: відсутність у Warning List не означає законності діяльності фірми – тому клуби зобов'язані здійснювати власні незалежні перевірки; і за потреби – отримання спеціалізованої юридичної думки. Лист також сповіщає про активний моніторинг FCA спонсорських угод і про взаємодію з Прем'єр-лігою, що свідчить про готовність регулятора до секторальних виконавчих заходів у разі ігнорування вимог.

Europol: ліквідація промислового виробництва підроблених документів в Іспанії та його роль у фінансуванні контрабанди людей [12]

27 травня 2026 року в Аліканте (Іспанія) у рамках спільної французько-іспанської операції було ліквідовано нелегальну базу виробництва підроблених документів, що функціонувала в промислових масштабах. Обшук орендованої під фіктивним іменем квартири, яка одночасно слугувала виробничим цехом і логістичним вузлом, виявив повністю функціональний

[11] https://www.fca.org.uk/publication/correspondence/sponsorship-arrangements-football-clubs.pdf
[12] https://www.europol.europa.eu/media-press/newsroom/news/fake-document-factory-dismantled-in-spain-around-800-ids-seized

підпільний комплекс: правоохоронні органи вилучили близько 800 підроблених європейських документів, виробниче обладнання для виготовлення документів, цифрові пристрої, транспортний засіб та €1 580 готівкою; затримано одного підозрюваного. Операцію очолювала французька поліція (Police Nationale/OLTIM) за підтримки іспанської Національної поліції (Policía Nacional/UCRIF) і аналітичних ресурсів Europol. Слідство розпочалося після виявлення французькою стороною відкрито функціонуючого веб-сайту, що рекламував підроблені документи до продажу.

Слідча логіка операції розкриває нову типологію шахрайства, що поєднує промислове масштабне виробництво з організованим онлайн-каналом дистрибуції, що різко знижує транзакційні витрати для кінцевих злочинних структур – мереж контрабанди людей. За версією слідства, підозрюваний адміністрував онлайн-платформу, що пропонувала клієнтам по всій Європі підроблені ідентифікаційні та адміністративні документи – як у фізичному, так і в цифровому форматах. Europol встановив пряме функціональне підключення цієї платформи до мереж перевезення нелегальних мігрантів: підроблені документи нібито використовувалися для обходу прикордонного контролю, незаконного отримання дозволів на проживання та полегшення вторинних переміщень у межах ЄС. Характеристика підпільного об'єкта як такого, що демонструє «промислово-масштабні методи виробництва», підкреслює якісну трансформацію цього виду злочинності: від кустарного виготовлення документів до організованого фабричного підходу.

Системне значення операції підкреслює ширший контекст: Europol у своєму звіті SOCTA 2025 прямо ідентифікував документарне шахрайство як ключовий чинник, що уможливлює нелегальну міграцію та підтримує злочинні мережі в довгостроковій перспективі, генеруючи значний нелегальний прибуток. У грудні 2025 року Europol заснував спеціалізований Європейський центр протидії контрабанді мігрантів (ECAMS), а у березні 2026 – розширив його мандат відповідно до нового регламенту ЄС; дана операція є одним з перших оперативних результатів посиленої координаційної спроможності структури. З точки зору ПВК/ФТ, грошовий потік від реалізації підроблених документів є задокументованим каналом фінансування організованих злочинних мереж контрабанди людей, а самі підроблені документи є предметом шахрайства та фальшування офіційних документів – предикатних злочинів для відмивання коштів у всіх юрисдикціях ЄС. СПФМ, що обслуговують клієнтів у секторах, де можливе зловживання підробленими документами (оренда нерухомості, грошові перекази, відкриття рахунків), повинні враховувати цю оперативну типологію при калібруванні сценаріїв моніторингу.

Колумбія на межі: кримінальні виклики для наступного президента [13]

На тлі президентських виборів, Колумбія опинилася перед безпрецедентним загостренням організованої злочинності, що неминуче визначить порядок денний безпекової політики нової адміністрації.

Чотири роки правління Густаво Петро ознаменувалися радикальним поворотом у безпековій стратегії країни: його флагманська політика «Тотального миру» передбачала переговори зі збройними угрупованнями як головний інструмент стримування насильства. Водночас антинаркотична стратегія Петро відмовилася від традиційного тиску на найслабші ланки наркотрафіку, зосередившись на складних міжнародних фінансових схемах і транснаціональних угрупованнях. Однак на практиці цей підхід зіткнувся з хронічною нестачею координації, високою адаптивністю злочинних груп і постійним тиском з боку громадськості, яка вимагала негайних результатів.

За останні чотири роки кримінальний ландшафт Колумбії не просто змінився – він зміцнів і фрагментувався, створивши якісно нові загрози. У рамках «Тотального миру» опозиційні

[13] https://insightcrime.org/news/criminal-challenges-colombia-next-president/

фракції колишніх Революційних збройних сил Колумбії (FARC) продовжили розпадатися. Спочатку, щоб виглядати сильнішими перед обличчям переговорів з урядом, вони об'єдналися, проте вже 2024 року цей союз зруйнувався, породивши нові угруповання, як-от «Генеральний штаб блоків і фронтів» (EMBF) та «Національна координаторія Болівараїнської армії» (CNEB). На думку аналітика Міжнародної кризової групи Гледіс Гонсалес, ці дрібніші групи виявилися набагато живучішими за своїх попередників: вони гнучкі, добре адаптуються до тривалих військових операцій і тому їх надзвичайно важко нейтралізувати. Аналогічний розкол стався і в лавах Армії національного визволення (ELN): у 2024 році в департаменті Нариньо відокремилася фракція «Комунерас-дель-Сур». І хоча ця група продовжила переговори з урядом, основне ядро ELN розірвало мирний діалог.

Найтривожнішим трендом стало різке зростання чисельності та вогневої спроможності збройних угруповань. Згідно зі звітом Фундації Conflict Responses, між 2018 та 2025 роками кількість бійців основних кримінальних груп подвоїлася – з приблизно 13 до понад 27 тисяч осіб. Найстрімкіше зростання продемонстрували Гаїтанські сили самооборони Колумбії (також відомі як «Клан затоки»), за ними йдуть EMBF та Центральний генеральний штаб (EMC), що об'єднує колишніх повстанців FARC. У підсумку наступна адміністрація успадкує понад десять різних регіонів, охоплених внутрішніми збройними конфліктами. Серед найбільш критичних департаментів – Вальє-дель-Каука, Каука, Нариньо, Путумайо, Уїла, Мета, Чоко, Антіокія, Болівар, Норте-де-Сантандер, Магдалена, Араука та Ґуав'яре. Як наголошує Гонсалес, новому уряду доведеться стратегічно пріоритезувати загрози, оскільки ресурси обмежені, а цивільне населення дедалі частіше опиняється просто «між двох вогнів».

Соціальний контроль з боку злочинних груп набув нової жорсткості. Якщо раніше угруповання мали певну легітимність у громадах, то тепер вони застосовують силу, не залишаючи простору для переговорів. Найяскравіший приклад – регіон Кататумбо на кордоні з Венесуелою. Із січня 2025 року там тривають безперервні сутички між ELN та 33-м фронтом (який діє під егідою EMBF), що спричинило переміщення понад 100 тисяч осіб, численні масові вбивства, цілеспрямовані ліквідації та блокади цілих громад.

Крім того, технологічна еволюція війни – зокрема використання безпілотників – змінила правила гри. Дрони застосовуються не лише для спостереження, але й як носії вибухівки для атак на сили безпеки. В департаментах Каука, Вальє-дель-Каука та Нариньо саме цивільне населення найчастіше стає жертвою таких ударів.

Економічне підґрунтя злочинності залишається надзвичайно міцним. Колумбія – найбільший світовий виробник кокаїну. Хоча адміністрація Петро зробила акцент на перехопленні вантажів і знищенні лабораторій, площі посівів коки зросли з 253 тисяч гектарів у 2023 році до 262 тисяч у 2024-му. Потенційне виробництво кокаїну, за даними ООН, підскочило з 2 664 метричних тонн до понад 3 000 тонн за той самий період.

Водночас доходи від незаконного видобутку золота майже не відстають: рекордні світові ціни на золото спонукали такі групи активно брати участь у нелегальній розробці копалень у Чоко, регіоні Бахо-Каука в Антіокії та значній частині Амазонії. Там кримінальні групи вимагають данину як від легальних, так і від нелегальних шахтарів, натомість пропонуючи «охорону», постачання та допомогу в уникненні правосуддя. Паралельно продовжують зростати вимагання та викрадення людей, які стали важливими джерелами фінансування для підтримки діяльності злочинних синдикатів.

На іншій стороні цієї кризи – системне послаблення колумбійських сил безпеки. З приходом Петро розпочалося «зачистка» лав вищого офіцерського керівництва: між 2022 та 2024 роками було звільнено 355 поліцейських високих рангів. До 2025 року Національна поліція Колумбії мала найменше за 15 років число генералів, полковників та підполковників – трохи більше ніж 680 осіб. В армії між лютим та квітнем 2026 року залишили службу 49 полковників та майорів. Загальна чисельність сил безпеки скоротилася на 25,8% між 2008 та 2024 роками – з 682 до 506 активних співробітників на 100 тисяч населення, що формально ще відповідає міжнародним стандартам, але вже свідчить про тривалу ерозію. Звільнення найвищих ланок

безпосередньо вдарило по оперативній спроможності: планування складних операцій, особливо тих, що потребують глибокої військової та поліцейської розвідки для протидії транснаціональним злочинним мережам, стало надзвичайно проблемним. Вербування новобранців не заповнює прогалини в управлінні та стратегічному мисленні. Як зазначає Гледіс Гонсалес, новий президент успадкує дисбаланс між зростаючою міццю злочинних груп та виснаженими, перевантаженими силами безпеки, які працюють на межі своїх можливостей. Відновлення цього балансу стане одним із головних завдань.

Додатковою вагомою змінною є невизначеність у стосунках зі Сполученими Штатами, які історично були головним союзником Колумбії у боротьбі з наркотрафіком та організованою злочинністю. За часів президентства Петро ці відносини досягли найнижчої точки. США додали Колумбію до списку країн, які, на думку Вашингтону, «недостатньо співпрацюють» у боротьбі з наркотиками. Міністерство фінансів США запровадило санкції проти самого Петро, кількох членів його родини та міністра внутрішніх справ Армандо Бенедетті. Хоча зустріч обох президентів у лютому 2026 року дещо розрядила напругу, безпекова співпраця залишається виборчим питанням. Дослідник Фундації «Ідеї для миру» Герсон Аріас наголошує: наступний уряд успадкує близько 30 тисяч членів збройних угруповань, і незалежно від того, чи прийде до влади лівий, чи правий кандидат, буде потрібен масштабний перегляд безпекової стратегії. А це неминуче передбачає перемовини зі США. У контексті, де Дональд Трамп чинить вирішальний вплив на регіональну безпеку, характер відносин Колумбії з Вашингтоном також визначить координацію з ключовими сусідами – Еквадором та Венесуелою.

Таким чином, безпекова криза в Колумбії набула характеру системної, багатовимірної загрози, яка вимагатиме від наступного президента не лише силових рішень, але й тонкої дипломатії, глибокої військової реформи та здатності діяти в умовах, коли традиційні методи боротьби з організованою злочинністю вже не працюють.

Для загального розвитку

Терористичний ярлик США: як удар по PCC загрожує економіці Бразилії [14]

Рішення Державного департаменту США, ухвалене 28 травня 2026 року, про внесення двох найвпливовіших бразильських злочинних угруповань – «Першого столичного командування» (PCC) та «Червоного командування» (CV) – до списку іноземних терористичних організацій, спричинило ефект бомби, що розірвалася не лише у кримінальному середовищі, але й у легальному фінансовому секторі десятої за величиною економіки світу.

Попри те, що цей крок довго очікувався багатьма прихильниками жорсткої лінії, його практичні наслідки виявилися парадоксальними: головний удар може прийтись не стільки по самих угрупованнях, скільки по звичайних компаніях, банках та іноземних інвесторах, які так чи інакше дотичні до бразильського ринку.

Президент Бразилії Луїс Інасіо Лула да Сілва, який перебуває у складній передвиборчій боротьбі з Флавіо Болсонару, сином колишнього президента, одразу ж різко розкритикував це рішення, назвавши його загрозою економічному добробуту країни. Він слушно зауважив, що такий крок може стати кроком назад у боротьбі зі злочинністю, створивши ризики для життя людей та завдавши відчутних економічних втрат. Цікаво, що Флавіо Болсонару, який відвідав США напередодні оголошення, поспішив приписати це рішення собі, однак насправді ні він, ні чинний президент не мають підстав святкувати перемогу – адже тепер під ударом опинилася вся бразильська економіка, а не лише злочинні клани.

На перший погляд, додавання двох злочинних угруповань до терористичного списку виглядає як логічне посилення тиску на організовану злочинність, що давно вийшла за межі Бразилії.

[14] https://insightcrime.org/news/us-terrorism-designations-will-hit-the-pccs-money-and-everyone-elses/

Однак реальність набагато складніша і тривожніша. Щомісяця Бразилія торгує зі США товарами на понад 8 мільярдів доларів, а такі гіганти американського бізнесу, як представники технологічного, енергетичного, харчового та автомобільного секторів, активно працюють на бразильському ринку. Рішення про визнання PCC та CV терористичними організаціями означає, що будь-яка особа, підприємство або банк, навіть ненавмисно співпрацюючи з цими угрупованнями, ризикує заморожуванням активів або кримінальним переслідуванням за підтримку тероризму.

Меліна Piccо, директор з досліджень інституту Igarapé, наголошує, що найбільш негайним наслідком стане перегляд банківською системою своїх ризиків та контролю за відмиванням грошей, що призведе до суттєвого зростання витрат на комплаєнс для компаній з міжнародними операціями. Це не просто чергове загострення – це фактично запровадження режиму фінансової облоги, в якому опиняється бразильський бізнес.

Найбільше занепокоєння викликає те, наскільки глибоко PCC, яке є значно інтегрованішим у фінансову систему, ніж CV, проникло у легальну економіку. Прокурор Лінкольн Гакія, який присвятив розслідуванню діяльності PCC понад два десятиліття, оцінює щорічні доходи угруповання приблизно у 2 мільярди доларів. Ці гроші відмиваються по всій фінансовій системі, часто без відома самих банків. І коли він каже, що під загрозою може опинитися кожен, це не перебільшення.

Показовою є операція «Прихований вуглець», яка розкрила механізм імпорту пального PCC та контролю над автозаправними станціями. Зовні ці підприємства виглядали абсолютно легальними, але фактично керувалися угрупованням. У другій фазі цієї операції, запущеній у 2025 році, влада ідентифікувала приблизно 5 мільярдів доларів грошей PCC, відмитих за чотири роки через фінтех-компанії та інвестиційні фонди, що працюють на проспекті Фарії Лімі – справжньому серці фінансового сектору Бразилії. Особливо цинічним видається той факт, що навіть бразильський уряд, включаючи поліцію та військових, купував пальне у компанії, контрольованої PCC, оскільки документація була оформлена настільки бездоганно, що жодних підозр не виникало.

За таких умов новий терористичний ярлик створює безпрецедентні правові ризики для всіх, хто працює в Бразилії або має з нею ланцюги постачання. Ключовим меседжем для бізнесу є необхідність термінової перекалібровки комплаєнс-процедур, адже нове правове середовище суттєво підвищує ставки щодо санкційних ризиків, незаконних фінансів, ризиків, пов'язаних з третіми сторонами, логістикою, платежами та репутацією. І хоча слабо регульована фінтех-індустрія стала основною мішенню, оператори PCC також використовували традиційні банки, такі як Bradesco, які підпадають під набагато жорсткіший нагляд. Структура схеми була спеціально вибудувана так, щоб приховати прямі зв'язки з угрупованням, розподіляючи прибутки між різними банками та підприємствами. Тепер, після терористичного визнання, навіть ті банки, які ненавмисно обробляли платежі таких компаній, та підприємства, які купували в них пальне, можуть бути санкціоновані.

Колишній американський дипломат Рікардо Суніга, який нині працює консультантом у фірмі Dinamica Americas, вважає практично неминучим, що бразильські фінансові інституції зіткнуться з пильною увагою з боку американських прокурорів та позовами з боку приватних осіб. І навіть якщо компаніям не будуть пред'явлені прямі звинувачення, вони можуть стати надзвичайно обережними, скорочуючи свій бізнес у Бразилії, або ж витрачати величезні кошти на безпрецедентні заходи перевірки контрагентів.

Особливу тривогу викликає те, що вразливими є не лише фінансовий сектор та ринок пального. Під загрозою опиняються гірничодобувна промисловість, сільське господарство, лісозаготівля та багато інших галузей, які працюють на територіях, де активні PCC або CV. Обидва угруповання активно присутні у ланцюгах постачання видобутку золота в Амазонії та за її межами, особливо на тлі рекордних цін на золото. Крім того, вони мають багаторічний досвід роботи з криптовалютами. Прокурор Гакія підкреслює, що фізичного руху готівки більше немає: гроші надходять через фінансових операторів, обмінників валют та

криптовалюти. Саме ця еволюція методів відмивання коштів робить традиційні підходи до боротьби зі злочинністю все менш ефективними.

Незважаючи на те, що верхівка PCC перебуває у в'язницях суворого режиму, а їхні кримінальні схеми неодноразово викривалися, угруповання не тільки виживає, але й продовжує диверсифікувати свою діяльність, піднімаючись все вище політичними та економічними сходами. PCC укладає альянси з бізнесменами, податковими шахраями та операторами фінансового ринку, створюючи або купуючи компанії в різноманітних секторах – від інвестиційних фондів до будівельних фірм. До операції «Прихований вуглець» угруповання вже проникло у транспортний сектор, отримавши муніципальні контракти на управління автобусами в Сан-Паулу, а також на послуги з прибирання та управління відходами.

Отже, рішення США, проголошене як інструмент тиску на організовану злочинність, на практиці ризикує перетворитися на важкий тягар для всієї бразильської економіки, спричинивши ланцюгову реакцію відтоку капіталу, зростання вартості позик та підвищення страхових премій. Іронія долі полягає в тому, що найбільше від цього постраждають саме легальні компанії та громадяни, тоді як самі злочинні угруповання, які вже десятиліттями демонструють здатність адаптуватися до будь-яких викликів, ймовірно, знайдуть нові способи легалізації своїх доходів. Відмивання грошей через складні мережі, фіктивні компанії та криптовалюти залишатиметься їхньою стихією, тоді як офіційний бізнес опиниться під постійним страхом ненавмисного порушення нових терористичних заборон.

Це класичний випадок, коли погано прорахований захід, хоч і з добрим наміром, може завдати більше шкоди, ніж користі, фактично покаравши тих, кого він мав захищати, і лише трохи ускладнивши життя тим, проти кого був спрямований. Світова спільнота, і особливо європейські країни, які є головними споживачами наркотиків, що надходять з Бразилії, мають уважно стежити за цим прецедентом, адже він створює небезпечну модель, коли спроба боротьби зі злочинністю перетворюється на опосередковану атаку на цілі національні економіки.

Як безвізовий режим перетворюється на канал нелегальної міграції до ЄС [15]

Наприкінці 2025 року група громадян Китаю прибула рейсовим літаком до Белграда. Їхні документи були в порядку, вони пройшли паспортний контроль – їхній в'їзд був цілком законним. Але за лічені дні вони вже рухалися далі, намагаючись нелегально перетнути Дунай і потрапити до Хорватії за допомогою місцевого посередника. Їхній човен перекинувся на середині річки: одна людина загинула, дев'ятьох врятували.

Цей випадок не є поодиноким. Щороку сотні китайських громадян легально в'їжджають до країн Західних Балкан, а потім звертаються до мереж контрабандистів, щоб потрапити до Європейського Союзу. Це явище отримало назву «гібридної контрабанди» (hybrid smuggling), і воно стрімко поширюється глобально, стаючи дедалі помітнішим на багатьох маршрутах.

Для Західних Балкан це явище не є чимось абсолютно новим. На початку 2020-х років спостерігалося значне зростання кількості мігрантів, що прилітали до аеропорту Белграда – переважно громадян північноафриканських країн, яких потім переправляли через сухопутні кордони до ЄС. З того часу збільшилися не лише обсяги, а й різноманіття національностей: люди з Туреччини, Бангладеш, Індії, Куби, Йорданії та інших країн регулярно користуються послугами гібридних контрабандних мереж у регіоні. Це зростання відображає адаптивність і професіоналізацію місцевих злочинних угруповань, а також розвиток складніших форм кримінальної діяльності вздовж так званого балканського маршруту.

[15] https://globalinitiative.net/analysis/legal-entry-irregular-exit-the-growing-role-of-the-western-balkans-in-human-smuggling-into-the-eu/

Контрабандні мережі у цьому регіоні суттєво відрізняються від традиційної нелегальної міграції тим, що вони ґрунтуються на стратегічному зловживанні легальними механізмами в'їзду. Вони поєднують три основні канали в'їзду – дозволи на роботу, безвізові режими та туристичні візи – із класичними методами транскордонного переправлення людей. Така комбінація дозволяє мігрантам спочатку легально потрапити до країн Західних Балкан, а звідти нелегально рухатися далі до Західної та Північної Європи.

Іноземні злочинні мережі відіграють центральну роль у цих операціях, зазвичай контролюючи весь маршрут – від планування до фінальних точок передачі мігрантів. Вони координують найприбутковіші аспекти бізнесу, зокрема планування маршрутів, підробку документів, встановлення цін і місць передачі. Якщо вище керівництво часто перебуває в країнах походження, то посередники середньої та нижчої ланки діють безпосередньо на території Західних Балкан, забезпечуючи переправлення через кордони. Місцеві злочинці надають логістичну підтримку: транспорт, житло, допомогу з отриманням віз і дозволів на проживання. До цієї діяльності можуть бути залучені приватні компанії, а в окремих випадках – корумповані чиновники. Весь процес є високоорганізованим: люди виконують спеціалізовані ролі на різних ділянках маршруту. Насильство використовується як засіб контролю – як у конкуренції між угрупованнями (особливо в Сербії та Боснії і Герцеговині), так і проти мігрантів, які намагаються уникнути послуг контрабандистів.

Першим ключовим шляхом є легальні схеми трудової міграції. Економіки Західних Балкан продовжують страждати від дефіциту робочої сили, щороку залучаючи тисячі іноземних працівників – головним чином із Бангладеш, Філіппін, Непалу та Індії. Організовані злочинні групи інтегрувалися в цей процес, часто співпрацюючи з посередниками та приватними компаніями як у країнах походження мігрантів, так і на місцях, щоб отримувати візи через фіктивні трудові контракти та підроблені документи.

Щойно опинившись у Західних Балканах, групи мігрантів швидко переправляються далі до Хорватії, Угорщини чи Греції, що свідчить про високий рівень координації та попереднього планування. У квітні 2025 року албанська Спеціальна структура проти корупції та організованої злочинності (SPAK) завершила розслідування щодо 27 членів двох злочинних угруповань, яких звинувачували у сприянні незаконному перетину кордону близько 650 іноземців (переважно з Бангладеш і Камеруну) через Косово та Сербію до ЄС. Водночас існують і менш структуровані випадки: працівники, найняті через легальні канали, просто тікають із робочих місць і через кілька місяців, накопичивши кошти, звертаються до контрабандистів.

Другим важливим чинником, що сприяє гібридному смаргінгу в регіоні, є неузгодженість безвізових режимів країн Західних Балкан із політикою ЄС. У рамках процесу євроінтеграції ці країни мають запроваджувати візи для громадян третіх держав відповідно до списку, ухваленого Європейським Союзом. Однак оскільки гармонізація візової політики не є негайним юридичним зобов'язанням, уряди Західних Балкан іноді адаптують свої правила, керуючись власними політичними та економічними інтересами. Громадяни Туреччини, Китаю, росії та білорусі потребують візи для в'їзду до ЄС, але можуть подорожувати без візи до деяких країн Західних Балкан – наприклад, Албанії, Боснії і Герцеговини, Косова, Чорногорії, Північної Македонії та Сербії. Так, Туреччина має безвізовий доступ до всіх шести зазначених балканських економік, Китай – до п'яти, а росія – до чотирьох. Європейське агентство з питань прикордонної та берегової охорони (Frontex) та кілька держав-членів ЄС неодноразово наголошували, що саме такі винятки сприяють потокам нелегальної міграції до ЄС.

Це регуляторне середовище також породило вторинні нелегальні ринки, зокрема продаж і повторне використання паспортів країн із безвізовим доступом. У грудні 2025 року поліція Косова заарештувала громадянина Йорданії та Туреччини, підозрюваних у причетності до контрабанди людей до ЄС, і вилучила 53 йорданські паспорти, які, ймовірно, використовувалися в злочинних цілях.

Третім чинником є доступність туристичних, спортивних та освітніх віз. Вони зазвичай легші в отриманні, ніж інші типи віз, оскільки вимагають меншого обсягу документів і перевірок. Мігранти прибувають до країн, близьких до кордонів ЄС, залишаються на кілька днів, а потім нелегально прямують далі. Лише за 2021–2025 роки Північна Македонія видала понад 3190 таких віз, а Косово – 1460.

Дані Frontex про нелегальні перетини кордону на Західних Балканах ілюструють масштаби явища. У 2025 році першість за кількістю випадків утримує Туреччина (3 913), далі йдуть Афганістан (1 672) та Сирія (1 578). Китай посідає шосте місце (706), що підтверджує згаданий вище тренд. Особливо показовою є динаміка: якщо у 2021 році сирійців було виявлено 38 723, у 2022-му – вже 79 932, а в 2023-му – 72 937, то в 2025-му їх кількість різко падає до 1 578. Це може свідчити про зміну маршрутів, посилення контролю або ж про те, що гібридні схеми стають ефективнішими для певних національностей. Натомість для Китаю, Марокко чи Єгипту спостерігається поступове зростання, що підкреслює адаптацію контрабандних мереж до нових умов.

Оскільки попит на іноземну робочу силу зростає, а візові режими залишаються лише частково узгодженими зі стандартами ЄС, урядам Західних Балкан слід посилити заходи для запобігання експлуатації цих прогалин злочинними мережами. Протидія цій загрозі вимагає зміщення фокусу з суто прикордонних заходів на ширшу екосистему, яка уможливлює контрабанду людей.

Хоча гармонізація візової політики з ЄС є передумовою вступу, необхідні більш комплексні зусилля: покращення перевірки та оцінки ризиків під час видачі віз, посилення нагляду за каналами трудової міграції, особлива увага до ролі місцевих та іноземних компаній у створенні фіктивних трудових договорів.

Потрібна більш інтегрована правоохоронна відповідь, зокрема через трудові інспекції. Створення мультидисциплінарних слідчих груп дозволило б тісніше співпрацювати правоохоронним органам із відповідними інституціями, посилюючи спроможність виявляти та блокувати використання легальних систем в'їзду дедалі більш витонченими організованими злочинними угрупованнями.

Ваша думка важлива!

1. Як впровадження токенізованих грошей центральних банків і програмованих платіжних платформ може змінити підходи до ПВК/ФТ, санкційного контролю та міжнародного обміну фінансовою інформацією, особливо в умовах зростання цифровізації фінансових послуг?
2. Яку роль можуть відігравати територіальні громади, екологічні організації та громадянське суспільство України у запобіганні незаконній вирубці лісів і корупції в управлінні природними ресурсами, та чи достатньо для цього існуючих механізмів громадського контролю?
3. Як розвиток штучного інтелекту, великих даних та автоматизованих систем аналізу може змінити роль ПФР у найближчі 10 років? Чи стане технологічна перевага окремих держав новим фактором нерівності у глобальній системі ПВК/ФТ, і як Україні забезпечити конкурентоспроможність своїх аналітичних спроможностей?
4. Чи готова, на вашу думку, судова система до використання доказів, згенерованих або оброблених ШІ, і які зміни до Кримінального процесуального кодексу чи інших законів потрібно внести, щоб такі докази мали юридичну силу?
5. Наскільки досвід США щодо визнання іноземних злочинних груп терористичними може бути використаний Україною для тиску на російські приватні військові компанії, їхні фінансові ланцюги та міжнародних посередників, які навіть опосередковано співпрацюють з ними?
6. Як повоєнна відбудова України може бути використана злочинними мережами, оскільки після війни Україна потребуватиме сотень тисяч робітників з Азії та Африки. Наскільки готові українські інституції до цього ризику?

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-2026-23

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].