Міністерство
фінансів
України

Методологічний бюлетень AML

№44/2026



Зміст

Захист прав споживачів фінансових послуг: подолання дискримінації за політичними, релігійними та галузевими критеріями в банківській системі США 3

Банк Японії про фінансову стабільність: фронтирний штучний інтелект як макропруденційний кіберризик і нові підходи до стейблкоїнів 6

Глобальні тенденції у сфері злочинності та кримінального правосуддя: виклики технологій, транснаціональної організованої злочинності та безпеки 10

Практичний стандарт вимірювання шахрайства: професійні вимоги, процеси та методики для державного сектору 13

Нові орієнтири регулювання криптоактивів у Великій Британії 15

Американський регуляторний експеримент: що означає нове правило OCC щодо стейблкоїнів 18

Цифровізація ринку дорогоцінних металів: регуляторний підхід до токенізованого золота у Великій Британії 22

Партнери Росії як інфраструктура обходу санкцій: свідчення Українського центру безпеки та співпраці для британського парламенту 24

Глобальний звіт PwC про регулювання криптоактивів 2027: від нормотворення до наглядової архітектури – і місце України в ній 27

Від правил до результатів: європейські професійні асоціації закликають AMLA переглянути проєкти технічних стандартів для нефінансових професій 31

Транзитні коридори Карибського басейну: відродження колумбійських маршрутів та їхній вплив на європейський ринок 34

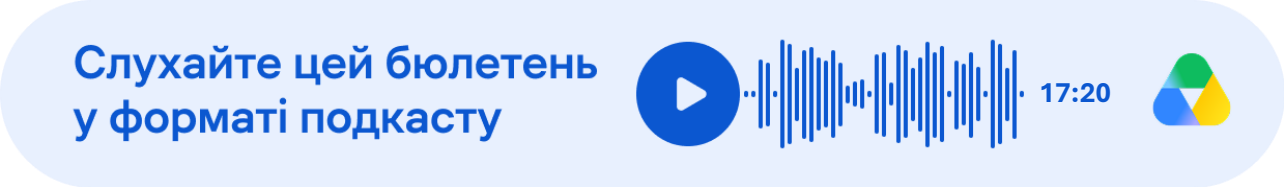
Як військові операції та експансія банд формують нову кримінальну реальність ПАР 36

Сирійський нарко-ринок після падіння режиму Асада 39

Регіональний воркшоп Егмонтської групи з віртуальних активів для підрозділів фінансової розвідки Європи: Відень, 10–11 грудня 2026 року 42

Вебінар RUSI: використання соціальних мереж для фінансування тероризму 44

Як організовані злочинні групи стали загрозою вантажним перевезенням в Коста-Риці 45



Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 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.

Захист прав споживачів фінансових послуг: подолання дискримінації за політичними, релігійними та галузевими критеріями в банківській системі США [1]



Офіційний звіт Управління контролера грошового обігу США (OCC) у складі Міністерства фінансів США, представляє результати масштабного перевірочного дослідження щодо припинення обслуговування або відмови у наданні фінансових послуг американським громадянам і підприємствам, відомого як «дебакінг». Це дослідження було ініційоване на виконання Указу Президента США № 14331 «Гарантування справедливого банкінгу для всіх американців» з метою з'ясувати, чи вимагали або заохочували політики великих банків обмеження доступу до послуг через політичні, релігійні погляди чи законну підприємницьку діяльність клієнтів. У межах перевірки, що охоплювала період із 2020 по вересень 2025 року, OCC проаналізувало діяльність дев'яти найбільших національних банків країни, які акумулюють більшість активів комерційного банківського сектору, опрацювавши близько 100 000 скарг, сотні індивідуальних рішень та приблизно 420 000 сторінок внутрішньої документації.

У звіті детально розглядаються дві головні категорії банківських практик, що створювали найвищі ризики дискримінації: політика управління ризиками репутації та галузеві обмеження. Перевірка виявила, що через розмиті та вкрай суб'єктивні критерії оцінки репутаційних ризиків, часто сформовані під тиском публічної думки, активістів чи політичної кон'юнктури, банки необґрунтовано відмовляли в обслуговуванні релігійним організаціям, консервативним медіа, продавцям продукції з політичною символікою (зокрема руху MAGA), а також представникам законних, але «соціально суперечливих» секторів економіки, таких як видобуток викопного палива, виробництво зброї чи приватні виправні заклади. Водночас автори документа зафіксували яскраво виражені подвійні стандарти: високовірогідні репутаційні ризики щодо заможних клієнтів часто ігнорувалися банками заради збереження прибуткових фінансових відносин.

[1] https://www.occ.gov/news-issuances/news-releases/2026/nr-occ-2026-90a.pdf

Окрему увагу в дослідженні приділено проблемі неналежної комунікації банків із клієнтами під час раптового закриття рахунків, коли замість прозорого пояснення реальних причин використовувалися розмиті стандартні формулювання з посиланням на дискретні права за договором. Крім того, звіт викриває факти викривлення вимог федерального законодавства про протидію легалізації доходів, здобутих злочинним шляхом (BSA/AML), які окремі співробітники банків використовували як зручне прикриття для політично або соціально вмотивованих рішень про розрив відносин. Унаслідок цього постраждали сотні малих і середніх підприємств та громадських організацій, які зіткнулися з реабстракцією доступу до критичної фінансової інфраструктури.

У фінальній частині документа узагальнено комплекс заходів, які вже вжило OCC спільно з іншими регуляторами задля викорінення подібних зловживань. Зокрема, було прийнято остаточне правило про заборону використання «репутаційного ризику» у банківському нагляді, оновлено критерії оцінки банків під час ліцензування та проведення перевірок за Законом про реінвестування в громади (CRA), а також вдосконалено процедури подання скарг через профільний державний портал HelpWithMyBank.gov. Водночас регулятор підкреслює, що досягнутий прогрес потребує подальшого постійного моніторингу, підвищення загальної прозорості ринку та активного нагляду з боку Конгресу задля остаточного гарантування того, що жоден американський громадянин не буде позбавлений доступу до базових фінансових послуг через свої переконання.

Висновки

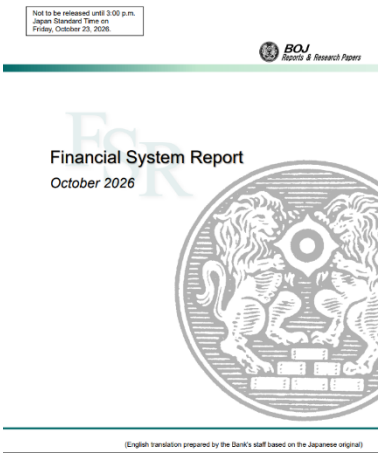
Суб’єктивність та зловживання поняттям «репутаційного ризику»: Найбільші банки США не мали чітких, вимірюваних чи об’єктивних стандартів оцінки репутаційних ризиків, через що розмиті політики використовувалися для обмеження прав громадян і компаній на основі їхніх захищених законом політичних, релігійних чи соціальних поглядів.

Реальна шкода для законного бізнесу та конкуренції: Галузеві обмеження, запроваджені банками під тиском суспільних чи політичних настроїв (наприклад, щодо виробників зброї, енергетики чи виправних установ), завдали реальної шкоди підприємствам малого та середнього бізнесу, створивши бар’єри для конкуренції та інновацій.

Непрозорість комунікації та приховування мотивів: Поганий рівень комунікації з боку банків під час закриття рахунків залишав клієнтів у невіданні та приховував реальні причини дискримінації, чому також сприяли надмірні та хибно тлумачені обмеження щодо конфіденційності звітів про підозрілу діяльність.

Попри рішучі кроки регуляторів (зокрема скасування перевірок за критерієм репутаційного ризику), для остаточного викорінення дебакінгу необхідні постійний моніторинг, прозорість та законодавчі зміни з боку Конгресу.

Банк Японії про фінансову стабільність[2]



Департамент фінансової системи та банківських перевірок Банку Японії оприлюднив піврічний Звіт про фінансову систему (Financial System Report) з даними станом на кінець вересня 2026 року. Документ є основним інструментом макропруденційної оцінки: його висновки центральний банк використовує під час виїзних перевірок і дистанційного моніторингу фінансових установ, а також у міжнародних дискусіях щодо регулювання та нагляду. Загальна оцінка залишається стабільною: банки мають достатній капітал і стабільну базу фінансування, що підтверджено макрострес-тестами, зокрема за сценарієм комбінованого шоку – одночасної реалізації геополітичних ризиків зі зростанням цін на нафту, зниження очікувань щодо прибутковості інвестицій у штучний інтелект і суттєвого підвищення процентних ставок. Водночас звіт фіксує глибшу взаємопов'язаність японської системи з іноземним сектором небанківських фінансових посередників: кредити та інвестиції японських банків у цей сектор зросли з 8 трлн єн у березні 2008 року до 126 трлн єн у червні 2026 року, а вкладення іноземних інвестиційних фондів у японські ринки – з 111 до 408 трлн єн.

Для фахівців із протидії фінансовим злочинам найбільшу цінність мають підрозділ V-C та окремий аналітичний блок (Box 2), присвячені кіберзагрозам. Кількість атак програм-вимагачів у Японії утримується на високому рівні; фішингові атаки, попри зниження, також залишаються масовими, причому Рада з протидії фішингу Японії пояснює скорочення їхньої кількості в першому півріччі 2026 року тимчасовим збоєм закордонної поштової інфраструктури та ретельнішою верифікацією особи з боку постачальників безготівкових платіжних послуг. Збитки від незаконних онлайн-переказів через інтернет-банкінг суттєво зменшилися, зокрема завдяки запровадженню багатофакторної автентифікації, однак зросла кількість підозрілих спроб доступу, зокрема сканування вразливостей з-за кордону. Мотиви атак різняться: поряд із фінансовою вигодою дедалі помітнішими стають атаки суб'єктів, імовірно пов'язаних із державами, та атаки, зумовлені геополітичною напруженістю.

Центральне аналітичне положення звіту стосується так званого фронтирного штучного інтелекту – моделей із найвищими можливостями, доступними на поточний момент. Банк Японії наголошує, що генеративний ШІ вже використовується для підготовки фішингових листів, соціальної інженерії та розробки шкідливого програмного забезпечення, а розвиток агентних технологій і здатності до аналізу коду створює перспективу автоматизації всього ланцюга атаки – від розвідки цілі та виявлення вразливостей до розробки й застосування експлойтів. Головна загроза полягає не стільки в появі принципово нових технік, скільки в автоматизації та прискоренні процесів, які раніше потребували високої кваліфікації й часу: інтервал між виявленням уразливості та її

[2] https://www.boj.or.jp/en/research/brp/fsr/data/fsr261023a.pdf

використанням скорочується, у захисників залишається менше часу на встановлення оновлень, а зловмисники навіть з обмеженими людськими ресурсами можуть розширювати коло цілей.

Звіт відтворює хронологію реакції регуляторів у 2026 році. 7 квітня компанія Anthropic оголосила про модель Claude Mythos Preview, яку через розвинені кіберможливості не було відкрито для публічного доступу, та про ініціативу Project Glasswing, у межах якої близько 50 компаній і організацій використовували модель для виявлення й усунення вразливостей; 13 квітня Інститут безпеки AI Великої Британії (AISI) оприлюднив оцінку її кіберможливостей. 24 квітня Агентство фінансових послуг Японії (FSA) провело публічно-приватну координаційну нараду, 22 травня FSA і Банк Японії спільно звернулися до фінансових установ щодо короткострокових заходів, 16 червня Японська банківська асоціація опублікувала рекомендації щодо систем управління кібербезпекою, 7 липня ЄЦБ направив значущим установам лист із вимогою оцінити загрози кібербезпеці, спричинені AI, і подати плани дій до кінця жовтня, а 31 серпня Голова Ради з фінансової стабільності (FSB) у листі до міністрів фінансів і керівників центральних банків G20 назвав кіберризики фронтирного ШІ однією з найнагальніших загроз для фінансової системи. Банк Японії розглядає кіберінциденти як суттєвий макропруденційний ризик, оскільки їхні наслідки можуть поширюватися на інші установи.

Спільне звернення FSA і Банку Японії містить дев'ять заходів: визнання реагування на загрози передових AI управлінським пріоритетом; визначення пріоритетних сервісів та IT-систем; ліквідацію технічного боргу в цих активах; забезпечення персоналом для встановлення оновлень; перевірку договорів технічного супроводу з постачальниками; ризик-орієнтований підхід до встановлення оновлень; посилення заходів захисту, що виходять за межі оновлень; підготовку до порушення роботи пріоритетних сервісів; підтримання й розвиток зовнішньої взаємодії. Японські установи вже оцінюють пріоритетні системи з доступом до інтернету, насамперед інтернет-банкінг. Паралельно звіт фіксує стрімке поширення генеративного AI в самому фінансовому секторі: за опитуванням 150 установ у квітні–травні 2026 року близько 80 % уже використовують такі інструменти, а з урахуванням тих, що проводять випробування, – понад 90 %; сфера застосування розширилася від адміністративних завдань до основних операцій з даними клієнтів, тоді як серед невирішених проблем установи найчастіше називають заходи протидії кібератакам і готовність даних.

Окремо Банк Японії звертає увагу на перехід до постквантової криптографії. Державні органи Японії встановили орієнтир завершення такого переходу в принципі до 2035 року, а фінансовим установам рекомендовано вже зараз за участі вищого керівництва провести інвентаризацію систем, що використовують криптографію, сформувати плани міграції та забезпечити криптографічну гнучкість. Обґрунтуванням є загроза атак типу «зібрати зараз – розшифрувати пізніше», коли зашифровані дані, викрадені сьогодні, можуть бути розшифровані після появи достатньо потужних квантових комп'ютерів.

Завершує розділ аналіз стейблкоїнів. Банк Японії констатує, що сфера їх використання розширюється – від розрахунків за операціями з криптоактивами та утримання коштів для таких операцій до транскордонних переказів і розрахунків за цифровими цінними паперами, – і що,

хоча масштаби поки обмежені, ринкова капіталізація зростає. Оскільки резерви найбільших емітентів значною мірою складаються з короткострокових державних цінних паперів та операцій репо, посилюються зв'язки стейблкоїнів із традиційними грошовими ринками. Звіт фіксує регуляторну динаміку в ключових юрисдикціях: запропоновані OCC і FDIC правила імплементації GENIUS Act у США, розпочату Європейською комісією в травні 2026 року консультацію щодо перегляду Регламенту MiCA, зокрема в частині токенів електронних грошей, а також зміни до японського Закону про платіжні послуги, які набули чинності в червні 2026 року: вони запровадили більшу гнучкість в управлінні резервними активами трастових стейблкоїнів і вимогу до постачальників послуг обміну криптоактивів, зокрема тих, що працюють зі стейблкоїнами, утримувати певні активи всередині країни.

Висновки

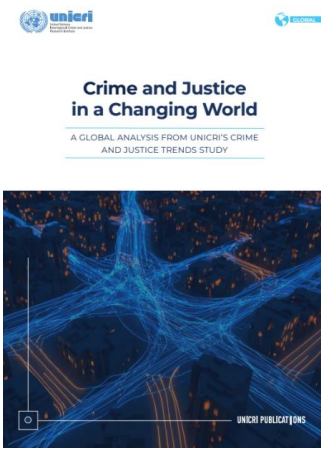
Кіберризик передових AI переходить із площини операційного ризику окремої установи в площину системного ризику: Банк Японії прямо кваліфікує кіберінциденти як суттєвий макропруденційний ризик, а FSA, ЄЦБ і FSB упродовж квітня–серпня 2026 року перевели тему у формат конкретних наглядових запитів із дедлайнами. Це означає, що стійкість критичних систем, насамперед інтернет-банкінгу, дедалі більше розглядатиметься в міжнародному наглядовому діалозі як елемент фінансової стабільності, а не лише як питання IT-безпеки.

Дев'ять короткострокових заходів FSA і Банку Японії є готовою основою для самооцінки: інвентаризація пріоритетних сервісів, ліквідація технічного боргу, кадрове забезпечення встановлення оновлень, перевірка договорів із постачальниками та ризик-орієнтоване встановлення оновлень дозволяють швидко визначити, чи здатна установа реагувати тоді, коли інтервал між виявленням уразливості та її експлуатацією скорочується до днів.

Для протидії шахрайству вирішальною залишається якість автентифікації та ідентифікації: японська статистика пов'язує зменшення збитків від незаконних онлайн-переказів із багатофакторною автентифікацією, а зниження кількості фішингових атак – частково з ретельнішою верифікацією особи постачальниками безготівкових платежів. Оскільки генеративний AI вже застосовується для фішингу й соціальної інженерії, сценарії моніторингу операцій, пов'язаних із шахрайськими переказами та транзитними рахунками, потребують регулярного оновлення.

Регулювання стейблкоїнів зміщується до вимог щодо резервів і локалізації активів: японські зміни до Закону про платіжні послуги поєднують гнучкіше управління резервами трастових стейблкоїнів з обов'язком постачальників послуг обміну криптоактивів утримувати певні активи всередині країни. Такі механізми доцільно аналізувати під час формування національних правил щодо забезпечених віртуальних активів, прив'язаних до валютних цінностей.

Глобальні тенденції у сфері злочинності та кримінального правосуддя: виклики технологій, транснаціональної організованої злочинності та безпеки [3]



Глобальний аналітичний звіт, опублікований Міжрегіональним науково-дослідним інститутом ООН з питань злочинності та правосуддя (UNICRI), узагальнює результати масштабного дослідження еволюції злочинності та систем правосуддя в усьому світі за останнє десятиліття. Документ ґрунтується на дев'яти регіональних звітах і охоплює ключові глобальні трансформації, зокрема стрімкий розвиток технологій, еволюцію транснаціональної організованої злочинності, наслідки екологічних змін, процеси урбанізації, збройні конфлікти та нові тенденції у реформуванні систем кримінального правосуддя. У звіті підкреслюється парадоксальна тенденція: попри тривале глобальне зниження неорганізованих форм насильства (зокрема рівня умисних вбивств), у світі спостерігається стрімке зростання полікримінальності та посилення інтеграції злочинних мереж у легальні економічні структури.

Окрему увагу в дослідженні приділено новітнім технологічним загрозам, які докорінно змінили ландшафт глобальної злочинності. Широка доступність передових кіберможливостей, генеративного штучного інтелекту, безпілотників та бізнес-моделей на кшталт «злочинності як послуги» знизила поріг входу для зловмисників і призвела до безпрецедентного вибуху глобальної віктимізації. Мільярди людей по всьому світу стають мішенями складних онлайн-шахрайств і кіберзлочинів, тоді як організовані угруповання дедалі частіше використовують віртуальні активи та лазівки в міжнародному регулюванні для відмивання коштів і переправлення незаконних товарів. Ці процеси супроводжуються утворенням так званих «зон конвергенції» у слабо регульованих регіонах, де злочинність зливається з корупцією та тіньовою економікою, інколи перевершуючи за обсягами легальні сектори ВВП окремих країн.

У відповідь на ці виклики державні системи кримінального правосуддя по всьому світу зазнають серйозного тиску, що призводить до поступової трансформації принципів державної політики безпеки. На зміну міжнародному консенсусу, що сформувався після завершення холодної війни щодо правничих стандартів, демократичного нагляду та реабілітації приходить доба сек'юритизації – моделі, що спираються на мілітаризоване патрулювання, жорсткіші каральні практики в пенітенціарній системі, масове впровадження систем цифрового нагляду та зниження віку кримінальної відповідальності. Водночас міжнародне співробітництво у сфері боротьби зі злочинністю стає дедалі фрагментованим, вразливим до геополітичних розбіжностей і

[3] https://unicri.org/sites/default/files/2026-10/Crime-and-Justice-in-a-Changing-World-2026.pdf

підпорядкованим вузьким національним інтересам. У фінальній частині звіту розглядаються п’ять ключових перетинних тем – взаємозв’язок конфліктів і тероризму, екологічні злочини, виклики швидкої урбанізації, гендерно зумовлене насильство та залучення молоді до кримінальної діяльності – і наголошується на нагальній потребі посилення транснаціональної координації задля протидії цим викликам.

Додатково у звіті наголошується на критичній важливості п’яти взаємопов’язаних тем, які слугують каталізаторами глобальних трансформацій безпекового середовища. Наприклад, зміни клімату та деградація довкілля створюють умови бідності та витіснення, якими користуються озброєні угруповання для залучення нових членів. Водночас швидка та нерегульована урбанізація перетворює мегаполіси й транспортні вузли на осередки нелегальної економіки, а вразливі категорії населення, особливо жінки та молодь, усе частіше стають жертвами як фізичного насилля, так і новітніх форм експлуатації в цифровому середовищі. Усе це вимагає від міжнародної спільноти не лише розвитку технологічного нагляду, а й глибокого переосмислення соціальних і економічних передумов злочинності.

Висновки

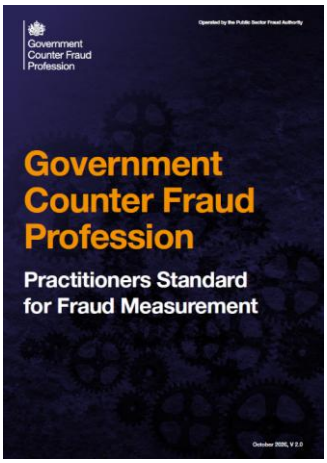
Зростання полікримінальності та стирання меж між ринками: Злочинні мережі по всьому світу активно диверсифікують свою діяльність, використовуючи глобалізацію та цифровізацію для експлуатації легальних галузей і ланцюгів постачання, що призводить до зростання транснаціональної організованої злочинності на тлі глобального зниження неорганізованих насильницьких злочинів.

Технологічні інновації та масова кібервіктимізація: Доступність сучасних технологій, дронів, штучного інтелекту та платформ «злочинності як послуги» знизила поріг входу для злочинців, спричинивши масштабний глобальний ріст онлайн-шахрайства та кіберзлочинності з мільярдними збитками для суспільства.

Сек'юритизація систем кримінального правосуддя: Через зростання занепокоєння щодо безпеки уряди багатьох країн відходят від правничих стандартів і принципів реабілітації на користь мілітаризованих методів поліції, жорсткіших тюремних режимів, зниження віку кримінальної відповідальності та переоцінки міграційних ризиків.

Багатополярність реформ та транзакційне співробітництво: Традиційний консенсус, сформований після завершення холодної війни щодо реформування правосуддя на основі стандартів ООН розмивається через появу нових учасників і різноманітних моделей допомоги, а міжнародна кооперація стає все більш нерівномірною, вразливою до політичних розбіжностей і підпорядкованою вузьким національним інтересам.

Практичний стандарт вимірювання шахрайства: професійні вимоги, процеси та методики для державного сектору [4]



Документ, розроблений Управлінням з питань запобігання шахрайству в державному секторі (PSFA) та Професійною спільнотою у сфері протидії шахрайству уряду Великої Британії (GCFP), є фундаментальним і всеосяжним керівництвом для практиків і державних установ. Основною метою цього стандарту є запровадження єдиного узгодженого міжвідомчого підходу до кількісного визначення та оцінки масштабів шахрайства й помилок у процесах державного управління, підвищення професійної кваліфікації фахівців і радикальне покращення якості аналітичної роботи в організаціях. У документі наголошується, що ефективна протидія економічним злочинам неможлива без точного вимірювання вже відомих фактів шахрайства та прогнозування прихованих втрат. Автори детально описують архітектуру урядових функцій Великої Британії, ключову роль PSFA та GCFP, а також подають розгорнутий огляд Рамкової програми протидії шахрайству із виділенням Кластера контролю шахрайства, що дозволяє органічно інтегрувати вимірювання у загальну систему управління ризиками.

Центральне місце в документі посідає структурована модель компетентностей, яка визначає професійні знання, навички та практичний досвід за вісьмома ключовими компонентами – від стратегічного планування вимірювань і статистичного аналізу до збору доказів, оцінювання та підготовки детальної звітності – для двох рівнів професійної підготовки: базового та практичного. Практична частина керівництва містить покрокові інструкції щодо виявлення відомих втрат (включно з категоріями запобігання, виявлення та помилок), проведення досліджень залишкових ризиків через спеціальні процедури «Вимірювання збитків від шахрайства» (FLM) та детальне «Тестування контролів». У документі суворо регламентовано методологію статистичної вибірки (включаючи випадкову, стратифіковану, монетарну одиницю та кластерну вибірки) із точним розрахунком довірчих інтервалів, рівнів довіри та допустимих похибок, правила роботи з компаративними даними й джерелами доказів, а також підходи до розрахунку майбутніх і тактичних чи стратегічних заощаджень.

Водночас у керівництві окрему увагу приділено управлінню процесами на рівні цілих організацій: побудові комплексних програм вимірювання, розробці річних планів дій, створенню практичних карт забезпечення та забезпеченню належного рівня внутрішнього контролю. Документ детально розкриває концепцію «айсберга шахрайства», розмежовуючи виявлені випадки шахрайства, невиявлені збитки, які піддаються кількісному оцінюванню, та глибинні приховані загрози. Такий

[4] https://assets.publishing.service.gov.uk/media/6accd119ec9d3aba1e013c46/gcfp-practitioners-standard-for-fraud-measurement-oct26.pdf

підхід дає змогу керівникам установ виявляти недооцінені ризики, приховані вразливості та організаційні проблеми. Крім того, стандарт окреслює порядок взаємодії з незалежними аудиторськими структурами та визначає правила управління випадками виявлених помилок задля очищення баз даних і запобігання хибнопозитивним спрацьовуванням у майбутньому.

Додатково в документі розглядаються питання побудови стійкої культури протидії правопорушенням, яка спирається на безперервний цикл освіти, вимірювання, моніторингу та постійного вдосконалення внутрішніх процесів. Практики отримують інструменти для подолання внутрішнього опору чи відсутності випадків у звітах окремих підрозділів через порівняльний аналіз та адресні запити до керівників. Завершується стандарт чіткими вимогами до прозорості звітності перед вищим керівництвом та комітетами з аудит-контролю, підкреслюючи, що оцінка ефективності стратегії має базуватися виключно на верифікованих емпіричних даних для раціонального розподілу ресурсів та захисту інтересів платників податків.

Висновки

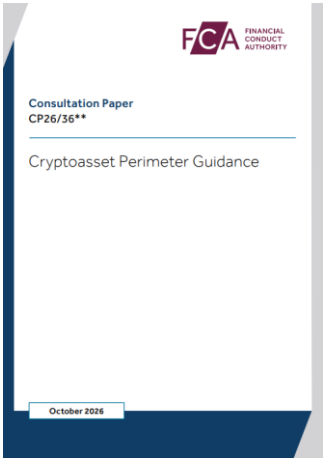
Вимірювання як основа ефективної стратегії: Точне кількісне визначення масштабів шахрайства та помилок є базовим елементом державного управління, без якого неможливо сформувати адекватну стратегію захисту публічних фінансів та оцінити рентабельність контрольних заходів.

Поєднання виявлених фактів та оцінки прихованих ризиків: Повноцінна система вимірювання повинна охоплювати не лише зафіксовані й попереджені випадки (відоме шахрайство), а й застосовувати спеціальні тести вибірки та аналіз залишкових ризиків для виявлення прихованих, не зафіксованих поточними контролями втрат.

Суворі вимоги до статистичної достовірності вибірок: Для конкретного узагальнення результатів на всю сукупність даних практика вимагає використання виключно ймовірнісних методів вибірки з чітко визначеними рівнем довіри (наприклад, 95%) та межею похибки, повністю виключаючи суб’єктивні чи нерепрезентативні підходи.

Чіткий ланцюжок підзвітності та стандартизація продуктів звітності: Організації зобов’язані інтегрувати програми вимірювання у свої загальні системи внутрішнього контролю й забезпечення, закріплюючи персональну відповідальність керівництва вищого рівня за управління ризиками та прозорість звітних показників.

Нові орієнтири регулювання криптоактивів у Великій Британії [5]



Консультаційний документ, опублікований Управлінням фінансового нагляду Великої Британії (FCA), є важливим кроком у підготовці до фундаментальної зміни регуляторного ландшафту криптоактивів. Документ, присвячений "Настановам щодо периметру криптоактивів" (Cryptoasset Perimeter Guidance), детально роз'яснює, як FCA тлумачитиме нові законодавчі акти, зокрема Регламент про криптоактиви 2026 року (Cryptoassets Regulations) та різні поправки 2026 року (Cryptoassets Amendment Regulations). Ці нормативні акти, які набудуть чинності 25 жовтня 2027 року, запроваджують нові види регульованої діяльності: будь-яка особа, яка здійснює діяльність з криптоактивами у Великій Британії в якості бізнесу, повинна буде отримати авторизацію FCA, якщо вона не підпадає під винятки. Цей документ є не просто технічним оновленням, а стратегічним інструментом, покликаним забезпечити ясність для учасників ринку, сприяти конкуренції та інноваціям, а також захистити споживачів, допомагаючи фірмам уникнути ненавмисного порушення регуляторних вимог.

Центральна тема документу – це тлумачення нових винятків із регульованої діяльності, які були запроваджені законодавчими поправками. FCA пропонує оновити свій Посібник (PERG), щоб чітко пояснити, як ці винятки застосовуються на практиці. Зокрема, документ зосереджується на кількох ключових сферах: тимчасові угоди про розрахунки, винятки для кваліфікованих стейблкоїнів Великої Британії (UK qualifying stablecoins) та їхніх резервних активів, діяльність центральних депозитаріїв цінних паперів (CSD), а також винятки для пропрієтарної торгівлі та маркет-мейкінгу. Кожен із цих пунктів супроводжується запитаннями для громадського обговорення, що свідчить про прагнення FCA до прозорого та інклюзивного процесу формування політики. Важливо розуміти, що FCA не має повноважень змінювати законодавчо визначений периметр, а лише тлумачити його, тому всі пропозиції спрямовані на роз'яснення, а не на розширення чи звуження регуляторного поля.

Одним із найбільш значущих аспектів документу є спроба FCA надати визначеність щодо децентралізації, яка вважалася "сірою зоною" у фінансовому регулюванні. FCA наголошує, що регуляторний периметр є технологічно нейтральним, і використання програмного забезпечення,

[5] https://www.fca.org.uk/publication/consultation/cp26-36.pdf

смарт-контрактів, розподілених реєстрів або децентралізованих механізмів управління не є визначальним фактором для встановлення необхідності авторизації.

Аналіз завжди базується на фактах, і ключовим питанням залишається: чи існує особа, яка здійснює регульовану діяльність?

FCA чітко заявляє, що автоматизація процесів не означає відсутність відповідальної особи. Якщо особа визначає параметри, критерії або логіку роботи автоматизованої системи, вона може вважатися такою, що здійснює діяльність через цю систему. Це надзвичайно важливий сигнал для розробників DeFi-протоколів та DAO (децентралізованих автономних організацій): FCA чітко дає зрозуміти, що ярлики "децентралізований" або "DeFi" не звільняють від регулювання, і аналіз буде зосереджуватися на сутності відносин, розподілі ролей та контролі над ключовими функціями. Документ навіть вводить поняття "спектру децентралізації", визнаючи, що вона не є бінарним явищем, і пропонує розглядати такі фактори, як управління, операційна структура та економічна вигода, як потенційно релевантні для визначення наявності відповідальної особи.

Ще одним критично важливим блоком є роз'яснення щодо кваліфікованих стейблкоїнів. FCA вводить нове поняття "UK qualifying stablecoin" – це стейблкоїн, випущений особою, яка має відповідний дозвіл FCA на цю діяльність. Це розмежування є ключовим, оскільки багато нових винятків, зокрема щодо резервних активів та тимчасового утримання під час платежів, застосовуються виключно до цього підтипу. Документ також проводить чітку межу між кваліфікованими стейблкоїнами та електронними грошима (e-money), наголошуючи, що продукт не може бути одночасно і тим, і іншим. FCA наводить ознаки, які можуть вказувати на те, що продукт є кваліфікованим стейблкоїном, а не електронними грошима, наприклад, використання технології розподіленого реєстру, намір випуску для цілей, відмінних від здійснення платежів, або маркетинг як стейблкоїна. Це має величезне значення для емітентів, оскільки від цієї класифікації залежить, які саме винятки та регуляторні вимоги до них застосовуватимуться.

Документ також приділяє значну увагу технічним постачальникам послуг. FCA пропонує новий виняток для компаній, які надають суто технічні послуги, що дозволяють іншим особам отримати доступ до послуг третіх сторін або до децентралізованого протоколу. Однак, FCA чітко наголошує, що це не є загальним винятком для всього, що пов'язано з технологіями чи DeFi. Виняток застосовується лише тоді, коли послуга є "виключно технічною" і не передбачає суттєвого посередництва чи дискреції. FCA детально роз'яснює, що означає "виключно надавати" (merely providing) та "технічна послуга", наводячи численні приклади та фактори, які вказують на те, чи є діяльність компанії просто наданням доступу, чи вона вже є суттєвою участю в транзакції. Це особливо актуально для постачальників гаманців, інтерфейсів та інфраструктурних рішень, які повинні будуть самостійно оцінити, чи підпадає їхня діяльність під цей виняток, чи вони все ж таки потребують авторизації як особи, що "організовують угоди" (arranging deals).

Окремо варто відзначити розділ, присвячений торгівлі та маркет-мейкінгу. FCA вводить цільовий виняток для тих, хто торгує криптоактивами від власного імені і не надає послуг третім особам. Документ роз'яснює, коли така діяльність вважається наданням послуги, наводячи приклади, як-

от торгівля з роздрібними інвесторами, стягнення комісій або виступ у ролі постачальника ліквідності. Також надаються критерії для визначення маркет-мейкера на кваліфікованій платформі торгівлі криптоактивами (QCAPT), що дозволяє їм сподіватися на цей виняток.

Насамкінець, документ наголошує на важливості підготовки до нового режиму. Період подання заявок на авторизацію вже відкритий і триватиме до 28 лютого 2027 року. FCA закликає фірми, які вже мають авторизацію, перевірити, чи мають вони необхідні дозволи для нових видів діяльності, і за необхідності подати заявку на їх розширення. Для тих, хто подасть заявку вчасно, FCA обіцяє розглянути її до початку нового режиму, що дозволить їм скористатися "перехідними положеннями" (savings provisions) і продовжувати роботу безперервно.

Висновки

Технологічна нейтральність та кінець "сірої зони" DeFi: FCA наголошує, що використання смарт-контрактів, автоматизації чи децентралізованих протоколів не звільняє від регуляції. Аналіз базується на сутності діяльності та ролі конкретних осіб, які контролюють параметри системи, а не на ярликах "DeFi" чи "DAO".

Чітке розмежування стейблкоїнів та електронних грошей: Введено нове поняття "UK qualifying stablecoin" (стейблкоїн, випущений з дозволу FCA), і продукт не може бути одночасно стейблкоїном та електронними грошима. Це визначає, які саме винятки (щодо резервних активів чи платежів) застосовуються до емітента.

Вузький виняток для технічних постачальників послуг: Компанії, що надають суто технічний доступ до послуг або децентралізованих протоколів, можуть уникнути регуляції, але лише за умови відсутності посередництва в транзакціях.

Практичний дедлайн для підготовки: Період подання заявок відкритий до 28 лютого 2027 року, а новий режим набуває чинності 25 жовтня 2027 року. Фірмам, які вчасно подадуть заявку, гарантовано розгляд до початку режиму для використання перехідних положень.

Американський регуляторний експеримент: що означає нове правило OCC щодо стейблкоїнів [6]



Сфера криптовалютної регуляції продовжує перебувати в стані турбулентності, і одним із ключових маркерів цього процесу є безпрецедентна увага до такого сегменту, як стейблкоїни.

21 жовтня 2026 року Управління контролера грошового обігу США (OCC) представило остаточну версію правил щодо платіжних стейблкоїнів, які набувають чинності 18 січня 2027 року. Ця подія викликала жваві дискусії в аналітичних колах, адже на перший погляд здається, що для європейських інвесторів нічого не змінюється.

Однак, якщо заглибитися в деталі, стає очевидним, що найважливішим аспектом нового регулювання є не сама заборона на виплату відсотків, яка зберігається, а вилучення з фінального тексту певної презумпції, що стосується винагородних програм. Це рішення переводить питання дозволеності тих чи інших фінансових моделей з площини чітких законодавчих норм у площину суб'єктивного нагляду, створюючи невизначеність, яка може мати далекосяжні наслідки для глобального ринку.

Для того щоб зрозуміти суть цих змін, необхідно розглянути контекст, у якому вони відбуваються. Американське законодавство, зокрема GENIUS Act, чітко забороняє емітентам платіжних стейблкоїнів виплачувати своїм власникам відсотки або прибутковість, якщо ця виплата здійснюється виключно за факт володіння, використання або збереження токена. Водночас закон зобов'язує OCC та інші банківські наглядові органи запобігати обходу цієї заборони.

Саме на етапі конкретного дизайну правил і виникають найбільші суперечності. Обґрунтування цієї заборони не є суто криптовалютним; воно бере витоки з банківського права і має назву «відтік депозитів». Логіка тут проста: якщо емітент стейблкоїнів виплачує відсотки на свої баланси, він вступає в пряму конкуренцію з поточними рахунками та депозитами, але при цьому не підпадає під повний спектр страхування депозитів та банківського нагляду. Що ширшою є ця процентна ставка, то більше грошей мігрує з традиційної банківської системи, що своєю чергою скорочує кредитні можливості банків. Той самий аргумент лежить в основі статті 50 європейського регламенту MiCAR, який забороняє емітентам токенів електронних грошей нараховувати відсотки.

Однак, якщо європейський підхід є досить прямолінійним і широким, то американський регулятор у своєму фінальному рішенні пішов на компроміс, який викликав критику з боку банківського сектору. Весняний проєкт правил OCC містив так звану презумпцію: певні домовленості між емітентом та третьою стороною щодо виплати прибутковості мали вважатися

[6] https://cryptoticker.io/en/stablecoin-interest-genius-act-grandfathering/

порушенням заборони на відсотки без необхідності доводити це в кожному конкретному випадку. Йшлося про структури, в яких емітент не платить сам, а це робить афілійована компанія, торгова платформа або дистриб'ютор, з якими існують договірні чи економічні відносини. У фінальній версії правила ця презумпція зникла. Замість неї OCC має намір розглядати такі домовленості в індивідуальному порядку. Це рішення зазнало критики з боку Bank Policy Institute, асоціації великих американських банків, яка вже 21 жовтня 2026 року заявила, що без чіткої презумпції та прозорої процедури важко визначити, які практики перетинають межу дозволеного.

Ця зміна, яка на перший погляд здається послабленням, насправді створює значну невизначеність. З вилучення презумпції випливає, що існуюча програма винагород не є ні прямо забороненою, ні прямо дозволеною новим правилом, а потрапляє під індивідуальний наглядовий розгляд. Той, хто керує такою програмою, дізнається про свій статус лише через наглядову практику, а агентство наразі відмовляється публікувати результати таких перевірок за будь-якою фіксованою процедурою.

Для власників стейблкоїнів з ЄС це поки що є радше спостереженням, аніж безпосереднім ризиком, адже користувачі і так не отримують відсотків на токени електронних грошей на регульованих європейських платформах. Однак для тих, хто використовує винагородні програми на платформах поза межами ЄС, ситуація стає заплутаною, оскільки з січня 2027 року в США така практика перебуватиме під загрозою індивідуального наглядового розгляду.

Важливо зазначити, що новий розділ 12 CFR 15, який регулює ці питання, охоплює широкий спектр діяльності емітента: від дозволених операцій та резервних активів до викупу, управління ризиками, зберігання, ліцензування та нагляду. Порядок тем у документі свідчить про наміри законодавця: резерви та викуп стоять на першому місці, оскільки платіжний стейблкоїн є засобом платежу лише тоді, коли він може бути повернутий за номінальною вартістю в будь-який час. Зберігання та відкликання ліцензії стоять поруч, оскільки наглядач повинен мати важіль впливу, якщо ця умова перестає виконуватися. Крім того, OCC отримує наглядові повноваження над іноземними емітентами платіжних стейблкоїнів. Це означає, що європейський емітент, який бажає вивести стейблкоїн, номінований в євро, на американський ринок, буде змушений працювати в двох наглядових системах одночасно, що створює додаткове регуляторне навантаження.

Окремої уваги заслуговує той факт, що фінальне правило навмисно залишає поза увагою велику сферу – положення про Bank Secrecy Act, протидію відмиванню коштів (AML) та санкційні списки OFAC. Для цих питань OCC анонсувало окремий процес розробки правил у координації з Міністерством фінансів, не називаючи жодних дат. Це є більше ніж формальністю, адже саме нагляд за AML визначає, які адреси можуть бути заморожені і за яких умов емітент блокує токени. Поки ця частина відсутня, американська рамка є завершеною в частині ринкових правил, але не в частині контрольної архітектури. Більше того, на момент публікації статті остаточний текст правил ще не був опублікований у Федеральному реєстрі, офіційному віснику США. Практично це означає, що наразі публічно доступними є лише бюлетень агентства та супровідні повідомлення, тоді як юридичний текст, з яким працюватимуть юристи та емітенти, з'явиться пізніше. Тому всім,

кому потрібна конкретна відповідь щодо тієї чи іншої моделі винагород, краще зачекати на цей текст.

Повертаючись до європейського контексту, варто підкреслити, що стаття 50 MiCAR є коротшою, але водночас жорсткішою. Вона забороняє емітентам токенів електронних грошей надавати відсотки, і ця заборона не зупиняється на емітенті: вона однаково поширюється на постачальників криптоактивних послуг, які працюють з такими токенами, навіть якщо вони не є емітентами, а лише зберігають або торгують ними. Європейське поняття відсотків є широким і охоплює будь-яку винагороду, прив'язану до періоду володіння, незалежно від того, як вона називається і хто її платить. Саме тому моделі кешбеку та винагород на балансах стейблкоїнів у ЄС переважно зникли, тоді як в інших регіонах вони продовжували існувати.

Для європейського ринку американське регулювання не несе негайних змін: воно адресоване емітентам і наглядачам, а не власникам. Але є два аспекти, на які варто звернути увагу. Перший – це місцезнаходження платформи: постачальник, ліцензований у ЄС, повністю підпадає під MiCAR, тоді як неєвропейський постачальник – ні. Другий – це оподаткування: якщо винагорода за такою програмою нараховується вам, цей дохід потрібно оцінити для податкових цілей, і класифікація залежить від конкретного випадку, тому надійну відповідь може надати лише податковий консультант.

Підсумовуючи аналітичну оцінку, можна стверджувати, що справжньою подією є саме вилучення презумпції, а не збереження заборони на відсотки. Заборона вже містилася в законодавчому тексті, і агентство не могло її послабити, тоді як презумпція була наглядовим рішенням, яке тепер переглянуто. Однак ніхто не може кількісно оцінити практичний ефект цієї зміни сьогодні, оскільки законодавчий текст ще не опублікований, а OCC не назвало жодної процедури для своїх індивідуальних рішень. Як зазначила Пейдж Парідон, виконавчий віце-президент і співголова з регуляторних питань Bank Policy Institute, «рішення вилучити презумпцію щодо відсотків замінює ясність на неоднозначність і наражає банківську систему та її клієнтів на ризик відтоку депозитів». Це позиція банківської асоціації, а отже, зацікавленої сторони, але документально зафіксованим на даний момент є факт вилучення, а не його наслідок.

Для ЄС висновки з цього обмежені. Стаття 50 MiCAR не визначає жодної презумпції, яку можна було б скасувати, оскільки вона прямо забороняє відсотки і включає постачальників послуг. Європейське послаблення вирішувалося б законодавцем, а не наглядовим органом, і наразі жодних ознак цього немає. Тому для європейських інвесторів і користувачів стейблкоїнів ситуація залишається стабільною.

Висновки

Збереження заборони, але зміна підходу: OCC зберігає заборону на виплату відсотків за володіння стейблкоїнами (закон GENIUS Act), але скасовує автоматичну презумпцію порушення для винагород, що реалізуються через треті сторони.

Перехід до індивідуального нагляду: Замість чітких правил OCC запроваджує розгляд кожної моделі винагород в індивідуальному порядку (case-by-case), що створює правову невизначеність для учасників ринку, які не отримують жодних гарантій щодо вже існуючих програм.

Незмінність для Європи: Для європейських інвесторів американські правила не створюють негайних змін, оскільки стаття 50 регламенту MiCAR вже давно й жорстко забороняє будь-які відсотки на токени електронних грошей, включно з моделями кешбеку та винагород.

Незавершеність архітектури: Американське регулювання наразі є фрагментованим – воно не включає норми щодо AML та санкційного контролю, а остаточний текст правил ще не опубліковано у Федеральному реєстрі, що ускладнює практичне застосування норм.

Цифровізація ринку дорогоцінних металів: регуляторний підхід до токенізованого золота у Великій Британії [7]



Документ, опублікований Управлінням з фінансового регулювання та нагляду Великої Британії (FCA), є офіційним закликом до подання відгуків і досліджує перспективи інтеграції технології розподіленого реєстру (DLT) у ринок дорогоцінних металів. Ця ініціатива є частиною ширшої стратегії британських регуляторів щодо майбутнього токенізації оптових фінансових ринків і має на меті з'ясувати, чи здатна цифровізація підвищити ефективність, ліквідність та конкурентоспроможність лондонського спотового ринку золота – найбільшого у світі – без шкоди для ринкової цілісності та захисту прав споживачів. Автори документа підкреслюють, що завдяки блокчейну фізичне золото, яке традиційно є складним в операційному управлінні активлом, може стати набагато зручнішим інструментом для швидкого поділу, передачі та використання як високоякісного оптового забезпечення у репо, операціях із цінними паперами й деривативами.

Окрему увагу в публікації приділено юридичним, регуляторним та операційним умовам, необхідним для безпечного функціонування токенізованого золота, зокрема критичній важливості сумісності між новими блокчейн-платформами та традиційною ринковою інфраструктурою сховищ, клірингу й розрахунків. Документ детально аналізує виклики, пов'язані з регуляторним периметром, адже класифікація токенів відповідно до правил щодо колективних інвестиційних схем (CIS) та альтернативних фондів (AIF) може суттєво вплинути на їхню привабливість для інституційних і роздрібних інвесторів. У зв'язку з цим FCA розглядає широкий спектр можливих політичних та регуляторних заходів: від надання цільових роз'яснень і методичних рекомендацій щодо кращих практик до запровадження спеціальних винятків або навіть розробки окремого регуляторного режиму у тісній співпраці з Міністерством фінансів Великої Британії (HMT). Збір відгуків та експертних оцінок від учасників ринку та зацікавлених сторін тривав до 23 жовтня 2026 року, а отримані результати послугують основою для формування подальшої політики регулятора.

Окрім оптового сегмента та використання золота як забезпечення, звіт окрему увагу приділяє роздрібним інноваціям, зокрема можливостям фракційного володіння через мобільні додатки. Токенізація дозволяє роздрібним інвесторам купувати й продавати частки золота у зручний час, поза стандартними ринковими годинами, що розширює можливості диверсифікації. Водночас регулятор зазначає, що на відміну від добре налагодженого ринку біржових фондів (ETF), у сфері

[7] https://www.fca.org.uk/publication/call-for-input/tokenised-gold-opportunities-risks-uk-wholesale-markets.pdf

роздрібних токенізованих продуктів спостерігається значна неоднорідність практик розкриття інформації, що створює потенційні ризики для споживачів.

Саме тому регуляторні органи наполягають на мінімальних стандартах захисту, які включають прозорі умови зберігання фізичного золота, наявність страхового покриття, чітко визначені механізми викупу та захист інтересів інвесторів у разі неплатоспроможності емітента чи технологічного провайдера. FCA очікує, що більшість інновацій у цій сфері будуть ініційовані самим ринком, проте держава має встановити чіткі рамки для усунення правової невизначеності й запобігання ризикам фінансових злочинів.

Висновки

Потенціал токенізації як оптового забезпечення: Токенізоване золото здатне поєднати надійність фізичного зберігання з перевагами цифрового переказу, забезпечивши учасникам ринку швидше залучення недовикористаних активів як високоякісного забезпечення.

Необхідність ринкових стандартів та інтероперабельності: Успіх масштабування токенізованого золота залежить від розробки ринкових стандартів безпеки, аудиту, кіберзахисту та забезпечення технічної сумісності між різними розподіленими реєстрами та традиційними сховищами.

Виклики в межах регуляторного периметра (CIS/AIF): Чинні правила щодо колективних інвестиційних схем та альтернативних інвестиційних фондів можуть створювати правову невизначеність для певних структур токенізованого золота, обмежуючи їхній доступ до ринку та інвесторів.

Гнучкість майбутньої регуляторної політики: Британські регулятори (FCA та HMT) розглядають широкий спектр можливих дій – від точкових роз'яснень і цільових винятків до створення окремого регуляторного режиму, який сприятиме інноваціям без зниження стандартів захисту споживачів.

Партнери Росії як інфраструктура обходу санкцій: свідчення Українського центру безпеки та співпраці для британського парламенту [8]

Комітет закордонних справ Палати громад Великої Британії оприлюднив письмові свідчення (RUS0017), подані Українським центром безпеки та співпраці (УЦБС) у межах парламентського розслідування «Russia». Розслідування присвячене двостороннім відносинам Великої Британії з росією та чіткості довгострокового стратегічного підходу до неї, а одним із визначених Комітетом напрямів є міжнародні союзи та стратегічні партнерства з росією. Центральна теза документу полягає в тому, що здатність Росії підтримувати військовий та економічний потенціал безпосередньо залежить від мережі держав-партнерів – Китаю, КНДР, Ірану та Білорусі, – відносини з якими закріплено договорами про всеосяжне стратегічне партнерство, а у випадку Білорусі – договором про Союзну державу. Для кожного партнера автори окремо аналізують політичний, економічний і військово-промисловий виміри, а також стійкість відносин.

Розділ про Китай наголошує на асиметричному характері партнерства, за якого Москва перебуває у структурній залежності від Пекіна. Після 2022 року значну частину російської торгівлі переорієнтовано з Європи на Китай із розрахунками в рублях і юанях, а Банк Росії визнає ключову роль юаня у формуванні резервів на тлі обмеженого доступу до долара та євро. Торгівля сільськогосподарською та промисловою продукцією між двома країнами за перші сім місяців 2026 року зросла на 34,4 %; залізничні перевезення між росією та Китаєм у січні–липні 2026 року збільшилися на 6 % до рекордних 114 млн т, зокрема відвантаження до Китаю зросли на 4,5 % до 99,6 млн т (вугілля, залізна руда, нафтопродукти, добрива), а постачання з Китаю – на 17,5 % до 14,4 млн т. Автори фіксують масштабні поставки продукції подвійного призначення: мікросхем, двигунів для БПЛА, наукового обладнання, верстатів, оптики та сировини для виробництва дронів.

Найбільш деталізованим є кейс, що ґрунтується на власних даних УЦБС. Державну китайську компанію Jilin Chemical Fibre Group автори розглядають як потенційно ключову ланку ланцюга постачання поліакрилонітрильного (ПАН) прекурсора – спеціального хімічного волокна, основної сировини для високоміцного вуглецевого волокна, – до підприємства російського ВПК «Алабуга-Волокно». Встановлено, що «Алабуга-Волокно» з 2022 року оприлюднило щонайменше дев’ять

[8] https://committees.parliament.uk/writtenevidence/168808/html/

тендерів на експедиторські послуги, включно з доставкою, експортним митним оформленням і страхуванням вантажів із КНР; останній зафіксовано 6 червня 2026 року. У восьми з них предметом є поставка ПАН-прекурсора в контейнерах зі складу, адреса якого відповідає адресі Jilin Chemical Fibre Group, а загальний обсяг, передбачений документацією з жовтня 2022 року, становить щонайменше 177 морських контейнерів 40HQ та 51 єврофуру. Підприємство входить до інфраструктури особливої економічної зони «Алабуга» й переробляє сировину на вуглепластикові композити, що використовуються у виробництві БПЛА «Герань» та інших видів озброєння.

Білорусь, за оцінкою авторів, є не периферійним партнером, а складовою військово-політичної інфраструктури росії. Окрім надання території, повітряного простору, полігонів і аеродромів, білоруські підприємства інтегровані в російський ВПК: вони постачають оптико-електронні системи, приціли, компоненти систем керування вогнем, колісні шасі та пускові установки, ремонтують пошкоджену техніку й передають боєприпаси зі своїх складів. Натомість росія допомагає білоруським підприємствам отримувати дефіцитні технологічні товари через непрямі зовнішні канали. Автори окремо наголошують на зростанні ролі Білорусі як промислового та логістичного каналу обходу санкцій.

Щодо КНДР документ констатує, що економічні контакти з росією передусім спрямовані на обхід санкцій: йдеться не про звичайну торгівлю, а про створення каналів переміщення товарів, сировини, пального й фінансів, обмежених резолюціями Ради Безпеки ООН. У 2026 році спостерігалися ознаки відновлення експорту з КНДР вугілля та мінеральної сировини, активізація портової діяльності та спроби приховати походження вантажів. Розпуск Групи експертів ООН, що здійснювала моніторинг санкцій щодо КНДР, після накладення росією вето на продовження її мандата в березні 2024 року не скасував самих санкцій, однак послабив механізм незалежної верифікації й публічного документування порушень. Інфраструктурним маркером поглиблення відносин є будівництво автомобільного мосту через річку Туманну, першого прямого автосполучення між країнами, а військовим, плани передачі Росії щонайменше 120 балістичних ракет і шести пускових установок.

Партнерство з Іраном автори характеризують як прагматичне й інструментальне зближення двох держав під санкціями. У 2022 році набрав чинності договір про науково-технічне співробітництво, а у 2025 році підписано угоду про всеосяжне стратегічне партнерство строком на 20 років, що охоплює оборону, енергетику, фінанси та безпеку. Іран не лише постачав ударні БПЛА, а й допоміг налагодити їхнє виробництво в Татарстані, перетворивши закупівлі на спільний військово-промисловий проєкт. Двостороння торгівля у 2024 році зросла більш ніж на 15 % і продовжувала зростати у 2026 році; сторони запроваджують розрахунки в національних валютах і використовують російську платіжну систему «Мир» для обходу обмежень SWIFT, а також розвивають транспортний коридор «Північ – Південь».

Методологічно документ поєднує відкриті джерела, значною мірою офіційні російські ЗМІ та відомчі публікації, з даними закупівельних агрегаторів і власними напрацюваннями УЦБС. Він не є офіційним рішенням чи доказовим матеріалом, проте пропонує цілісну карту каналів, через які росія компенсує дію санкцій: торгівлю в національних валютах, транзитну залізничну й морську

інфраструктуру, закупівлі через особливі економічні зони, участь підприємств третіх країн у виробничих ланцюгах і приховування походження вантажів. Підсумкова оцінка авторів – формування «альянсу держав під санкціями», у якому війна проти України є центральним, але не єдиним елементом протистояння із Заходом.

Висновки

Відкриті закупівельні дані можуть слугувати джерелом доказів ланцюгів постачання: кейс Jilin Chemical Fibre Group та «Алабуга-Волокно» побудовано на тендерній документації (щонайменше дев'ять тендерів із 2022 року, останній – 6 червня 2026 року), збігу адрес складів і заявлених обсягів (177 контейнерів 40HQ, 51 єврофура). Аналогічне зіставлення тендерів на експедиторські послуги, адрес відправлення та специфікацій товарів може застосовуватися під час перевірки контрагентів у торговельному фінансуванні.

Розрахунки в національних валютах та альтернативна платіжна інфраструктура знижують прозорість потоків: перехід торгівлі з Китаєм на рублі та юані й використання системи «Мир» у розрахунках з Іраном виводять операції за межі доларових і єврових кореспондентських ланцюгів, що звужує можливості західних банків і ПФР відстежувати платежі та підвищує значення аналізу товаросупровідної документації й маршрутів поставок.

Білорусь слід розглядати як виробничий, а не лише логістичний канал обходу санкцій: постачання оптоелектроніки, прицілів, компонентів систем керування вогнем і колісних шасі, а також ремонт техніки означають, що ризик-індикатори мають охоплювати не тільки реекспорт товарів, а й участь білоруських підприємств у виробничих ланцюгах кінцевої продукції.

Послаблення міжнародних механізмів верифікації підвищує вагу незалежних і національних розслідувань: після припинення мандата Групи експертів ООН щодо КНДР документування порушень ускладнилося, а ознаки відновлення експорту вугілля й мінеральної сировини та приховування походження вантажів у 2026 році вимагають від фінансових установ посиленої уваги до морських перевезень, посередників і транзитних юрисдикцій.

Глобальний звіт PwC про регулювання криптоактивів 2027[9]



PwC оприлюднила п'яте видання Глобального звіту про регулювання криптоактивів (Global Crypto Regulation Report 2027) під назвою «Navigating the global landscape». Звіт відображає стан регулювання на жовтень 2026 року і охоплює діяльність міжнародних органів зі встановлення стандартів – FSB, Базельського комітету, FATF і BIS, – окремий розділ про Європейський Союз та профілі 33 юрисдикцій, серед яких і Україна (профіль підготовлено фахівцями PwC Україна). Центральна теза видання полягає в тому, що регулювання криптоактивів вступило в нову фазу: у провідних юрисдикціях фокус змістився з нормотворення на імплементацію, нагляд і правозастосування, а сила регуляторного середовища визначається не кількістю ухвалених правил, а здатністю забезпечити функціонування цифрових фінансів у масштабі.

У передмові запропоновано періодизацію еволюції регулювання. У 2018–2022 роках ключовим було питання визначення того, що таке криптоактив і де проходить межа регуляторного периметра; у 2022–2025 роках – питання посередника, тобто хто може випускати та обслуговувати активи; у 2025–2026 роках – питання режиму: хто здійснює нагляд за системою, а не лише за окремою фірмою. Саме на цьому етапі виявилися межі суб'єктно-орієнтованого нагляду: регулятор може чітко бачити ліцензовану фірму, але не систему, в якій вона працює. На 2027 рік автори ставлять питання архітектури – чи здатні базові механізми фінансової системи (остаточність розрахунків, режим забезпечення, розкриття інформації, транскордонне визнання), розраховані на посередництво, робочі години й національні кордони, працювати в умовах конвергенції цифрових грошей, токенізованих активів і нової ринкової інфраструктури. Ілюстрацією слугує одна операція: частка токенізованого фонду, передана в забезпечення на ніч і розрахована стейблкоїном у неділю між контрагентами з двох юрисдикцій, – кожен її елемент десь урегульований, але чи спрацює операція в цілому, залишається відкритим питанням.

З цієї логіки випливає ключове застереження звіту. Прогалини в регулюванні рідко є прогалинами в охопленні: вони виникають там, де цифрові активи функціонують лише завдяки тому, що щось «вимкнено», обійдено чи мовчазно допущено, – пілотні режими, які не застосовують чинні правила, токени, що лише дзеркалять традиційний реєстр, наглядові позиції, які тримаються, поки обсяги малі. Автори називають це «пристосуваннями, а не архітектурою» і прогнозують, що вони навряд чи витримають масштабування. Звідси практична рекомендація для фірм: визначити, де саме таке пристосування несе навантаження, і що станеться в день його скасування. Серед восьми трендів 2027 року звіт виокремлює розвиток цифрових і токенізованих

[9] https://www.pwc.de/de/unterlagen/pwc-global-crypto-regulation-report-2027.pdf

грошей у ширшу ринкову архітектуру, посилену увагу до інфраструктури фінансового ринку, зростання ролі транскордонної сумісності, розбіжності моделей токенізованих акцій, перетворення нагляду та правозастосування на мірило регуляторної зрілості, інституційну участь, автономну фінансову діяльність (DeFi, смарт-контракти, агенти на основі AI), де регуляторам доведеться визначати відповідальність між розробниками, механізмами управління, постачальниками інфраструктури та автоматизованими системами, а також безстрокові деривативи на традиційні активи, що забезпечують цілодобову торгівлю з кредитним плечем без володіння базовим активом.

У частині міжнародних стандартів звіт спирається на сьоме цільове оновлення FATF щодо віртуальних активів (липень 2026 року): частка опитаних юрисдикцій, що ухвалили законодавство про Travel Rule, зросла з 73 % у 2025 році до 83 %, ще 11 юрисдикцій повідомили про імплементацію, що триває. Водночас FATF констатує, що законодавчий прогрес не завжди перетворюється на ефективне впровадження: суттєві прогалини зберігаються в операціоналізації ліцензування та реєстрації, у виявленні осіб, які фактично надають послуги VASP, і в застосуванні ризик-орієнтованого нагляду та санкцій. FATF також наголошує на зростанні ризиків, пов'язаних зі стейблкоїнами, нехостинговими гаманцями, офшорними VASP і децентралізованими фінансами, а в окремому звіті щодо DeFi рекомендує функціональний ризик-орієнтований підхід до визначення того, де існує контроль. FSB у жовтні 2026 року оприлюднила аналіз транскордонних уразливостей глобальних стейблкоїнів і прогалин у даних для моніторингу фінансової стабільності, не змінюючи своєї рамки 2023 року, а Базельський комітет, стандарт якого щодо криптоактивних експозицій банків набрав чинності в січні 2026 року, проводить прискорений цільовий перегляд з очікуваним оновленням до кінця 2026 року.

Розділ про ЄС описує регуляторну рамку як взаємопов'язану архітектуру. Регламент MiCAR застосовується в повному обсязі з 30 грудня 2024 року і проходить перший формальний перегляд: цільова консультація Європейської комісії, завершена 30 вересня 2026 року, охоплювала периметр, токени, прив'язані до активів, токени електронних грошей, вимоги до CASP, поведінку на ринку, DeFi, стейкінг, кредитування криптоактивами, NFT, ринки прогнозів, безстрокові продукти та взаємодію з токенізованими традиційними активами; звіт Комісії за статтею 140 MiCAR має бути підготовлений до 30 червня 2027 року і може супроводжуватися законодавчими пропозиціями. Пакет з інтеграції ринків і нагляду (MISP), представлений у грудні 2025 року, передбачає можливий прямий нагляд ESMA за CASP і підвищення ліміту пілотного режиму DLT з 6 до 100 млрд євро (порогу переходу – з 9 до 150 млрд євро); позиція Ради ЄС, погоджена в жовтні 2026 року, передбачає негайну передачу ESMA нагляду за найбільш значущими транскордонними CASP. У сфері операційної стійкості ESMA з другого півріччя 2026 року до першого півріччя 2027 року проводить спільну наглядову дію щодо зберігання активів CASP, управління ключами, контролю транзакцій і ризиків смарт-контрактів.

Для сфери ПВК/ФТ найважливішими є три дати. Регламент AMLR застосовуватиметься з 10 липня 2027 року і додатково гармонізує вимоги, зокрема щодо CASP і операцій із самостійно розміщеними адресами. Протягом 2027 року AMLA обере суб'єктів для першої групи прямого нагляду, що розпочнеться у 2028 році. Директива DAC8 застосовується з 1 січня 2026 року:

перший цикл звітування охоплює операції 2026 року, а подання та обмін даними відбудуться у 2027 році. Автори підкреслюють, що фірми мають враховувати не лише вимоги MiCAR до авторизації та поведінки на ринку, а й операційну стійкість, залежність від третіх сторін, контроль фінансових злочинів і податкову прозорість одночасно. Серед інших юрисдикцій звіт фіксує набрання чинності в січні 2027 року рамкою GENIUS Act у США (резерви високоліквідними активами у співвідношенні 1:1, щомісячне розкриття, стандарти ПВК і санкційного контролю, відсутність страхування депозитів) і перехід Великої Британії від реєстрації криптофірм за Регламентом про відмивання коштів до повної авторизації FCA з 25 жовтня 2027 року, із закриттям вікна для заяв у перехідному періоді 28 лютого 2027 року.

Зведена таблиця регуляторного статусу показує, що в більшості охоплених юрисдикцій режими ліцензування, регулювання стейблкоїнів і Travel Rule уже діють. Україна – єдина юрисдикція, у якій усі три параметри мають статус «проєкт правил» (Саудівська Аравія діяльність із криптоактивами забороняє). Профіль України пояснює причини: Закон «Про віртуальні активи» № 2074-IX від 17 лютого 2022 року набере чинності лише після внесення змін до Податкового кодексу щодо оподаткування віртуальних активів, які станом на жовтень 2026 року не ухвалено. Законопроєкт № 10225-д, прийнятий за основу у вересні 2025 року, станом на жовтень 2026 року очікує другого читання, хоча профільний комітет заявляв про його ухвалення в серпні 2026 року; альтернативних законопроєктів не зареєстровано.

Закон № 2074-IX визначає класифікацію віртуальних активів на незабезпечені та забезпечені, зокрема забезпечені валютними цінностями й забезпечені цінними паперами чи похідними фінансовими інструментами, запроваджує ліцензування постачальників послуг і розподіляє регуляторні повноваження між НБУ (віртуальні активи, забезпечені валютними цінностями) та НКЦПФР (інші категорії). PwC підкреслює, що постачальники послуг, пов'язаних з обігом віртуальних активів, уже мають окремі обов'язки у сфері фінансового моніторингу, однак повноцінний ліцензійний і пруденційний режим не функціонує. Законопроєкт № 10225-д має створити наглядову рамку, узгоджену з MiCAR: мінімальні вимоги до капіталу та ліквідності, прозора структура власності, ділова репутація керівництва, ефективний внутрішній контроль, відокремлення активів клієнтів, розкриття ризиків через «білі книги», заборона маніпулювання ринком, а також обмеження використання стейблкоїнів як засобу платежу за товари й послуги; віртуальні активи не матимуть статусу законного платіжного засобу.

Щодо цифрових грошей і токенізації звіт констатує, що запровадження е-гривні у 2027 році залишається невизначеним через війну: НБУ продовжує дослідження й підготовку пілотного проєкту, а повне розгортання залежить від припинення бойових дій і стабілізації економіки. Окремої законодавчої рамки для токенізованих фінансів в Україні немає; НКЦПФР планує до кінця 2026 року подати законопроєкт про технологію розподіленого реєстру, що має уможливити торгівлю акціями, цінними паперами й віртуальними активами через спрощену систему як альтернативу депозитарній моделі. Автори пов'язують темпи подальшого розвитку ринку з прогресом законодавчого процесу та безпековою й економічною ситуацією.

Висновки

Розрив між законом і практикою стає головним фокусом FATF: попри зростання частки юрисдикцій із законодавством про Travel Rule до 83 %, FATF фіксує прогалини в операціоналізації ліцензування, виявленні осіб, що фактично надають послуги VASP, і ризик-орієнтованому нагляді. Для України, де постачальники послуг, пов'язаних з обігом віртуальних активів, уже мають окремі обов'язки з фінансового моніторингу, але ліцензійний режим не запрацював, саме виявлення нелегальних і офшорних провайдерів залишатиметься предметом міжнародного оцінювання.

Україна – єдина з охоплених юрисдикцій зі статусом «проєкт правил» за всіма трьома ключовими параметрами: ліцензування, регулювання стейблкоїнів і Travel Rule. Відкладене друге читання законопроєкту № 10225-д і залежність набрання чинності Законом № 2074-IX від змін до Податкового кодексу відсувають створення наглядової інфраструктури, тоді як інші юрисдикції вже переходять до етапу нагляду та правозастосування.

Наближення до права ЄС має орієнтуватися не лише на MiCAR, а й на AMLR та DAC8: з 10 липня 2027 року AMLR застосовуватиметься до операцій із самостійно розміщеними адресами, у 2027 році AMLA обере перших суб'єктів прямого нагляду, а DAC8 запускає перший цикл обміну податковою інформацією про криптоактиви. Українські провайдери, що обслуговують клієнтів з ЄС, стикатимуться з цими вимогами через контрагентів незалежно від темпів національного законодавства.

Тимчасові регуляторні «пристосування» створюють відкладені ризики: PwC застерігає, що пілотні режими, винятки та толерантні наглядові позиції, які працюють за малих обсягів, навряд чи витримають масштабування. Під час формування національного режиму це актуалізує завчасне визначення відповідальних осіб у DeFi-структурах і за операції автономних агентів, а не покладання на винятки з загальних правил.

Від правил до результатів: європейські професійні асоціації закликають AMLA переглянути проєкти технічних стандартів для нефінансових професій [10]

20 жовтня 2026 року асоціації, що представляють європейських бухгалтерів, аудиторів, юристів і податкових консультантів, оприлюднили спільну позицію «From rules to results: 6 priorities for effective EU AML implementation» (документ, зокрема, поширено Accountancy Europe та Європейською федерацією податкових консультантів ETAF). Підписанти підтримують мету ЄС посилити боротьбу з відмиванням коштів і фінансуванням тероризму, створення AMLA та єдиного зводу правил, наголошуючи, що їхні професії завдяки знанню клієнтів і бізнесу відіграють важливу роль у виявленні незвичної поведінки та повідомленні про підозри. Відправною точкою документа є виступ єврокомісарки Марії Луїш Албукерке на інавгураційній конференції AMLA в червні 2026 року із закликом до справді ризик-орієнтованої системи з простішим, розумнішим і пропорційнішим регулюванням і наглядом, а також до розуміння того, що нове законодавство є лише початком, а справжнім випробуванням стане імплементація.

Основний аргумент асоціацій полягає в тому, що проєкти регуляторних технічних стандартів (RTS) AMLA через надмірну деталізацію зосереджуються на процесах відповідності, документуванні й зборі даних, а не на ефективному ризик-орієнтованому контролі, тобто забезпечують «паперовий слід» відповідності замість реального запобігання й виявлення. Автори висловлюють юридичні застереження: на їхню думку, нова рамка може суперечити намірам законодавців ЄС, закладеним у пакеті AML, і цілям Комісії щодо конкурентоспроможності, пропорційності, скорочення надмірного адміністративного навантаження та принципу «спершу думай про малих». Водночас вони прямо зазначають, що йдеться не про зниження стандартів, а про те, щоб вони працювали, і що проєкти RTS можна змінити, не виходячи за межі мандата, встановленого актами першого рівня.

Перший пріоритет – «більше даних не означає кращої протидії відмиванню коштів». Там, де акти першого рівня залишають простір для вибору, AMLA, за спостереженням асоціацій, систематично додає деталізацію, обсяг даних, вимоги до документування та приписи, що формує дедалі жорсткішу рамку і залишає менше простору для концентрації на реальних ризиках. Великий обсяг інформації без чіткої ризикової мети створює «стіг сіна», в якому губиться «голка» – особи, що становлять реальну загрозу, – і відволікає ресурси як практиків, так і наглядових органів, включно із саморегулівними організаціями. Пропонований тест для кожної нової вимоги: як саме вона допоможе запобігти фінансовому злочину чи виявити його. Другий пріоритет

[10] https://etaf.tax/wp-content/uploads/2026/10/2610191.pdf

стосується малих фірм: більшість суб'єктів нефінансового сектору – невеликі практики, значна частина – одноосібні фахівці без комплаєнс-підрозділів і технологічних систем великих установ. Автори підкреслюють, що «малий не означає низькоризиковий», однак кумулятивне навантаження може зробити такі практики економічно нежиттєздатними, не підвищивши здатності Європи виявляти фінансові злочини.

Третій пріоритет – не прирівнювати нефінансові професії до банків. Бухгалтери, аудитори, юристи й податкові консультанти не ведуть рахунків клієнтів, не здійснюють платежів і, як правило, не управляють коштами клієнтів; вони не мають доступу до транзакцій у момент їх здійснення, а отже, не можуть запобігти їх проведенню, і часто бачать лише частину операції, тоді як банк, зокрема через кореспондентські відносини, має значно ширшу картину. Основними чинниками ризику для цих професій є клієнтська база та характер послуг, а не транзакційна діяльність, тому рамка має спиратися на ризики, пов'язані з клієнтом, послугою, метою та обставинами залучення, а не відтворювати банківську модель комплаєнсу. Єдиний звід правил, на думку авторів, має прагнути спільних результатів, а не однакових процесів для секторів із принципово різними бізнес-моделями; для цього AMLA потребує достатньої експертизи щодо нефінансового сектору.

Четвертий пріоритет – операційна здійсненність. Асоціації вважають, що низка проєктів RTS є щонайменше надмірно складною, а в гіршому разі юридично неможливою до виконання. Прикладом є RTS щодо групових вимог: стаття 16(4) AMLR доручає AMLA визначити мінімальні вимоги до групових політик і контролю та умови їх застосування до мереж і партнерств, а преамбула (пункт 45) закликає уникати надмірного навантаження й враховувати пропорційність. Проте багато професійних мереж складаються з юридично незалежних фірм без материнської структури, здатної встановлювати й забезпечувати виконання вимог ПВК у мережі. Автори визнають, що AMLA врахувала частину зауважень в останній редакції, поданій Комісії, однак вплив на мережі залишається значним. Вони закликають до реалістичних строків імплементації та такого підходу нагляду на початковому етапі, за якого увага зосереджується на підтримці, роз'ясненнях і вирішенні практичних труднощів, а не на негайному застосуванні санкцій до фірм, що добросовісно намагаються виконати вимоги. Подібні зауваження стосуються RTS щодо оцінки ризиків нефінансових професій: асоціації пропонують зосередитися на інформації, яка справді допомагає наглядовим органам ідентифікувати ризики, допускати рідші переоцінки за обґрунтованих підстав і спрощені вимоги для фірм із нижчим ризиком, а також спиратися на національну наглядову експертизу.

П'ятий пріоритет – збереження професійного судження: детальні процеси та документування можуть підтримувати послідовність нагляду, але не мають замінювати судження, необхідне для виявлення незвичної поведінки, інакше ризик-орієнтований підхід перетворюється на формалістичне «проставлення галочок». Шостий пріоритет формулює чотири принципи для наступного етапу: зосередженість на ризику, за якої кожна вимога має доводити свій внесок у запобігання, виявлення чи пом'якшення фінансових злочинів; секторальна специфіка; практична, а не декларативна пропорційність; збереження професійного судження там, де воно додає цінності. У заключній частині автори зауважують, що інші провідні фінансові юрисдикції

переглядають законодавство з орієнтацією на ефективність, тоді як RTS ризикують спрямувати ЄС до дороговартісної системи відповідності, і пропонують вимірювати успіх тим, чи стала Європа краще виявляти й зупиняти фінансові злочини, а не обсягом наданої інформації.

Документ має характер позиції зацікавлених професійних спільнот і не містить кількісної оцінки навантаження чи ефективності, однак він чітко окреслює ключову суперечність етапу імплементації пакета ЄС 2024 року – між гармонізацією через детальні технічні стандарти та пропорційністю для різнорідних секторів. Від того, як AMLA і Комісія збалансують ці підходи, залежатиме практичний зміст обов'язків нефінансових професій у всьому ЄС.

Висновки

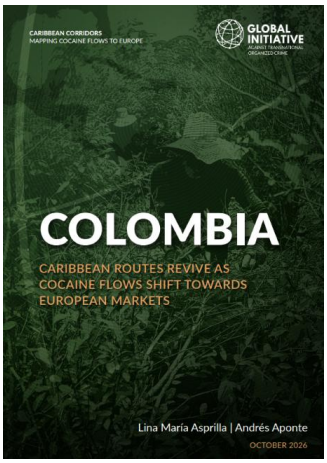
Технічні стандарти AMLA визначатимуть практичний зміст вимог до нефінансових професій: саме RTS щодо групових політик і оцінки ризиків перетворюють норми AMLR на конкретні процедури. Для України, яка наближає законодавство до пакета ЄС 2024 року, дискусія про ступінь їх деталізації має практичне значення, оскільки ухвалені Комісією стандарти стануть частиною acquis, що підлягає імплементації.

Ризик-орієнтований підхід для бухгалтерів, аудиторів, юристів і податкових консультантів має будуватися на інших чинниках, ніж для банків: ключовими є клієнтська база, характер послуги та обставини залучення, а не транзакційний моніторинг, до якого ці професії, як правило, не мають доступу в момент здійснення операції. Перенесення банківських моделей контролю створює формальні обов'язки без відповідного ефекту для виявлення ризиків.

Пропорційність має бути закладена безпосередньо у вимоги: для невеликих практик і одноосібних фахівців асоціації пропонують рідші переоцінки ризику за обґрунтованих підстав і спрощені вимоги для суб'єктів із нижчим ризиком; без цього кумулятивне навантаження може витіснити дрібних учасників із ринку, не покращивши виявлення фінансових злочинів.

Перехідний період потребує наглядової підтримки, а не лише санкцій: на початковому етапі впровадження нагляд, на думку асоціацій, має зосереджуватися на роз'ясненнях і усуненні практичних труднощів, а для мереж юридично незалежних фірм – враховувати реальну здатність забезпечувати виконання групових правил, як того вимагають стаття 16(4) і пункт 45 преамбули AMLR.

Транзитні коридори Карибського басейну: відродження колумбійських маршрутів та їхній вплив на європейський ринок [11]



Аналітичний звіт, підготовлений експертами Глобальної ініціативи проти транснаціональної організованої злочинності (GI-TOC), досліджує масштабне відродження та трансформацію карибських маршрутів постачання кокаїну з Колумбії до європейських ринків, які останніми роками перетворилися на критично важливий вузол у глобальних ланцюгах постачання наркотиків. Автори детально аналізують основні виробничі анклави в Колумбії (зокрема регіони Кататумбо, Сур-де-Болівар, Бахо-Каука та Путумайо), де попри десятиліття боротьби з наркотиками обсяги посівів коки та потенційне виробництво кокаїну продовжують неухильно зростати через економічну маргіналізацію місцевих громад. У документі докладно описано внутрішні сухопутні, річкові й повітряні маршрути транспортування, а також методи контрабанди через комерційні, приватні та альтернативні порти узбережжя Карибського моря, які активно використовуються кримінальними мережами для обходу державних перевірок і стабільного переправлення вантажів.

Особливу увагу у звіті приділено ролі домінуючих озброєних угруповань, насамперед Армії гайтаністів Колумбії (EGC або «Клан дель Гольфо») та Армії національного визволення (ELN), які здійснюють жорсткий територіальний контроль над ланцюгами виробництва та тісно співпрацюють із транснаціональними синдикатами, включаючи балканські картелі й італійські мафіозні клани («Ндрангета», Каморра і Коза Ностра). Через посилення контролю на кордонах США та стрімке зростання попиту в Європі, де споживання кокаїну за останнє десятиліття значно збільшилося, наркотрафік переорієнтувався на карибський напрямок. У результаті цього такі країни і території, як Венесуела, Домініканська Республіка, Панама та Малі Антильські острови, набули ключового значення як транзитні хаби та центри логістичного перерозподілу вантажів перед їхнім фінальним відправленням до європейських портів.

Додатково у звіті розглядається еволюція державної політики та наслідки політичних змін у Колумбії, зокрема перехід адміністрації колишнього президента Густаво Петро від рутинного знищення посівів до тактики масштабних морських і сухопутних перехоплень, а також можливі наслідки приходу до влади нового уряду Абелардо де ла Еспрієльї, який задекларував жорсткіший силовий курс у межах боротьби з наркотиками. Автори наголошують, що попри встановлення історичних рекордів за обсягами вилученого кокаїну, силові методи не здатні кардинально переломити ситуацію, оскільки темпи зростання виробництва значно

[11] https://globalinitiative.net/wp-content/uploads/2026/09/Lina-Maria-Asprilla-and-Andres-Aponte-Colombia-Caribbean-routes-revive-as-cocaine-flows-shift-towards-European-markets-GI-TOC-October-2026.pdf

випереджають можливості перехоплення з боку держави. Це вимагає перегляду стратегій та акценту на послабленні кримінального управління територіями, а не лише на кількості конфіскованих партій.

Окрім геополітичних та логістичних аспектів, звіт глибоко занурюється у соціально-економічні виміри проблеми, підкреслюючи надзвичайну вразливість прибережних і прикордонних громад. У регіонах із високим рівнем бідності, безробіття та слабкою присутністю державних інституцій (зокрема серед корінного населення ваюу в Ла-Гуахірі) участь у логістиці наркотрафіку – чи то через будівництво катерів, чи то через управління швидкохідними човнами – стала для багатьох мешканців єдиною стратегією економічного виживання та соціальної мобільності. Водночас ця діяльність несе руйнівні наслідки для місцевого соціуму, призводячи до високого рівня насильства, зникнень і масових арештів за кордоном. На завершення автори пропонують комплексні рекомендації для урядів і Європейського Союзу, наголошуючи, що політика виключно силової інтердикції є неефективною без усунення глибинних структурних причин і трансформації економічних умов у регіонах виробництва.

Висновки

Відродження карибських коридорів: Карибський регіон Колумбії знову став стратегічним транзитним вузлом для масштабного переправлення кокаїну до Європи через насичення ринку США та зміцнення там контролю.

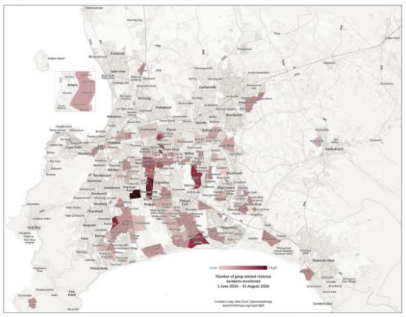
Зростання ролі регіональних хабів: Венесуела, Домініканська Республіка та Малі Антильські острови відіграють ключову роль у зберіганні, перерозподілі та подальшому транспортуванні наркотиків до європейських портів.

Гібридні кримінальні мережі та транснаціональна мафія: Контроль над ланцюгами постачання здійснюється потужними місцевими збройними структурами (наприклад, EGC) у тісній кооперації з балканськими та італійськими організованими злочинними угрупованнями.

Обмежена ефективність політики заборон: Незважаючи на рекордні показники національних конфіскацій та вилучень, стрімке зростання потенціалу виробництва кокаїну в Колумбії зводить нанівець результати виключно силових методів боротьби без усунення глибинних соціально-економічних причин.

Як військові операції та експансія банд формують нову кримінальну реальність ПАР [12]





Звіт GI-TOC змальовує тривожну та багатогранну картину кримінального ландшафту Західнокапської Провінції Південно-Африканської Республіки, яка перебуває у стані перманентної турбулентності. Аналіз квартальних даних свідчить про те, що бандитські угруповання не лише зберігають, а й розширюють свій вплив, адаптуючись до нових умов, зокрема до присутності армії, та використовуючи системні вади правоохоронної та пенітенціарної систем.

Однією з центральних подій кварталу стало розчарування громад після шести місяців військової операції «Проспер» (Operation Prosper), розгорнутої на Кейп-Флетс з 1 квітня 2026 року. Якщо на початку мешканці сподівалися на припинення хвилі насильства, то станом на жовтень ейфорія змінилася глибоким розчаруванням. Свідчення мешканців, активістів та самих членів угруповань вказують на те, що солдати не лише не припинили стрілянину, а й часто поводяться агресивно, вдаючись до невмотивованих обшуків та побиття молоді. Це створило небезпечний вакуум довіри до держави.

Бандитські лідери, своєю чергою, вправно маніпулюють цим невдоволенням, позиціонуючи себе як «захисників» та «годувальників» громад. Один із ватажків у Мітчеллс-Плейн, наприклад, заявив, що щотижня витрачає 10 000 рандів на їжу, ліки та електрику для місцевих жителів, що дозволяє йому купувати лояльність і мовчання. Таким чином, неефективність армії не лише не вирішує проблему, а й підриває авторитет держави, підживлюючи паралельне кримінальне управління. Статистика вбивств у гарячих точках, як-от Філіппі, де кількість убивств зросла з 4 у березні до 11 у червні, підтверджує, що короткострокові військові кампанії не здатні подолати циклічну природу бандитського насильства, яке живиться суперечками за території та ринки збуту наркотиків. Аналітики наголошують, що армія має діяти в тандемі з поліцією, забезпечуючи безпеку для проведення глибоких розслідувань, а не підміняти собою спеціалізовану кримінальну поліцію.

Ще одним критичним виміром проблеми є перетворення в'язниць на справжні оперативні штаби організованої злочинності. Виступаючи на Комісії Мадланги у вересні 2026 року, Національний комісар виправних служб Макготі Тобакгале визнав, що пенітенціарні установи стали базою для координації злочинної діяльності. Незважаючи на заборону, мобільні телефони, які масово проносять у в'язниці (лише під час операції «Вала» вилучено 1010 пристроїв), дозволяють

[12] https://globalinitiative.net/wp-content/uploads/2026/10/WC-gang-monitor-no-10-GI-TOC-October-2026.pdf

ув'язненим лідерам, таким як Джордж «Гевельд» Томас (відомий як «Лорд»), керувати вуличними бандами, замовляти вбивства свідків та координувати постачання наркотиків.

Більше того, в'язниця функціонує як окремий ринок збуту: ціни на наркотики там значно вищі, ніж на волі, що стимулює контрабанду. Слідчі встановили, що цей процес, відомий як «стимела» (поїзд), передбачає не лише переміщення контрабанди, а й навмисне ув'язнення членів банд для зустрічей з лідерами та отримання вказівок. Система функціонує завдяки корупції серед наглядачів: лише за один фінансовий рік 137 співробітників були викриті в контрабанді. Експерти закликають перейняти італійський досвід ізоляції мафіозних босів, але застерігають, що без подолання корупції серед персоналу будь-які реформи будуть марними.

Тривожною тенденцією є експансія бандитських угруповань за межі у менші міста, що яскраво ілюструє кейс Малмсбері. Це сільськогосподарське містечко, розташоване на стратегічній трасі N7, стало ареною жорстокої війни між бандами «Американс» та «Монгрелс» після вбивства ватажка останніх на прізвисько «Фрог» у червні 2026 року. У відповідь на це в липні стався масовий розстріл, внаслідок якого загинули двоє людей, а восьмеро отримали поранення, включаючи однорічну дитину. Причини цієї експансії криються у перенасиченні ринку Кейп-Флетс та пошуку нових, менш конкурентних ніш для збуту наркотиків. Малмсбері також виконує роль транзитного вузла для зберігання кокаїну, що надходить через порти, та слугує місцем для розміщення лабораторій з виробництва мандраксу. Слабший поліцейський нагляд та менша конкуренція роблять такі містечка привабливими для угруповань, які витісняються з мегаполісу.

Водночас у Малмсбері спостерігається зростання «кримінального управління»: місцеві кримінальні авторитети, часто пов'язані з тюремними бандами, займаються філантропією, спонсорують спорт та допомагають бідним, що дозволяє їм вербувати дітей (зокрема, з'явилася банда «Sesde Straat se Kinders», до якої входять діти 11-14 років) та отримувати підтримку громади.

Завершальним акордом звіту є висвітлення судового процесу над фігурантами справи про постачання зброї бандам, яка тягнеться з 2015 року. Колишній полковник поліції Крістіан Прінслу, засуджений за незаконну передачу тисяч одиниць зброї, у вересні 2026 року постав перед судом як свідок у справі проти колекціонера Алана Рейвса та ресторатора Іршаада Лахера. Справа, яку називають найстарішою у списку Вищого суду, розкриває масштаби державної зради: Прінслу та його спільник Девід Найду викрадали зброю з поліцейських сховищ і продавали її бандам на Кейп-Флетс. Хоча офіційно йдеться про 2400 одиниць, реальна кількість може сягати 9000. За даними Gun Free SA, зброя з цієї партії була пов'язана з 1066 вбивствами, серед яких 89 дітей. Цей процес не лише підкреслює глибоку корупцію в правоохоронних органах, а й ставить питання про спроможність судової системи ефективно розслідувати складні мережі, адже розгляд справи затягнувся на десятиліття, а багато фігурантів уникають відповідальності.

Підсумовуючи, звіт демонструє, що кримінальний ландшафт Західнокапської Провівнції є надзвичайно стійким та адаптивним. Незважаючи на військові операції та судові переслідування, банди продовжують функціонувати завдяки корупції, здатності керувати процесами з-за ґрат та експансії на нові території. Ефективна протидія вимагає не лише силових методів, а й

комплексного підходу: реформування пенітенціарної системи, посилення місцевих громад, боротьби з вербуванням дітей та подолання системної корупції в державних структурах, які продовжують «живити» вуличні угруповання зброєю та наркотиками.

Висновки

Військова неефективність підриває довіру до держави. Операція «Проспер» не зупинила насильства, а агресія солдатів щодо цивільного населення змушує громади сприймати бандитів як «захисників», що посилює паралельне кримінальне управління.

В'язниці перетворилися на командні центри. Ув'язнені лідери за допомогою телефонів керують вуличними бандами, замовляють убивства свідків та контролюють внутрішній наркоринок, що функціонує завдяки корупції серед наглядачів.

Банди виходять за межі мегаполісів. Перенасичення ринку на Кейп-Флетс штовхає угруповання до малих міст, де слабший поліцейський нагляд, вищі прибутки та можливість вербувати дітей через «благодійність» кримінальних авторитетів.

Державна зброя досі живить вуличне насильство. Справа полковника Прінслу демонструє системну корупцію: тисячі одиниць зброї з поліцейських арсеналів потрапили до банд і досі пов'язані з сотнями вбивств, а судові процеси затягуються на десятиліття.

Сирійський нарко-ринок після падіння режиму Асада [13]

Протягом понад десятиліття Сирія перебувала в епіцентрі глобальної торгівлі каптагоном – подібним до амфетаміну стимулятором, який дешево виробляти, легко транспортувати й на який існує високий попит у країнах Перської затоки.

Цей ринок не просто толерувався режимом Асада, а був глибоко вбудований у політичні та економічні структури, що оточували сирійську державу. Торгівля каптагоном широко розглядається як одне з ключових джерел фінансування державного бюджету Сирії та воєнної економіки протягом років конфлікту й санкцій. Кілька впливових членів родини Асада були піддані санкціям західними урядами за ймовірну причетність до цієї діяльності, зокрема Махер аль-Асад, молодший брат колишнього президента Башара аль-Асада. У період між 2019 і 2025 роками Сирія визначалася як країна походження у 80% випадків вилучення каптагону, зафіксованих по всьому регіону. По суті, каптагон перетворився на кримінальний ринок, що забезпечував джерело твердої валюти в умовах санкцій і слугував розмінною монетою в стосунках Сирії з сусідніми державами.

Коли уряд Асада пав у грудні 2024 року, увага швидко звернулася до майбутнього цієї торгівлі. Понад рік потому ситуація стає дедалі зрозумілішою, і вона виявляється складнішою, ніж простий наратив про шок пропозиції. Протягом трьох видань Глобальний індекс організованої злочинності послідовно документував позицію Сирії в центрі регіональної нелегальної економіки каптагону. Видання 2025 року, яке відображає умови до кінця 2024 року, пропонує останній знімок ситуації перед падінням режиму Асада. У кожному виданні Індексу оцінка Сирії за торгівлею синтетичними наркотиками, яка відстежує каптагон, залишалася на рівні або близько до максимуму: 9,50 у 2021 році, 10 у 2023 році та 9,50 у 2025 році. Стабільне перебування країни на вершині шкали є ознакою ринку, що керується зсередини самої держави.

Торгівля каптагоном ніколи не обмежувалася кордонами Сирії, і Індекс зафіксував її зростаючий вплив по всьому регіону. Оцінки торгівлі синтетичними наркотиками в Йорданії, Туреччині, Лівані та Іраку неухильно зростали з 2021 року, тоді як Саудівська Аравія та Іран, який сам по собі є давнім паралельним хабом, також зафіксували зростання за цей період. Загалом середня оцінка торгівлі синтетичними наркотиками в 14 країнах Західної Азії зросла з 6,71 у 2021 році до 7,54 у 2025 році, що зробило синтетичні наркотики третім за поширеністю кримінальним ринком регіону станом на 2025 рік, поступаючись лише фінансовим злочинам (7,89) та торгівлі людьми

[13] https://globalinitiative.net/analysis/captagon-syria-western-asia/

(7,82). Ринки синтетичних наркотиків розширилися по всій Західній Азії між 2021 і 2025 роками, що відображає зростаючу регіоналізацію виробничих і торговельних мереж.

Перехідна влада Сирії під керівництвом тимчасового президента Ахмеда аль-Шараа швидко вжила заходів проти торгівлі каптагоном у рамках ширших зусиль із відновлення міжнародних зв'язків, що сприяло пом'якшенню деяких міжнародних обмежень. До середини 2025 року Сполучені Штати, Європейський Союз і Велика Британія вжили заходів щодо внесення змін до своїх санкцій проти Сирії або їх скасування.

Через рік після завершення правління Асада Управління ООН з наркотиків і злочинності повідомило, що великомасштабне виробництво всередині країни було порушено, і що ці зусилля суттєво змінили регіональний ринок. Масштаб кампанії був значним: згідно з даними УНЗ ООН, у 2025 році було демонтовано 16 промислових лабораторій і 15 менших складських приміщень. Також посилилася регіональна співпраця проти виробництва й торгівлі каптагоном, зокрема через обмін розвідувальними даними та скоординовані дії. Щонайменше 177 мільйонів таблеток – приблизно 30 тонн – було перехоплено по всьому арабському регіону за рік з грудня 2024 року, причому кілька найбільших вилучень стали результатом спільних операцій. Самі сирійські органи влади наводять ще вищу цифру – близько 365 мільйонів пігулок. УНЗ ООН також відзначило ознаки дефіциту каптагону на деяких ринках призначення, а також зростання цін у частинах Перської затоки та країнах, що межують із Сирією.

Незважаючи на ці досягнення, наркотик не зник. До грудня 2024 року виробництво могло сягати кількох мільйонів пігулок на день, і існуючі запаси могли підтримувати регіональне постачання протягом років. Менш масштабне виробництво також, ймовірно, збережеться всередині Сирії та в сусідніх країнах, а торговці пристосувалися, змінюючи маршрути й використовуючи повітряні кулі та дрони для транспортування пігулок через сухопутні кордони. Одним із найясніших свідчень переміщення торгівлі є південь Сирії. Провінція Сувейда з переважно друзьким населенням значною мірою залишалася поза контролем Дамаска, і після того, як домінуюча збройна фракція консолідувала свою владу в липні 2025 року, вона стала головним центром виробництва й розподілу каптагону. Повідомляється, що торгівля з Сувейди в напрямку Йорданії різко зросла – на понад 325% – після липневого захоплення. Йорданія перехопила 21 спробу наркоторгівлі між січнем і липнем 2025 року та 128 між липнем 2025 року й квітнем 2026 року. Останні повідомлення вказують на те, що тиск на йорданські кордони продовжувався: органи влади зафіксували 231 спробу контрабанди протягом першої половини 2026 року.

Ліван є ще одним ключовим вузлом у цьому трансформованому ландшафті. Вилучення каптагону в Сирії неодноразово простежувалися до Лівану, де залишки мереж режиму Асада та пов'язані з «Хезболлою» суб'єкти продовжують діяти. Ця динаміка була виявлена задовго до падіння режиму, але з того часу стала більш помітною. За шість місяців до квітня 2026 року сирійська влада перехопила майже 33 мільйони пігулок, що надходили з Лівану, що становить близько 77% їхніх загальних вилучень за цей період. Далі на південь у Ємені з'явилося виробництво, пов'язане з хуситами, яке орієнтується на той самий саудівський споживчий ринок, що колись підтримував сирійську торгівлю.

Порушення також може змінювати моделі споживання синтетичних наркотиків. УНЗ ООН повідомило, що торговці використовують глобальну нестабільність для диверсифікації ринків наркотиків і просування на нові ринки. Після скорочення каптагону ціна пігулки в Лівані більш ніж подвоїлася – з 2–3 доларів США до 5–7. Обмеження постачання також збіглися зі зростанням споживання метамфетаміну по всій Західній Азії. Вважається, що метамфетамін укорінився серед колишніх споживачів каптагону в Саудівській Аравії, де він тепер входить до трьох найбільш вживаних речовин країни. Він також став основним наркотиком і пов'язується зі зростанням передозувань у країнах Перської затоки. Більшість метамфетаміну, що споживається в регіоні, виробляється далі на схід і транспортується через Іран. Але він поділяє хімічний прекурсор із каптагоном, а це означає, що ті самі потужності можуть виробляти обидва наркотики. У вересні 2025 року під час рейду на промислову лабораторію в Аль-Махрі (Ємен) було виявлено, що обидва наркотики виробляються пліч-о-пліч, що свідчить про те, що деякі пов'язані із Сирією оператори перемістилися туди після падіння Асада.

З сьогоднішньої перспективи висновки Індексу 2025 року та наступних звітів про проблему каптагону в Сирії ведуть до одного й того ж. Наприкінці 2024 року країна залишалася в центрі торгівлі, але зростання оцінок синтетичних наркотиків по всій Західній Азії вказувало на те, що виробничі, торговельні та розподільчі мережі ставали дедалі більш регіоналізованими. Хоча ринок, зосереджений в одній країні, можна демонтувати, коли змінюється влада, економіку, вбудовану в регіон, набагато важче порушити. Вилучення, закриття лабораторій і поява нових хабів з 2025 року, здається, підтверджують це. Ліквідація головного виробника просто підштовхнула діяльність до найближчих слабких місць, таких як Сувейда, ліванський кордон і Ємен, тоді як попит із Перської затоки залишився незмінним.

Наступне видання Індексу зафіксує довгострокові наслідки цих змін, але траєкторія вже зрозуміла. За Асада каптагон був регіональним ринком із сирійським ядром. Хоча ядро розпалося, попит зберігається. Торгівля розпорошилася, з'явилися нові виробники й маршрути, а метамфетамін рухається слідом. Хоча перемога над найбільшим у світі виробником каптагону була справжнім досягненням, стримування регіонального ринку синтетичних стимуляторів буде іншим і значно складнішим завданням.

РЕКОМЕНДОВАНІ ПОДІЇ



Регіональний воркшоп Егмонтської групи з віртуальних активів для ПФР[14]

Центр передового досвіду та лідерства ПФР Егмонтської групи (ECOFEL), Підрозділ фінансової розвідки Австрії (A-FIU) та Управління ООН з наркотиків і злочинності (UNODC) проводять 10–11 грудня 2026 року у Відні регіональний воркшоп «Virtual Assets» для регіонів Європа I та Європа II. Програма призначена для представників ПФР – членів Егмонтської групи з цих регіонів; кожен підрозділ може зареєструвати до двох учасників. Місця розподіляються в порядку черговості, а реєстрація закривається після заповнення квоти; інформацію про місце проведення, проїзд і проживання містить логістичний посібник, а детальну агенду обіцяють надати ближче до дати заходу. Реєстраційна форма: https://www.research.net/r/X5K88X5.

Перший день присвячено технічним основам і регуляторним ризикам. Фахівці Crystal Intelligence Федеріко Паезано та Андрій Совершенний проведуть три модулі: еволюція ринку криптовалют, основи блокчейну та відмінності моделей UTXO (Bitcoin і споріднені мережі) й EVM (Ethereum і сумісні мережі); стейблкоїни, встановлення належності криптовалюти, типи криптовалютних сервісів і ризики віртуальних активів у Європі; кейс Stablr і тіньова економіка, а також тема «Санкції в блокчейні: перевірка європейських криптообмежень на практиці». Представники VASPnet Ніл Самтані та Нікі Гомес розглянуть правові та регуляторні індикатори ризику (red flags) щодо VASP, Амін Сафаді (UNODC) – подання й аналіз повідомлень про операції з віртуальними активами в системі goAML. День завершиться панельною дискусією всіх спікерів про виклики та можливості, пов’язані з віртуальними активами.

Другий день зосереджено на розслідуваннях. Фабріціо Фіороні (UNODC) та Алехандро Перес (Європол) представлять можливості Європейського центру з протидії фінансовій та економічній злочинності (EFECC) і методи OSINT у криптовалютних розслідуваннях; міжнародний експерт з

[14] https://egmontgroup.my.canva.site/agenda-vienna

питань ПВК, кіберзлочинності, даркнету та розслідувань щодо віртуальних активів Олексій Фещенко розкаже, як отримувати розвідувальну інформацію з OSINT і блокчейн-аналітики та перетворювати її на докази. Леві Іцик (Whitestream) розгляне використання терористичними організаціями позабіржових (OTC) дилерів і стейблкоїнів для фінансування проксі-війн, а також відстеження коштів, що відмиваються через торговельну інфраструктуру Hyperliquid. Професор Клаудіо Тессоне (Блокчейн-центр Цюрихського університету) присвятить модуль ончейн-аналітиці – від встановлення ідентичностей до виявлення маніпулювання ринком. Програма завершиться врученням нагороди за найкращий кейс щодо віртуальних активів.

Вебінар RUSI: використання соціальних мереж для фінансування тероризму [15]

Центр досліджень фінансових злочинів і безпеки (CFS) Королівського об'єднаного інституту оборонних досліджень (RUSI) проведе 2 грудня 2026 року з 14:00 до 15:00 за Гринвічем (16:00–17:00 за київським часом) онлайн-вебінар «The Abuse of Social Media for Terrorist Financing». Участь безкоштовна та відкрита для всіх охочих за попередньою реєстрацією на сторінці заходу. Дискусію проведуть науковий співробітник CFS Гонсало Саїс та асоційований науковий співробітник RUSI Ендрю Маккей.

Учасники розглянуть, як терористичні суб'єкти використовують соціальні мережі для збору коштів і чому фінансову активність, пов'язану з онлайн-контентом екстремістського спрямування, складно ідентифікувати. Окремо йтиметься про те, як публічні заклики та приватні повідомлення спрямовують прихильників до конкретних платіжних каналів, про ризики фінансування тероризму, пов'язані з механізмами монетизації платформ, а також про те, як покращення звітування та тісніша взаємодія між платформами й фінансовими установами можуть допомогти виявляти та припиняти терористичні збори.

Вебінар ґрунтується на новому дослідницькому брифінгу Гонсало Саїса «The Abuse of Social Media and Messaging Platforms for Terrorist Financing», підготовленому в межах проєкту Project CRAAFT і доступному на його вебсайті. Захід буде корисним для аналітиків ПФР, підрозділів фінансового моніторингу банків і платіжних установ, а також правоохоронних органів, які працюють із зборами коштів, що оголошуються в соціальних мережах і месенджерах.

[15] https://my.rusi.org/events/webinar-the-abuse-of-social-media-for-terrorist-financing.html



Як організовані злочинні групи стали загрозою вантажним перевезенням в Коста-Риці [16]

У нічній тиші на кордоні Коста-Рики та Нікарагуа, поблизу контрольно-пропускного пункту Пеньяс-Бланкас, вишиковується довжелезна колона вантажівок. Двокілометрова черга – це лише початок; буває, що вона розтягується на двадцять кілометрів, і водії змушені чекати по кілька діб, аби перетнути кордон. Ця зона є не просто бюрократичною перепоною, а справжнісінькою кримінальною «гарячою точкою». Це не поодинокий випадок, а симптом глибокої системної кризи, яка охопила транспортну систему Коста-Рики. Країна, яка ще донедавна вважалася островом стабільності у неспокійному регіоні, тепер перетворилася на епіцентр викрадень вантажів у Центральній Америці, де організовані злочинні угруповання діють із зухвалістю, притаманною військовим операціям.

За даними Судового слідчого департаменту (OIJ), у 2025 році банди пограбували щонайменше 156 вантажівок із товарами, що становить приблизно три пограбування на тиждень. Це виводить Коста-Рику на перше місце в регіоні за цим показником. Статистика свідчить про тривожну тенденцію: з 2016 року, коли було зафіксовано 121 пограбування, кількість нападів неухильно зростала, сягнувши піку в 155 випадків у 2017 році, і після певного спаду під час пандемії у 2020 році (91 випадок) знову повернулася до критичних позначок. Лише за перші сім місяців 2026 року

[16] https://insightcrime.org/news/highwaymen-how-cargo-theft-gangs-operate-in-costa-rica/

сталося 71 пограбування, що тримає країну на траєкторії, аналогічній до попереднього року. За останнє десятиліття банди пограбували понад 1300 вантажівок на двох основних транспортних коридорах, що перетинають країну.

Головною рушійною силою цієї кризи є складна та розгалужена мережа організованої злочинності, яка не обмежується лише «дорожніми грабіжниками». Це професійні угруповання, які спеціалізуються на викраденні вантажів, і їхня діяльність є лише початковою ланкою величезного ланцюга незаконного розподілу та перепродажу товарів. Мова йде про використання державних систем, таких як TICA (Інформаційні технології для митного контролю) та DUCA (Єдина центральноамериканська декларація). Після внесення даних до цих систем, інформація про вміст вантажу, його вартість, номерні знаки, реєстраційні дані та навіть паспортні дані водія стає доступною митникам у всіх країнах, через які прямує вантажівка, а також вантажним компаніям. Хоча ця інформація має бути захищеною, на практиці вона часто витікає до злочинців, які використовують її для точного наведення на цілі.

Цілі злочинців є чітко визначеними: вантажівки з найбільш цінними вантажами, вартість яких коливається від 100 000 до 500 000 доларів США. Найпопулярнішими товарами для викрадення є одяг, електроніка, кухонна техніка, алкоголь та шини. Банди діють зухвало та професійно. Вони використовують «навідників» на кордонах, які передають інформацію про вантажівку та її вміст групам, що здійснюють напад. Для подолання захисту перевізників, які встановлюють GPS-трекери на вантажівки та причепи і намагаються їздити в колонах у денний час, банди застосовують глушники сигналу. Вони також розривають колони, вклинюючись між вантажівками своїми автомобілями або оточуючи їх кількома машинами. Після зупинки транспорту злочинці діють за відпрацьованою схемою: погрожуючи зброєю, вони змушують водія зупинитися, після чого один із нападників сідає за кермо.

Наслідки цієї кризи є руйнівними для всієї транспортної галузі та економіки країни. Викрадення вантажівок завдає прямих фінансових збитків. Лише вартість причепа, якщо його не вдається повернути, може сягати 14 000 доларів. Але набагато більших збитків завдає втрата товару, який, як правило, зникає безвісти, потрапляючи до паралельної, неформальної економіки. Брокери продають викрадені товари слабо контрольованим роздрібним торговцям, де вони потім перепродуються на невеликих ринках, у складах та магазинах. У 2025 році Коста-Рика ухвалила закон № 10736, який посилює кримінальну відповідальність за отримання викрадених товарів високої вартості, але, незважаючи на це, незаконний ринок перепродажу продовжує процвітати.

Попри всі зусилля, включаючи встановлення GPS-трекерів, подорожі в колонах та наймання озброєної охорони, проблема залишається нерозв'язаною. Для тих, хто має збройну охорону, ситуація дещо краща, але навіть охоронці з пістолетами визнають свою обмеженість перед обличчям добре озброєних банд.

Таким чином, Коста-Рика опинилася в лещатах безпрецедентної хвилі організованої злочинності, яка використовує прогалини в державних системах безпеки та інформаційних технологіях для

отримання надприбутків. Ця проблема не є ізольованою; вона є частиною ширшої регіональної тенденції, де слабкі інституції та корупція дозволяють кримінальним синдикатам процвітати.

Викрадення вантажівок – це не просто крадіжка товарів, це складна логістична операція, яка живиться інформацією, насильством та безкарністю. Для водіїв, це щоденна боротьба за виживання, а для країни – серйозний виклик її економічній стабільності та верховенству права.

Без комплексного підходу, який включає реформування митних та інформаційних систем, посилення правоохоронних органів та міжнародне співробітництво, Коста-Рика ризикує залишитися «епіцентром» викрадень вантажів у Центральній Америці, а її дороги – небезпечними артеріями, де щохвилини може статися чергове пограбування.

Ваша думка важлива!

Як могли б працювати законодавчі гарантії «справедливого банкінгу» за американським зразком у контексті євроінтеграції України та адаптації банківських стандартів ЄС?

Які з дев'яти короткострокових заходів, запропонованих FSA і Банком Японії щодо загроз фронтирного ШІ, найреалістичніше впровадити українським банкам в умовах воєнного стану?

Які ознаки в тендерній, логістичній і товаросупровідній документації найнадійніше допомагають банкам виявляти постачання товарів подвійного призначення до російського ВПК через треті країни?

Як в умовах відкладеного другого читання законопроєкту № 10225-д забезпечити виявлення та нагляд за постачальниками послуг з віртуальними активами, які вже мають обов'язки з фінмоніторингу, але не мають ліцензійного режиму?

Як забезпечити пропорційність вимог фінансового моніторингу для адвокатів, аудиторів і бухгалтерів, що працюють одноосібно, під час наближення українського законодавства до технічних стандартів AMLA?

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-2026-44

Архів

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.

Міністерство фінансів України

AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE