Методологічний бюлетень

Серійний номер: МінФін-AML-2026-17

Квітень 2026

“Ми шукаємо ключі там, де горить ліхтар!”

Ходжа Насреддін

Мета

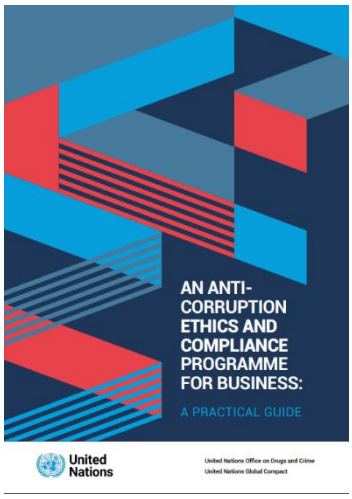
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для суб’єктів первинного фінансового моніторингу (СПФМ), регуляторів та правоохоронних органів.

Містить актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

Для регуляторів та правоохоронних органів є інструментом для розробки ефективних стратегій боротьби з ВК, включаючи навчання та координацію дій між різними установами для забезпечення належної співпраці та обміну інформацією.

Звіти міжнародних організацій та окремих юрисдикцій

Практичний посібник UNODC з антикорупційних програм для бізнесу [1]



Посібник UNODC, підготовлений у рамках тематичної програми «Дії проти корупції, економічного шахрайства та злочинів, пов'язаних з ідентифікаційними даними», є синтезуючим операційним інструментом, метою якого є не запровадження нових нормативних стандартів, а практична операціоналізація принципів, що містяться в Конвенції ООН проти корупції (UNCAC, 2005), Конвенції ОЕСР про боротьбу з підкупом іноземних посадових осіб (1999), Керівних принципах ОЕСР з питань внутрішнього контролю, етики та відповідності (2010), Принципах PACI Всесвітнього економічного форуму, Принципах TI для протидії хабарництву та Керівних принципах цілісності Групи Світового банку (2010). Документ консолідує ці стандарти відповідно на прямий запит Антикорупційної робочої групи G20, виражений у рамках

[1] https://businessintegrity.unodc.org/bip/uploads/documents/resources/An_Anti-Corruption_Ethics_and_Compliance_Programme_for_Business-_A_Practical_Guide.pdf

Антикорупційного плану дій 2010 року, та є результатом спільної роботи UNODC, OECP та Світового банку.

Перший розділ посібника формує юридичну рамку зобов'язань приватного сектору. UNCAC — єдиний універсально обов'язковий антикорупційний інструмент — містить низку статей з прямим впливом на корпоративне регулювання: ст. 12 зобов'язує держави-учасниці вжити заходів щодо запобігання корупції у приватному секторі; ст. 26 встановлює відповідальність юридичних осіб за корупційні дії; ст. 37–39 регулюють співпрацю з правоохоронними органами та між державними та приватними структурами; ст. 40 торкається банківської таємниці. Ключовим практичним наслідком є екстериторіальна дія ряду законодавств — зокрема американського FCPA та британського UK Bribery Act — яка поширюється як на вітчизняні компанії, що діють за кордоном, так і на іноземні компанії, що оперують на відповідній території. Санкційна система Світового банку, в свою чергу, охоплює публічне застереження, відсторонення від тендерів та вимоги реституції.

Методологічним ядром документа є ризик-орієнтований підхід, що має застосовуватися до кожного елемента антикорупційної програми. Оцінка ризиків структурована у три послідовні фази. Перша — ідентифікація ризиків — здійснюється через аналіз правових вимог юрисдикцій, консультації з персоналом, безпосередньо схильним до корупційних ризиків (торговельні представники, менеджери із закупівель), вивчення попередніх інцидентів та залучення зовнішніх консультантів. Друга — кількісна та якісна оцінка ризиків — базується на поєднанні ймовірності настання події та ступеня її наслідків (прямих: штрафи, анулювання ліцензії; та непрямих: репутаційні втрати, судові витрати). Третя — стратегії зниження — включає три опції: пом'якшення (посилений нагляд, автоматизований моніторинг платіжних потоків, цільові навчання), уникнення (відмова від ризикових ринків або контрагентів) та передачу ризику (делегування функцій належної перевірки спеціалізованим зовнішнім постачальникам).

Архітектура антикорупційної програми охоплює дванадцять взаємопов'язаних елементів. Демонстративна підтримка вищого керівництва є відправною точкою: вона повинна бути не декларативною, а операційно реалізованою через конкретні ресурсні зобов'язання, персональну участь керівництва у

Висновки:

- **Екстериторіальне застосування антикорупційного законодавства ряду юрисдикцій означає, що відповідність лише національним нормам є недостатньою:** підприємства, що ведуть міжнародну діяльність або залучають агентів у зонах підвищеного ризику, зобов'язані формувати програми, що відповідають міжнародним стандартам UNCAC та рекомендаціям OECP — незалежно від вимог вітчизняного законодавства.
- **Ризик бізнес-партнерів є системним та не може бути нейтралізований формальними KYC-процедурами:** необхідний масштабований, ризик-диференційований цикл належної перевірки третіх сторін, з особливою увагою до агентів та посередників у юрисдикціях з підвищеним корупційним ризиком.
- **Функціональна незалежність наглядового органу над антикорупційною програмою від бізнес-підрозділів є необхідною умовою ефективності:** підпорядкування функції відповідності комерційним структурам підриває як об'єктивність оцінки ризиків, так і здатність виявляти внутрішні зловживання.
- **Механізм захисту викривачів є не опціональним інструментом, а базовою умовою функціонування антикорупційної системи:** відсутність захищеного та анонімного каналу для повідомлень фактично унеможливлює виявлення значної частини корупційних схем через внутрішні канали та суперечить вимогам UNCAC.

навчаннях та пряме персональне призначення відповідальних осіб. Наглядовий орган над програмою повинен бути функціонально незалежним від бізнес-підрозділів і мати доступ до вищих органів управління. Антикорупційна політика повинна бути зовні задекларованою, перекладеною для всіх операційних юрисдикцій та доведеною до відома усіх стейкхолдерів — і внутрішніх, і зовнішніх. Деталізовані політики для специфічних зон ризику охоплюють: хабарництво та «платежі за прискорення» (статус яких залишається дискусійним у різних юрисдикціях), подарунки та представницькі витрати, державні закупівлі та урядові контракти, а також транзакційні ризики у сфері злиття і поглинання.

Особливу операційну значущість серед дванадцяти елементів має розділ про застосування програми до бізнес-партнерів. Посібник наголошує, що агенти, посередники та субпідрядники перебувають поза прямим охопленням компанії, однак корупційні дії з їхнього боку в інтересах або від імені принципала можуть генерувати повну правову відповідальність останнього. Це вимагає впровадження ризик-диференційованого циклу належної перевірки партнерів, параметри якого визначаються рівнем ризику, юрисдикцією присутності та типом взаємодії. Внутрішній контроль та ведення документації, у свою чергу, забезпечують доказову базу для захисту в рамках можливих регуляторних розслідувань: регулятори оцінюють не лише факт відповідності, але й задокументовану логіку прийнятих рішень.

Механізм реагування на порушення, описаний у розділах J та K, є критично важливим інституційним елементом, що забезпечує замкнутий цикл управління ризиками. Він включає: захищений та конфіденційний канал для повідомлення про порушення (whistleblowing mechanism); систему реагування, що передбачає незалежне внутрішнє розслідування та документування всіх рішень; систематичний перегляд і коригування програми за результатами аудитів та перевірок. Посібник завершується закликом до виходу за межі суто корпоративного комплаєнсу та участі у механізмах колективних дій: партнерства з торговельними асоціаціями, галузеві пакти щодо доброчесності та координаційні ініціативи в ланцюжках постачання є необхідними для нейтралізації системних корупційних ризиків, що виходять за межі можливостей однієї організації. Для малих та середніх підприємств посібник окремо акцентує на стратегіях агрегації зусиль — через торговельно-промислові палати та галузеві об'єднання — для скорочення ресурсних витрат на оцінку ризиків.

Еволюція типологій відмивання коштів та фінансування тероризму [2]

Тематичне дослідження №34, опубліковане Підрозділом фінансової розвідки Банку Італії (UIF) є черговим видом систематичної кодифікації значущих схем ВК та ФТ, виявлених у ході аналізу повідомлень про підозрілі операції. Тематична рамка 34-го випуску зосереджена на трьох взаємопов'язаних аналітичних вісях: зловживання публічними коштами та заходами підтримки, зокрема коштами ЄС та Національного плану відновлення PNRR; злочинне використання криптоактивів як інструменту відмивання коштів та фінансування тероризму; та масштабні транскордонні потоки коштів злочинного походження з Італії до країн Азії. Видання включає десять детально описаних схем із зазначенням аномальних індикаторів.

Найбільш операційно значущою схемою є «відмивання коштів як послуга» (Money Laundering as a Service), реалізована через платіжного агента. Платіжний агент Alfa, зареєстрований у країні X Євросоюзу та авторизований

[2] https://uif.bancaditalia.it/pubblicazioni/quaderni/2026/quaderno-34-2026/QAR-34.pdf

виключно як агент PSP Beta, публічно позиціонував себе як банк або платіжна установа, не маючи відповідних ліцензій, та цілеспрямовано акумулював злочинні потоки від мереж італійських підприємств — учасників схем податкового шахрайства (із застосуванням підпільного банкінгу) та зловживань із субсидіями PNRR. Перевірка через центральні реєстри EBA засвідчила, що Alfa не є ні банком, ні PSP, а лише агентом — що дозволяло класифікувати її як «фінансову компанію» та застосовувати спрощену належну перевірку. Кошти накопичувались на рахунку Alfa у PSP Gamma (країна Y, держава-член Євросоюзу), а потім переводились до країн Південно-Східної Азії через кореспондентський рахунок у банку Євросоюзу. Загальна сума транзакцій, виявлена лише завдяки Joint Analysis з ПФР країн X та Y, склала кілька сотень мільйонів євро з кількох європейських країн.

Схеми зловживання публічними коштами (схеми 2, 8 та 9) формують другий аналітичний кластер. Схема 2 документує систематичне нецільове використання субсидій для сільськогосподарського сектору (кошти фондів FEAGA та FEASR): кошти, що надходили на рахунки сільськогосподарських підприємств Alfa та Gamma, переводились до компанії Delta та профконсультанту Tizio — реальному організатору схеми, ідентифікованому як «справжній вигодоодержувач» завдяки аналізу ланцюжка фінансових потоків через кілька юридичних осіб.

Висновки:

- **Схема ML-as-a-Service через платіжного агента, що помилково кваліфікується як банк або PSP, є системним попередженням для комплаєнс-підрозділів:** верифікація реального регуляторного статусу іноземного контрагента через реєстри EBA є обов'язковою процедурою перед маршрутизацією платежів — особливо при значних регулярних переказах до Азії.
- **Зловживання коштами ЄС через складні корпоративні структури вимагає посиленого моніторингу операційних патернів підприємств-реципієнтів субсидій та пов'язаних із ними осіб:** аналіз при відкритті рахунку є недостатнім — необхідний динамічний перегляд ризикового профілю у відповідь на зміни у структурі транзакцій.
- **Криптоактиви як інструмент легалізації доходів від шахрайства та ФТ вимагають від СПФМ інтеграції інструментів блокчейн-аналітики до систем виявлення підозрілої діяльності:** класичний моніторинг банківських рахунків є недостатнім без відстеження крипто-ланцюжків і пов'язаних гаманців.
- **Ефективне виявлення "справжнього вигодоодержувача" через мережевий аналіз підкреслює необхідність переходу від індивідуального профілювання до аналізу відносин між суб'єктами:** виявлення реального організатора схеми є неможливим без комплексного картографування зв'язків між юридичними та фізичними особами, зокрема у сімейних та підставних структурах.
-

Схема 8 демонструє використання компанії в ролі фідуціарія для незаконного отримання публічних пільг через непрозорий ланцюжок корпоративних транзакцій. Схема 9 виявляє аномальний обіг податкових кредитів та викривлене застосування договорів ескроу, що свідчить про системний характер зловживань у сфері держпідтримки.

Третій аналітичний кластер охоплює шахрайство, пов'язане з фінансовими інноваціями (схеми 3 та 10). Схема 3 ілюструє маніпуляції з сек'юритизацією фіскальних кредитів у рамках законодавства про будівельні бонуси (DL 34/2020): консультаційні компанії Alfa та Beta, що представляли осіб без підприємницького досвіду, акумулювали значні кошти за нібито надані послуги зі структурування гіпотетичних операцій цесії фіскальних кредитів, які так і не були реалізовані. Кошти в кінцевому рахунку потрапили через рахунок в азіатській країні до Mevio — іноземного

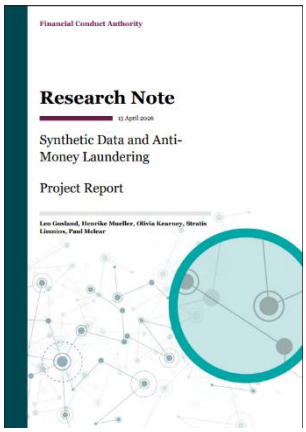
підприємця, що вже фігурував у попередніх повідомленнях про підозрілі операції. Схема 10 описує піраміду у секторі відновлюваної енергетики: залучення цифрових платформ для пропозиції надвисокодохідних «інвестицій», масштабне залучення жертв та подальше швидке розосередження коштів через злочинні фінансові канали, уже задокументовані в інших справах.

Схеми 4 та 5 присвячені використанню криптоактивів у ВК та ФТ. Схема 4 документує потенційне злочинне застосування неформальних систем міжособових переказів (підпільний банкінг / гавала) у поєднанні з криптоактивами: задіяна децентралізована інфраструктура для приховування руху коштів і уникнення банківського нагляду, а транснаціональність та швидкість операцій унеможливлює стандартний моніторинг. Схема 5 ілюструє реінвестування доходів від шахрайства типу «imposter scam» через криптовалюти: конвертація злочинних коштів у криптоактиви дозволила задіяти псевдоанонімність децентралізованих мереж для маскування злочинного походження коштів. UIF наголошує, що саме застосування інноваційних методів фінансового аналізу є умовою відновлення суб'єктних зв'язків та виявлення глибинної динаміки криміналізованих потоків.

Схеми 6 та 7 документують масштабні трансграничні потоки з Італії до Азії. Схема 6 описує переміщення доходів від фіскальних злочинів через мережу підприємств: підприємства відкривалися, здійснювали короткострокові схеми ухилення від ПДВ та ліквідувались до виявлення порушень. Схема 7 — відмивання через віртуальний IBAN, керовані PSP з юридичною адресою в Азії, — демонструє, як технологічна інфраструктура слугує прикриттям: технічний інструмент віртуальних IBAN надавав видимість легітимності транзакціям, фактично спрямованим до злочинних мереж. В обох схемах UIF виявив характерний географічний патерн — Північна Італія → Південно-Східна Азія — що є систематичним явищем, задокументованим у кількох попередніх випусках.

З методологічного боку видання вирізняється трьома аналітичними інноваціями. По-перше, механізм Joint Analysis між кількома ПФР Євросоюзу підтвердив свою незамінність для виявлення транскордонних схем ВК, недоступних для аналізу в межах однієї юрисдикції: без скоординованого обміну даними між ПФР країн X та Y загальний обсяг операцій Alfa залишився б прихованим. По-друге, залучення даних електронної фактури відкрило нові аналітичні можливості для відстеження торговельних потоків поза традиційними банківськими даними. По-третє, техніка мережевого аналізу дозволила ідентифікувати реальних організаторів схем через картографування зв'язків між юридичними та фізичними особами, що є кроком вперед порівняно з ізольованим транзакційним аналізом.

Синтетичні дані в системі ПВК: регуляторний проєкт FCA та нова модель тестування детекційних систем [3]



Дослідницький звіт Управління з фінансового регулювання та нагляду Великої Британії (Financial Conduct Authority, FCA) «Синтетичні дані та протидія відмиванню коштів» документує результати регуляторного проєкту зі створення статистично реалістичного, конфіденційно захищеного синтетичного набору даних з вбудованими типологіями відмивання коштів. Відправним контекстом є масштаб глобальної проблеми: за оцінками фахівців, щороку відмивається від 2 до 5% світового ВВП — еквівалент 800 мільярдів - 2 трильйонів доларів США. Існуючий регуляторний бар'єр полягає у відсутності легального та безпечного доступу до реальних транзакційних даних для розробки та тестування AML-інструментів: реальні дані несуть правові та етичні

[3] https://www.fca.org.uk/publication/research-notes/synthetic-data-anti-money-laundering-project-report.pdf

ризики та практично не піддаються повній анонімізації без втрати аналітично значущих патернів. Проєкт реалізується у межах FCA Digital Sandbox і передбачає проведення AML Data Sprint — відкритого майданчика для тестування AML-технологій у контрольованому середовищі.

Архітектура проєкту є структурно інноваційною: FCA забезпечила регуляторне супроводження, нагляд та технічні компетенції; Інститут Алана Тюрінга — дослідницький та технічний досвід у сфері синтетичних даних; Plenitude Consulting — фахову підтримку у сфері фінансових злочинів та галузевий досвід; Napier AI — прикладні технологічні компетенції в виявленні фінансових злочинів. Таке публічно-приватне партнерство між регулятором, академічним інститутом та приватним сектором долає традиційне розмежування між регуляторним наглядом та технологічними інноваціями в AML-сфері і є моделлю для регуляторів інших юрисдикцій.

Методологія проєкту реалізується у три послідовних етапи. Перший: реальні банківські дані анонімізуються ще на рівні джерела — без включення персональних даних. Другий: анонімізовані дані доповнюються синтетичними типологіями ВК, розробленими експертами та такими, що відображають реальні злочинні схеми, відомі з практики. Третій: за допомогою методу AIM (Adaptive and Iterative Mechanism) генерується повністю синтетичний набір даних із механізмами диференційованої конфіденційності (differential privacy). Метод AIM захищає конфіденційність через введення контрольованої випадковості, що унеможливлює відновлення даних про конкретного клієнта чи транзакцію, одночасно зберігаючи патерни, необхідні для змістовного аналізу. Вбудовані типології охоплюють: структурування транзакцій нижче порогів звітності (смерфінг), швидке переміщення коштів між множинними рахунками для приховування їх походження та кругові транзакції, де кошти повертаються до відправника через ланцюжок посередників. Для підвищення реалістичності вводились варіації навколо цих типологій, щоб підозрілі патерни не з'являлися в ідентичних формах.

Оцінка набору даних проводилась за трьома критеріями. Статистична достовірність: порівняння статистик між анонімізованими вихідними та синтетичними даними виявило мінімальне розходження, що підтверджує адекватне відтворення статистичних властивостей реальних транзакцій. Конфіденційність: застосовані механізми забезпечили надійний захист від повторної ідентифікації фізичних осіб та

Висновки:

- **Синтетичні дані з вбудованими типологіями відкривають новий регуляторний механізм для тестування AML-рішень:** компанії зможуть демонструвати ефективність своїх інструментів без доступу до конфіденційних банківських даних, що знижує бар'єри для інновацій та вирівнює конкурентне поле між великими банками та фінтех-стартапами.
- **Метод диференційованої конфіденційності у поєднанні з AIM задає нову технологічну рамку для регуляторної обробки чутливих фінансових даних:** баланс між аналітичною реалістичністю та захистом конфіденційності є досяжним, але вимагає постійного управлінського нагляду на всіх етапах генерації та розповсюдження.
- **Обмеженість синтетичних даних лише відомими типологіями є критично важливим застереженням для СПФМ та постачальників AML-рішень:** такий набір є цінним тренувальним та тестовим інструментом, але не може замінити оперативний моніторинг, оскільки нові злочинні схеми неминуче виходитимуть за межі кодифікованих патернів.
- **Проєкт задає нову модель публічно-приватного партнерства в AML-інноваціях:** регулятор виступає як активний технологічний партнер, що формує та стандартизує конкурентне середовище для розробників AML-рішень — аналогічна модель може бути відтворена регуляторами інших юрисдикцій.

організацій, при цьому більш сильний захист конфіденційності інколи призводив до зниження деталізованості даних, що вимагало постійного управлінського балансування. Виявлення типологій: тестування за галузевими стандартними підходами виявило «спектр виявлення» — від тих патернів, що легко виявити до тих, які важко виявити, — що є оптимальним для максимальної практичної цінності в рамках Data Sprint. При цьому не всі виявлені патерни можна було однозначно атрибутувати до вбудованих типологій: частина з них могла бути артефактами механізмів конфіденційності або реально виникаючими закономірностями.

Проєкт виявив кілька структурних обмежень. Основна дилема — балансування між реалістичністю та конфіденційністю: найбільш детальні дані несуть найвищий ризик повторної ідентифікації. Внутрішня узгодженість набору даних є додатковим викликом: типології ВК залежать від відносин між клієнтами, рахунками та транзакціями, тоді як метод AIM генерує транзакції незалежно, що ускладнює відтворення поведінки, яка залежить від часових послідовностей. Найбільш концептуально важливим обмеженням є те, що набір містить лише відомі типології: Невідомі схеми, які злочинці вже використовують, але які ще не ідентифіковані та не кодифіковані залишаються поза охопленням будь-якого синтетичного набору.

Стратегія розвитку проєкту після Data Sprint включає кілька напрямів. Масштабування доступу до набору даних — за межі пісочниці FCA — вимагатиме ретельного врегулювання питань управління, ліцензійних рамок та узгодженості з міжнародними стандартами конфіденційності. Поповнення типологій є постійним процесом: злочинні поведінки не статичні, і набір ризикує застаріти без регулярного оновлення відповідно до актуального ландшафту загроз. Ненавмисні наслідки синтетичних даних включають ризик того, що фірми оптимізуватимуть системи виявлення під конкретні вбудовані патерни замість розвитку широких можливостей виявлення, а також ризик надмірної довіри до синтетичних даних як замінника оперативних живих даних. Стратегічне значення проєкту виходить за межі конкретного набору даних: він встановлює прецедент для переходу від ізольованих, закритих AML-тестів до відкритих, колаборативних інновацій під регуляторним наглядом.

Міністерська декларація FATF: аналіз глобальної стратегії протидії нелегальним фінансам в епоху геополітичних потрясінь [4]

Оприлюднена у квітні 2026 року Міністерська декларація Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) стала розгорнутим маніфестом трансформації світової архітектури протидії нелегальним фінансовим потокам.

Автори декларації з перших рядків заявляють про «непохитну та тверду відданість» підтримці FATF як глобального стандартизатора, підкреслюючи, що з моменту свого заснування ця інституція ефективно сприяла посиленню внутрішніх дій у сфері запобігання, виявлення, розслідування та переслідування, а також поверненню активів, зміцненню правових рамок, пришвидшенню міжнародної співпраці та глибшому розумінню ризиків.

[4] https://www.fatf-gafi.org/en/publications/Fatfgeneral/Ministerial-Declaration-2026.html

Однак головний меседж полягає в тому, що у глобалізованому світі, де технології дозволяють миттєво переміщувати гроші через будь-які кордони, боротьба з ML/TF/PF має бути «негайною та рішучою» – це більше не питання технічного комплаєнсу, а нагальний глобальний пріоритет, що лежить в основі міжнародної безпеки.

Міністри не лише згадують, але й акцентовано нагадують про публічну заяву FATF від лютого 2023 року щодо призупинення членства російської федерації. Більше того, вони закликають усі юрисдикції зберігати пильність щодо загроз цілісності, безпеки та стабільності міжнародної фінансовій системі, які виникають «внаслідок війни російської федерації проти України». Це положення є важливим, адже FATF, яка традиційно позиціонувалася як технократичний орган, дедалі частіше виступає інструментом колективної безпекової політики. Використання механізмів FATF для ізоляції країни-агресора показує, що стандарти фінансової чистоти нерозривно пов'язані з дотриманням норм міжнародного права.

Переходячи до організаційно-процесуальних питань, декларація детально описує стратегічні пріоритети на дворічний період 2026-2028 років. Ключовим елементом є новий раунд взаємних оцінювань, який має розпочатися саме у 2026 році. Цей технічний процес визнаний фундаментальним для надання персоналізованих рекомендацій юрисдикціям, визнання та просування національних реформ. Міністри наголошують на необхідності забезпечення підзвітності серед членів, а також постійного вдосконалення та оптимізації процесу оцінювання з сильним фокусом на ризик та ефективність. Важливим є визнання значних зусиль, які вимагає кожна взаємна оцінка, та заклик до надання достатніх ресурсів для забезпечення сталості цієї роботи.

У цьому контексті вітається внесок Міжнародного валютного фонду та Світового банку як кваліфікованих оцінювальних органів. Окремо підкреслюється важливість посилення голосу регіональних структур за типом FATF (FSRB) у робочих процесах – це має на меті зробити глобальну мережу більш інтегрованою та справедливою, враховуючи інтереси понад 200 юрисдикцій, які входять до неї. FATF визнає, що багато країн із низькою спроможністю, включаючи мікродержави, мають стратегічні недоліки, тому було уточнено ризик-орієнтовані критерії для кращого виявлення тих, хто становить найвищу загрозу. Водночас обіцяно розробити адаптовані підходи до оцінювання, що враховують специфічні ризики та контекст таких країн – це визнання того, що універсальні стандарти мають бути гнучкими, щоб не створювати надмірного тиску на слабкі фінансові системи, але водночас не залишати прогалин для зловживань.

Концептуальним ядром усієї діяльності FATF продовжує бути ризик-орієнтований підхід (risk-based approach), який декларація називає «наріжним каменем» стандартів та методології оцінювання. Визнаючи розмаїття внутрішніх інституційних та правових систем, міністри зобов'язуються підтримувати юрисдикції та приватний сектор у повному та ефективному впровадженні цього підходу, включаючи нагляд, що базується на ризиках. Це має сприяти глибшому розумінню ключових ризиків та пріоритетів серед регуляторів, наглядових органів, фінансових розвідок, правоохоронних органів та бізнесу, а також мати конкретний вплив на запобігання та боротьбу з нелегальним фінансуванням.

Особливо цікавим є застереження щодо «уникнення регуляторних надмірностей та непотрібних витрат на комплаєнс, особливо для низькоризикових секторів», а також зменшення фінансової виключеності. Це свідчить про те, що FATF усвідомлює ризики надмірного контролю і намагається знайти баланс між безпекою та доступністю фінансових послуг. Така позиція є особливо актуальною для країн, що розвиваються, де доступ до банківських послуг і так обмежений, а також для малого та середнього бізнесу, який може страждати від надмірних перевірок.

Окремий блок присвячено прозорості платежів та фінансовій інклюзії. Декларація вітає переглянуті стандарти FATF щодо прозорості платежів, включаючи боротьбу з обходом санкцій та шахрайством. Очікується, що ці зміни підвищать безпеку транскордонних переказів та підтримають дорожню карту G20 щодо пришвидшення, здешевлення, підвищення прозорості та інклюзивності таких переказів. Водночас схвалено оновлені рекомендації, які заохочують юрисдикції застосовувати заходи, пропорційні до ризиків, що має сприяти залученню більшої кількості людей і компаній до офіційного фінансового обігу. Це є прямим визнанням того, що надто жорсткі правила можуть виштовхувати клієнтів у тіньовий або нерегульований сектор, що є ще більш небезпечним з точки зору ML/TF/PF.

Технологічний аспект займає одне з центральних місць у декларації. Міністри заявляють про підтримку «відповідальних інновацій у фінансах» та визнають, що технології, включаючи штучний інтелект, можуть підвищити ефективність нагляду та комплаєнсу. Однак водночас вони зобов'язуються реагувати на технологічний розвиток та цифровізацію фінансів таким чином, щоб заохочувати інновації, зберігати фінансову цілісність та уникати регуляторного надлишку. Це надзвичайно делікатний баланс, адже штучний інтелект може використовуватися як для виявлення підозрілих транзакцій, так і для створення складних шахрайських схем або автоматизованого відмивання грошей через децентралізовані платформи.

Особливу увагу приділено віртуальним активам. Враховуючи їхній «природньо транскордонний характер», FATF закликає до швидкого та ефективного впровадження своїх стандартів у секторі віртуальних активів по всій глобальній мережі. Більше того, через механізм взаємного оцінювання FATF обіцяє «притягувати до відповідальності» країни, які не зможуть оперативно імплементувати ці стандарти. Це означає, що криптобіржі, а згодом, ймовірно, й децентралізовані фінансові протоколи (DeFi) потраплять під пильний нагляд, а країни, де регулювання віртуальних активів є слабким або відсутнім, можуть бути внесені до «сірих» або «чорних» списків FATF.

Найбільш тривожним та водночас новаторським розділом декларації є той, що стосується епідемії шахрайства та транснаціональної організованої злочинності. Міністри прямо заявляють, що організовані злочинні групи дедалі частіше використовують телекомунікації, соціальні мережі та штучний інтелект для розширення своїх транскордонних шахрайських схем, і ця «епідемія шахрайства» зростає у розмірах, масштабах та охопленні. Її вплив на жертв виходить далеко за межі фінансових втрат, завдаючи глибокого психологічного стресу.

FATF заявляє про рішучість повністю задіяти весь арсенал інструментів AML/CFT/CPF для виявлення, зриву та боротьби з шахрайством, включаючи платіжне. Визнається ключова роль посилених державно-приватних партнерств, покращеного обміну інформацією та відповідального використання передових технологій (зокрема ШІ) із належними гарантіями та відповідно до належної правової процедури. Також згадуються організовані scam-центри, зловживання юридичними особами та використання ШІ для вчинення цих злочинів. Не менш детально розглядаються транснаціональні організовані злочинні угруповання, включаючи міжнародні наркокартелі, які займаються торгівлею людьми, зброєю, корупцією, а особливо – наркотрафіком, включаючи незаконні синтетичні опіоїди (що спричинили сотні тисяч смертей) та рослинні наркотики, такі як кокаїн.

Декларація констатує, що багато країн досі мають труднощі з виявленням та підривом професійних мереж відмивання грошей, які дозволяють злочинцям збагачуватися. Вирішення цього транскордонного виклику вимагає швидкої, конструктивної та ефективної міжнародної співпраці. Це положення є прямим закликом до правоохоронних органів та фінансових розвідок усього світу об'єднувати зусилля, обмінюватися даними в реальному часі та координувати спільні розслідування, адже традиційні, повільні канали взаємодії вже не працюють у світі миттєвих криптопереказів та децентралізованих платформ.

Щодо класичних загроз – тероризму та розповсюдження зброї масового знищення – декларація залишається непохитною. Тероризм продовжує становити серйозну загрозу глобальному миру та безпеці, і FATF підтверджує свою відданість боротьбі з його фінансуванням, надаючи юрисдикціям та приватному сектору відповідний інструментарій. Окремо наголошується на важливості відповідних резолюцій Ради Безпеки ООН щодо КНДР та Ірану.

Висновки:

- **Геополітична позиція FATF.** Декларація не лише підтверджує призупинення членства росії, але й прямо пов'язує її війну проти України із загрозами міжнародній фінансовій системі.
- **Ризик-орієнтований підхід як домінанта.** Стандарти FATF вимагають пропорційності заходів: посилення контролю для високоризикових сфер та пом'якшення регуляторного навантаження для низькоризикових секторів задля фінансової інклюзії.
- **Технологічний виклик – від ШІ до криптовалют.** FATF закликає до «відповідальних інновацій» та швидкої імплементації стандартів для віртуальних активів, погрожуючи «притягненням до відповідальності» країн, які зволікають. Штучний інтелект визнається як інструмент нагляду, так і джерело нових загроз.
- **Епідемія шахрайства та організованої злочинності.** Вперше на такому рівні шахрайство визнано глобальною проблемою, а транснаціональні злочинні угруповання – прямою загрозою цілісності фінансової системи, що вимагає негайної міжнародної співпраці.

З огляду на повторне застосування резолюцій ООН щодо Ірану через його недотримання зобов'язань з нерозповсюдження ядерної зброї, FATF нагадує всім юрисдикціям про їхні обов'язки щодо ризиків фінансування розповсюдження, які походять від Ірану. Це є сигналом для банків та інших фінансових установ посилити комплаєнс-контроль щодо будь-яких транзакцій, пов'язаних з іранськими контрагентами.

На завершення, міністри підтверджують відданість зміцненню надійного врядування FATF, прозорості та зовнішнім комунікаціям. Це має підвищити видимість інклюзивного підходу FATF та вплив її роботи на всю глобальну мережу. Конкретні ініціативи щодо посилення партнерства в рамках мережі сприятимуть якнайширшому впровадженню стандартів.

Визнаючи критичну роль FATF у захисті цілісності міжнародної фінансової системи, члени зобов'язуються забезпечити сталість бюджету та ресурсів FATF, а також їх ефективне використання для досягнення стратегічних пріоритетів та робочої програми. Це прагматичне визнання того, що амбітні плани потребують відповідного фінансування, і країни-учасниці готові інвестувати в цю інституцію.

Регулювання

Нормативні оновлення ЦБ ОАЕ [5]

Оновлення загальних керівних принципів ПВК/ФТ/ФР для ліцензованих фінансових установ

Оновлення нормативної бази Центрального банку Об'єднаних Арабських Еміратів (CBUAE) для ліцензованих фінансових установ (ЛФУ) становить собою фундаментальний зсув у регуляторній парадигмі, що нерозривно пов'язаний із Національною стратегією ОАЕ у сфері ПВК/ФТ/ФР на 2024–2027 роки. Виключення ОАЕ із "сірого списку" FATF ознаменувало перехід юрисдикції від етапу інтенсивного виправлення технічних недоліків до фази забезпечення довгострокової,

[5] https://www.centralbank.ae/media/njvnahyo/cbuae-updates-amlcftcpf-guidance-for-licensed-financial-institutions-en.pdf

стійкої та ризик-орієнтованої ефективності. Відповідно до положень, затверджених Кабінетом міністрів ОАЕ, нова архітектура комплаєнсу ґрунтується на одинадцяти стратегічних цілях, які вимагають безпрецедентного рівня інтеграції фінансової розвідки, оптимізації ресурсів та аналізу даних у реальному часі. Регуляторна логіка CBUAE наразі диктує, що ЛФУ повинні відмовитися від реактивних моделей комплаєнсу на користь проактивних гнучких (agile) стратегічних циклів, здатних адаптуватися до складних загроз, таких як операції з віртуальними активами та використання непрозорих корпоративних структур.Оновлені керівні принципи (які доповнюють Повідомлення CBUAE № 79/2019 та наступні директиви) формалізують вимогу щодо безпосередньої імплементації результатів Національної оцінки ризиків (НОР) у внутрішні політики ЛФУ. Це означає, що ідентифіковані на національному рівні вразливості повинні автоматично транслюватися в налаштування скорингових моделей та сценаріїв моніторингу транзакцій на мікрорівні кожної фінансової установи. Значним аспектом цієї еволюції є посилення правової інфраструктури, що супроводжується розширенням сфери застосування предикатних злочинів та зниженням юридичних порогів для їх доведення. Більше того, запровадження персональної кримінальної відповідальності для керівників юридичних осіб за недоліки в системах контролю радикально змінює концепцію корпоративного управління ризиками, перетворюючи ПВК/ФТ з операційної функції на питання стратегічної відповідальності рівня Ради директорів.

Методологічно CBUAE вимагає від ЛФУ впровадження комплексних систем, які не лише відповідають букві закону, але й демонструють високу операційну ефективність у виявленні, розслідуванні та блокуванні незаконних фінансових потоків. Національна стратегія наголошує на критичній важливості міжвідомчої координації та державно-приватного партнерства, вимагаючи від ЛФУ активної участі в обміні фінансовою розвідувальною інформацією. Цей підхід підсилюється вимогами до прозорого аналізу розвідувальних даних із використанням передових баз даних та систем аналітики, що дозволяє регуляторам і правоохоронним органам діяти на випередження.

Стратегічний рівень	Основні фокуси Національної стратегії 2024–2027	Імплементація для ліцензованих фінансових установ
Регуляторний	Перехід від технічної відповідності до ефективності	Необхідність валідації комплаєнс-моделей на результативність
Технологічний	Аналіз великих даних та фінансова розвідка	Інвестиції в системи штучного інтелекту для моніторингу транзакцій
Юридичний	Персональна кримінальна відповідальність менеджменту	Посилення протоколів документування рішень Ради директорів

Стратегічний рівень	Основні фокуси Національної стратегії 2024–2027	Імплементація для ліцензованих фінансових установ
Національний	Динамічна адаптація до Національної оцінки ризиків	Гнучкі цикли перегляду внутрішніх ризик-апетитів

Відповідно, загальний вектор нормативних оновлень вимагає від ЛФУ трансформації їхніх комплаєнс-підрозділів у високотехнологічні аналітичні центри. Очікується, що установи не лише виявлятимуть відомі типології, але й будуть здатні ідентифікувати нові патерни легалізації доходів, отриманих злочинним шляхом, забезпечуючи таким чином безперервну цілісність фінансової системи ОАЕ на глобальній арені.

Управління ризиками фінансування розповсюдження зброї масового знищення (ФР) [6]

Керівництво CBUAE щодо управління ризиками ФР встановлює жорстку методологічну межу між ФР та класичними фінансовими злочинами, вимагаючи від ЛФУ принципово іншого підходу до ідентифікації загроз. На відміну від ВК, де метою є приховування незаконного походження активів через стадії розміщення, розшарування та інтеграції, ФР характеризується лінійним переміщенням ресурсів (часто цілком легального походження) для підтримки розробки, придбання або експорту ядерної, хімічної чи біологічної зброї та технологій подвійного призначення. Регулятор спирається на визначення FATF, формулюючи ризик ФР як функцію трьох критичних змінних: загрози (особи чи організації з наміром заподіяти шкоду), вразливості (слабкі місця в системі, які можна експлуатувати) та наслідків (масштаб впливу).

Центральним елементом керівництва є імперативна вимога щодо проведення відокремленої Інституційної оцінки ризиків ФР (PFRA), яка має інтегрувати результати Національної оцінки ризиків ФР (PFNRA) та офіційну інформацію від наглядових органів і підрозділів фінансової розвідки. Цей аналітичний процес вимагає від установ глибокого аудиту невід'ємних факторів ризику: специфіки клієнтської бази (особливо взаємозв'язків із підсанкційними суб'єктами), характеристик продуктів, складності каналів постачання та географічних особливостей. Особлива увага приділяється операційним ризикам ЛФУ, зокрема вразливостям, що виникають через дефіцит кваліфікованого персоналу або технологічні збої в роботі автоматизованих систем скринінгу, що може призвести до пропуску транзакцій, пов'язаних із підсанкційними юрисдикціями.

Стратегії пом'якшення ризиків ФР, згідно з директивами CBUAE, вимагають глибокої технологічної інтеграції та розширеної належної перевірки клієнтів (CDD). Установи зобов'язані збирати додаткові дані на етапі онбордингу для створення деталізованих профілів, здатних виявляти нетипові інтереси клієнтів у закупівлі високотехнологічного обладнання або товарів подвійного призначення. Для ЛФУ з високим рівнем ризику обов'язковим є використання програмного забезпечення для аналізу мережевих зв'язків, що дозволяє виявляти приховані патерни між фіктивними компаніями та кінцевими бенефіціарами. Окрім цього, керівництво приділяє критичну увагу кореспондентським банківським відносинам, класифікуючи їх як головне джерело ризику ФР, що вимагає застосування посиленої належної перевірки (EDD).

Законодавча база, що підкріплює ці вимоги (зокрема, Федеральний декрет № 20 від 2018 року та Постанова Кабінету Міністрів № 74 від 2020 року), встановлює нульову толерантність до порушень у сфері цільових фінансових санкцій. ЛФУ зобов'язані забезпечити миттєве

[6] https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_6725_VER1.pdf

застосування директив Ради Безпеки ООН згідно з Главою 7 Статуту ООН. Будь-які затримки або збої в імплементації цих вимог розглядаються як кримінальне правопорушення, що тягне за собою штрафи у розмірі не менше 50 000 дирхамів ОАЕ та позбавлення волі на строк від одного до семи років. Це перетворює управління ризиками ФР з процедурного обов'язку на питання екзистенційної безпеки для фінансових інституцій.

Протидія відмиванню коштів через торговельні операції (TBML) [7]

ОАЕ як провідний глобальний логістичний та фінансовий хаб об'єктивно піддається підвищеному ризику інтеграції незаконних доходів через механізми міжнародної торгівлі. Керівництво CBUAE щодо протидії TBML розкриває складність цього явища, наголошуючи, що фінансові установи стикаються з критичною асиметрією інформації: вони рідко мають фізичний доступ до вантажів або вичерпне розуміння всього ланцюга постачання. Ця непрозорість створює сприятливе середовище для таких типологій, як навмисне завищення або заниження фактурної вартості товарів (переміщення вартості без реального переміщення грошей), маніпуляції з описами вантажів, а також "фантомні відвантаження", коли товаросупровідні документи генеруються для фіктивних транзакцій, за якими не відбувається жодного реального руху товарів.

Категорія індикаторів TBML	Приклади "червоних прапорців"	Стратегія пом’якшення з боку ЛФУ
Товари та ціноутворення	Завищення/заниження інвойсів, відсутність незалежних цінових орієнтирів	Використання сторонніх аналітичних платформ для валідації ринкової вартості сировини
Корпоративні структури	Використання посередників без чіткої комерційної мети, компанії-оболонки	Обов'язкова EDD для визначення економічного сенсу ланцюга постачання
Документарні аномалії	"Фантомні відвантаження", маніпуляції з коносаментами	Перевірка автентичності транспортних документів через глобальні логістичні реєстри
Транзакційна поведінка	Масштабні операції за відкритим рахунком від нових клієнтів	Встановлення лімітів на не-документарне фінансування, посилений післяопераційний моніторинг

Методологічний підхід CBUAE до моніторингу торговельного фінансування вимагає від ЛФУ диференціації ризиків залежно від типу продукту. Документарне фінансування (наприклад,

[7] https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_6788_VER1.pdf

акредитиви) надає банку більше точок контролю, оскільки виплата прив'язана до надання жорстко регламентованого пакету документів. Натомість операції за відкритим рахунком (Open Account Trade) визнаються регулятором як такі, що несуть значно вищий рівень загрози. У таких транзакціях товар постачається до здійснення оплати, а товаросупровідні документи пересилаються між контрагентами напряму, оминаючи банківську систему. Роль ЛФУ зводиться до банального проведення "чистого" платежу, що унеможливлює традиційну перевірку економічної суті угоди та вимагає впровадження спеціалізованих алгоритмів поведінкового аналізу корпоративних клієнтів. Крім того, особливо вразливими визнано сектори торгівлі золотом, дорогоцінними металами та мінералами, оскільки ці товари можуть функціонувати як альтернативна форма вартості і легко піддаються фізичній трансформації (наприклад, переплавлення золотих злитків у форми, що нагадують промисловий свинець) для приховування під час митного контролю.

Для ефективної ідентифікації підозрілої діяльності CBUAE надав вичерпний перелік індикаторів ("червоних прапорців"), які ЛФУ зобов'язані інтегрувати у свої системи транзакційного моніторингу. Ці індикатори поділяються на категорії, що охоплюють аномалії у платежах (нетипові обсяги або юрисдикції), невідповідності в описі товарів (розбіжності між заявленою та ринковою вартістю), а також складнощі корпоративних структур. CDD повинна супроводжуватися жорстким посиленим вивченням у випадках використання численних підставних компаній, транзакцій через юрисдикції, що не мають виходу до моря (для морських перевезень), або залучення торговельних посередників, економічна мета присутності яких є неочевидною.

Регулятор підкреслює, що виявлення ризиків TBML не може бути статичним процесом. Від установ вимагається оперативно реагувати на затримки в обробці алертів (backlogs) та забезпечувати адекватне кадрове забезпечення підрозділів комплаєнсу для своєчасного оновлення профілів клієнтів. Якщо в процесі застосування EDD установа не здатна досягти достатнього рівня прозорості угоди або переконатися у легітимності походження коштів чи товарів, єдиним прийнятним регуляторним рішенням є застосування процедур де-рискінгу, що передбачає обмеження доступу клієнта до продуктів торговельного фінансування або повне розірвання ділових відносин.

Управління ризиками кореспондентських банківських відносин [8]

Специфіка кореспондентського банкінгу створює одні з найскладніших викликів в архітектурі ПВК/ФТ/ФР, оскільки ліцензована фінансова установа (кореспондент) відкриває свої платіжні шлюзи для транзакцій клієнтів іншого банку (респондента), фактично втрачаючи прямий контроль над процедурами онбордингу та ідентифікації кінцевих ініціаторів або отримувачів. Згідно з інструкціями CBUAE, які суворо гармонізовані з Рекомендаціями FATF 13 та 16, ЛФУ зобов'язані розробити та впровадити комплексну стратегію управління цими ризиками, яка повинна бути задокументована у формі Загальнокорпоративної оцінки ризиків (EWRA) або окремої оцінки безпосередньо для лінії кореспондентського бізнесу. Ця оцінка має безперервно аналізувати чотири критичні вектори: клієнтську базу респондента, його географічну присутність, портфель продуктів та каналів постачання послуг.

Особливе занепокоєння викликають багаторівневі архітектури, зокрема "вкладені відносини" (nested activity або downstream banking). Це ситуації, коли рахунок прямого респондента в ЛФУ використовується третіми (вкладеними) фінансовими установами або провайдерами послуг з переказу коштів (MVTS) для доступу до міжнародної фінансової системи. Керівництво визначає такі структури як фактор надзвичайно високого ризику, що вимагає "ще вищого рівня перевірки", ніж стандартні кореспондентські рахунки. Найбільшу загрозу становлять транзитні

[8] https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_6587_VER1.pdf

рахунки (payable-through accounts), які надають клієнтам респондента можливість здійснювати транзакції безпосередньо через рахунок кореспондента від свого імені. В таких сценаріях ЛФУ несе відповідальність за верифікацію того, що респондент здійснив бездоганну належну перевірку цих клієнтів і здатний надати повний пакет ідентифікаційних даних на першу вимогу CBUAE.

Процедура встановлення кореспондентських відносин позбавлена будь-яких спрощень. ЛФУ зобов'язані провести вичерпний збір інформації для розуміння природи бізнесу респондента, оцінити репутацію установи, проаналізувати її регуляторну історію на предмет попередніх розслідувань у сфері ПВК/ФТ та оцінити якість внутрішнього контрольного середовища і нагляду в юрисдикції реєстрації. Більше того, жодні відносини не можуть бути встановлені без письмового схвалення вищого керівництва ЛФУ. Абсолютною забороною є будь-яка взаємодія з банками-оболонками — установами, які не мають фізичної присутності в країні реєстрації та не належать до регульованих фінансових груп.

Тип ризику / Сценарій	Характеристика	Обов'язкові заходи контролю з боку ЛФУ
Стандартний респондент	Іноземний банк замовляє розрахункові послуги	Оцінка ризиків ВК/ФТ, збір політик ПВК/ФТ респондента, схвалення вищим керівництвом
Транзитні рахунки	Клієнти респондента мають прямий доступ до рахунку в ЛФУ	Верифікація якості CDD, проведеної респондентом, забезпечення доступу до даних
Вкладені відносини	Рахунок респондента використовується іншими банками або MVTS	Глибоке вивчення клієнтської бази респондента, моніторинг транзакцій третіх сторін
Високоризикові респонденти	Респонденти з юрисдикцій із слабким наглядом або високим рівнем корупції	Інтерв'ю з MLRO, незалежний зовнішній аудит систем респондента, обмеження транзакцій

Для пом’якшення залишкових ризиків у відносинах із високоризиковими респондентами ЛФУ повинні застосовувати EDD. Ці заходи включають не лише паперовий аудит, але й проведення глибинних інтерв'ю з керівником підрозділу комплаєнсу (MLRO) респондента, вивчення звітів внутрішнього аудиту, проведення виїзних перевірок та залучення незалежних експертів для валідації ефективності контролів. На операційному рівні ЛФУ повинні впроваджувати жорсткі обмеження: обмеження обсягів транзакцій для третіх сторін, заборону певних продуктів (наприклад, міжнародних касових листів), а також застосування вибіркового тестування

транзакцій у реальному часі для забезпечення безперервного дотримання вимог Рекомендації 16 FATF щодо супроводу електронних переказів повною інформацією про відправника та одержувача.

Належна перевірка клієнтів та ведення обліку [9]

Концепція "Знай свого клієнта" (KYC) та CDD розглядаються CBUAE як абсолютний фундамент будь-якої дієвої архітектури фінансового комплаєнсу. Сучасні регуляторні стандарти відкидають формальний підхід до ідентифікації, вимагаючи від ЛФУ переходу до глибинного динамічного профілювання. Установа повинна не просто верифікувати особу за паспортом, а сформувати цілісне розуміння суті ділових відносин, що включає детальний аналіз професійної діяльності, джерел доходу, джерел багатства, походження конкретних коштів та очікуваного патерну майбутніх транзакцій. Лише таке структуроване прогнозування дозволяє автоматизованим системам моніторингу ефективно розпізнавати девіації та генерувати алерти щодо підозрілої діяльності.

Процес ідентифікації та верифікації повинен бути стійким до складних загроз, таких як використання багаторівневих корпоративних структур або синтетичних ідентичностей. Для мінімізації людського фактору та захисту від внутрішнього шахрайства CBUAE рекомендує інтегрувати принцип "чотирьох очей" в усі операційні процедури валідації ідентифікаційних документів та їх введення в корпоративні бази даних. Працівники фронт-офісу наділяються обов'язком критично оцінювати поведінку клієнта під час онбордингу. У разі надання клієнтом недостовірної інформації, ухилення від відповідей або підозри у викраденні особистості, ЛФУ зобов'язані застосувати політику відмови в обслуговуванні та негайно ескалювати інцидент для формування звіту про підозрілу діяльність.

Вимоги до проведення CDD не обмежуються етапом встановлення ділових відносин. Регулятор чітко визначає операційні тригери, які вимагають обов'язкового застосування заходів належної перевірки: проведення разових транзакцій на суму від 55 000 дирхамів ОАЕ (як одиничних, так і серії пов'язаних операцій), здійснення електронних переказів від 3 500 дирхамів ОАЕ, а також у будь-яких випадках виникнення сумнівів щодо достовірності раніше зібраних даних або при появі найменших підозр у причетності до фінансових злочинів.

Безперервний моніторинг розглядається як життєвий цикл управління ризиками, що ґрунтується на постійній звірці фактичної транзакційної поведінки із задекларованим профілем. Цей процес поєднує періодичні перегляди досьє з перевірками, що ініціюються змінами у поведінці клієнта або зовнішніми факторами. Невід'ємною ланкою цього ланцюга є надійне збереження записів. Архітектура баз даних ЛФУ повинна гарантувати можливість ретроспективної реконструкції кожної окремої транзакції з ідентифікацією всіх залучених сторін, валют і сум. Інформація має бути надійно захищеною, але миттєво доступною для компетентних органів та аудиторів. Порушення вимог щодо ведення обліку розглядається як критичний провал, що тягне за собою адміністративні штрафи у розмірі від 50 000 до 5 000 000 дирхамів ОАЕ.

Впровадження ризик-орієнтованого підходу (РОП) [10]

Відповідно до найкращих практик CBUAE, РОП являє собою не просто статичний набір процедур, а цілісну корпоративну філософію та операційну модель, розроблену для раціонального розподілу ресурсів фінансової установи. Суть РОП полягає у відмові від неефективного підходу "one-size-fits-all" на користь таргетованого фокусування людського, технологічного та фінансового капіталу на зонах найвищої вразливості до ВК/ФТ/ФР. Структурно імплементація РОП складається з двох фундаментальних етапів: розробки глибокої

[9] https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_6593_VER1.pdf
[10] https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_6531_VER1.pdf

інституційної оцінки ризиків та подальшого розгортання архітектури контролів, математично пропорційної виявленим загрозам.

Методологія оцінювання вимагає від ЛФУ чіткої послідовності аналітичних дій. Первинним кроком є калькуляція "невід'ємного ризику" (Inherent Risk) — рівня загрози, притаманного самій бізнес-моделі установи за відсутності будь-яких засобів контролю. Цей показник розраховується на основі щонайменше чотирьох макро-векторів: профілю клієнтської бази, специфіки продуктів та послуг, ризиків транзакційних каналів (наприклад, дистанційне обслуговування) та географії ринків присутності. Наступним кроком є критичне тестування операційної ефективності існуючої системи внутрішнього контролю (Control Framework). Завершальний розрахунок визначає "залишковий ризик" (Residual Risk) — ту частку загрози, яку не змогли нівелювати наявні фільтри ПВК/ФТ. Саме рівень залишкового ризику безпосередньо диктує управлінські рішення щодо застосування спрощених, стандартних або посилених заходів контролю.

Регулятор наголошує на принципі пропорційності: архітектура моделі оцінювання повинна ідеально відповідати масштабам та складності ЛФУ. Якщо локальні обмінні пункти можуть ефективно використовувати стандартизовані ризик-матриці та чек-листи, то глобальні фінансові конгломерати зобов'язані інвестувати у складні статистичні моделі, здатні агрегувати дані з різних бізнес-ліній в єдиний консолідований корпоративний звіт (enterprise-level report).

Етап імплементації РОП	Опис процесу	Очікуваний результат / Дія
1. Ідентифікація притаманного ризику	Аналіз клієнтів, продуктів, географії та каналів надання послуг.	Формування мапи первинних загроз, притаманних бізнес-моделі ЛФУ.
2. Оцінка середовища контролю	Аудит ефективності IT-систем, політик CDD/EDD, якості моніторингу та персоналу.	Виявлення "сліпих зон" та недоліків у процесах комплаєнсу.
3. Визначення залишкового ризику	Математичне обчислення ризику, що залишається після застосування контролів.	Калібрування системи: застосування EDD або SDD.
4. Корпоративне управління	Документування результатів, затвердження радою директорів.	Формальне прийняття ризику (risk acceptance) або рішення про де-рискінг.

Найкритичнішим елементом успішної імплементації РОП є чітка структура корпоративного управління та підзвітності. Незважаючи на те, що технічне виконання та моделювання оцінки делегується керівнику підрозділу комплаєнсу (MLRO), абсолютним власником ризику є

виключно Рада директорів, засновники та вище керівництво ЛФУ. Вони несуть повну відповідальність за визначення корпоративного ризик-апетиту та формальне затвердження інституційної оцінки, що унеможливлює перекладання відповідальності виключно на комплаєнс-підрозділ у разі виявлення системних збоїв регулятором.

Впровадження рольового навчання з ПВК/ФТ/ФР [11]

Перехід фінансового сектору ОАЕ до інтелектуальних ризик-орієнтованих моделей комплаєнсу диктує необхідність докорінної трансформації філософії корпоративного навчання. CBUAE категорично відходить від практики універсальних, формальних тренінгів, запроваджуючи парадигму багаторівневого рольового навчання (Role-Based Training). Ефективна програма повинна формувати комплексну екосистему знань, що інтегрує шість основних модулів: вступний курс для нових співробітників, щорічні загальнокорпоративні сесії, глобальні стандарти (для міжнародних груп), вузькоспеціалізовані локальні тренінги, стратегічні сесії для Ради директорів та, найважливіше, рольові програми безпосередньо на робочому місці, адаптовані до конкретного ризик-профілю посади. Технічний контент цих програм повинен безперервно актуалізуватися, відображаючи зміни в нормативній базі ОАЕ, міжнародних стандартах FATF, типологіях фінансових злочинів та продуктовому портфелі самої ЛФУ.

Методологія визначення цільової аудиторії суворо базується на концепції "Трьох ліній захисту", вимагаючи глибокої диференціації навчального матеріалу. Перша лінія (менеджери по роботі з клієнтами, касири) перебуває на вістрі атаки і потребує інтенсивних тренінгів з поведінкового аналізу та ідентифікації прихованих "червоних прапорців". Друга лінія (комплаєнс та MLRO) вимагає фокусу на методології проведення розслідувань, складних процедурах EDD та структуруванні звітності для фінансової розвідки. Третя лінія (незалежний аудит) має спеціалізуватися на методиках тестування ефективності контрольного середовища. Окремо CBUAE виокремлює критично важливу групу — технічний персонал та спеціалістів з даних (Data Scientists). Їхня підготовка повинна концентруватися виключно на алгоритмічній логіці, тестуванні, налаштуванні (tuning) та валідації комплаєнс-систем, оскільки помилки в архітектурі моделей моніторингу призводять до системного пропуску загроз.

Ефективність навчальної екосистеми визначається її динамічністю. ЛФУ

Висновки:

- **Стратегічна реорганізація управління ризиками:** Рішення Ради директорів щодо прийняття ризиків та визначення ризик-апетиту повинні спиратися на формалізовані математичні моделі залишкового ризику та бути юридично задокументованими, з огляду на нові норми щодо персональної кримінальної відповідальності.
- **Технологічна інтеграція процесів:** Установи повинні впровадити спеціалізовані аналітичні алгоритми для перевірки не-документарного торговельного фінансування та ідентифікації товарів подвійного призначення, оскільки стандартні системи транзакційного скринінгу не здатні виявляти загрози ФР та TBML.
- **Глибокий аудит кореспондентських зв'язків:** Наявність вкладених рахунків або транзитних рахунків вимагає проведення обов'язкових виїзних або дистанційних глибинних аудитів комплаєнс-культури банку-респондента до моменту надання доступу до клірингової інфраструктури ЛФУ.
- **Адаптивна екосистема навчання:** HR-процеси ЛФУ мають бути синхронізовані з комплаєнс-вимогами для автоматичного призначення вузькопрофільних навчальних модулів (зокрема для алгоритмічних валідаторів та data scientists) при кожній ротації персоналу або зміні ризик-профілю продуктового портфеля.

[11] https://rulebook.centralbank.ae/sites/default/files/en_net_file_store/CBUAE_EN_6530_VER1.pdf

зобов'язані переглядати матеріали щонайменше раз на рік, або частіше — у разі змін бізнес-моделі (впровадження нових технологій), оновлення результатів НОР або виявлення прогалин під час регуляторних перевірок. Інноваційною вимогою є впровадження індивідуальних тригерів для призначення позачергового навчання. До таких ситуацій належать внутрішні ротації персоналу на нові посади, поява специфічних індикаторів ризику в конкретних бізнес-лініях, або ж зафіксовані факти порушення співробітником процедур комплаєнсу (наприклад, випадкове розголошення клієнту факту проведення розслідування — "tipping off"). Для забезпечення зворотного зв'язку CBUAE створив спеціальну електронну скриньку, яка дозволяє ЛФУ консультуватися щодо ефективності своїх навчальних програм та отримувати таргетовані роз'яснення від регулятора.

Новий венесуельський гірничий закон: лібералізація, старі схеми та небезпека «брудного золота» [12]

У квітні 2026 року Венесуела здійснила, на перший погляд, довгоочікуваний та прагматичний крок, ухваливши новий Органічний закон про шахти (Ley Orgánica de Minas). Цей документ, який 9 квітня одностайно підтримала Національна асамблея, мав би символізувати розрив із неефективним та ізоляціоністським минулим. Він скасовує норми 1999 року, що забороняли приватне та іноземне інвестування в розробку стратегічних корисних копалин, передусім золота.

Політичне тло ухвалення закону є не менш драматичним: ще 3 січня 2026 року Сполучені Штати Америки захопили та усунули від влади Ніколаса Мадуро, що докорінно змінило геополітичний баланс. Вашингтон не лише послабив санкції, запроваджені проти венесуельської золотодобувної галузі ще у 2019 році, але й видав спеціальну ліцензію на імпорт золота від державної компанії Minerven (Compañía General de Minería de Venezuela). Міжнародні сировинні трейдери вже шикуються в чергу, щоб інвестувати в золотий потенціал країни.

Здавалося б, перед нами класична історія успіху — відкриття ринку, залучення капіталу, економічне відродження. Однак, якщо заглибитися в текст самого закону, стає очевидним, що цей нормативний акт не стільки вирішує системні проблеми, скільки консервує їх під новою, більш привабливою для інвесторів вивіскою.

Щоб зрозуміти глибину проблеми, варто спочатку детально розглянути те середовище, в якому функціонуватиме новий закон. Венесуела — країна, багата на мінеральні ресурси, але її золотодобувна промисловість десятиліттями була оточена корупцією, насильством та безкарністю. Згідно з даними InSight Crime, переважна більшість венесуельського золота походить не з легальних рудників, а з неформальних, а точніше — кримінальних, копалень, які контролюються збройними угрупованнями. Головний осередок видобутку — так званий Гірничорудний пояс Оріноко (Arco Minero del Orinoco, AMO), створений декретом Мадуро у 2016 році. Це величезна територія, що охоплює переважно штат Болівар, а також частини Амасонасу та Дельта-Амакуро. Саме тут, у джунглях та на берегах річок, діють справжні кримінальні імперії. Збройні групи, включно з Армією національного визволення (ELN), а також фракції колишніх FARC, наприклад угруповання Акасіо Медіни (Acacio Medina Front), контролюють цілі операції в Амасонасі та частині Болівару. Поряд із ними діють дрібніші, але не менш жорстокі банди, відомі як синдикати (sindicatos) — серед них Організація R (Organización R) та «Трен де Гуаяна» (Tren de Guayana). Вони контролюють окремі копальні, постачають

[12] https://iusdata.com/wp-content/uploads/2026/03/Proyecto-LEY-ORGANICA-MINAS-MAR26.pdf

робочу силу та, що найважливіше, виконують функції квазіурядових органів на території АМО. Це не маргінальні гравці — це основні постачальники золота.

Найбільш шокуючим є не просто існування цих угруповань, а їхній симбіоз із державою. Як наголошують журналісти, сьогодні держава здійснює контроль над АМО саме через тісну співпрацю з кримінальними групами. Державні гірничі компанії, зокрема Minerven (яка тепер є частиною більшої структури — Венесуельської гірничої корпорації, CVM), регулярно отримують золото з рудників або збагачувальних фабрик, що перебувають під контролем озброєних формувань.

Крім того, існує практика так званих «стратегічних альянсів» (alianzas estratégicas) — договорів, які держава укладає з політично пов'язаними особами або високопосадовцями військового відомства. Ці альянси отримують дозволи на видобуток, доступ до державної техніки та пального, а потім фактично координують свою роботу з тими ж синдикатами. Озброєні банди виконують чорнову роботу, забезпечують безпеку та охорону, а держава через підставних осіб легалізує результат. Цей замкнений ланцюг десятиліттями годував корупційні схеми та дозволяв вимивати капітал. І ось тепер на цей ґрунт падає новий закон.

Погляньмо, що саме пропонує новий Органічний закон про шахти.

На перший погляд, він справляє враження прогресивного документа, написаного в дусі сучасного ресурсного лібералізму. Стаття 6 закріплює принципи, згідно з якими гірничі роботи мають виконуватися «науково та раціонально», з урахуванням сталого розвитку, охорони довкілля та територіального планування. Стаття 47 категорично забороняє використання речовин, що забруднюють навколишнє середовище.

Закон створює потужну інституційну структуру: передбачено створення Національного банку геологічних даних (стаття 12), Національної гірничої охорони як допоміжного органу (стаття 13), Управління з гірничої діяльності SUNAMIN (стаття 11) та Національного гірничого фонду (стаття 20). Останній, згідно зі статтею 21, має спрямовувати кошти на «продуктивний розвиток золота та стратегічних мінералів, соціальний розвиток громад, соціальне забезпечення гірників, а також захист навколишнього середовища». При цьому стаття 22 встановлює, що до фонду надходить 1% від валового видобутку за концесійними контрактами та 0,5% для середньої та дрібної промисловості. Здавалося б, ось воно — сучасне, соціально відповідальне та екологічне законодавство.

Проте справжня суть закону розкривається не в деклараціях, а в його прогалинах та структурних особливостях. Головна вада полягає в тому, що закон фактично не пропонує механізмів демонтажу існуючої корупційної системи. Він не розриває зв'язок між державою та кримінальними групами, а навпаки — створює нову юридичну форму, яка може бути легко використана для їхньої легалізації.

Йдеться про статті 77-79 та запровадження «гірничих бригад» (Brigadas Mineras). Ці бригади визначаються як асоціації осіб, що займаються кустарним (artesanal) та дрібним видобутком, які отримують «сертифікат видобування» (Certificado Minero) на тимчасовій основі. Закон детально описує процедуру створення бригад, їхні пільги (податкові стимули, фінансування, навчання) та навіть обмеження. Однак він не містить жодної норми, яка б регулювала долю вже існуючих «стратегічних альянсів» — тих самих, де кримінальні синдикати виступають партнерами держави. Більше того, закон жодним чином не пропонує критеріїв відокремлення законних гірників від озброєних банд. У реальності Венесуели будь-який ватажок синдикату може зареєструвати «бригаду», номінально передавши управління підставним особам, і отримати легальний доступ до дозволів, палива, техніки та ринків збуту. Фактично, закон легітимізує низовий рівень злочинної ієрархії, не пропонуючи жодних інструментів контролю за реальним бенефіціарним власником або джерелами зброї та робочої сили.

Друга фундаментальна проблема закону — контролюючий орган, якому доручено нагляд за цією складною системою. Стаття 14 проголошує, що функцію Національної гірничої охорони здійснюватиме Міністерство оборони через Боліваріанську національну гвардію. Саме ця структура впродовж останніх років неодноразово звинувачувалася міжнародними та місцевими правозахисними організаціями в участі в незаконному видобутку, поборах з неформальних шахтарів та прямій корупції. Гвардійці часто виступали не як переслідувачі злочинних синдикатів, а як їхні охоронці або навіть партнери в розподілі прибутків.

Доручити тій самій силі, яка десятиліттями була частиною проблеми, тепер контролювати виконання закону — це означає залишити контроль суто номінальним. Закон не передбачає жодних механізмів цивільного нагляду, не створює незалежних інспекційних органів, не запроваджує обов'язкових процедур аудиту самих контролерів. Більше того, стаття 18 залишає розробку детальних норм організації та функціонування гвардії в цій ролі на майбутній регламент (який має бути прийнятий протягом 180 днів). Таким чином, закон відкладає найбільш чутливі питання на потім, але вже зараз визначає головного виконавця — структуру з кримінальною репутацією.

Третій аспект — це небезпечна лібералізація для іноземних інвесторів без відповідних механізмів належної перевірки (due diligence). Стаття 9 закону дозволяє включати в контракти положення про вирішення спорів через міжнародний арбітраж та медіацію, що є стандартною вимогою великих транснаціональних корпорацій. Стаття 94 звільняє інвесторів від низки місцевих податків — на великі статки, внесків на науку, спорт, боротьбу з наркотиками, захист пенсій, а також повністю скасовує будь-які місцеві (штатні або муніципальні) податки. Це надзвичайно щедрі умови, покликані залучити капітал.

Однак водночас стаття 34 наділяє Центральний банк Венесуели виключним переважним правом купівлі всього видобутого золота, а держава через Міністерство шахт визначає умови експорту. Інвестор змушений продавати золото державному монополісту або отримувати його дозвіл на експорт. У цьому ланцюгу повністю відсутні вимоги щодо прозорості походження металу. Немає жодної статті, яка б зобов'язувала концесіонера або покупця перевіряти, чи не походить золото з рудників, контрольованих ELN, FARC або іншими угрупованнями, внесеними до міжнародних санкційних списків. Немає механізмів сертифікації «чистого золота», які є обов'язковими в багатьох юрисдикціях, включаючи країни ЄС та США. Це означає, що міжнародний інвестор, купуючи золото за новим законом, несе повний ризик репутаційних та юридичних наслідків, пов'язаних із фінансуванням збройних конфліктів. Адже ланцюг постачання від копальні до покупця проходить через ті самі «стратегічні альянси» та синдикати, яких новий закон не скасував.

Четвертий аспект — екологічні ризики та потенційне знищення заповідних територій. Попри те, що закон проголошує «екологічний гірничий розвиток» (Desarrollo Minero Ecológico) у статті 8, стаття 32 надає президенту країни право оголошувати будь-які золотоносні або інші стратегічні райони «зонами безпеки» (Zonas de Seguridad). Режим такої зони визначатиметься спеціальним декретом, який може скасувати звичайні природоохоронні обмеження. Враховуючи, що більша частина нелегального видобутку відбувається саме в заповідних територіях Амасонасу та Дельта-Амакуро, ця норма створює юридичний механізм для їхньої повної відкритої розробки. Замість боротьби з вторгненням у національні парки, держава отримує можливість легалізувати це вторгнення постфактум.

Стаття 52 забороняє видобуток у населених пунктах, на цвинтарях, священних землях, водосховищах, річках, каналах та територіях з особливим природоохоронним режимом, але з однією важливою умовою: «за винятком випадків, коли Міністерство шахт дозволить дослідницькі роботи». Це виняток, який з легкістю може стати правилом. На практиці, через відсутність незалежного екологічного контролю, «дослідження» можуть легко перетворитися

на промисловий видобуток. І хоча стаття 115 подвоює штрафи за незаконну діяльність у природоохоронних зонах, а стаття 116 встановлює тюремне ув'язнення від 10 до 15 років для таких випадків, ефективність цих санкцій дорівнює нулю в умовах, коли суди підконтрольні виконавчій владі, а правоохоронна система є частиною корупційного ланцюга.

П'ятим важливим спостереженням є питання власності на інфраструктуру та правової визначеності. Стаття 28 встановлює, що всі системи, споруди, дороги, залізниці, збагачувальні фабрики, обладнання, машини, створені або придбані концесіонером, після припинення дії прав переходять у власність Республіки без жодної компенсації, вільними від будь-яких обтяжень. Це жорстка умова, яка може відлякувати довгострокових інвесторів, адже вони фактично будують інфраструктуру для держави за власний кошт без права продажу або відшкодування залишкової вартості. Стаття 57 проголошує концесії та ліцензії передаваними за попереднім повідомленням міністерства, але стаття 64 додає, що контракт є неподільним, а часткові переуступки не мають сили щодо держави. Це створює ризики для синдикованих інвестиційних структур.

Стаття 71 містить перелік посадовців, яким заборонено отримувати гірничі права — від президента та віцепрезидентів до депутатів, суддів, губернаторів, мерів та навіть посадовців міністерств шахт та довкілля. Ця заборона поширюється на подружжя, співмешканців та родичів до четвертого ступеня споріднення. Здавалося б, потужна антикорупційна норма. Однак на практиці вона легко обходиться через підставних осіб, компанії-оболонки, друзів або відтерміновані виплати. Крім того, заборона діє лише п'ять років після звільнення з посади, що створює стимули для відкладеної корупції. Головне ж — закон не створює органу, який би реально перевіряв кінцевих бенефіціарів. Реєстр єдиного гірничого запису (RUM), створений статтею 86, не передбачає публічного розкриття інформації про власників.

Не можна оминути й фіскальний аспект. Стаття 89 встановлює максимальну ставку роялті у 13% від валового видобутку, але точний розмір визначатиметься міністерством залежно від типу мінералу, умов розробки, обсягу інвестицій, ринкової вартості та навіть планів соціального розвитку. Це надає міністерству величезний дискреційний простір, що створює ризики для вибіркового застосування та корупції. Інвестор ніколи не знає наперед, яку ставку йому встановлять. Стаття 92 вводить деталізовану таблицю поверхневого податку (від 0,5 до 5,5 умовних одиниць за гектар залежно від року та площі), а також податку на видобуток у розмірі 3% для золота, срібла та платини, 4% для діамантів та 3% для інших копалин. Примітно, що податок на видобуток для золота застосовується до комерційної вартості рафінованого металу, що є доволі звичним. Однак стаття 93 нагадує про старий інструмент контролю: машини та обладнання, ввезені з податковими пільгами, не можна продавати або вивозити без дозволу держави. Це зберігає важіль тиску на інвестора.

Показовим є також підхід до кримінальної відповідальності. Стаття 116 передбачає позбавлення волі на строк від 6 місяців до 10 років за здійснення первинних, допоміжних або супутніх видобувних робіт без відповідних контрактів чи дозволів. Якщо ж ця діяльність ведеться на території з особливим природоохоронним режимом, термін зростає до 10–15 років. Це суворі санкції, які на папері виглядають грізно. Крім того, стаття 117 наказує конфіскувати всі стратегічні мінерали, отримані незаконним шляхом, і передавати їх до Центрального банку для зарахування до міжнародних резервів. Це створює парадоксальну ситуацію: держава поповнює свої резерви за рахунок конфіскованого «брудного золота», не несучи жодної відповідальності за ланцюг його походження. Це нагадує легалізацію злочинних доходів на найвищому рівні.

Отже, новий Органічний закон про шахти Венесуели 2026 року є глибоко суперечливим документом. Він, безперечно, знімає багато формальних бар'єрів для входу приватного та іноземного капіталу, пропонує ліберальний податковий режим, створює інституційну структуру,

яка імітує сучасне гірниче регулювання, і навіть декларує турботу про екологію та місцеві громади.

Для зовнішнього спостерігача це може виглядати як успішний перехід до відкритої ринкової економіки після падіння режиму Мадуро. Але він не чіпає корінь проблеми — симбіоз державних інституцій, військових та збройних злочинних угруповань, які десятиліттями ділили золотий потік. Він не пропонує реального механізму очищення ланцюга постачання від «брудного золота». Він замінює термін «стратегічний альянс» на «гірнича бригада», але не змінює суті — ті самі люди, ті самі банди, та саме золото.

Для міжнародних інвесторів, які зважаться на роботу в таких умовах, це означає прийняття величезного репутаційного, юридичного та морального ризику. Купуючи венесуельське золото, вони ризикують фінансувати ELN, залишки FARC та інші угруповання, визнані терористичними в багатьох країнах світу. І жодна стаття нового закону не захистить їх від цього ризику. Справжня реформа потребувала б не зміни законів, а зміни політичної культури, демілітаризації гірничої промисловості, створення незалежних судів та реальної громадянської верифікації. Натомість Венесуела отримала черговий акт, який може законсервувати минуле під вивіскою майбутнього.

Регулювання стейблкоїнів у США: аналіз нових вимог FinCEN та OFAC [13]

Міністерство фінансів Сполучених Штатів, об'єднавши зусилля двох своїх ключових підрозділів — Мережі боротьби з фінансовими злочинами (FinCEN) та Управління з контролю за іноземними активами (OFAC) — оприлюднило спільний проєкт нормативно-правових актів, який докорінно змінює правила гри для емітентів платіжних стейблкоїнів. Цей крок став прямим наслідком ухвалення Закону GENIUS (Guiding and Establishing National Innovation for U.S. Stablecoins Act), який створив законодавчу базу для федерального регулювання платіжних стейблкоїнів. Тепер, через низку деталізованих підзаконних актів, ця база наповнюється реальним змістом, і цей зміст виявився набагато жорсткішим, ніж очікувало багато учасників ринку.

Найбільш фундаментальна зміна полягає в офіційному та беззастережному визнанні емітентів дозволених платіжних стейблкоїнів (Permitted Payment Stablecoin Issuers, PPSI) фінансовими установами. Це не просто символічний жест або формальне перейменування. Відтепер на ці організації поширюється вся повнота Закону про банківську таємницю (Bank Secrecy Act), а також усі федеральні закони, що стосуються економічних санкцій, запобігання відмиванню грошей, ідентифікації клієнтів та належної перевірки. Іншими словами, стейблкоїн-платформи більше не можуть вважати себе «сірою зоною» або технологічними стартапами з підвищеними ризиками — вони стають рівноправними (і рівновідповідальними) учасниками традиційної банківської системи.

Найбільш промовистою ілюстрацією цієї нової реальності є норма про цивільну відповідальність: за кожен день недотримання ефективних санкційних програм передбачено штраф у розмірі до 100 000 доларів США. Уявімо собі емітента, який ігнорує свої зобов'язання протягом місяця — потенційний штраф сягатиме трьох мільйонів доларів, що для багатьох середніх платформ є фінансово нищівним. Цей потужний стримувальний механізм сигналізує

[13] https://www.govinfo.gov/content/pkg/FR-2026-04-10/pdf/2026-06963.pdf

ринку про нульову толерантність регулятора до порушень у сфері протидії відмиванню грошей (AML) та фінансуванню тероризму (CFT).

Але штрафи — це лише вершина айсберга. Документ містить детальну, багатошарову структуру вимог, які охоплюють усі аспекти діяльності емітента: від внутрішньої організації комплаєнсу до технічних можливостей блокування транзакцій та багаторічного зберігання записів. Перший рівень цієї структури стосується внутрішньої архітектури програми дотримання вимог. Кожен PPSI зобов'язаний розробити та підтримувати письмову програму AML/CFT, яка має бути затверджена радою директорів або вищим керівним органом. Це означає, що комплаєнс перестає бути справою «галочок» або другорядною функцією — він підноситься до рівня стратегічного пріоритету, який особисто затверджується найвищим керівництвом. Крім того, емітент має призначити окремого посадовця, відповідального за щоденну координацію та моніторинг програми. Ця особа повинна фізично перебувати на території Сполучених Штатів, не мати судимостей за тяжкі фінансові злочини та мати реальні важелі впливу всередині організації. Така вимога створює чітку, юридично фіксовану лінію підзвітності: у разі порушення регулятор точно знатиме, до кого ставити запитання.

Важливо, що програма комплаєнсу не може бути статичним документом, який розробляється один раз і зберігається на полиці. Регулятор прямо наголошує, що вона має бути «активною, еволюціонуючою структурою». Це означає, що емітент зобов'язаний постійно виділяти ресурси на підтримку комплаєнс-функції. Складність програми має відповідати ризик-профілю емітента: чим більший емітент, тим глибшою та деталізованішою має бути його програма. Регулятор особливо наголошує, що очікування щодо комплаєнсу мають бути сфокусовані на ефективності, а не на формальному виконанні приписів. Іншими словами, регулятор хоче бачити реальне зменшення ризиків, а не просто красиві звіти.

Другий критичний блок нових вимог стосується оцінки ризиків та належної перевірки клієнтів (Customer Due Diligence, CDD). Документ вимагає проведення глибоких, а не поверхневих або формальних оцінок ризиків відмивання грошей та фінансування тероризму. Емітент повинен оцінювати ризики, пов'язані з кожним конкретним продуктом, послугою, типом клієнта та географічним регіоном, де він працює. Це означає, що недостатньо просто сказати «ми перевіряємо всіх клієнтів». Потрібно зрозуміти, які саме вразливості можуть використати зловмисники: чи можна через платформу обходити санкції, чи використовувати її для конвертації незаконних коштів, чи здійснювати транзакції в юрисдикціях з високим рівнем корупції. Особливу увагу приділено вимозі оновлювати ці оцінки щоразу, коли відбуваються суттєві зміни в бізнес-операціях або профілі ризику. Якщо емітент запускає новий продукт, виходить на новий ринок або навіть проводить злиття чи поглинання, він зобов'язаний зупинитися, переоцінити свої ризики та, за потреби, скоригувати комплаєнс-програму.

Процедури належної перевірки клієнтів зазнали найбільш драматичних змін. Більше не достатньо просто зібрати ім'я та електронну адресу. Емітенти зобов'язані верифікувати особу клієнта за допомогою незалежних, надійних джерел документів або даних. Це означає, що потрібно перевіряти паспорти, водійські права, інші офіційні ідентифікатори. Емітент повинен мати «розумну впевненість», що він знає справжню особу кожного клієнта. Далі, потрібно розуміти природу та мету ділових відносин, розробити профіль клієнта, який дозволяє відрізняти нормальну активність від підозрілої. Для клієнтів-юридичних осіб (компаній, фондів, трастів) емітент зобов'язаний ідентифікувати кінцевих бенефіціарних власників — фізичних осіб, які фактично контролюють або володіють юридичною особою. Це спрямовано на закриття однієї з найбільших вразливостей глобальної фінансової системи: використання підставних компаній, складних корпоративних структур та анонімних рахунків для приховування незаконної діяльності.

Моніторинг транзакцій має бути безперервним, із особливим фокусом на великі перекази та активність, яка виглядає невідповідною до відомого профілю клієнта. Системи моніторингу повинні бути досить складними, щоб виявляти патерни поведінки, які свідчать про структурування (structuring) — спроби клієнта розбити велику суму на багато дрібних транзакцій, щоб уникнути порогів звітування. Документ рекомендує автоматизацію цих систем, але наголошує на обов'язковому людському контролі. Автоматизація ефективна для виявлення простих патернів та великих обсягів даних, але складну або незвичну поведінку має інтерпретувати навчений фахівець. Це баланс між ефективністю та глибиною аналізу.

Третій ключовий елемент пропозиції — це механізми правозастосування та нагляду, які перетворюють правила з декларацій на реальність. FinCEN отримує повноваження вживати формальних або неформальних заходів у разі невідповідності. Якщо в емітента виявлено системну неспроможність впровадити ефективну програму або якщо під час перевірок знайдено матеріальні недоліки, можуть бути застосовані значні наглядові заходи.

Але найцікавішим є делегування наглядових повноважень первинним федеральним регуляторам платіжних стейблкоїнів — зокрема Управлінню контролера грошового обігу (OCC) та Федеральній резервній системі. Це визнання того, що ринок стейблкоїнів є надто складним і технологічно специфічним, щоб його контролювала лише одна агенція. Такий багатоагентський підхід дозволяє використовувати спеціалізовані знання OCC у сфері платіжних систем та ліквідності, а також глибоку експертизу Федеральної резервної системи в моніторингу системних ризиків. Це зменшує ризик регуляторних прогалин, коли емітент може опинитися між юрисдикціями різних регуляторів.

Окремою вимогою є незалежне тестування програм комплаєнсу. Це не внутрішня аудиторська перевірка, яку можна провести «для галочки». Тестування має проводитися кваліфікованими внутрішніми або зовнішніми особами, які є незалежними від функції комплаєнсу, що перевіряється. Іншими словами, не можна, щоб комплаєнс-офіцер перевіряв сам себе. Цей незалежний погляд слугує другим рівнем захисту, виявляючи слабкі місця, які могли бути пропущені внутрішньою командою. Тести мають охоплювати всі аспекти AML/CFT та санкційних програм, включно з ефективністю програмного забезпечення для моніторингу транзакцій та адекватністю навчання персоналу. Якщо виявлено недоліки, емітент зобов'язаний створити план виправлення з чіткими термінами вирішення проблем. Результати цих аудитів мають бути задокументовані та передані вищому керівництву для вжиття необхідних заходів.

Надзвичайно важливим є правило про зберігання записів: мінімум десять років. Це вдвічі більше за стандартний п'ятирічний термін для багатьох інших фінансових операцій. Така глибина архівації є не випадковою. Вона необхідна для складних розслідувань, які можуть розгортатися роками, особливо у справах про фінансування тероризму або складні санкційні схеми. Слідчі повинні мати змогу відстежити ланцюжок транзакцій через роки, отримати історичний контекст та побудувати доказову базу, яка витримає юридичну перевірку.

Санкційний компонент пропозиції є не менш деталізованим та суворим. Емітенти зобов'язані впровадити ефективну програму дотримання санкцій, яка складається з п'яти ключових елементів. Перший — зобов'язання вищого керівництва: senior management має особисто затвердити програму, забезпечити її ресурсами, інтегрувати в операційну діяльність та регулярно отримувати звіти про ризики та результати тестувань. Другий — оцінка ризиків, яка має проводитися на регулярній основі та враховувати нові продукти, злиття, поглинання та будь-які виявлені порушення. Третій — внутрішній контроль, включно з технічними можливостями ідентифікувати, блокувати та/або відхиляти транзакції, які можуть порушувати або порушують санкції США. Це стосується всієї діяльності, пов'язаної зі стейблкоїнами, як на первинному, так і на вторинному ринках. Четвертий — незалежне тестування та аудит, яке має бути підзвітним вищому керівництву та мати достатньо ресурсів, експертизи та повноважень

для виявлення слабких місць. П’ятий — навчання, яке має проводитися принаймні раз на рік, бути адаптованим до ролі кожного співробітника та оновлюватися з урахуванням результатів оцінок ризиків та аудитів.

Особливу увагу приділено скринінгу транзакцій та клієнтів проти списків OFAC. Емітент зобов’язаний перевіряти всі транзакції та всіх клієнтів на предмет співпадінь з особами, організаціями та країнами, які перебувають під санкціями. Будь-яке співпадіння має бути негайно розслідуване. У разі підтвердження, активи мають бути заблоковані або заморожені, а про це — повідомлено відповідні органи влади. Це не просто рекомендація, а пряма юридична вимога.

Документ навіть заохочує використання інноваційних технологій, зокрема штучного інтелекту та передової аналітики блокчейну, для підвищення ефективності скринінгу. Це свідчить про те, що регулятор готовий схвалювати нові інструменти, якщо вони підвищують безпеку системи.

У ширшому контексті цей регуляторний крок має глибокі геополітичні та економічні наслідки. Стейблкоїни, особливо номіновані в доларах США, стають критичним мостом між традиційною доларовою системою та новою цифровою економікою. Вони використовуються для міжнародних переказів, торгівлі, децентралізованих фінансів. Дозволити цьому мосту бути вразливим до зловживань означає створити гігантську діру в глобальній фінансовій системі. Тому інтеграція стейблкоїнів у федеральний регуляторний периметр є життєво необхідним кроком для модернізації фінансової системи США для двадцять першого століття. Це визнання того, що цифрові активи не є тимчасовим трендом, а стали невід'ємною частиною фінансового ландшафту, і вони мають працювати за тими ж правилами, що й традиційні.

Документ також підкреслює важливість співпраці між державним і приватним секторами. Регулятор не збирається діяти лише як караючий орган. Навпаки, він заохочує емітентів впроваджувати інноваційні технології для виявлення та запобігання фінансовим злочинам. Він обіцяє залишатися гнучким, дозволяючи впровадження нових інструментів скринінгу на основі штучного інтелекту.

Надаючи чіткий правовий статус для дозволених платіжних стейблкоїнів, уряд, по суті, легітимізує новий клас активів, але одночасно оточує його необхідними запобіжниками. Цей баланс між легітимізацією та регулюванням є наріжним каменем стратегії Міністерства фінансів США щодо сприяння американському фінансовому лідерству в цифрову епоху.

Підсумовуючи, запропоновані правила є не просто черговим регуляторним оновленням або технічним коригуванням. Це фундаментальна перебудова всього правового поля для стейблкоїнів у

Висновки:

- **Емітенти платіжних стейблкоїнів (PPSI) відтепер прирівнюються до фінансових** установ з усіма зобов'язаннями за Законом про банківську таємницю та санкційними програмами, що ліквідує «сіру зону» для цифрових активів.
- **Рекордні штрафи та десятирічне зберігання даних.** Недотримання санкційних вимог карається штрафом до $100 000 за кожен день порушення, а всі записи про транзакції мають зберігатися щонайменше 10 років — вдвічі довше за стандартні вимоги.
- **Тотальна верифікація та розкриття бенефіціарів.** Простий збір імен та адрес більше не працює — емітенти зобов'язані перевіряти клієнтів через незалежні джерела, ідентифікувати кінцевих бенефіціарних власників юридичних осіб та здійснювати безперервний моніторинг транзакцій.
- **Багатоагентський нагляд із делегуванням повноважень.** FinCEN та OFAC передають частину наглядових функцій OCC та Федеральній резервній системі, створюючи комплексну систему контролю, яка унеможливлює регуляторні прогалини.

Сполучених Штатах. Вони встановлюють безпрецедентно високу планку вимог до комплаєнсу, санкційної відповідності, належної перевірки клієнтів та технічних можливостей. Вони перетворюють стейблкоїн-платформи з відносно вільно регульованих технологічних підприємств на повноцінних суб'єктів фінансової системи з усіма супутніми обов'язками, ризиками та відповідальністю.

Цей крок, ймовірно, стане зразком для інших юрисдикцій, які спостерігають за розвитком подій у США. Він остаточно закріплює принцип, який багато років обговорювався, але ніколи не був реалізований так послідовно: «та ж діяльність — ті ж ризики — ті ж правила» для цифрових і традиційних активів. Перехід до цієї нової рамки вимагатиме від емітентів значних зусиль, ресурсів та, можливо, болючих змін у бізнес-моделях. Але, як наголошує сам документ, довгострокові вигоди безпечного, прозорого та надійного ринку значно переважають початкові витрати.

Звіти окремих інституцій та експертів

Корпоративна прозорість під загрозою: як США та Європа демонтують механізми боротьби з прихованими активами [14]

Упродовж останнього десятиліття світове співтовариство поступово вибудовувало систему стримування для тих, хто ховає статки за лабіринтами офшорних компаній, трастів та номінальних директорів. Викриття, здійснені в межах численних розслідувань, стали тими поштовхами, які змусили законодавців у Вашингтоні та Брюсселі запровадити безпрецедентно жорсткі правила розкриття кінцевих бенефіціарних власників (КБВ).

Однак сьогодні світ спостерігає тривожний, майже драматичний розворот. Замість того, щоб зміцнювати прозорість, ключові гравці – Сполучені Штати та Європейський Союз – почали демонтувати власні ж захисні механізми, створюючи небезпечний прецедент для решти світу.

Почнемо зі Сполучених Штатів, де події розгортаються з драматичною швидкістю та відкритою політичною боротьбою. У грудні 2020 року було ухвалено Закон про корпоративну прозорість (Corporate Transparency Act, CTA) – історичну, двопартійну норму, яка вперше в американській історії зобов’язувала американських підприємців та власників бізнесу розкривати справжніх власників своїх компаній перед урядом. Цей закон став прямою відповіддю на міжнародний тиск після гучних витоків даних. Його метою було припинити використання підставних фірм для торгівлі наркотиками, ухилення від сплати податків, фінансування тероризму та інших тяжких злочинів. До того моменту Делавер, Вайомінг та інші штати десятиліттями слугували «раєм для корпоративної таємності», де можна було зареєструвати компанію за кілька хвилин, навіть не вказуючи імені засновника. CTA мав нарешті закрити цю прогалину.

Однак у 2025 році, після повернення до влади президента Дональда Трампа, адміністрація різко змінила курс. Хоча Трамп особисто підписав CTA під час свого першого терміну в 2020 році,

[14] https://www.occrp.org/en/feature/how-europes-retreat-from-corporate-transparency-is-shielding-the-corrupt; https://www.occrp.org/en/news/us-congressional-committee-chips-away-at-corporate-transparency-act

через п’ять років він наказав Міністерству фінансів припинити збір інформації від американських громадян, обмеживши цю вимогу виключно іноземними юридичними особами. Фактично це означало легалізацію анонімності для місцевих бізнесменів, які тепер могли засновувати безліч компаній, не залишаючи жодних слідів для правоохоронців, податкової служби чи навіть судів у випадках банкрутства чи шахрайства. Цей крок викликав шок не лише серед демократів, але й серед багатьох експертів з протидії відмиванню грошей.

Кульмінацією стало голосування 26 проти 25 у Комітеті з фінансових послуг Палати представників США, де республіканці, скориставшись своєю більшістю, просунули так званий «Repealing Big Brother Overreach Act» – закон про скасування «нагляду великого брата». Цей документ звільняє громадян США від будь-якої звітності про КБВ, залишаючи вимогу лише для іноземців, які володіють американськими компаніями.

Під час слухань, які описуються як «напружені», демократи намагалися вказати на абсурдність ситуації: іноземний злочинець зобов’язаний звітувати, а американський торговець фентанілом чи організатор трафікінгових мереж – ні. Критики не випадково називають це «найбільшим подарунком фентаніловим торговцям, шахраям та супротивникам США», які покладаються на анонімність.

Демократи в комітеті наводили жахливі приклади з реального життя. Конгресмен Стівен Лінч, демократ від Массачусетсу, попередив, що без цих даних прокурори стають «сліпими» під час розслідування торгівлі зброєю, людьми та фінансування тероризму. Він наголосив, що підставні компанії є улюбленим інструментом для приховування маршрутів контрабанди та відмивання виручки від незаконної діяльності.

Демократи також зазначали, що Національна асоціація окружних прокурорів та численні громадські організації публічно підтримують існуючий закон, адже він надав слідчим безцінний інструментарій. Республіканці ж, зокрема голова комітету Френч Гілл, республіканець від Арканзасу, парирували, що CTA 2020 року – це надмірне регуляторне навантаження, яке несправедливо обтяжує до 33 мільйонів малих американських підприємств, багато з яких і так звітують перед своїми кредиторами та банками. Він наголосив, що власники невеликих пекарень, ферм чи магазинчиків не повинні витрачати сотні годин на юридичне оформлення та подання звітності про КБВ.

Ще більш красномовною стала несподівана підтримка з боку впливової редакційної ради Washington Post, яка напередодні голосування опублікувала матеріал на підтримку перегляду закону через судові виклики та величезні витрати на дотримання вимог. У редакційній статті зазначалося, що за деякими оцінками, закон коштує понад 1 мільярд доларів на рік, водночас приносячи «майже нульову суспільну користь». Автори статті також критикували розмите визначення «істотного контролю» у законі, яке теоретично могло б змусити кожного працівника невеликої фірми з десятьма співробітниками реєструватися як КБВ. Ця критика з боку ліберального видання стала потужним інформаційним приводом для республіканців.

Водночас захисники прозорості наголошували, що вартість виконання вимог є разовою, тоді як вигоди від розкриття шахрайських схем можуть обчислюватися мільярдами врятованих податкових коштів. У підсумку законопроєкт про скасування вирушає на розгляд повного складу Палати представників, де республіканці мають незначну більшість – місця розподілені майже порівну, і кожен голос має критичне значення. Якщо він не пройде як самостійний документ (а шанси на це невизначені через внутрішні розбіжності в Республіканській партії), його можуть додати у вигляді поправки до великого оборонного бюджету або до іншого «необхідного» законопроєкту – так само, як оригінальний CTA був прийнятий у 2020 році в якості частини оборонного бюджету.

Доки Сполучені Штати відступають під тиском лобістів та адміністративних змін, Європейський Союз демонструє не менш болісну картину, але з власною складною юридичною та політичною специфікою.

Історія прозорості в Європі мала своїх героїв та символічні перемоги, які змінили долі цілих країн. Достатньо згадати масштабне розслідування щодо Ріада Саламе, колишнього голови центрального банку Лівану. У 2020 році, після вибуху в порту Бейруту та на тлі економічного колапсу, суспільний гнів зосередився на Саламе, якого колись називали економічним генієм, а тепер вважали головним винуватцем катастрофи.

Згодом з'ясувалося, що його офшорні компанії через три фірми, зареєстровані в Люксембурзі, інвестували майже 100 мільйонів доларів у міжнародну імперію нерухомості, що простяглася від Європи до Близького Сходу. І саме те, що Люксембург у 2019 році на вимогу ЄС відкрив публічний реєстр КБВ, дозволило журналістам з'єднати всі крапки. Том Стокс, журналіст OCCRP, який працював над цим проєктом, прямо зазначив: цей реєстр був визначальним, необхідним елементом розслідування. Результатом стали санкції з боку США, Великої Британії та Канади, відкриття розслідувань про відмивання грошей у Франції, Німеччині та Швейцарії, а згодом – висунення звинувачень у розтраті, підробці документів та незаконному збагаченні самому Саламе (хоча він продовжує стверджувати, що не порушив жодних законів, оскільки накопичив статки ще до роботи в центробанку). Цей випадок став хрестоматійним доказом того, що навіть невелика країна, як Люксембург, може мати глобальне значення у боротьбі з корупцією, якщо її реєстр відкритий.

Однак у 2022 році люксембурзькі двері, як і двері більшості європейських реєстрів КБВ, зачинилися. Рішення Суду Європейського Союзу (CJEU), який визнав, що публічний доступ до інформації про КБВ порушує фундаментальне право на приватність та захист персональних даних, спричинило ланцюгову реакцію. Країни-члени, які лише нещодавно з гордістю відкрили свої реєстри, почали один за одним закривати їх або суттєво обмежувати доступ.

Парадоксально, але це рішення ініціював маловідомий бізнесмен – генеральний директор приватної авіакомпанії, який оскаржив публікацію даних про себе в люксембурзькому реєстрі, посилаючись на ризики для своєї безпеки. Суд став на його бік, і весь європейський антикорупційний проєкт опинився під загрозою. Тепер замість відкритого доступу журналісти, громадські активісти та навіть правоохоронці з інших країн мають доводити «законний інтерес» (legitimate interest) – концепція, яка трактується по-різному в кожній державі. Для цього потрібно надавати національні посвідчення особи, прес-картки, докази проживання, а іноді – навіть публікації про конкретну компанію, які свідчать про підозри.

Це створює абсурдну ситуацію: журналіст повинен майже довести провину компанії ще до того, як отримає доступ до даних. У деяких країнах, як-от Ірландія, вимагають докази кримінального провадження проти фірми – тобто неможливо перевірити компанію, доки проти неї не порушено справу. Чехія вимагає судову ухвалу, що робить доступ практично неможливим для розслідувачів без підтримки прокуратури. У Німеччині, яка традиційно ставиться до захисту даних із особливою ретельністю, необхідно надати документальний доказ зв'язку компанії з підозрюваним КБВ – це неможливо без попереднього доступу до тих самих даних. У Франції система виявилася внутрішньо суперечливою: спочатку вимагали акредитацію журналіста, але потім пом'якшили вимоги. Греція, Словаччина та Кіпр повністю закрили свої реєстри для журналістів, фактично створивши «чорні діри» для прозорості в Європі.

Це особливо драматично для Кіпру, адже саме ця країна фігурувала в гучному проєкті «Кіпрський конфіденціал», де розкривалося, як російські олігархи після вторгнення в Україну продовжували ховати активи та обходити санкції саме через кіпрську фінансову інфраструктуру.

Європейська комісія, усвідомлюючи катастрофічні наслідки такого розмаїття підходів, зобов'язала держави-члени до липня 2026 року ухвалити спільні стандарти того, що саме означає «законний інтерес», та надати журналістам і організаціям громадянського суспільства узагальнений доступ без необхідності постійного отримання дозволів.

Однак на момент цієї публікації, Брюссель навіть не випустив інструкцій, як ця система має працювати на практиці. Термін тисне, а конкретики немає.

На противагу цьому, Велика Британія – хоча вона вже не є членом ЄС – зберегла повністю відкриті та вільно доступні реєстри через портал Companies House. Це два реєстри: Persons with Significant Control (особи зі значним контролем) та Register of Overseas Entities (реєстр іноземних юридичних осіб). Але, навіть ця передова британська система має свої прогалини – трасти, наприклад, не підлягають розкриттю, що створює лазівку для багатомільярдних статків. Також журналісти виявили випадок, коли в реєстрі фігурував неіснуючий власник двох криптобірж, які, за даними Міністерства фінансів США, переказували гроші для Ірану.

Таким чином, перед нами постає похмура, але дуже показова геополітична закономірність. У той час, як глобальні журналістські розслідування знову і знову доводили ефективність прозорості інформації про КБВ – від викриття ліванського банкіра до відставки прем'єр-міністра Литви, від санкцій проти корумпованих політиків до заморожування активів російських олігархів – політичні та судові еліти як у США, так і в Європі системно демонтують ці інструменти.

Республіканці в Конгресі США відкрито звільняють американських власників бізнесу від контролю, створюючи двокласну систему: іноземці звітують, місцеві – ні. Це не просто технічна зміна – це філософський зсув: від прозорості як загальної цінності до прозорості як інструменту контролю над «чужинцями». Європейський суд, прикриваючись благородними принципами права на приватність, змусив країни закрити реєстри, а бюрократична тяганина з «законним інтересом» часто робить доступ неможливим навіть для найдосвідченіших розслідувачів.

У результаті злочинці знову отримують те, що їм потрібно найбільше, – тишу, темряву та безкарність навколо своїх фінансових потоків. Як зазначає OCCRP, сучасна журналістика, необхідна для того, щоб викрити таємні активи чи приховані зв'язки, є дорогою та трудомісткою. Вона вимагає міжнародного партнерства, місяців роботи, а іноді – щасливих витоків даних, як це сталося з Panama Papers. Але без законних механізмів доступу до реєстрів, без відкритих баз даних, журналісти залишаються змушені покладатися на випадковість.

Висновки:

- **Республіканці в США системно демонтують Corporate Transparency Act**, звільняючи американських власників бізнесу від обов'язку розкривати справжніх КБВ. Це створює двокласову систему, де іноземці звітують, а місцеві отримують легальну анонімність.
- **Рішення Суду Європейського Союзу (CJEU) про пріоритет права на приватність фактично знищило публічність реєстрів КБВ** у більшості країн ЄС, замінивши їх процедурою «законного інтересу» (legitimate interest).
- **Відкриті реєстри Великої Британії (Companies House) залишаються взірцевим інструментом**, який дозволив викрити корупційні схеми на сотні мільйонів доларів.
- **Історія Литви**, де обмежений доступ до реєстру через доведення «законного інтересу» призвів до відставки прем'єр-міністра після викриття схеми з коштами ЄС, демонструє критичну важливість навіть часткової прозорості для боротьби з корупцією на найвищому рівні.

Якщо цей тренд не буде зупинено, світ повернеться в епоху, коли анонімні компанії процвітають, а розслідування стають можливими лише завдяки випадковим витокам або

героїчним інформаторам. Відновлення довіри до глобальних фінансових систем потребує не послаблення, а навпаки – посилення та гармонізації правил розкриття КБВ, з обов'язковим публічним доступом для журналістів та громадянського суспільства.

Як наркотрафік підриває охорону найбільшого природного скарбу Коста-Рики [15]

Аналітичний центр InSight Crime оприлюднив результати поглибленого польового дослідження, яке викриває тривожний та багато в чому унікальний симбіоз двох злочинних економік у самому серці Коста-Рики.

Національний парк Корковадо, розташований на півострові Оса на півдні країни та відомий як одне з найбіорізноманітніших місць на планеті – тут досі можна зустріти ягуарів, пум, червоних ара та десятки видів колібрі, – несподівано перетворився на арену жорстокої боротьби. З одного боку, державні рейнджери, об'єднані в Національну систему природоохоронних територій (SINAC), намагаються зберегти цю екосистему. З іншого – добре фінансовані та технічно оснащені злочинні угруповання, які вміло поєднують незаконний видобуток золота з транзитом і відмиванням кокаїнових грошей.

Проблема набула критичних, майже незворотних масштабів на початку березня 2026 року, коли вісім інспекторів SINAC вирушили з форпосту Патос о другій ночі, щоб подолати десять кілометрів важкого тропічного маршруту до секретного табору незаконних золотодобувачів. Інформація від анонімного джерела, яке не знало ані точних розмірів копальні, ані кількості працівників, але надало координати в найвіддаленішій частині парку, підтвердила те, що працівники природоохоронної системи підозрювали вже давно.

Традиційний кустарний видобуток золота, офіційно заборонений у країні ще 2010 року, не просто відродився – він трансформувався на новому, набагато небезпечнішому рівні. Тепер старателі використовують металошукачі, супутникові телефони та налагоджену мережу спостерігачів, які попереджають про появу патрулів. Таке обладнання є недоступним для звичайних бідних мігрантів або місцевих жителів з низьким соціально-економічним статусом, які раніше шукали золото в річках, щоб прогодувати сім'ї. За словами одного з рейнджерів: «це наркогроші». Кошти від продажу кокаїну, які транспортні мережі відмивають через незаконні копальні, дозволяють купувати техніку, організовувати логістику та, що найважливіше, ефективно уникати правосуддя.

Коста-Рика сьогодні перебуває в епіцентрі світового буму кокаїнового бізнесу, і це не перебільшення. Країна виконує критичну роль транзитного вузла для наркотиків, що прямують з Південної Америки до найприбутковіших споживчих ринків – Сполучених Штатів та Європи. Географічне положення, відносно слабкі інституції та велика кількість важкодоступних пляжів і мангрових лісів роблять Коста-Рику ідеальним перевалочним пунктом. Офіційна статистика, наведена в документі вражає: у 2025 році влада конфіскувала 46,5 тонни кокаїну, що на понад 70 відсотків більше порівняно з 27 тоннами, вилученими протягом 2024 року. Аби зрозуміти

[15] https://insightcrime.org/news/cocaine-gold-costa-rica-corcovado-national-park/

масштаб, варто зазначити, що навіть ці цифри відображають лише невелику частку реальних обсягів транзиту.

Показовим є випадок наприкінці серпня 2025 року, коли берегова охорона перехопила швидкісний катер без реєстраційних номерів неподалік узбережжя Пуерто-Хіменеса – найбільшого міста на півострові Оса, що колись славилося золотою лихоманкою, а тепер приваблює туристів своїми незайманими пляжами. На борту виявили двох костариканців та двох колумбійців, а також 1,6 тонни кокаїну. За кілька місяців до того двомоторний літак, завантажений більш ніж 300 кілограмами кокаїну, зазнав аварії та розбився неподалік того ж узбережжя.

Ці події ілюструють не лише масштаби, але й диверсифікацію методів доставки – від морських швидкісних суден до повітряного транспорту. Більше того, минулого року костариканська влада викрила так званий Південно-Карибський картель – перше в історії країни транснаціональне угруповання, яке активно використовувало транспортні мережі, що розвантажують кокаїн на віддалених пляжах узбережжя Пуерто-Хіменес, після чого наркотики відправляли на склади для подальшого експорту або розповсюдження всередині країни.

Однак найбільшу тривогу викликає не стільки сам транзит кокаїну через національний парк, скільки глибока ерозія природоохоронних інституцій через проникнення наркокапіталів у інші нелегальні промисли.

Фінансові органи Коста-Рики у 2025 році зафіксували 700 мільйонів доларів підозрілих коштів, які потрапили до банківської системи. І хоча частина з них безсумнівно пов’язана безпосередньо з торгівлею наркотиками, прямий фізичний та екологічний вплив на екосистему Корковадо чинять саме гроші, вкладені в незаконну розробку надр. Таким чином, боротьба з кустарними старателями, яка ще п’ять-десять років тому зводилася до профілактичних бесід та невеликих штрафів, трансформувалася у повноцінне протистояння з добре організованими злочинними угрупуваннями. Ці організації мають ресурси для підкупу місцевої влади, створення розгалужених мереж спостерігачів, придбання сучасних засобів зв’язку та транспорту. Як наслідок, будь-яка операція ризикує перетворитися на засідку.

Висновки:

- **У національному парку Корковадо відбулося злиття наркотрафіку та незаконного видобутку золота:** кошти від продажу кокаїну інвестуються в оснащення нелегальних копалень, що перетворило кустарний промисел на добре фінансовану злочинну індустрію.
- **Обсяги транзиту кокаїну через Коста-Рику стрімко зростають**, а наркоугруповання використовують віддалені пляжі та стежки Корковадо для своїх операцій.
- **Природоохоронна система SINAC паралізована хронічним недофінансуванням:** бюджет скоротився на 40% четвертий рік поспіль, а рейнджери не мають навіть базового радіозв’язку, тоді як злочинці користуються супутниковими телефонами та мережами спостерігачів.
- **Окремі успішні операції є тимчасовими та локальними перемогами,** які не вирішують системної проблеми через величезний розрив у фінансових можливостях держави та злочинних угруповань.

Парадоксальність та драматизм ситуації полягають у тому, що ресурси самої природоохоронної системи катастрофічно скорочуються, тоді як можливості злочинців зростають. Річний бюджет SINAC у 2025 році впав на 40 відсотків четвертий рік поспіль. Це означає не просто брак коштів на нове обладнання – йдеться про нездатність підтримувати навіть базове функціонування. Як наслідок, години патрулювання в Корковадо скорочуються, а рейнджери проводять все менше часу

безпосередньо на місцевості. Вони змушені покладатися на партнерство з приватними природоохоронними неурядовими організаціями, які забезпечують їх харчами, паливом, іноді – аварійним спорядженням та логістичною підтримкою.

Операція в останній тиждень березня 2026 року, детально описана в документі, стала рідкісним прикладом успіху. Але як слушно зазначають автори звіту, цей успіх є лише локальним, тимчасовим і, по суті, символічним. Ціна золота на світових ринках продовжує оновлювати історичні рекорди, а потужні фінансові структури, що стоять за незаконними копальнями, нікуди не зникли.

Кожна успішна операція – це лише епізод у безперервному конфлікті, де ресурси та ініціатива дедалі більше переходять на бік злочинності. Рейнджери продовжують свою роботу, ризикуючи життям без належного оснащення та зв'язку, покладаючись на донати неурядових організацій та власну відданість справі. Але питання залишається відкритим: як довго зможе протриматися система, коли її щорічний бюджет скорочується майже вдвічі, а злочинці, яких вона має зупиняти, отримують фінансування з глобального ринку наркотиків, вартість якого обчислюється мільярдами доларів?

Інші новини

Санкційний тупик: чому криптовалюта залишається поза фокусом антиросійської коаліції [16]

Аналітичний коментар Тома Кітінга, директора Центру з фінансів та безпеки RUSI (Royal United Services Institute) є критичним аналізом поточного стану санкційної стратегії Заходу щодо Росії. Відправним контекстом є ситуація початку лютого 2026 року: на тлі нафтових цін близько 65 доларів за барель та слабкого глобального нафтового ринку Захід активно готувався до нового санкційного удару по доходах Росії. Єврокомісія анонсувала запровадження повної заборони на морські послуги для російської сирої нафти в рамках 20-го пакету санкцій, Велика Британія ввела найбільший за чотири роки пакет заходів, Франція та Бельгія здійснювали висадки на кораблі «тіньового флоту» у Середземному морі та Північному морі відповідно. Тодішня ціна нафти й умови ринку, що склалися, були максимально сприятливими для реалізації амбітних санкційних планів.

Ситуація кардинально змінилася внаслідок ескалації конфлікту на Близькому Сході: масштабні авіаційні удари Ізраїлю та США по Ірану, відповідні іранські удари по регіональній енергетичній інфраструктурі та фактичне блокування Ормузької протоки — незважаючи на тимчасове перемир'я — призвели до зростання ціни нафти Brent майже на 70%, до рівня близько 100 доларів за барель. Цей ціновий шок поставив Захід перед стратегічною дилемою: посилення тиску на Росію через нафтові доходи ризикує ще більше загострити і без того критичну глобальну енергетичну кризу. Паралельно адміністрація Трампа демонструє систематичну незацікавленість у застосуванні санкційних повноважень для підтримки України — єдиним значущим кроком залишились санкції проти Лукойлу та Роснєфті, введені ще у жовтні 2025 року. Угорщина знову заблокувала 20-й пакет санкцій ЄС. Результат — де-факто регуляторний та стратегічний параліч Заходу.

[16] https://www.rusi.org/explore-our-research/publications/commentary/wests-ukraine-sanctions-strategy-has-lost-its-way?utm_campaign=sifmanet-brief-26&utm_medium=email

Ключовим аналітичним внеском статті є акцент на криптовалюті як систематично ігнорованому векторі санкційного тиску. Автор документує, що Росія активно використовує криптоактиви для оплати критично важливих військових матеріалів — передусім з Китаю — обходячи таким чином традиційні банківські санкції. Невелика, але ресурсно обмежена група слідчих акумулювала достатній обсяг доказів для організації скоординованої кампанії з виявлення та порушення відповідних гаманців, бірж та платіжних інструментів. Попри наявність цих доказів, систематичного регуляторного відгуку з боку коаліційних урядів немає: доступні лише фрагментарні ad hoc санкції, тоді як стратегічна, скоординована кампанія виявлення та руйнування крипто-платіжної інфраструктури Росії практично відсутня. Автор характеризує цю бездіяльність як «дивну відсутність» реакції, враховуючи наявні докази.

Стратегічний висновок Кітінга відображає більш широкий діагноз дисфункції санкційного мислення. Оскільки дестабілізація Близького Сходу де-факто блокує традиційний вектор тиску на нафтові доходи Росії, він закликає до переорієнтації санкційної коаліції з логіки «обмеження доходів» на активний підрив «механізмів витрат» Кремля. Цей концептуальний зсув вимагає нових регуляторних та розвідувальних інструментів — зокрема, активної взаємодії з блокчейн-аналітичним співтовариством, якому вже відома операційна архітектура крипто-платіжних схем Росії. Специфіка цього вектора полягає у його технічній реалістичності та відсутності ризику глобальної енергетичної дестабілізації. Аналіз Кітінга, по суті, є обґрунтуванням необхідності системного регуляторного прориву — від реактивних, ситуативних санкцій до стратегічної, скоординованої кампанії проти крипто-фінансування російського воєнного апарату.

Монетарний суверенітет у токенізовану епоху: як Європі вибудувати політику навколо стейблкоїнів [17]

У березні 2026 року на високому рівні в межах семінару EUROFI відбулася дискусія, що визначила стратегічні контури європейської політики щодо стейблкоїнів.

Перший заступник керуючого Банку Франції Дені Бо запропонував учасникам не просто оцінити виклики, а й зазирнути за горизонт поточної токенізації фінансів. Його виступ — це маніфест обережності, технологічного прагматизму та жорсткої позиції щодо захисту грошового суверенітету Європи. Головна дилема, яку він окреслює, звучить парадоксально: як Європі використати переваги стейблкоїнів, не віддавши при цьому контроль над власною платіжною системою на поталу долару та небанківським емітентам?

Почнімо з контексту, який Бо окреслює лаконічно, але з надзвичайною точністю. Станом на початок 2026 року ринок стейблкоїнів є ареною домінування двох взаємопов'язаних явищ: по-перше, абсолютна більшість цих цифрових активів номінована в доларах США, по-друге, емітентами виступають переважно неєвропейські, часто небанківські структури. Це створює асиметрію, яку не можна виправити простим регуляторним наказом. Якщо європейські компанії, банки та навіть домогосподарства почнуть масово використовувати доларові стейблкоїни для розрахунків — а це вже відбувається в окремих секторах, зокрема в міжнародній торгівлі та крипто-екосистемах, — то Європа опиниться в ситуації "тихої доларизації". Вона не буде схожа на класичну заміну національної валюти, але призведе до того

[17] https://www.banque-france.fr/en/governors-interventions/stablecoins-what-strategic-choices-europe

самого результату: втрати контролю над грошовою масою, процентними ставками та, зрештою, над здатністю проводити незалежну монетарну політику.

Однак Дені Бо також наголошує на позитивному зрушенні: на горизонті з'являються європейські альтернативи. Йдеться не про абстрактні плани, а про реально функціонуючі або близькі до запуску продукти. По-перше, це стейблкоїни в євро, які пропонують фінансові провайдери, зареєстровані в ЄС та підзвітні європейським наглядовим органам. По-друге, і це навіть важливіше, — токенізовані версії традиційних розрахункових активів: банківських депозитів і, що ключове, грошей центрального банку. Саме ці дві опори мають стати фундаментом, на якому будуватиметься європейська токенізація. Бо прямо говорить: альтернативи доларовим стейблкоїнам не просто можливі — вони вже існують у зародковому стані, і їхнє масштабування є пріоритетом. Але для цього потрібна чітка стратегічна рамка, яку він і пропонує.

Ця рамка спирається на непорушний принцип: токенізація в жодному разі не повинна руйнувати дворівневу монетарну систему, яка є основою сучасного фінансового устрою Європи.

Що це означає на практиці? У нинішній системі гроші існують у двох формах: гроші центрального банку та гроші комерційних банків. Вони співіснують, доповнюють одна одну та є взаємозамінними за номіналом — один євро в банку завжди дорівнює одному євро в центральному банку. Ця архітектура забезпечує довіру, стабільність і можливість центрального банку виконувати роль кредитора останньої інстанції.

Коли ми переходимо до токенізованого світу, спокуса зруйнувати цю систему стає величезною: технологія DLT дозволяє створювати розрахункові активи, які не є ані готівкою, ані традиційним депозитом. Саме тут ховається головна небезпека. Якщо стейблкоїни, особливо випущені небанківськими емітентами без нагляду та без доступу до ліквідності центробанку, стануть домінуючим розрахунковим активом, ми отримаємо фрагментовану, вразливу до паніки систему. Під час стресових ситуацій власники стейблкоїнів кинуться обмінювати їх на традиційні гроші, але емітент, який не має доступу до ліквідності центробанку, не зможе виконати зобов'язання. Це класичний сценарій "банківської паніки" 2.0, тільки без банку та без страхування депозитів. Тому вимога Бо зберегти співіснування, доповнюваність і взаємозамінність публічних і приватних грошей у токенізованому світі — це не консервативний рефлекс, а умова виживання фінансової системи.

Як досягти цього в реальності? Бо формулює триєдине завдання, яке має виконуватися паралельно, а не послідовно.

Перше: Євросистема, тобто Європейський центральний банк та національні центробанки, зокрема Банк Франції, повинні адаптувати свої послуги до цифрової ери. Це означає пропозицію грошей центрального банку в токенізованій формі як для оптового (міжбанківського), так і для роздрібного сегментів.

Друге: європейські фінансові інституції — банки, електронні грошові установи, платіжні системи — повинні отримати підтримку у створенні токенізованих приватних грошей.

Третє: регуляторна рамка має бути не просто адекватною, а випереджальною, здатною закривати прогалини, які виникають у міру технологічного розвитку.

І тут Дені Бо переходить від загальних декларацій до конкретних проєктів, що втілюються Банком Франції. Він згадує три ініціативи: Pontes, Appia та цифровий євро. Він повідомляє, що вже до кінця 2026 року — тобто протягом кількох місяців після виступу — будуть розгорнуті послуги в токенізованих грошах центрального банку. Це означає, що європейські банки зможуть проводити між собою розрахунки в цифрових токенах, які будуть забезпечені центральним банком. Це революція в платежах, яка залишиться непоміченою для широкої публіки, але кардинально змінить ландшафт для фінансових інституцій.

Що ж до цифрового євро, то Бо займає виважену, але чітку позицію. Він називає його критичним внеском у роздрібний сегмент, але категорично заперечує будь-які спроби розглядати цифровий євро як панацею або єдину відповідь на виклики стейблкоїнів. Це важливе застереження, адже в публічному дискурсі часто звучить спрощена теза: "запровадимо цифровий євро — і проблеми з криптоактивами зникнуть". Ні, це не так. Цифровий євро — це одна з ланок, безсумнівно, міцна, але не єдина.

Водночас він підкреслює, що інші ланки — токенізовані депозити, приватні стейблкоїни в євро, панєвропейські платіжні рішення — мають бути розвинуті з такою ж інтенсивністю. Саме тому Банк Франції разом із Міністерством фінансів та Управлінням фінансових ринків (AMF) створив стратегічну групу, яка об'єднує всю екосистему французького фінансового центру навколо інновацій, DLT та токенізації.

Бо особливо відзначає ініціативи консорціуму Європейської платіжної ініціативи (EPI), який намагається створити реальну альтернативу Visa та Mastercard, а також проєкти, спрямовані на розробку токенізованих депозитів і стейблкоїнів у євро для міжнародних корпорацій. Останнє є надзвичайно важливим: транснаціональні компанії, які працюють у Європі, сьогодні потребують ефективних інструментів для крос-кордонних розрахунків та управління ліквідністю. Якщо євро не запропонує їм таких інструментів у токенізованій формі, вони звернуться до доларових стейблкоїнів. І тоді програш буде остаточним.

Переходячи до регуляторної частини, Дені Бо нагадує, що MiCA — це перший у світі всеосяжний регуляторний режим для криптоактивів, і Європа має право пишатися цим. Франція, завдяки закону Pacte 2019 року, підійшла до імплементації MiCA з унікальним досвідом — французькі регулятори вже кілька років наглядають за провайдерами послуг криптоактивів, що дало їм змогу виявити слабкі місця ще до того, як вони стали системними. І перший рік роботи MiCA, за словами Бо, підтвердив правильність загального напрямку: з'явилася правова визначеність для емітентів стейблкоїнів та постачальників послуг, ринок отримав чіткі правила гри. Однак саме цей досвід імплементації показав, що MiCA є лише першим, але не останнім словом. Бо прямо заявляє про необхідність посилення регуляції.

Перша пропозиція: обмежити використання стейблкоїнів для повсякденних платежів, особливо якщо вони забезпечені не євро, а іншою валютою. Це надзвичайно сміливий крок, адже він вторгається в саму сутність стейблкоїна як платіжного засобу. Але логіка Бо проста: якщо стейблкоїн, номінований у доларах, почне масово використовуватися для купівлі кави в Берліні чи оплати рахунків у Ліоні, то євро перестане бути реальним платіжним засобом у власній країні. Тому він наполягає на кількісних або функціональних обмеженнях — без конкретних цифр, але з чітким посилом: Європа не дозволить доларовим стейблкоїнам стати засобом обігу на своїй території.

Друга пропозиція стосується мульти-емісії — ситуації, коли той самий стейблкоїн випускається одночасно всередині ЄС та за його межами, часто за різними регуляторними стандартами. Бо попереджає: у період стресу це створює канал регуляторного арбітражу, коли капітал і ліквідність перетікають у юрисдикцію з м'якшими правилами. Його вимога — жорстка координація або навіть унеможливлення такої мульти-емісії, що означає: якщо ти хочеш працювати в Європі, твій стейблкоїн має бути випущений за європейськими правилами без подвійних стандартів.

Третя пропозиція стосується токенів електронних грошей (EMT). Тут Бо вказує на необхідність уточнень у майбутніх директивах PSD3 та ревізіях MiCA, щоб усунути нормативну невизначеність, яка зараз гальмує розвиток цих інструментів.

Особливої уваги заслуговує пасаж Бо про типи емітентів стейблкоїнів. Він проводить чітку межу: стейблкоїни, випущені банком або електронною грошовою установою (EMI), що входить до

банківської групи, несуть структурно нижчий ризик, ніж випущені незалежними небанківськими структурами. Чому? Банки мають прямий доступ до центральної банківської ліквідності, вони підлягають європейському банківському нагляду (SSM), вимогам до капіталу (CRR) та страхуванню депозитів. У разі кризи вони можуть отримати підтримку від центробанку.

Небанківський емітент стейблкоїна не має жодного з цих захистів. Його резерви можуть бути високоякісними, але у випадку паніки він не зможе залучити ліквідність центробанку, і його крах буде раптовим та некерованим. Тому Бо констатує, що за поточними правилами небанківські емітенти не мають доступу до рахунків центрального банку. Однак він залишає теоретичну можливість для майбутніх змін: якщо небанківський емітент також надає платіжні послуги і готовий виконати сукупність вимог, доступ до рахунків центробанку міг би розглядатися. Це дуже обережний сигнал, але сигнал: центральний банк не відкидає інновації апріорі, але вимагає, щоб будь-який гравець, який претендує на системну роль, приймав системні правила.

Нарешті, Бо звертається до глобального виміру. Він наголошує, що жодна європейська регуляція, навіть найдосконаліша, не буде ефективною, якщо інші юрисдикції гратимуть за іншими правилами. Тому він закликає до повного, своєчасного, узгодженого та глобального впровадження стандартів Ради з фінансової стабільності (FSB) щодо криптоактивів. Принцип "однакові види діяльності, однакові ризики, однакові правила" та технологічна нейтральність — це не просто гасла, а єдина можливість обмежити регуляторний арбітраж, коли гравці реєструються на Багамах чи в ОАЕ, але обслуговують європейських клієнтів. Бо не називає конкретні країни, але контекст зрозумілий: США, Велика Британія, Сінгапур, ОАЕ — всі вони рухаються різними траєкторіями в регулюванні стейблкоїнів. Європа обрала шлях найсуворішої рамки, і цей вибір має сенс лише в тому випадку, якщо інші великі економіки наслідують її приклад або принаймні узгодять свої підходи.

Підсумовуючи, виступ Дені Бо не закликає до ізоляції чи заборони, але вимагає, щоб Європа перестала бути пасивним спостерігачем на ринку, де домінують долар та небанківські емітенти. Головне послання, яке він адресує і європейським політикам, і ринковим гравцям, і міжнародним партнерам, звучить гранично ясно: пасивність закінчилася. Європа має технології, регуляторний досвід і політичну волю, щоб побудувати власний токенізований платіжний простір.

Для загального розвитку

Справа Магнітського та швейцарська юстиція: методологічний провал, інституційна вразливість і міжнародний тиск [18]

Стаття опублікована на платформі SWI swissinfo.ch, є журналістським розслідуванням триваючих правових, регуляторних та міжнародних суперечок навколо обробки Швейцарією злочинних активів у справі Магнітського — одного з найрезонансніших транснаціональних справ відмивання коштів XXI ст. Механізм самої злочинної схеми полягав у такому: у 2007–2008 роках російські чиновники незаконно вилучили корпоративну

[18] https://www.swissinfo.ch/eng/swiss-position/how-switzerland-got-caught-in-the-magnitsky-case-again/91255290?twclid=26wlej2fw2osgecdae3wk3b9nc

документацію та печатки дочірніх компаній Hermitage Fund, перереєстрували їх на підставних осіб, зфабрикували судові рішення про фіктивні збитки та подали заяву на повернення раніше сплаченого податку на прибуток на суму 230 мільйонів доларів до Казначейства Росії. Гроші були виведені через мережу офшорних рахунків. Сергій Магнітський, адвокат, що розкрив схему в інтересах Hermitage, загинув у слідчому ізоляторі у 2009 році.

Швейцарський вимір справи розпочався у 2011 році із кримінальної скарги Hermitage Capital у Швейцарії — одного з перших міжнародних розслідувань, ініційованих компанією. Швейцарські органи заморозили близько 18 мільйонів франків на рахунках трьох осіб, пов'язаних із шахрайством: Владлена Степанова, Дениса Кацива та Дмитра Клюєва. У липні 2021 року Федеральна прокуратура Швейцарії закрила розслідування: встановивши зв'язок частини активів із предикатним злочином, вона не виявила доказів для висунення кримінальних звинувачень. Підсумком стала конфіскація лише 4 мільйонів франків та повернення 14 мільйонів власникам рахунків. Теоретичною та практичною основою такого результату стала «пропорційна методологія розрахунку», розроблена прокурорами: відповідно до неї, на кожному «шарі» відмивання лише певна частка коштів може бути математично пов'язана з предикатним злочином — і саме ця частка підлягає конфіскації, тоді як «розбавлений» залишок підлягає поверненню.

Правова та методологічна дискусія навколо цього підходу є центральною для розуміння справи. «Пропорційна методологія» є практично унікальною для Швейцарії і суперечить підходу більшості міжнародних юрисдикцій, де суди зосереджуються на злочинному походженні коштів у цілому, не намагаючись математично простежити їх трансформацію через складні фінансові ланцюжки. Марк Піт, колишній член FATF та керівник відділу економічної злочинності Федерального Міністерства юстиції Швейцарії, публічно прокоментував: «Якщо прокурори праві, Швейцарія є раєм для відмивання грошей». Паралельна юридична суперечка стосувалася статусу Hermitage Capital як «постраждалої сторони»: швейцарська прокуратура виключила компанію з провадження, визнавши єдиною жертвою Казначейство Росії — позиція, що збігається з позицією самих російських властей і принципово відрізняється від підходу США та Франції, де Hermitage визнавалась постраждалою.

Відсутність кваліфікації відмивання коштів як дій злочинної організації є вузловим юридичним питанням справи зі значними практичними наслідками. За швейцарським законодавством, якщо відмивання пов'язане зі злочинною організацією, обертається тягар доведення: підозрювані зобов'язані самостійно доводити законне походження коштів, а активи підлягають повній конфіскації. Прокуратура Швейцарії не змогла встановити ознак злочинної організації, тоді як Міністерство юстиції США та французькі органи дійшли протилежного висновку — що відмивання здійснювалось злочинною організацією, до якої входили російські державні чиновники. Ця розбіжність частково пояснює відмінність у підходах до конфіскації. Окремо слід зазначити обвинувачення на адресу самих швейцарських посадовців: слідчий Вінцент Шнель, причетний до розслідування, у 2021 році був засуджений за «прийняття неналежної вигоди» від російської сторони під час роботи над справами, пов'язаними з Росією; у 2023 році комісія Конгресу США з питань безпеки та співробітництва в Європі закликала до введення санкцій проти кількох швейцарських посадовців.

Міжнародний парламентський контроль через ПАРЄ є паралельним і дедалі потужнішим треком тиску. У квітні 2024 року естонський парламентар Єрік-Нілес Кросс ініціював нове розслідування, а у жовтні 2024 року ПАРЄ призначила спеціальним доповідачем українського парламентаря і адвоката Лесю Василенко. У березні 2025 року місія Василенко у Берні зіткнулась із тим, що вона охарактеризувала як «сильні» та «неналежні» реакції окремих членів швейцарської делегації. Підсумкова резолюція, прийнята Комітетом з правових питань та прав людини 27 січня 2026 року та запланована до голосування на пленарному засіданні 22 квітня 2026 року, констатує: американські та французькі органи дійшли висновку, що відмивання

здійснювалось злочинною організацією з участю державних чиновників Росії. Резолюція є юридично необов'язковою, але несе значний політичний вплив та включає рекомендації щодо розширення конфіскації без обвинувального вироку та зміни відповідного законодавства.

Поворотним юридичним моментом став грудень 2025 року: Федеральний суд Швейцарії, розглядаючи апеляцію Кацива, визнав «пропорційну методологію» несумісною зі швейцарським правом та зобов'язав Федеральний кримінальний суд перерахувати компенсаційну вимогу держави за одним із двох альтернативних методів — «методом навмисної корекції» (де повна конфіскація можлива за доказаного умислу) або «залишковим методом» («седиментація», більш обмежувальний підхід). Це рішення потенційно формує нову юриспруденційну рамку для майбутніх справ, однак залишає відкритими ключові питання: що відбудеться з 75% коштів, вже повернутих власникам рахунків? Чи поширюється рішення й на активи Степанова? Паралельно встановлено, що Кацив зняв щонайменше 6 мільйонів франків з рахунків у банку UBS та перевів їх до банків в Ізраїлі та Вірменії, що ставить під сумнів практичну можливість конфіскації навіть за оновленими правовими стандартами. Справа залишається в активній стадії, а її результат матиме прецедентне значення для швейцарського підходу до конфіскації активів у складних транскордонних справах ВК.

Ваша думка важлива!

1. Як Україні, яка не є членом ЄС, але прагне до євроінтеграції та активно використовує криптоактиви для залучення донатів і розрахунків (зокрема USDT), вибудувати власну регуляторну політику щодо стейблкоїнів, щоб не стати «сірою зоною» для регуляторного арбітражу між MiCA та більш ліберальними юрисдикціями?
2. Joint Analysis між кількома ПФР дозволив виявити схему на кілька сотень мільйонів євро, яка залишалась невидимою для кожної юрисдикції окремо — які структурні бар'єри (правові, технічні, інституційні) найбільше гальмують розширення такого формату співпраці як стандартної практики, а не виняткового інструменту?
3. Синтетичний датасет містить лише відомі типології, і FCA визнає ризик «оптимізації під патерн» замість розвитку широких детекційних можливостей. Як не допустити аби така модель тестування не закріпила ретроспективне мислення в AML-системах у той момент, коли злочинці вже адаптуються до нових технологій?
4. Переорієнтація санкційної стратегії з «обмеження доходів» на «підрив механізмів витрат» через атаки на крипто-гаманці та біржі потребує якісно нової координації між фінансовими розвідками, компаніями з блокчейн-аналітики та приватними криптобіржами — яка модель міжнародного публічно-приватного партнерства є тут реалістичною і які правові рамки її унеможливлюють або ускладнюють?
5. Різниця між швейцарською та американською/французькою кваліфікацією щодо наявності злочинної організації в справі Магнітського призвела до кардинально різних результатів щодо конфіскації — чи свідчить це про необхідність гармонізації самого поняття «злочинна організація» в контексті міжнародних справ ВК, і якщо так, то хто і через який механізм може таку гармонізацію забезпечити?

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-2026-17

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

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