Методологічний бюлетень

Серійний номер: МінФін-AML-2025-48

Листопад 2025

“Перемога починається з першого кроку”

Роберт Шуллер

Мета

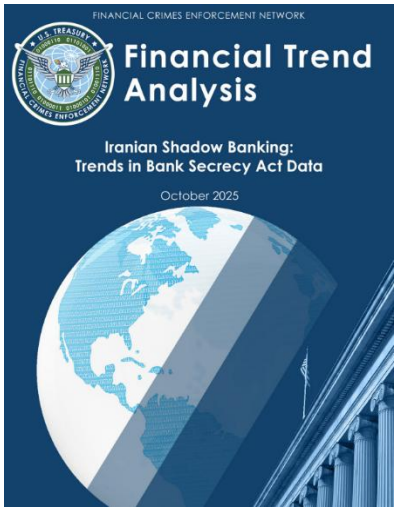
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Глобальна схема обходу санкцій: як Іран використовує міжнародну фінансову систему для конвертації нафти у військовий потенціал [1]



Документ є ґрунтовним аналітичним звітом FinCEN, у якому представлено комплексну картину функціонування іранської системи тіньового банкінгу у 2024 році — системи, що була створена для обходу санкцій США, отримання доходів від незаконного експорту нафти та нафтохімічних продуктів, а також подальшого спрямування цих коштів на фінансування стратегічних військових програм Ірану, включно з ядерними технологіями, балістичними ракетами та безпілотними системами. На основі аналізу звітності за Законом про банківську таємницю (BSA) було встановлено, що близько 9 мільярдів доларів США було залучено до таких схем протягом 2024 року, і майже всі транзакції відбувалися через складну інфраструктуру підставних компаній, офшорних юрисдикцій, нерезидентських рахунків, фірм-посередників та логістичних операторів, що у своїй взаємодії формують

[1] https://www.fincen.gov/system/files/2025-10/FTA-Iranian-Shadow-Banking.pdf

надзвичайно стійку, децентралізовану, але координовану багаторівневу систему прихованих платежів.

Центральним джерелом і рушійним чинником фінансових потоків є незаконний продаж іранської нафти, здебільшого незалежним приватним малим нафтопереробним заводам Китаю, проте із залученням так званих покупців-посередників у третіх юрисдикціях, насамперед у Сінгапурі та Об'єднаних Арабських Еміратах Саме нафтогазові компанії, пов'язані з Іраном, зафіксували операції на суму понад 4 мільярди доларів, причому ключові учасники маскували зв'язок з Іраном через складні структури корпоративної власності, номінальних директорів і використання контрактних схем із комерційно нелогічними умовами. Надалі фінансові потоки від реалізації нафти цілеспрямовано переказувалися на фіктивні юридичні особи (підставні компанії), які є ключовим елементом цієї фінансової схеми: через них пройшло понад 5 мільярдів доларів США, і саме цей сектор фактично становить "ядро" іранської системи тіньового банкінгу. Такі фіктивні компанії не здійснюють реальної господарської діяльності, але створюють штучний розрив між фактичними продавцями та кінцевими одержувачами коштів, що унеможливлює відстеження походження активів і бенефіціарів. Особливу роль відіграють компанії, зареєстровані у Спеціальному адміністративному районі Гонконг, які використовують банківські рахунки в материковому Китаї для нерезидентів, що дає змогу проводити великі валютні операції в доларах США поза межами посиленого регуляторного контролю західних фінансових систем.

Подальшим критично важливим напрямом фінансових потоків є судноплавні компанії — близько 707 мільйонів доларів було використано для розрахунків за транспортування нафти та логістичні витрати, включно із платежами на ескроу-рахунки (рахунки умовного зберігання) міжнародних юридичних фірм для придбання суден. Іран формує так званий «тіньовий флот» — сукупність суден, які експлуатуються через номінальних операторів і змінюють прапори, схеми управління й географію зупинок для унеможливлення відстеження маршруту і власності. Цей флот забезпечує фізичне транспортування санкційних енергоресурсів, що є основою фінансових потоків.

Подальша частина фінансових потоків спрямовувалася до інвестиційних компаній, зареєстрованих у Сполученому Королівстві та Об'єднаних Арабських Еміратах, які забезпечували іранським структурам доступ до міжнародних інвестиційних ринків, у тому числі до ринків торгівлі сировинними товарами. Такий сегмент свідчить про перетворення незаконно отриманих доходів на фінансові інструменти, які використовуються як для накопичення капіталу, так і для подальшого переміщення активів до юрисдикцій із підвищеним рівнем захищеності. Іншим напрямом є фінансування придбання технологій подвійного призначення: FinCEN ідентифікувало приблизно 413 мільйонів доларів США транзакцій, спрямованих на компанії, задіяні у закупівлі західних електронних, оптичних, турбінних та авіаційних компонентів. Ці фінансові операції є одними з найбільш показових з точки зору загроз міжнародній безпеці, оскільки демонструють пряме перетворення доходів від незаконного продажу нафти на ресурси, що сприяють зміцненню військово-промислового потенціалу Ірану.

Географія тіньового банкінгу також показує виняткову концентрацію у трьох центрах: Дубай, Гонконг і Сінгапур. Через компанії в Дубаї пройшло близько 6,4 мільярда доларів — більше, ніж через будь-яку іншу юрисдикцію. Гонконгові структури генерували другий за обсягом рух — приблизно 4,8 мільярда доларів, головним чином як відправники коштів. На Сінгапур припадає 2,2 мільярда доларів, причому більшість — пов'язані з компаніями, що торгують нафтою. Окремо документ наголошує на залученні фінансової інфраструктури Великої Британії і Швейцарії, що забезпечили іранським компаніям можливість доступу до платіжної та брокерської інфраструктури Європи. Важливим елементом є також прямий зв'язок із фінансовою інфраструктурою США: понад 534 мільйони доларів пройшли через американські банківські рахунки, а ще близько півмільярда — через зарубіжні філії американських банків, що

свідчить про успішне маніпулювання кореспондентськими відносинами банків для отримання доступу до доларової ліквідності.

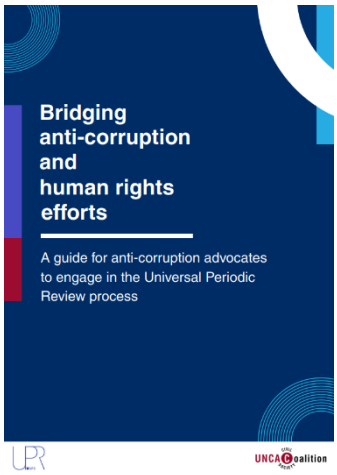
Звіт підкреслює, що поточні BSA-повідомлення дозволили ідентифікувати масштаби явища, однак його реальні обсяги можуть бути значно вищими, оскільки дані відображають тільки виявлену й задокументовану активність. Фінансова модель Ірану побудована на багаторівневій анонімізації потоків через комбінацію фіктивних компаній, середніх торгових хабів, офшорних реєстрацій, нерезидентських рахунків, юридичних посередників та інвестиційних структур, що робить її стійкою до традиційного банківського моніторингу та забезпечує стратегічну автономність у фінансуванні військових програм.

Документ завершується попередженням FinCEN про необхідність підвищення глобальної фінансов ої пильності, оскільки Іран продовжує системно використовувати міжнародну фінансову систему — включно з доларовими розрахунками — для фінансування дестабілізаційної діяльності та розвитку озброєнь, а тіньовий банкінг залишається ключовим механізмом обходу міжнародних санкцій.

Висновки:

- **Банківські установи мають посилити моніторинг транзакцій, що включають Дубай, Гонконг і Сінгапур,** зокрема коли учасниками є нафтогазові, інвестиційні, логістичні або технологічні компанії — саме ці юрисдикції та сектори є центральними вузлами тіньового фінансування Ірану.
- **Операції зі підставними компаніями повинні автоматично запускати посилену перевірку клієнта (EDD),** оскільки саме вони забезпечили переміщення близько 5 млрд доларів і є головним механізмом приховування походження коштів.
- **Транзакції, пов'язані з електронікою, авіадвигунними й іншими технологіями подвійного призначення, слід відносити до ризику «фінансування розповсюдження ЗМЗ»,** адже документ підтверджує їхній безпосередній зв'язок із військовими програмами Ірану.
- **Розрахунки з судноплавними компаніями, які перевозять нафту, мають оцінюватися як високоризикові,** оскільки саме через «тіньовий флот» реалізується фізичне транспортування санкційної нафти та оплата логістики.

Коли корупція стає порушенням прав людини: чому UPR відкриває новий фронт у глобальній боротьбі з корупцією [2]



Документ є комплексним практичним посібником, який пояснює, чому боротьба з корупцією не може розглядатися окремо від захисту прав людини, і як механізм Універсального періодичного огляду (UPR) ООН може бути використаний громадянським суспільством як потужний інструмент для просування системних антикорупційних реформ. Автори підкреслюють, що корупція не лише підриває верховенство права та демократичні інститути, а й безпосередньо завдає шкоди людям, обмежуючи доступ до освіти, медицини, житла, соціальних послуг та правосуддя, спричиняючи дискримінацію вразливих груп та посилюючи нерівність. У той час як антикорупційні ініціативи традиційно базуються на кримінально-

[2] https://upr-info.org/sites/default/files/general-document/2025-06/Bridging-anti-corruption-and-human-rights-efforts-A-guide-for-anti-corruption-advocates-to-engage-in-the-Universal-Periodic-Review-process-1.pdf

правовому підході та орієнтуються на притягнення винних до відповідальності, правозахисна система наголошує на захисті жертв і відновленні їхніх прав. Саме тому обидва підходи потрібно розглядати як комплементарні й взаємопідсилювальні — і це, на думку авторів, є новою стратегічною парадигмою, яка повинна лягти в основу сучасних політик доброчесності й державного управління.

Посібник детально розкриває, як функціонує UPR — глобальний механізм, у межах якого кожна держава-член ООН проходить регулярний огляд стану прав людини на національному рівні. Процес є циклічним і складається з трьох етапів: підготовка національної оцінки та подання інформації, інтерактивний діалог з державами-членами під час сесії UPR, а потім виконання підтриманих рекомендацій протягом наступних 4,5 років. За своєю природою UPR є відкритим, інклюзивним і прозорим, і на відміну від інших механізмів права людини дозволяє державам отримувати рекомендації не лише щодо ратифікованих міжнародних договорів, але й стосовно загальних міжнародних стандартів, добровільних зобов'язань та важливих викликів. Центральним елементом є участь громадянського суспільства: хоча воно не виступає під час діалогу держав, його подання, дані та адвокаційна робота безпосередньо впливають на формування порядку денного, формулювання рекомендацій і їхню подальшу імплементацію.

Документ порівнює UPR із механізмом огляду імплементації Конвенції ООН проти корупції — UNCAC Implementation Review Mechanism (IRM). IRM забезпечує глибокий технічний аналіз виконання антикорупційних норм державами, але має обмежену транспарентність і мінімальну інституціоналізовану участь громадянського суспільства. UPR, у свою чергу, відкритий, публічний і залучає ширший спектр учасників. Саме тому автори наголошують на необхідності використовувати обидва механізми паралельно: IRM дає зміст і експертизу, тоді як UPR створює політичні зобов'язання, генерує зовнішній тиск та формує міжнародну підзвітність держав. Посібник показує, що посилання на антикорупційні міжнародні рамки, такі як UNCAC, FATF, GRECO, OGP або SDG 16, у поданнях до UPR робить рекомендації держав більш конкретними, фокусованими та вимірюваними — і відповідно збільшує ймовірність їх прийняття та виконання.

На основі аналізу понад 120 000 рекомендацій UPR від 2008 до 2025 року автори виявляють, що лише 0,62% згадують тематику корупції, однак частота таких рекомендацій зростає від циклу до циклу, що свідчить про посилення глобального усвідомлення ролі корупції як бар'єра до реалізації прав людини. Водночас більшість

Висновки:

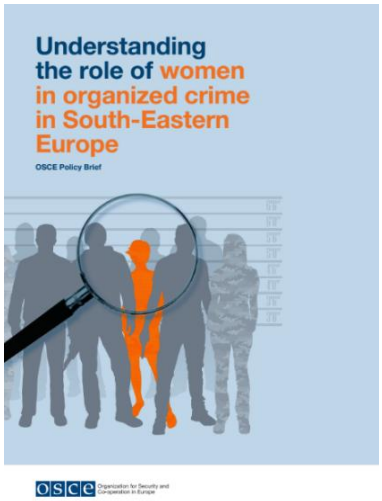
- **UPR може бути використаний як каталізатор для виконання антикорупційних рекомендацій IRM, FATF, GRECO та інших механізмів.** Внесення антикорупційних питань у UPR перетворює технічні рекомендації на міжнародні політичні зобов'язання держав, підвищуючи імовірність реального виконання.
- **Конкретність формулювань визначає результат.** Загальні рекомендації майже не виконуються; натомість SMART-рекомендації з чіткими індикаторами та посиланнями на міжнародні стандарти демонструють значно вищий рівень імплементації.
- **Громадянське суспільство є вирішальним суб'єктом у процесі UPR.** CSO формують порядок денний, надають ключову інформацію та здійснюють моніторинг виконання — значно ширше та впливовіше, ніж у механізмі IRM.
- **Ефективна боротьба з корупцією починається з її визнання як порушення прав людини.** Коли антикорупційні вимоги формулюються через призму доступу до послуг, недискримінації та справедливості, держави значно частіше підтримують і виконують такі рекомендації.

рекомендацій щодо корупції сформульовані надто загально («продовжити боротьбу з корупцією», «посилити заходи проти хабарництва»), що ускладнює їхнє відстеження і контроль виконання. Автори підкреслюють ключову значущість формування рекомендацій у форматі SMART — конкретних, вимірюваних, досяжних, релевантних та обмежених часовими рамками — і показують, як CSO можуть впливати на якість рекомендацій, пропонуючи державам чіткі формулювання, прив'язані до міжнародно-правових стандартів та реальних контекстних проблем.

Документ пропонує детальний алгоритм участі громадянського суспільства на всіх етапах UPR: від підготовки подань, адвокації з дипломатичними місіями й участі в національних консультаціях — до моніторингу реалізації рекомендацій та підготовки середньострокових оцінок виконання. Автори наголошують на важливості побудови коаліцій CSO, обміну даними та координації дій для посилення впливу — приклади з Мадагаскару, Перу, Кенії та інших країн показують, що саме колективна адвокація та використання UPR як довгострокового інструменту, а не разової події, призводять до реальних політичних змін.

Наприкінці документ підкреслює, що боротьба з корупцією — це не лише кримінальне переслідування винних, а передусім гарантування прав людини, доступу до ресурсів і справедливості для громадян. UPR дає унікальну можливість перетворити антикорупційні ініціативи на міжнародні зобов'язання держав і створити підзвітність, яка виходить за межі політичних циклів і зміни влади. Саме тому автори закликають громадянське суспільство у всьому світі використовувати UPR для того, щоб зробити корупцію видимою як правозахисну проблему, забезпечити адресні та вимірювані рекомендації і добиватися їх імплементації у довгостроковій перспективі — оскільки без подолання корупції не може бути повноцінного захисту прав людини та розвитку сильних демократичних інституцій.

Невидимі учасниці: як недооцінка ролі жінок знижує ефективність боротьби з ОЗГ у Південно-Східній Європі [3]



Документ висвітлює системну та досі недооцінену роль жінок у структурі організованої злочинності в Південно-Східній Європі, описуючи, як жінки залучаються до кримінальних мереж, які функції вони виконують та які бар'єри заважають їхньому виходу з цих структур. Попри те, що регіон Південно-Східної Європи є ключовим транзитним вузлом для наркотиків, зброї та інших незаконних товарів між Азією, Близьким Сходом та Західною Європою, а діяльність організованих злочинних груп формує суттєві ризики для безпеки, економіки та верховенства права, участь жінок у злочинних мережах все ще сприймається крізь призму стереотипу «допоміжних» або «пасивних» учасниць. Цей хибний підхід створює критичний аналітичний та операційний сліпий кут: жінки залишаються «невидимими» для системи кримінального правосуддя, що дозволяє їм діяти з відносною безкарністю та обмежує ефективність загальної протидії організованій злочинності.

Залучення жінок і дівчат до кримінальних структур у регіоні демонструє складну природу, у якій переплітаються соціальні, економічні та психологічні чинники. Найчастіше рекрутинг жінок відбувається через сімейні та романтичні зв'язки: у випадках, коли жінки народжуються в кримінальних сім'ях або стають частиною таких структур через шлюб, вони нерідко отримують підвищений рівень довіри та швидке просування всередині ієрархії, аж до рівня радниць,

[3] https://www.osce.org/files/f/documents/0/a/601494.pdf

координаторок та керівниць операціями. Однак наявні дані також свідчать про те, що жінки вербуються й поза межами сімейно-кримінальних традицій: соціально-економічна маргіналізація, попереднє насильство, потреба фінансового виживання та брак життєвих можливостей формують ґрунт для їхнього залучення. Окремо відзначається сучасний тренд, що знижує роль примусу і натомість посилює вплив романтизованої образності кримінального світу — гламуризації «легких грошей» і демонстративної розкоші на платформах соціальних мереж, що особливо впливає на підлітків і молодих жінок.

Роль жінок у злочинних мережах набагато ширша, ніж традиційно описується правоохоронною статистикою. Вони присутні в усіх сегментах кримінальної економіки — від низових і технічних функцій до ключових управлінських та стратегічних позицій. У сфері наркотрафіку жінки виступають як кур'єри, перевізниці, зберігачі та розповсюджувачі наркотичних засобів, а також як особи, які планують логістику, контролюють якість товару, організовують міжнародне постачання і приймають управлінські рішення. У торгівлі зброєю жінки залучені до укладання угод, транспортування, укриття та підтримки контактів між учасниками злочинних ланцюгів, а окремі жінки очолюють операції із закупівлі й продажу зброї різним злочинним групам. У торгівлі людьми фіксується подвійний характер жіночої участі: частина жінок, які колись були жертвами експлуатації, згодом залучаються до контролю інших жінок і набувають ролей вербувальниць або координаторок, тоді як інша частина має незалежну кримінальну активність і займає лідерські позиції, плануючи фінансові та логістичні операції. Особливо цікавою є жіноча агентність у відмиванні коштів: жінки стають фінансовими менеджерками, контролюють рух коштів через банківські канали, працюють із схемами легалізації через готівкові та безготівкові активи, займаються міжнародними переказами та використовують бізнес-структури для маскування кримінальних доходів. Доказування провини жінок у фінансових злочинах виявляється складним, оскільки активи часто формально зареєстровані на них, але без прямих документальних слідів управління.

Документ оскаржує поширений стереотип про «непритаманність насильства жінкам» і демонструє, що жінки беруть участь не лише у виконанні насильницьких дій, а й у їх плануванні та замовленні. В умовах кримінальних конфліктів, особливо пов'язаних із ринком кокаїну, жінки можуть виступати ініціаторками актів помсти, координувати «засідки», брати участь у залякуванні, в тому числі використовуючи особисті та емоційні зв'язки для заманювання цілей у пастки. Хоча реальна участь жінок у насильницьких сценаріях підтверджена на практиці, кількість вироків проти них залишається низькою через складність

Висновки:

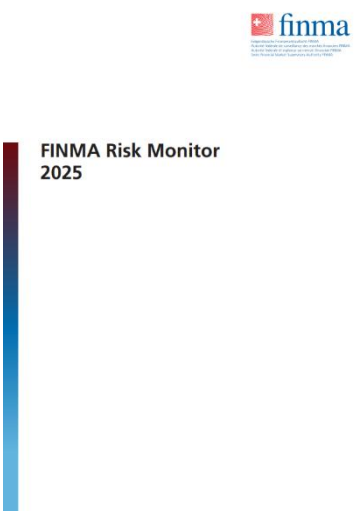
- **Боротьба з організованою злочинністю у регіоні має гендерний сліпий кут:** правоохоронні органи часто не розпізнають жінок як активних учасниць та керівниць ОЗГ, що знижує ефективність розслідувань і сприяє безкарності.
- **Жінки можуть бути вирішальним джерелом розвідувальної інформації для викриття кримінальних мереж,** однак вони майже не залучаються до програм співпраці та захисту свідків; їх включення здатне суттєво підвищити результативність кримінальних проваджень.
- **Причини залучення жінок до кримінальності здебільшого передбачувані — соціально-економічна вразливість, досвід насильства, романтизація злочину у соцмережах,** — тому ефективна профілактика має робити акцент на раннє втручання, фінансову стійкість та формування альтернативних моделей успіху.
- **У наркоторгівлі та відмиванні доходів жінки дедалі частіше виступають як організаторки, а не виконавиці;** для розслідувань потрібна адаптація інструментів доказування, аналітика активів і підсилення перевірки бенефіціарного контролю.

доведення їхньої ролі як «мозкового центру» злочину.

Вихід жінок з організованої злочинності пов'язаний з численними бар'єрами. Емоційні зв'язки, страх за життя дітей, брак фінансової самостійності, ризик помсти з боку кримінальних спільнот, психологічна травма й відсутність життєздатних альтернатив значно ускладнюють розрив із кримінальним середовищем. Особливо складною є відмова від участі у кримінальних мережах у сімейно-орієнтованих структурах, де особисте життя та злочинна діяльність є нероздільними. При цьому системи захисту свідків практично не адаптовані до специфічних потреб жінок і майже не передбачають підтримку материнства, що ще більше обмежує їхню включеність у співпрацю з органами правосуддя. Попри це, саме жінки часто володіють найціннішою інсайдерською інформацією щодо внутрішньої структури ОЗГ, каналів постачання, фінансових потоків та рішень керівництва, що робить їх потенційно найважливішими свідками для викриття злочинних мереж.

У фінальній частині документ підкреслює, що успішна боротьба з організованою злочинністю у Південно-Східній Європі неможлива без інтеграції гендерно-чутливого підходу, який визнає реальні ролі жінок у кримінальних структурах, а не зводить їх до статусу «жертв» або «периферійних фігур». Це стосується зміни методологій розслідування, модернізації інструментів доказування у фінансових злочинах, ранньої профілактики та розширення доступу жінок до програм виходу, реабілітації та захисту свідків. Поглиблення регіональної співпраці між правоохоронними органами, підвищення обізнаності про гендерні особливості злочинної діяльності та удосконалення механізмів збору даних визначаються критично необхідними для підвищення ефективності протидії транснаціональній організованій злочинності.

Нагляд нового покоління: як FINMA змінює правила гри у сфері ризик-менеджменту та комплаєнсу [4]



Документ є системним оглядом ключових ризиків, що визначають стійкість швейцарського фінансового сектору протягом найближчих трьох років, та одночасно демонструє, як фінансовий нагляд переходить від класичної фінансової стабільності до моделі превентивної, випереджувальної та операційно орієнтованої регуляції. У вступній частині FINMA підкреслює, що макроекономічне середовище змінилося — після короткочасного зниження темпів інфляції у низці країн світу спостерігається її повторне зростання під впливом зростання цін на енергоносії та торговельних рішень США, що провокують рецесійні очікування і посилюють нестабільність глобальних ринків. Це поєднується з підвищеною геополітичною напругою, а також із наслідками структурних економічних змін, що підвищують невизначеність для фінансових інститутів. FINMA наголошує, що відповідальність за управління ризиками належить не лише наглядовому органу, а насамперед самим установам — від якості їхньої ризик-культури, стратегічних рішень і внутрішніх систем залежить здатність протистояти шокам. Тому нагляд зосереджений на тому, щоб інститути не просто реагували на ризики, але й ефективно передбачали та попереджували їх.

У 2025 році ключовим системним ризиком FINMA визначає ризики, пов'язані з нерухомістю та іпотечним кредитуванням. Швейцарія має один із найвищих у світі рівнів іпотечної заборгованості відносно ВВП, а сповільнення цін на нерухомість після завершення періоду

[4] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/risikomonitor/20251117-finma-risikomonitor-2025.pdf?sc_lang=en

негативних ставок не усунуло ризик перегріву ринку. FINMA спостерігає, що банки широко використовують відступи від власних політик доступності кредиту, що може збільшувати кредитні збитки в умовах корекції ринку. Іпотека становить основний вид кредитних активів роздрібних банків і значну частку інвестиційних портфелів страхових компаній та нерухомих фондів, а тому корекція цін на нерухомість має потенціал трансформуватися у системну фінансову нестабільність. За цим слідує розділ про кредитний ризик за іншими позиками, у якому наголошено, що період низьких ставок спричинив надмірне розширення кредитування, зокрема у сфері корпоративних позик та ломбардного кредитування. Інститути стикаються з підвищеною вразливістю до коливань ринкової вартості застави, а розвиток приватних небанківських кредитних ринків створює канал потенційного поширення шоків у банківський сектор.

Ринок капіталу приносить інший вид системної загрози — ризики розширення кредитних спредів, які можуть викликати знецінення портфелів, зростання вартості хеджування, проблеми з ліквідністю та втрату довіри до установ. Це особливо актуально в умовах посиленої геополітичної напруженості, високого рівня державного боргу окремих країн і нестабільності суверенних облігацій. FINMA також приділяє значну увагу ризикам ліквідності та фінансування — швидкість і масштабність відтоку депозитів у цифрову епоху зросли настільки, що навіть короткочасні інциденти можуть перетворитися у масове вилучення депозитів, посилені соціальними мережами. Додатковим джерелом вразливості є можливі обмеження доступу до фінансування у іноземних валютах у разі геополітичних рішень.

Висновки:

- **Необхідно посилити контроль критеріїв платоспроможності та мінімізувати відступи від внутрішньої політики іпотечного кредитування,** інакше нагляд може встановити додаткові капітальні вимоги або обмежити межі прийнятного ризику.
- **У корпоративному та ломбардному кредитуванні потрібно забезпечити раннє виявлення погіршення кредитоспроможності, своєчасне формування резервів і зменшення концентраційних ризиків,** враховуючи можливу передачу шоків від небанківських кредитних ринків.
- **Операційну стійкість слід проєктувати наперед:** резервні механізми ІКТ, контроль постачальників, ефективне управління інцидентами та регулярні навчальні моделювання кібератак мають бути невід'ємними елементами системи ризик-менеджменту.
- **У сфері ПВК і санкцій важливо формалізувати толерантність до ризику** на рівні ради директорів і посилити процедури щодо клієнтів високого ризику, цифрових активів та санкційних юрисдикцій, з урахуванням ризику вторинних санкцій США.

Комплаєнс-ризики залишаються центральними: ризик відмивання коштів залишається на підвищеному рівні, особливо у сфері управління активами та при роботі з країнами високого ризику. FINMA наголошує на значенні чітко визначеної толерантності до ризику на рівні ради директорів і суворих процедур для клієнтів високого ризику. Поруч із цим документ визначає санкційні ризики як критично високі: фінансовим установам необхідно не лише виконувати швейцарські санкції, а й враховувати ризики вторинних санкцій США, які створюють серйозні правові та репутаційні загрози навіть для установ, що діють виключно у третіх юрисдикціях.

Особлива увага приділяється передачі критичних функцій на виконання третім особам, що розглядається як одним із ключових операційних ризиків фінансової системи. Зростає залежність від невеликої кількості ключових постачальників інформаційно-комунікаційних технологій (ІКТ) та хмарних сервісів, що породжує системну загрозу: інцидент у зовнішнього провайдера може одночасно

паралізувати діяльність багатьох фінансових установ. Ця вразливість перегукується зі стрімким зростанням кібератак, особливо тих, що здійснюються через вразливості третіх осіб. FINMA відзначає збільшення DDoS-атак, фішингу, шахрайства із цифровими методами оплати та інцидентів, спричинених внутрішніми користувачами. На додачу до кіберзагроз, документ фіксує окремий блок ризиків ІКТ, пов'язаних зі складністю цифрових систем, вразливостями оновлень, недостатньою відмовостійкістю, людськими помилками й експлуатацією застарілої інфраструктури. Інцидент CrowdStrike 2024 року використовується як ілюстрація того, що навіть короткочасна технічна помилка у постачальника програмного забез печення (ПЗ) може призвести до масштабних збоїв і доводить необхідність створення IT-систем із вбудованою стійкістю.

У заключній частині документа розглядаються кліматичні ризики — як фізичні (стихійні лиха, підвищення температур), так і перехідні (політика декарбонізації, технологічні зміни, судові рішення та ринкові трансформації). FINMA наголошує, що експозиції банків та страхових компаній у секторах, критичних щодо кліматичної політики, є суттєвими, але їхня точна оцінка ускладнюється дефіцитом даних. Кліматичні ризики дедалі чіткіше трансформуються у фінансові, актуарні, комплаєнс і репутаційні ризики, та в середньостроковій перспективі можуть значно вплинути на стійкість фінансового сектору.

Узагальнюючи, звіт показує трансформацію викликів у фінансовій системі: домінування класичних фінансових ризиків зберігається, але одночасно швидко зростають ризики операційної стійкості, ІКТ, кібербезпеки, комплаєнсу та клімату. FINMA підтверджує, що регуляторна модель майбутнього ґрунтується не лише на капіталі та ліквідності, а на зрілій системі управління ризиками, прозорій структурі контролю, відповідальності ради директорів за визначення толерантності до ризику та постійному тестуванні здатності установ залишатися функціональними в умовах стресу, незалежно від джерела загрози — ринкового, технологічного чи геополітичного.

82,3 млрд доларів тіньової економіки: як транснаціональна злочинність змінює реальність Австралії [5]

Документ відкриває для громадськості те, що раніше залишалося прихованим — реальні масштаби, глибину і характер серйозної та організованої злочинності, яка вже не є ізольованим кримінальним явищем, а стала системним фактором, що формує безпеку, економіку, соціальні відносини й майбутнє Австралії. Відправною точкою звіту є акцент на тому, що суспільне уявлення про злочинність застаріле: образи з фільмів і серіалів охоплюють лише поверхню й створюють оманливу романтизацію злочину, приховуючи справжні наслідки — смерті, насильство, руйнування громад, корупцію, державні втрати та величезну економічну шкоду. Саме ці наслідки документ прагне показати прозоро, у комплексі та без ілюзій, з метою сформувати суспільну обізнаність і національну стійкість до загрози

У 2025 році серйозна та організована злочинність характеризується трансформацією, масштаб якої колосальний: злочинні мережі більше не мають локальних рамок і не функціонують у межах традиційних структур мафіозного типу. Вони стали глобальними, децентралізованими та цифровізованими бізнес-механізмами з високим рівнем тактичної адаптивності. Для цих груп характерна корпоративна логіка: стратегічність,

[5] https://www.acic.gov.au/sites/default/files/2025-11/Opening%20the%20books.PDF

планування, диверсифікація злочинних активів, аналіз ринкових можливостей, перенесення ризику на нижчі рівні виконання, інноваційність і гнучкість. Злочинці використовують технології не як допоміжний інструмент, а як стратегічну основу своєї діяльності, що дозволяє їм масштабувати операції, переховуватися у цифровому просторі, проводити фінансові операції з мінімальними слідами, а також централізовано керувати злочинами на відстані, перебуваючи у безпечних юрисдикціях за межами Австралії

Фінансова шкода, яку завдає ця діяльність, сягає 82,3 мільярда доларів на рік, і хоча цифра вражає, документ підкреслює, що ще небезпечнішим є її прихований характер — вона розподіляється у вигляді підвищення страхової вартості, втрат державних доходів, зростання цін, падіння довіри до інституцій, підвищеного навантаження на соціальні та медичні служби, непрямих наслідків для бізнесу й довгострокового впливу на соціальну стабільність. Кожен громадянин — навіть той, хто ніколи не стикався зі злочинністю напряму — стає її жертвою, оскільки вона збільшує витрати всіх, знижує рівень безпеки й підриває добробут суспільства

Наркобізнес лишається центральною, найприбутковішою та найнебезпечнішою складовою кримінальної економіки. Звіт підкреслює, що споживання наркотиків в Австралії — рекордне за всю історію, і ця внутрішня потреба стає двигуном агресивної експансії злочинних мереж, які заробляють на залежності та масово постачають наркотики на ринок. Зростає жорстокість боротьби між угрупованнями: випадкові вбивства через неправильну ідентифікацію, напад на сторонніх людей, підпали бізнесів, атаки на сім'ї членів конкуруючих угруповань, а в цифровому просторі — кампанії онлайн-залякування й шантаж. Особливо тривожним є зростання кількості смертей від синтетичних наркотиків, а також тенденції потайного змішування наркотиків і рідин для електронних сигарет із надпотужними опіоїдами, які користувачі навіть не підозрюють, що містять летальні складники. Так наркотики стають не лише товаром з високим попитом, а й інструментом смерті з непередбачуваним і вибуховим ефектом

Інший виразний вимір — кримінальна війна за ринок тютюну і вейпів, яка стала одним із найжорсткіших напрямів організованої злочинності. Зафіксовано більше 200 підпалів і щонайменше 3 вбивства з 2023 року, що відображає боротьбу не лише за прибуток, а й за силове домінування на ринку. Постраждали й ті, хто не має стосунку до злочинності: малий бізнес, сусіди, покупці, перехожі. Масштаб насильства настільки великий, що він має хвильовий вплив на ціни, страхові тарифи, конкурентоспроможність легального бізнесу й загальне відчуття безпеки в містах

Окремим прошарком шкоди є експлуатація державних програм, особливо NDIS. Злочинні групи перемикають свою діяльність туди, де є високі бюджетні потоки й низький рівень персоналізованого контролю. Вони підкорюють собі клієнтів — найуразливіших людей — через маніпуляцію, погрози та залежність, і замість послуг фактично привласнюють бюджет, залишаючи людину без підтримки. Це не лише фінансові втрати для держави — це руйнування довіри суспільства до соціальних гарантій, що створює непрямі соціальні ризики майбутнього

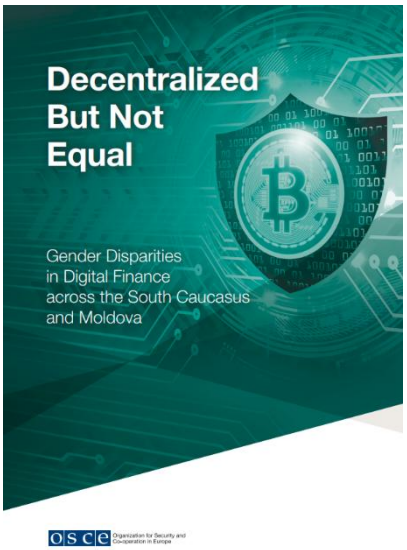
Найпомітніша трансформація злочинності — це її цифровізація, а також технологічне оснащення. У звіті детально зафіксовано появу нових цифрових злочинних екосистем, які працюють паралельно з легальним інтернетом і створюють середовище майже повної невразливості. Там здійснюються торгові операції, інструктаж, навчання, фінансові розрахунки в криптовалюті, замовлення послуг насильства, торгівля наркотиками, зброєю, експлуатаційними відеоматеріалами та викраденими особистими даними. Поширюється і співіснування фізичного та цифрового насильства: шантаж через інтернет, який переходить у реальні атаки, або реальні побиття, що транслюються і розповсюджуються онлайн як елемент психологічного контролю над аудиторією. Зростає використання штучного інтелекту, технологій, пов’язаних з діпфейками, автоматизованих кіберінструментів та 3D-друкованої

зброї — технології, що були експериментальними десять років тому, тепер стали частиною кримінального арсеналу, який розширює автономність і непередбачуваність злочинних груп

Нарешті, звіт описує тривожну тенденцію — цілеспрямоване вербування неповнолітніх, використання дітей для виконання брудної роботи й еволюцію молодіжних банд у повноцінні злочинні мережі. Молодь стає знаряддям злочинності завдяки вразливості, психологічному тиску, бажанню «статусності» та легкості цифрового доступу. Сучасні молодіжні групи мають потенціал перерости у найнебезпечніші кримінальні мережі майбутнього — приклад, наведений у документі, показує, як підліткова банда за два десятиліття перетворилася на повноцінне транснаціональне угруповання, що здійснює торгівлю наркотиками та фінансові злочини вже незалежно від старших кримінальних структур

Завершальна частина документа наголошує, що правоохоронні органи досягають помітних успіхів — масштаби вилучень наркотиків, розкритих шахрайств і ліквідованих мереж відображені в заголовках новин — але ці результати не означають зменшення загрози. Злочинність не просто масштабується — вона інтелектуалізується, уникає однотипності, реагує на тиск з боку держави і змінюється швидше, ніж змінюється система протидії. Тому ключовим стає не лише кримінальне переслідування, а й суспільне усвідомлення того, що серйозна організована злочинність — це системний і структурний виклик, у якому участь бере кожен рівень суспільства, і який впливає на всіх — від дитини, яка стикається з онлайн-шантажистом, до підприємця, чий бізнес згорів через ринкове рейдерство, до платника податків, який фінансує збитки, завдані злочинцями, не усвідомлюючи цього. Документ закінчується меседжем, що боротьба з організованою злочинністю вже не може базуватися виключно на зусиллях поліції — для створення стійкого суспільства потрібна поєднана реакція держави, бізнесу, медіа, місцевих громад і кожного громадянина, оскільки загроза набула масштабу, який робить її суспільним, а не лише кримінальним викликом.

Web 3.0 — нова економіка зі старими бар'єрами: Гендерний розрив у криптовалютах і DeFi [6]



Документ розглядає цифрові фінанси як подвійний феномен: з одного боку, вони руйнують історичні бар'єри доступу до капіталу й обіцяють демократизацію фінансової системи, а з іншого — вони спираються на нерівні передумови, унаслідок чого реальні вигоди отримують не всі, а передусім ті групи, які вже мали доступ до економічних і технологічних ресурсів. Ця суперечність є центральним парадоксом Web 3.0: технологія, створена для розширення можливостей кожної людини незалежно від статі, віку, географічного розташування чи економічного статусу, фактично стає простором, у якому беруть участь переважно чоловіки. Децентралізація усуває посередників, але не усуває соціально-економічну нерівність, яка визначає здатність людини розпочати інвестиційну діяльність, навчитися фінансовим інструментам, робити помилки без страху втратити останні ресурси та формувати власний капітал. Для того щоб використати можливості Web 3.0, потрібно увійти у нього з багажем навичок і ресурсів: впевненим користуванням технологіями, доступом до освітньо-інвестиційних можливостей, готовністю до фінансового ризику, досвідом прийняття рішень та наявністю заощаджень, які дозволяють ризиковані вкладення. Саме ці передумови структурно

[6] https://www.osce.org/files/f/documents/0/c/593639_0.pdf

частіше наявні у чоловіків, а не у жінок, що і пояснює різницю в їхній участі у цифрових активах та криптовалютній економіці.

Документ послідовно показує, що гендерний розрив у Web 3.0 не виникає у моменті — він починається задовго до появи криптовалют і не має нічого спільного з особистою зацікавленістю жінок, а є прямим наслідком того, як формуються соціальні ролі. Дівчат рідше заохочують до STEM, фінансової поведінки та технологічної кар'єри; жінки рідше потрапляють у технічні і високооплачувані сфери; вони стикаються з невидимими структурними обмеженнями доступу до керівних посад у корпоративному середовищі; їхня праця оплачується гірше; економічна поведінка жінок має бути обережнішою, оскільки саме вони частіше відповідають за добробут родини. У цих обставинах інвестиційні ризики набувають іншого виміру — для жінки невдала криптовалютна угода може стати критичним ударом по фінансовій безпеці сім'ї, тому відмова від ризикових інструментів — не недостатність амбіцій, а раціональна реакція на нерівні умови. Саме тому вислів «жінки менше інвестують, бо їм нецікаво» документ повністю спростовує: реальна причина полягає в тому, що соціум дозволяє чоловікові ризикувати, а жінці — ні.

Далі автори переходять до ще глибшого висновку: нерівність у Web 3.0 закладена не лише у доступі до фінансів, а й у структурі самої технологічної екосистеми. Web 2.0 був побудований здебільшого чоловіками, і саме вони визначали естетику, правила гри, комунікаційні патерни, цілі та навіть кодекс поведінки. Коли Web 3.0 почав формуватися, у нього перенесено не тільки програмні навички й технічний досвід старших поколінь IT-фахівців, а й закріплені в культурі патерни виключення, конкуренції, токсичної успішності, культу ризику й фінансової агресивності. Тому для жінки Web 3.0 — це не одна перешкода, а одразу кілька: технологічна необізнаність, ринкова необізнаність та культурна невключеність. Саме тому залучення жінок до криптовалютної екосистеми не є питанням одномоментної дії, а являє собою послідовність комплексних бар'єрів, подолання яких потребує часу, інституційної підтримки та доступу до відповідних ресурсів.

Регіональний аналіз, зосереджений на Вірменії, Азербайджані, Грузії та Молдові, показує, що ці бар'єри набувають різних форм, але завжди приводять до одного результату — жінка входить у цифрову економіку із суттєвим запізненням або не входить зовсім. У цих країнах жінки здобувають освіту не гіршу, ніж чоловіки, але система економічних можливостей не винагороджує їх за це: вони найчастіше залишаються у професіях з низькою оплатою і нестабільними перспективами, бо

Висновки:

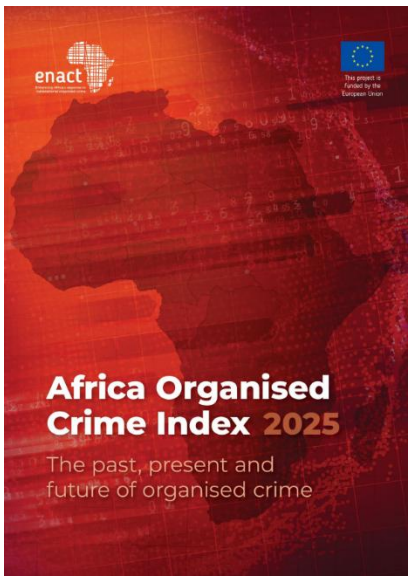
- **Децентралізовані фінансові технології об'єктивно створюють можливості для фінансової інклюзії жінок,** але без цілеспрямованих дій цей потенціал не реалізується — Web 3.0 відтворює існуючі структурні гендерні бар'єри.
- **Основні причини низької участі жінок у криптовалюті та DeFi —** дефіцит фінансової та технологічної освіти, культурні та соціальні стереотипи, недовіра до криптовалют і відсутність безпечних освітніх маршрутів для входу у сферу цифрових активів.
- **Державна та приватна політика у сфері цифрових фінансів у Вірменії, Азербайджані, Грузії та Молдові поки не забезпечує системного усунення гендерних розривів —** освітні, регуляторні та бізнес-ініціативи фрагментовані і не працюють на спільну інклюзійну мету.
- **Найбільш ефективні механізми для зменшення гендерної нерівності у цифрових фінансах —** створення інституційних програм фінансової грамотності для жінок, розвиток STEM-освіти, менторських мереж, інклюзивний дизайн Web 3.0-продуктів і залучення жінок до формування політик і ринку цифрових активів.

високооплачувані й технологічні позиції традиційно виявляються соціально «чоловічими». Наслідок — відсутність накопичень, а відсутність накопичень означає економічну неможливість інвестувати, а отже — неможливість створювати фінансовий капітал майбутнього. Формула, що повторюється в усіх країнах, звучить надзвичайно лаконічно і жорстко: освіта жінок не конвертується в економічні можливості.

Саме через це документ попереджає про один із найбільш недооцінених ризиків цифрової епохи: якщо Web 3.0 буде надалі зростати без інклюзійної політики, фінансова нерівність між чоловіками та жінками стрімко збільшиться, не тому що жінки роблять менше, а тому що вони почали пізніше. Ефект складного проценту працює не тільки у фінансах, але й у доступі до фінансової влади: хто починає інвестувати на старті технологічного циклу, той має експоненційно більше можливостей у майбутньому. Якщо ці можливості концентруються серед чоловіків, тоді майбутнє цифрової економіки — це новий виток чоловічої домінації у сфері фінансів, інвестицій, контролю над активами і формуванням економічних правил.

У найглибшому сенсі документ говорить про те, що питання доступу жінок до цифрових фінансів — це не соціальна «опція», а фундаментальний критерій того, чи Web 3.0 справді стане новою економічною моделлю або ж стане повторенням старої з іншою технологічною оболонкою. Якщо у Web 3.0 жінка не зможе бути не лише користувачкою, а й розробницею, інвесторкою, підприємницею, лідеркою спільноти, творцем ринку й архітекторкою фінансової інфраструктури, тоді цифрова революція не стане революцією рівних можливостей. Технологія не створює рівність — рівність створює політика, культура та інклюзивна архітектура системи. Тому майбутнє цифрової економіки залежить від того, чи будуть жінки частиною Web 3.0 зараз, а не потім.

Африка 2025: еволюція організованої злочинності та крах державної стійкості на тлі зростання кримінальних економік [7]



Документ є комплексним узагальненням еволюції організованої злочинності на африканському континенті та водночас індикатором того, наскільки кримінальні мережі стали системним елементом політичної економії значної частини держав. У звіті переконливо показано, що наявні тенденції набули довготривалого характеру: ступінь кримінальності в Африці протягом 2019–2025 років підвищувався безперервно, тоді як загальна інституційна стійкість континенту залишалася на нижчому рівні та не демонструвала тектонічних покращень. У цьому дисбалансі полягає ключовий і найбільш тривожний висновок — кримінальні ринки адаптуються, еволюціонують та розширюються швидше, ніж держави здатні модернізувати механізми протидії. Організована злочинність не є периферійним явищем чи «тіньовою» частиною економіки: вона інтегрована в структури управління державами, у форми господарювання, ланцюги постачання та політичні процеси, визначаючи економічні пріоритети та соціальну поведінку населення на великих територіях.

Континент одночасно виступає джерелом, транзитною артерією та кінцевим пунктом для різноманітних кримінальних ринків, які охоплюють широкі географічні простори та працюють у багаторівневій взаємодії. Вибухове зростання фінансових злочинів — від шахрайства до

[7] https://globalinitiative.net/wp-content/uploads/2025/11/Africa-Index-2025-WEBv2.pdf

відмивання коштів і незаконних транскордонних переказів — відображає цифрову трансформацію злочинності. Торгівля людьми, попри багаторічні програми протидії, залишається одним із найбільш маржинальних і стабільних ринків, який живиться бідністю, конфліктами та вразливістю кордонів. Незаконне добування й вивезення невідновлюваних ресурсів — золота, нафти, критичних мінералів і дорогоцінного каміння — формує економічні моделі, у яких держава формально володіє ресурсною базою, але фактично не контролює її. Ланцюги контрабанди наркотиків з'єднують Африку з глобальними потоками: кокаїн із Південної Америки рухається через Західну Африку до Європи, героїн з Афганістану — через Східну Африку, синтетичні наркотики розширюють ринки у Південній та Західній Африці, тоді як канабіс продовжує домінувати в Північній частині континенту. Ринок фальсифікованої продукції стрімко інтенсифікувався, поєднуючи місцеве неформальне виробництво, нелегальний імпорт і наднаціональні логістичні маршрути, що робить його одним із найгнучкіших і найменш контрольованих секторів злочинності.

Водночас звіт демонструє, що ключовим фактором поширення кримінальних ринків є не лише попит і прибутковість, а й те, хто саме виступає їх рушієм. Індекс однозначно встановлює, що найвпливовішими злочинними учасниками в Африці є державні посадові особи — представники влади, політичні лідери, службовці органів безпеки та державних структур, які через корупцію, тіньові договори й зловживання владою фактично гарантують кримінальним групам легітимність і недоторканність. У низці країн це не є відхиленням від норми, а частиною системи врядування: державні інституції та кримінальні інтереси переплітаються настільки, що кордон між ними стає практично нероздільним. Ці гібридні моделі створюють паралельні форми влади, в яких формально існує державне управління, але реально економічна й силова логіка контролю визначається злочинними мережами, що використовують державу для забезпечення власної вигоди.

Особливу увагу документ приділяє ролі конфліктів як каталізатора злочинності. У регіонах із хронічними війнами та політичним колапсом — таких як Сахель, Сомалі, Судан, ДР Конго — організована злочинність не просто супроводжує нестабільність, а стає її основоположним та стимулюючим елементом. На цих територіях кримінальні групи контролюють видобуток ресурсів, транспортування товарів, міграційні потоки, оподаткування населення та навіть функції безпеки. Торгівля людьми та зброєю, незаконна експлуатація природних ресурсів і

Висновки:

- **Кримінальність у Африці зростає швидше, ніж здатність держав протидіяти їй.** За 2019–2025 роки показники організованої злочинності стабільно підвищувались, тоді як інституційна стійкість більшості країн або не покращувалась, або знижувалась, що сформувало стійкий дисбаланс на користь злочинних груп.
- **Державні посадові особи, залучені у злочинність, є найпотужнішими кримінальними учасниками.** Саме державні структури та представники влади — а не зовнішні чи мафіозні організації — є основним фактором підтримки та відтворення кримінальних економік через корупцію та зловживання владою.
- **Кримінальні ринки розширюються та ускладнюються.** У 2025 році домінують фінансові злочини, торгівля людьми, незаконний видобуток ресурсів, підробка і торгівля зброєю, а найшвидший ріст відбувається у фінансових злочинах та підробці — з переходом до глобальних і цифрових моделей.
- **Збройні конфлікти та гуманітарні кризи безпосередньо підсилюють кримінальність.** Регіони з тривалими війнами та політичним колапсом систематично демонструють найвищі рівні торгівлі людьми, зброєю, ресурсами й найслабшу стійкість державних інститутів — формуючи середовище, де кримінальні структури фактично заміщують державу.

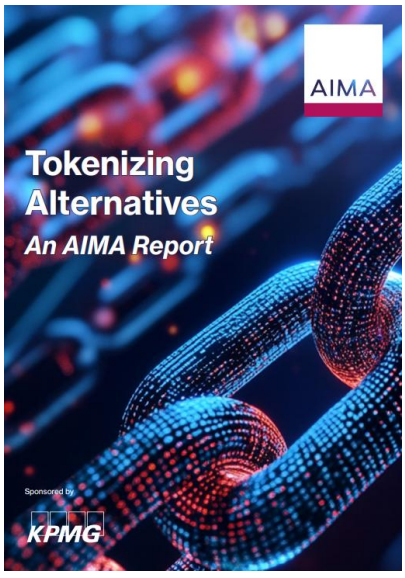
рекет сприяють фінансуванню конфліктів, зберігають вплив недержавних збройних формувань і виснажують інституційну стійкість держави. Конфлікти й злочинність у цьому контексті не є окремими явищами — вони живлять одне одного, створюючи замкнене коло, у якому зростання кримінальних прибутків забезпечує тривалість насильства та руйнування державності.

Новим і стрімко зростаючим виміром злочинності стала цифрова екосистема. Інтернет, фінансові технології, криптовалюти, цифрові гаманці та віддалені комунікаційні інфраструктури дали кримінальним мережам нові можливості уникати фізичних кордонів, анонімізувати платежі та масштабувати діяльність без територіальної прив'язки. Цифрові схеми фінансового шахрайства, злам даних, онлайн-рекрутування та вимагання поступово інтегруються з традиційними ринками, утворюючи єдину кримінальну мережу, у якій цегляні та «віртуальні» операції доповнюють одна одну.

Незважаючи на деякі позитивні зміни, переважна більшість африканських держав продовжує демонструвати низький рівень стійкості до організованої злочинності. Законодавчі реформи, міжнародні домовленості та участь у програмах протидії часто обмежуються декларативністю й не переходять у практичну площину. Найслабшими є саме ті компоненти, які безпосередньо протистоять кримінальному впливу на суспільство: захист жертв і свідків, превентивні програми для молоді, підтримка незалежних медіа та громадянського сектору, інструменти місцевої доброчесності та доброчесності публічних службовців. У підсумку звіт робить принциповий висновок: якщо інституційні реформи, соціальна політика та контроль над корупцією не випереджатимуть розвиток злочинних ринків, організована злочинність продовжить поглиблювати структурні проблеми Африки — підриваючи державність, економічний розвиток, безпеку та легітимність влади.

Звіти окремих інституцій та експертів

Токенізація як драйвер глобальної конкуренції на ринку альтернативних інвестицій: доступність, ліквідність, операційна ефективність [8]



Документ пропонує масштабне бачення того, як токенізація альтернативних інвестицій — через перенесення прав власності й операційних процесів у блокчейн-інфраструктуру — здатна переформатувати глобальну індустрію управління капіталом. У традиційному вигляді альтернативні інвестиції характеризуються обмеженою доступністю для інвесторів, високими мінімальними сумами входу, тривалими періодами замороження коштів та фрагментованою інфраструктурою, де розрахунки, облік, адміністрування, комплаєнс і перевірки здійснюються окремими суб'єктами з високим рівнем ручних операцій. Токенізація пропонує зміну не окремих елементів, а фундаментального принципу: замість централізованого обліку й посередницького характеру процесів інвестиційний фонд стає цифровим, програмованим, фракційним та взаємодійним фінансовим механізмом, у якому інвестор отримує частку не у вигляді паперової чи реєстрової позиції, а у вигляді токена, що несе всю економічну сутність активу, права власності й правила поведінки.

[8] https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2025/10/AIMA-Report-on-Tokenizing-Alternatives.pdf

Документ наголошує, що найбільш відчутний ефект токенізації полягає у здатності демонетизувати бар'єр входу в альтернативні інвестиції: інвестор, який раніше міг отримати доступ лише за наявності мільйона або десятків мільйонів доларів, тепер може володіти часткою активу у значно меншому розмірі завдяки фракціонуванню токенів. Це докорінно змінює структуру попиту: замість обмеженого пулу інституційних учасників формується глобальна база інвесторів, включно з високостатусними фізичними особами, користувачами цифрових активів, цифровими фондами, DAO, казначейськими фондами цифрових активів, що управляють резервами стейблкоїнів та платформами автоматичного управління активами. Традиційна географічна й юридична «прив'язаність» фондів втрачає значення, оскільки токенізація дає можливість залучати інвесторів без фізичної присутності на локальних ринках. Саме тому автори прогнозують перехід альтернативного інвестування від регіонально сегментованої моделі до глобальної розподіленої конкуренції між фондами.

Поряд із доступністю важливо місце займає ліквідність. Фонди альтернативного класу історично працюють за принципом довгострокового закритого капіталу і практично позбавлені вторинного ринку. Токенізація відкриває можливість формувати майже безперервну вторинну торгівлю частками та використовувати токенізовані активи як заставу для отримання фінансування або внутрішнього рефінансування всередині портфеля, що істотно зменшує неефективний простій капіталу в період між виходом з інвестиції та повторним залученням у нову угоду. Це означає, що капітал, замість того щоб залишатися бездіяльним, може працювати постійно та генерувати дохід у безперервному циклі. У довгостроковій перспективі токенізація здатна не лише усунути структурну проблему ліквідності, а й перетворити частки у фондах на повноцінні фінансові інструменти, придатні для маржинального фінансування, застосування кредитного плеча та інтеграції в алгоритмічні ринки. Проте нинішній рівень ліквідності все ще обмежений через відсутність стандартизованої інфраструктури вторинного ринку та нерівномірну зацікавленість інституційних інвесторів.

Окремий смисловий блок звіту присвячено тому, що токенізація приносить структурну операційну ефективність завдяки смарт-контрактам. Адміністрування фондів, яке сьогодні потребує окремих департаментів і зовнішніх провайдерів (агент з обліку прав власності інвесторів, адміністратор інвестиційного фонду, кастодіан (зберігач активів), податкова звітність), може виконуватися алгоритмічно. Вимоги щодо внесення капіталу, розрахунки з інвесторами, оновлення чистої вартості активів, перевірка інвесторів за переліком допущених, накладання обмежень для окремих юрисдикцій, автоматизація виплат комісій за управління та комісій за результативність, а також механізми корпоративного управління і голосувань можуть бути інтегровані безпосередньо у токен. Це означає, що індустрія переходить від моделі «адміністрування активів» до моделі «програмованих активів», де виконання правил забезпечується технологією, а не ручними процесами.

Водночас у документі наголошено, що масштабне впровадження токенізації неможливе без вирішення нормативно-правових і технологічних передумов. Однією з ключових є наявність регульованих стабільних цифрових засобів оплати, які дозволяють забезпечити повний інвестиційний цикл без виходу за межі блокчейн-середовища. Не менш важливою є роль кастодіального зберігання, до якого регулятори ставляться особливо уважно: токенізація не скасовує вимог щодо безпечного зберігання цінних паперів, а трансформує їх у вимоги до захисту приватних ключів, безпечності смарт-контрактів та надійності інфраструктури. Регулятори США, ЄС, Сінгапуру та Швейцарії поступово переходять від моделі «регулювання через санкції» до моделі «регулювання через визначені правила», визнаючи, що токен є способом фіксації прав власності, а не новим видом фінансового інструменту. Фондові юрисдикції, які швидше адаптують нормативні режими під токенізовані інвестиційні структури, зможуть отримати конкурентну перевагу як місця доміціляції фондів нового покоління — яскравим прикладом виступає Люксембург.

Висновки:

- **Токенізація альтернативних активів є структурною інновацією, що здатна радикально змінити ринок альтернативних інвестицій,** розширивши доступ до капіталу, знизивши поріг входу та забезпечивши потенційне масштабування інвестиційної бази через фракціонування та глобальний цифровий розподіл.
- **Смарт-контракти та програмовані цифрові токени можуть суттєво підвищити операційну ефективність фондів, автоматизувавши ключові процеси —** такі як вимоги щодо внесення капіталу, розподіл доходів, розрахунки, звітність та корпоративне управління — що змінює традиційну модель адміністрування альтернативних інвестицій.
- **Основним фактором, що стримує розгортання токенізації на інституційному рівні,** є регуляторна невизначеність та відсутність узгоджених підходів до кастодіального зберігання цифрових активів, кібербезпеки, відповідності KYC/ПВК/ФТ та захисту інвесторів.
- **Токенізація розглядається як потенційна третя фундаментальна еволюція індустрії управління активами —** після підйому взаємних фондів та ETF — але її реалізація залежить від досягнення критичної маси ліквідності, зрілої інфраструктури вторинних ринків і узгодженого регуляторного середовища.

Фінальна частина звіту підкреслює, що токенізовані активи ще не досягли масштабу, потрібного для повної трансформації ринку: глибина торгів поки недостатня, інфраструктура вторинних майданчиків фрагментована, а інституційні учасники стримані через вимоги комплаєнсу та ризики кібербезпеки. Проте тенденція є незворотною: зростання капіталізації стабільних цифрових активів, поширення активів реального сектору у децентралізованих фінансових сервісах, зростання кількості інвесторів, які прагнуть залишатися в блокчейн-середовищі, та прискорення нормативної еволюції вказують на наближення переломного моменту. У перспективі токенізація здатна сформувати нову модель глобального руху капіталу, у якій альтернативні інвестиції перестають бути прерогативою вузького кола інституцій, а стають інтегрованою складовою цифрової фінансової екосистеми — доступною, прозорою, безперервною та взаємодійною.

Фінтех як точка входу до фінансової системи: як уникнути використання платформ у схемах відмивання коштів та обходу санкцій [9]

Документ підкреслює, що екосистема фінтех не просто розширила спектр фінансових послуг, а повністю змінила їхню логіку, зсунувши центр тяжіння з традиційної банківської моделі до цифрових, гнучких і високотехнологічних платформ, де фінансові операції стають миттєвими, транскордонними і доступними в один клік. Це створило історичний прорив для фінансової інклюзії та споживацької зручності, однак одночасно сформувало нову площину ризиків, значно складнішу для контролю, ніж у традиційному фінансовому секторі. Автор наголошує, що сама природа фінтеху — швидкість, автоматизація, безперешкодне масштабування та мінімізація прямого контакту з клієнтом — формує середовище, у якому межа між легітимними транзакціями і злочинними схемами стає надто тонкою. Реалії цифрового середовища, у якому клієнт може створити рахунок, провести транзакцію або перемістити активи, не взаємодіючи фізично з установою, збільшують імовірність використання платформи для відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення, при цьому приховуючи кінцевий зміст, одержувачів та схеми переміщення коштів.

Автор наголошує, що саме через свою інноваційність компанії фінтех стикаються з ризиками, які відрізняються від банківських. У той час як банки працюють у середовищі з усталеними процедурами ієрархічного контролю й багатоетапної перевірки клієнта, сектор фінтеху часто функціонує за принципом максимальної швидкості, гнучкості та спрощеного доступу, що створює ризиковий ґрунт для експлуатації прогалин у перевірці особи, відстеженні транзакцій та контролі бенефіціарів. Особливу увагу створенню вікон вразливості приділено технологічним функціям: цифровий онбординг та електронна ідентифікація клієнта (eKYC) можуть стати інструментом для використання підроблених документів, синтетичних ідентичносттей, створених за допомогою технологій діпфейк і синтетичних цифрових профілів; міжнародні платіжні канали можуть бути використані для обходу санкцій через неправильну ідентифікацію платників або приховування юрисдикцій; P2P-платформи та цифрові гаманці можуть перетворюватися на механізм для непрозорого переміщення коштів між не пов'язаними один з одним особами; криптовалютні системи та DeFi-системи відкривають можливості для анонімності, необмеженого переміщення активів і використання міксинг-сервісів та конфіденційних монет, що робить встановлення походження та кінцевого одержувача активів надзвичайно ускладненим; модель інтеграції фінансових сервісів у нефінансові цифрові продукти та моделі Banking-as-a-Service створюють ситуацію, у якій контроль у сфері ПВК/ФТ часто делегується стороннім постачальникам, а отже виникає розрив між кінцевим ризиком користувача та рівнем контролю, застосованого платформою. Автор неодноразово наголошує, що фінтех може мимоволі стати «цифровим коридором» до банківської системи для суб'єктів, які прагнуть обійти складніші регуляторні процедури класичних фінансових інституцій.

Окремим важливим елементом документа є твердження, що сектор фінтеху у своїх підходах до ПВК/ФТ часто не приділяє належної уваги ризикам фінансування розповсюдження, хоча саме моделі фінтеху здатні значно полегшити проведення таких операцій. Зокрема, сервіси транскордонних платежів, торговельного фінансування й операцій з віртуальними активами

[9] https://media.licdn.com/dms/document/media/v2/D4D1FAQHL9w19jRvVhw/feedshare-document-pdf-analyzed/B4DZpifKcVGQAY-/0/1762588931699?e=1764806400&v=beta&t=Ya1YGaLP2TDApGGCFI__K8R0V3Ty-XR28R7pZlR3p1A

можуть забезпечити зручну інфраструктуру для оплати товарів подвійного призначення, створення проксі-компаній або проведення платежів у бік санкційних юрисдикцій. У документі наголошується, що схеми фінансування розповсюдження можуть зовні виглядати як звичайні комерційні транзакції, а виявлення зв'язку з військовими або стратегічними цілями можливе лише за умови наявності належних систем контролю кінцевого споживача товарів і коштів.

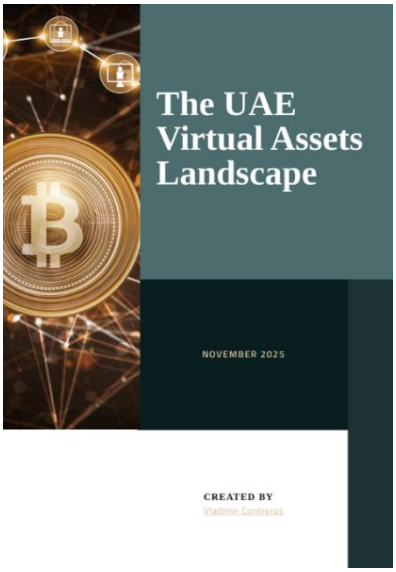
Далі автор переходить до сформованих у індустрії фінтеху практичних уроків і демонструє їх через реальні кейси Revolut, Wirecard та BitMEX, які стали прикладами компаній, що масштабувалися швидко, але не встигли — або свідомо не прагнули — налаштувати систему фінансового моніторингу відповідно до рівня своїх ризиків. Ці приклади покликані показати не кримінальний намір, а критичну структурну помилку: сприйняття комплаєнсу як бар'єра для інновацій, а не як механізму захисту довгострокового розвитку бізнесу.

У фінальній, концептуально найбільш важливій частині документа автор підкреслює, що інновації та комплаєнс не лише можуть співіснувати, а й мають співіснувати з першого дня розбудови продукту фінтеху. Ідея полягає не в тому, щоб зупинити розвиток або сповільнити технологічні вдосконалення, а в тому, щоб створити контроль, який працює не після появи ризиків, а одночасно з розвитком продукту. «Compliance-by-design» описано як підхід, що робить фінтех не просто законодавчо сумісним, а конкурентоспроможним: компанії, які з початку інтегрують санкційний і транзакційний моніторинг, цифрову перевірку клієнтів, управління ризиками, контроль підрядників і нагляд за підозрілими операціями, отримують доступ до швидшої регуляторної експансії, довіри банківських партнерів і готовності інвесторів фінансувати масштабування. Підсумковий меседж документа полягає в тому, що індустрія фінтеху не досягне стабільного успіху в умовах глобального розвитку, якщо сприйматиме комплаєнс як другорядний компонент. Інновації без контролю — тимчасові, а інновації, побудовані на контролі фінансових ризиків, формують масштабовану, безпечну і стійку бізнес-модель із довгостроковою перспективою та стратегічною перевагою на ринку.

Висновки:

- **Інновації у сфері фінансових технологій створюють нову площину фінансової злочинності,** оскільки швидкість, автоматизація та цифрова взаємодія підсилюють ризики ВК/ФТ/ФР.
- **Фінтех-компанії, які не інтегрують комплаєнс на етапі проєктування продукту,** неминуче стикаються з регуляторними санкціями, операційними збоями та репутаційними втратами під час масштабування бізнесу.
- **Ризики фінансування розповсюдження є особливо значущими для фінтех-індустрії,** оскільки транскордонні платежі, торговельне фінансування та операції з віртуальними активами можуть бути використані для обходу санкцій та маскування кінцевого призначення товарів і коштів.
- **Стійке зростання та розширення фінтех-бізнесу можливе лише за умови одночасного розвитку інновацій і комплаєнсу,** коли цифрова перевірка клієнтів, моніторинг транзакцій та санкційний контроль є невіддільними від бізнес-моделі.

Віртуальні активи в ОАЕ: поєднання інновацій та комплаєнсу як модель майбутньої фінансової системи [10]



Віртуальні активи в Об'єднаних Арабських Еміратах демонструють винятково динамічну трансформацію, яка перетворила країну на один із найпотужніших світових центрів цифрових фінансів. За останні роки ОАЕ зробили різкий перехід від статусу зростаючого ринку криптоінновацій до держави, що задає глобальний стандарт поєднання розвитку технологій і ефективного регулювання. Документ підкреслює, що основою цього підйому стало стратегічне бачення уряду, системне залучення міжнародного капіталу, інституційний попит на цифрові активи та формування регуляторної екосистеми, здатної одночасно підтримувати інновації й забезпечувати контроль за ризиками ПВК/ФТ. Особливо виділяється той факт, що вже на початку 2024 року кількість компаній у сфері віртуальних активів і Web3, присутніх в ОАЕ, перевищила 1 400 — що ілюструє стрімке чотириразове зростання галузі з 2022 року і свідчить про виняткову привабливість юрисдикції для світових учасників цифрової економіки.

Документ показує, що унікальність ОАЕ полягає не лише у відкритості до Web3 та криптотехнологій, а й у створенні високодеталізованої регуляторної вертикалі, що забезпечує прозорість, передбачуваність і стандартизовані умови входу на ринок. У Дубаї основою правового поля стала Virtual Assets Law № 4/2022, яка створила Virtual Assets Regulatory Authority (VARA), а згодом VARA розробила комплекс Регуляторних правил (Rulebooks) для бірж, зберігачів активів, брокерів, операторів DeFi і токенізаційних платформ. Водночас Абу-Дабі сформував власну модель регулювання через FSRA у межах ADGM — одну з найпрогресивніших юрисдикцій світу, яка охоплює такі сфери, як NFT-платформи, стейкінг, токенізовані цінні папери, фонди й цифрова інфраструктура зберігання. На материковій частині ринку діє регулювання SCA (CAAR), тісно пов'язане з компетенцією Центрального банку, що реалізує цифрову валюту Digital Dirham у межах глобального проєкту mBridge. Утворена система координації між VARA, FSRA, SCA і CBUAE мінімізує регуляторний арбітраж і створює єдиний режим нагляду, що є критично важливим у глобальному контексті фрагментованого регулювання криптосфери.

Документ наголошує на прискореній глобальній інституціоналізації цифрових активів, де ОАЕ виступають однією з небагатьох юрисдикцій, здатних одночасно підтримувати інноваційні бізнес-моделі та демонструвати прогрес у виконанні міжнародних стандартів FATF. Ключові світові тенденції — посилення вимог до стейблкоїнів, зростання уваги до токенізації реальних активів (RWA), встановлення норм щодо DeFi, впровадження дорожньої карти, вимоги до податкової звітності та міждержавного інформаційного обміну — знаходять у ОАЕ практичну регуляторну реалізацію. Таким чином, країна не пасивно реагує на глобальні тренди, а активно формує нові правила гри, пропонуючи інфраструктуру, яка поєднує цифрову інноваційність, безпечну ринкову поведінку та низькі бар'єри для міжнародних інвестицій.

Важливо, що ріст індустрії супроводжується новими викликами у сфері протидії відмиванню коштів та фінансуванню тероризму. Документ чітко демонструє, що складність фінансових злочинів у криптосередовищі не зменшується, а еволюціонує. Серед найбільш помітних ризиків

[10] https://media.licdn.com/dms/document/media/v2/D561FAQGZnhK0lBz23A/feedshare-document-pdf-analyzed/B56ZqVugtDHYAY-/0/1763448631469?e=1764806400&v=beta&t=FUuJyzxLonscsx4jKfeg_m04DoMg5kk69yg02gycJhE

визначено використання децентралізованих бірж (DEX), міжланцюгових мостів і міксерів для приховування походження коштів, ухилення від санкцій на основі протоколів з підвищеною конфіденційністю, класичні шахрайські схеми DeFi та NFT, соціальні атаки та фішингові маніпуляції, а також активне застосування стейблкоїнів злочинними угрупованнями для переводів ліквідних активів. Окремо виділено ризик використання криптоприбутків для купівлі нерухомості в ОАЕ, що спричинило появу обов'язкових процедур розкриття інформації для угод понад 55 000 дирхамів. У відповідь регулятори запроваджують обов'язкове використання блокчейн-аналітики, інтегровані RegTech-рішення для моніторингу транзакцій, посилені перевірки КБВ, а також нові формати міжвідомчої взаємодії між органами фінансової розвідки, зокрема ПФР, VARA і FSRA.

Після виходу ОАЕ із «сірого списку» FATF держава переходить до етапу стійкої ефективності, де головним критерієм успішності є не формальний комплаєнс, а здатність системно мінімізувати ризики ВК/ФТ. Очікується подальше інституційне зростання ринку: банки посилюють інтеграцію криптосервісів, токенізація фінансових інструментів і товарів стає новим стандартом, CBDC прискорює трансграничні розрахунки, а Web3 поєднується зі штучним інтелектом, створюючи нові бізнес-моделі. Стратегічний висновок документа полягає у тому, що ОАЕ переходять від етапу стрімкого розширення до етапу сталого розвитку, де успішність визначається відповідальним використанням технологій, захистом інвесторів, глобальною регуляторною інтеграцією та довгостроковою фінансовою стабільністю. Держава розглядає віртуальні активи як один із фундаментальних секторів майбутньої економіки, а не як короткотерміновий ринковий тренд, і саме тому формує нову архітектуру цифрових фінансів, яка впливає далеко за межі регіону.

Висновки:

- **ОАЕ сформували одну з найбільш комплексних і узгоджених у світі регуляторних систем для віртуальних активів,** у якій VARA, FSRA і SCA працюють не ізольовано, а як взаємодоповнюючі елементи єдиної екосистеми.
- **Інституційна участь у віртуальних активах у UAE зростає швидше, ніж роздрібна —** банки, фонди, сімейні офіси та корпоративні інвестори стають головними рушійними силами ринку.
- **Глобальні тенденції — регулювання стейблкоїнів, токенізація реальних активів, нагляд за DeFi і дорожня карта —** не просто відображені у нормативній базі ОАЕ, а інтегровані в неї системно та без відставання від міжнародних стандартів.
- **Злочинні схеми з використанням віртуальних активів стають складнішими,** тому регулятори ОАЕ відповідають підсиленням блокчейн-аналітики, суворішими вимогами до розкриття бенефіціарної власності та розширенням міжвідомчої координації.

Мобільність застави без погашення в готівку: як токенізація фондових інструментів усуває слабкі місця сучасної фінансової інфраструктури [11]

[11] https://www.gdf.io/wp-content/uploads/2020/12/GDF_-UKEU_TMMF-_report.pdf

У звіті представлено цілісну концептуальну та практичну дорожню карту трансформації колатеральної інфраструктури у глобальних фінансових ринках шляхом впровадження токенізованих фондів грошового ринку (TMMF), які об'єднують регуляторну надійність UCITS-сегменту із технологічною програмованістю цифрових активів. Документ побудований на критичному переосмисленні того, як сучасні механізми застави, маржові розрахунки та управління ліквідністю працюють у періоди нормальних ринкових умов та особливо у моменти системних потрясінь. Центральний акцент зроблено на ключовому виклику фінансової інфраструктури — недостатній мобільності застави, яка стає вузьким місцем не через дефіцит активів, а через повільні, фрагментовані, залежні від багатьох посередників та часових вікон процеси переходу власності на залікові активи. Ця проблема проявляється як у збільшенні витрат, так і у створенні системних ризиків, коли ринкові потрясіння посилюються саме затримками у колатеральних рухах.

Звіт демонструє, що чинна модель маржових розрахунків базується на використанні грошової застави та державних облігацій, тоді як фонди грошового ринку, попри їхню прийнятність відповідно до ISDA CSA, у реальності не використовуються безпосередньо як предмет застави, а виконують роль інструменту управління ліквідністю, який доводиться достроково викуповувати в готівку в момент маржинального виклику. Таким чином, MMF стає проміжною ланкою, а не кінцевим активом для розрахунку маржі. Саме це породжує непродуктивні операційні кола — інвестор продає частку MMF, отримує готівку, відправляє її як заставу, а потім отримувач, щоб не тримати ліквідність у готівковій формі, купує MMF знову. Ця логіка була лише неефективною у стабільні ринкові періоди, але виявилася небезпечною під час кризи LDI у 2022 році, коли маржинальні вимоги до британських пенсійних фондів призвели до масового перетворення MMF у готівку, що підсилило потребу в ліквідності, вдарило по грошових ринках і збільшило нестабільність на ринку державних облігацій, що, у свою чергу, потребувало надзвичайного втручання Банку Англії. У логіці документа саме це стає доказом, що проблема ліквідності під час стресу формується не дефіцитом активів, а неефективністю інфраструктури розрахунків і застави.

Токенізація, у трактуванні звіту, — не про створення нового класу ризикових цифрових активів, а про переведення традиційних фондів, що вже мають правовий і регуляторний статус, у технологічну форму, яка зберігає право власності, але усуває операційні бар'єри. TMMF являє собою цифрову частку фонду, яку можна передавати у режимі реального часу без її конвертації у готівку, з повною спадковістю прав інвестора та з відображенням трансферу титулу у реєстрі трансфер-агента. Саме цей момент — збереження титулу, а не економічного трекінгу NAV, — є визначальним елементом правової надійності, що відрізняє TMMF від стейблкоїнів або деривативів. Документ наголошує, що у TMMF поєднуються три властивості, які раніше не реалізовувалися одночасно: висока ліквідність, отримання доходу й миттєва передача прав власності у блокчейн-режимі. Внаслідок цього TMMF можуть виконувати функцію застави без знецінення доходу для постачальника забезпечення та без необхідності перепозиціонування активів на боці отримувача застави.

З погляду правової визначеності, звіт підкреслює, що три юрисдикції — Велика Британія, Люксембург та Ірландія — мають достатні нормативні передумови для того, щоб TMMF могли використовуватися як забезпечення у двосторонніх операціях за моделлю ISDA CSA. Велика Британія має судову практику щодо цифрових активів і наближається до ухвалення законодавства, що формально визнає цифрові активи як категорію майна. Люксембург має розвинену нормативну базу щодо дематеріалізованих та DLT-цінних паперів, а також корпоративні інструменти, які дозволяють вести реєстр часток фонду на ланцюгу. Ірландія не використовує спеціального регулювання цифрових активів, але визнає токенізовані частки як правовий аналог традиційних цінних паперів, що дозволяє реалізувати їхню заставу та примусове виконання через інфраструктуру електронних договорів і електронного реєстру власників. Звіт також зазначає, що у всіх трьох юрисдикціях право на примусове вилучення заставного активу у випадку дефолту боржника може бути реалізовано без участі боржника, що є ключовою ознакою забезпечення у моделі «передачі права власності».

Висновки:

- **TMMF довели свою юридичну, операційну та ринкову життєздатність як вид забезпечення** — пісочниця GDF показала, що перехід титулу, виконання прав та оперування TMMF під час дефолту чи нестандартних ринкових подій працює та відповідає існуючим законодавчим механізмам у Великій Британії, Люксембурзі та Ірландії.
- **Використання TMMF дозволяє прибрати необхідність погашення MMF у готівку під час маржинальних викликів,** тим самим зберігаючи прибутковість та ліквідність ринку і запобігає негативним циклам продажів активів у період ринкового стресу, подібним до кризи LDI у 2022 році.
- **Найбільшим каталізатором масштабування TMMF є не законодавство, а інтероперабельність технологічної інфраструктури,** оскільки саме здатність TMMF безперешкодно взаємодіяти з кастодіанами, маржинальними системами й традиційними розрахунковими платформами забезпечує можливість їхнього масового впровадження.
- **Подальше розгортання ринку залежить від стандартів: юридичної документації, транскордонних довідників, стандартизованих операційних регламентів та узгоджених критеріїв прийнятності предмета заставного забезпечення,** що уможливить перехід цифрових фондів грошового ринку до статусу повноцінного виду забезпечення в операціях із деривативами та операціями купівлі цінних паперів із зобов'язанням їх зворотного викупу.

Теоретичні висновки документа були перевірені через індустріальну пісочницю GDF, що включала понад 70 учасників та відтворювала реальні сценарії ринку. Учасники тестували моделі здійснення маржових розрахунків у забезпечувальних операціях, автоматизоване формування вимог щодо маржі, стресову подію зміни вартості активу (депегування) з автоматичною заміною предмета заставного забезпечення, сценарій дефолту зі здійсненням примусового звернення стягнення на предмет забезпечення, тристоронню модель фінансування з використанням договору застави, а також сценарій переходу від використання системи міжбанківських повідомлень SWIFT до моделі розрахунків забезпечення в режимі реального часу із завершенням операції протягом кількох секунд. Усі сценарії підтвердили, що токенізовані частки фонду можуть бути передані, повторно використані для маржинальних потреб і повернуті без жодних операційних розривів і з повним юридичним закріпленням переходу титулу. Найбільш показовими були два моменти: автоматична заміна забезпечення без участі людини у разі зміни NAV та

можливість виконання застави у сценарії дефолту з прозорим автоматизованим аудиторським слідом — фактично це означає, що технологія здатна не тільки прискорити операції, але й підвищити прозорість і чистоту дій у разі спорів.

Документ підводить до висновку, що майбутнє ринку застави залежить не від того, чи готові регулятори дозволити використання TMMF — регулятивні й юридичні передумови вже існують — а від здатності ринку стандартизувати операційні та інтеграційні механізми між традиційними кастодіанами, дилерами, кліринговими інфраструктурами та цифровими реєстрами. Іншими словами, головним вузьким місцем є взаємодія інфраструктур, а не правовий статус активів. На цій підставі звіт пропонує практичний шлях масштабування: юридична уніфікація документації, розроблення транскордонних довідників, визначення стандартизованих критеріїв прийнятності TMMF як забезпечення та створення постійного випробувального майданчика для ринку.

У фінальному баченні документа токенізовані фонди грошового ринку формують новий фундамент ринків забезпечення — коли активи, що приносять дохід, можуть переміщуватися у режимі реального часу між учасниками без втрати прибутковості, без конвертації у готівку, без операційних розривів, з повною юридичною визначеністю та з технологічними механізмами самовідновлення для стресових ситуацій. Це означає не лише підвищення операційної ефективності, а й структурну трансформацію моделі функціонування ринку заставного забезпечення — від підходу, за якого управління здійснюється навколо дефіциту ліквідності, до підходу, у межах якого ліквідність розглядається як повноцінний та постійно задіяний актив, що використовується безперервно, а не утримується у пасивному резерві. У цьому підході TMMF стає не тимчасовим елементом для отримання готівки, а повноцінним сучасним типом застави, сумісним із майбутньою цифровою інфраструктурою глобальних фінансових ринків.

Інші новини

Фінансова інфраструктура під загрозою блокування: нова модель впливу США у сфері ПВК/ФТ [12]

Стаття описує різкий і суттєвий злам у міжнародному підході до протидії відмиванню коштів і фінансуванню тероризму, який став очевидним після оголошення FinCEN 25 червня 2025 року щодо трьох мексиканських фінансових установ. На думку автора, ці дії не є черговим епізодом регуляторних санкцій, а сигналізують про нову епоху глобального застоування заходів у сфері ПВК, де боротьба з відмиванням доходів пов'язується із фінансуванням тероризму, наркотрафіком і загрозами національній безпеці. В основі цього зламу — оновлені правові механізми США, насамперед FEND Off Fentanyl Act, який дозволяє FinCEN застосовувати безпрецедентно жорсткі заходи проти іноземних фінансових установ, включно з негайним від'єднанням від доларової системи. Саме тому оголошення щодо CIBanco, Intercam і Vector стало важливою точкою у міжнародному фінансовому регулюванні: воно показало, що тепер навіть порівняно невеликі або непрямі транзакції, пов'язані з картелями, можуть спричинити наслідки, що змінюють долю інституції.

Автор акцентує на історичному підґрунті розвитку режиму блокувальних заходів США — від Bank Secrecy Act 1970-х років, коли вперше сформувалося підґрунтя фінансового контролю, через USA PATRIOT Act після 2001 року, що перетворив ПВК на питання національної безпеки, і

[12] https://internationalbanker.com/banking/a-new-wave-of-global-anti-money-laundering-enforcement-has-arrived-are-you-prepared/

до Section 311, який дав можливість визнання іноземних банків «організаціями первинної уваги» з точки зору відмивання коштів. Сучасний етап вирізняється тим, що традиційні механізми у сфері ПВК були інтегровані з антитерористичними інструментами, які раніше застосовувалися переважно в контексті міжнародних терористичних організацій. Оскільки фентаніл і пов'язані з ним картелі офіційно визначаються як загроза національній безпеці, фінансові установи, що сприяють їхнім операціям, опиняються в одному регуляторному полі з тими, хто забезпечує фінансові потоки таких структур як «Хезболла» чи суб'єкти, пов'язані з Північною Кореєю. Це означає, що логіка впливу США змістилася від «вибіркового застосування» до «глобальної екстериторіальної відповідальності».

У статті детально описано, чому саме мексиканські установи стали об'єктом дій FinCEN: вони, відповідно до даних FinCEN, дозволяли використання рахунків для операцій, пов'язаних із картелями, зокрема переказів на суми мільйонів доларів, що використовувались для постачання прекурсорів фентанілу або відмивання доходів від злочинної діяльності. У випадку CIBanco FinCEN заявив, що через рахунок працівника картелю Gulf пройшло близько десяти мільйонів доларів у 2023 році, а ще більше двох мільйонів доларів були спрямовані на рахунки китайських компаній для закупівлі прекурсорів у 2021–2024 роках. Intercam, згідно з повідомленням, пропустив транзакції на понад півтора мільйона доларів, що пов'язані з цими ж мережами, а Vector, за даними FinCEN, дозволив схеми руху коштів через «мули» картелю Sinaloa у 2013–2021 роках. Важливо, що автор наголошує: не йдеться про системний злочин чи пряму співпрацю банків із картелями — регулятор виходить із логіки, що навіть обмежена участь або невиявлений сегмент незаконного ланцюга є достатнім фактором для інтервенції.

Ключовим, на думку автора, є не конкретний перелік санкцій, а меседж, який FinCEN адресує глобальному фінансовому сектору: будь-яка фінансова установа, яка проводить кореспондентські операції у доларах США, повинна розуміти, що тепер не існує «географічного імунітету». Якщо раніше подібні дії США обмежувалися певними регіонами або стратегічними напрямами, то тепер рамка застосовується універсально, а критерії застосування стали жорсткішими. Саме тому стаття підкреслює, що найважливішим фактором успішності фінансових установ у новій реальності стає здатність «дивитися наперед», поєднувати моніторинг транзакцій із розумінням транснаціональної злочинності, геополітичної напруги, ринків прекурсорів і нових схем відмивання.

Автор наголошує, що сучасна модель комплаєнсу, орієнтована на

Висновки:

- **Оголошені FinCEN заходи проти трьох мексиканських фінансових установ позначили початок нового етапу глобального застосування заходів у сфері ПВК,** який відрізняється масштабністю, жорсткістю та здатністю впливати на міжнародні розрахунки.
- **Шостий спеціальний захід, передбачений законом FEND Off Fentanyl Act, став центральним інструментом тиску,** оскільки дозволяє негайно забороняти іноземним фінансовим установам участь у доларових операціях у разі залучення до схем, пов'язаних із фентанілом або картелями.
- **Випадки з CIBanco, Intercam і Vector продемонстрували, що навіть разові або непрямі транзакції можуть стати підставою для повномасштабного втручання США,** включно з повним від'єднанням установи від платіжної інфраструктури у доларах.
- **Ситуація не є унікальною для Мексики — вона створює новий глобальний прецедент,** який показує, що будь-яка фінансова установа, що працює на міжнародних ринках і має доступ до кореспондентських рахунків у доларах США, може опинитися під аналогічними заходами у разі недостатнього контролю ризиків, пов'язаних з фінансовими потоками злочинних організацій.

«перевірки як формальність» і виявлення підозр у ретроспективі, більше не відповідає вимогам регуляторів. Культурна зміна — від реактивного до проактивного управління ризиками — стає ключовою. Переосмислення має починатися з рівня правління: воно повинне не лише отримувати інформацію про ризики у сфері ПВК/ФТ, а бути відповідальним за їх стратегічне управління, розуміти слабкі місця системи контролю та вимагати реальної ефективності заходів. Технологічний аспект є не менш важливим: моніторингові системи мають враховувати не лише традиційні сценарії ризику, але й складні схеми транскордонної злочинності, включно з нетиповими маршрутами платежів, непрямими контрагентами, ланцюговими переказами, рольовими «мулами» та цифровими активами.

Заключна частина статті стверджує, що справа проти CIBanco, Intercam і Vector — це перший, але далеко не останній сигнал нової глобальної політики у сфері ПВК/ФТ. Вона змінює очікування щодо фінансових установ: тепер регулятори очікують не лише запобігання відмиванню коштів, а й активного виявлення та блокування операцій, які можуть бути частиною ширших кримінальних і терористичних мереж. Світ, на думку автора, входить у фазу, коли комплаєнс перестає бути питанням виконання норм і стає фактором виживання на міжнародному фінансовому ринку.

Для загального розвитку

Від статичної перевірки до цифрової довіри: модель Trulioo для безперервної верифікації фізичних і юридичних осіб [13]

У статті викладено, як компанія Trulioo представила свою оновлену платформу ідентифікації та автентифікації суб'єкта у цифровому середовищі, яка суттєво змінює підхід до боротьби з відмиванням коштів, фінансуванням тероризму та шахрайством — від старої моделі одноразової перевірки клієнтів (KYC/KYB) до динамічної, безперервної моделі «цифрової довіри». Автори підкреслюють, що в умовах глобальної цифрової економіки та посилення регуляторного тиску (зокрема нормами FATF, а також новими вимогами ЄС) фінансові установи змушені переглядати свої системи верифікації та моніторингу.

У розділі «Трансформація відповідності ПВК через цифрову аналітику ідентичності» зазначається, що Trulioo виводить перевірку з однократного процесу на етапі прийому клієнта до горизонту безперервного моніторингу, що охоплює поведінку клієнта, зміни у власній структурі, транзакційні аномалії та інші сигнали ризику. У зокрема, компанія поєднує KYC-контроль з біометрією, зокрема систему «known face recognition» (порівняння «один-до-багатьох»), що дозволяє ідентифікувати повторні застосування зловмисниками нових або штучно сформованих ідентичностей. Біометричні можливості доповнено перевіркою цілісності документів (для виявлення підробок або змінених файлів). У системі використовується понад 60 сигналів шахрайства/ризику, інтегрованих через AI-аналітику для створення «інтелектуальної» перевірки клієнта. Цей підхід охоплює і фізичних осіб, і корпоративні структури, у єдиній цифровій платформі. Стаття зауважує, що саме розрив між традиційною перевіркою особистості на вході і відсутністю подальшого моніторингу створює «діри», які зловмисники використовують для проведення транзакцій, транскордонних операцій і «перекочування» активів.

У розділі «Піднесення безперервної перевірки юридичних осіб та динамічного профілювання бізнес-ризику» глибше досліджується розширений модуль KYB (Знай свій бізнес) платформи

[13] https://fincrimecentral.com/trulioo-digital-id-aml-compliance-platform/

Trulioo. Тут підкреслено, що класична KYB-перевірка юридичних осіб, яка базується лише на реєстраційних даних (наприклад, реєстраційний номер, адреса, власник), вже недостатня. Trulioo пропонує модель, яка постійно моніторить зміни в статусі компанії — передача власності, зміна юрисдикції, реєстраційні заяви, санкції, негативні медіа-сигнали. Додається аналіз цифрової присутності компаній: веб-активність, соціальні сигнали, відображення в онлайні даних про діяльність. Наприклад, якщо компанія зареєстрована як аграрний експортер, але її цифровий слід показує активну рекламу криптовалютної біржі — це створює автоматичний сигнал внутрішньої невідповідності. Далі, Trulioo генерує комплексні рейтинги бізнес-ризику й репутації, які оновлюються динамічно — це знімає «замороження ризику», коли установи проводять перевірку лише раз на рік або два, і ризик на цей момент вже застарілий. Стаття вказує, що такий підхід дозволяє автоматично запускати внутрішні ремедіаційні потоки, створювати сповіщення для команд комплаєнсу, і тим самим бути ближчими до регуляторної вимоги «пропорційної і своєчасної відповіді».

У розділі «Інтеграція біометричного захисту в життєвий цикл ПВК» стаття виділяє, що одна з найбільших проблем у фінансових злочинах — це шахрайство з ідентичностями, у тому числі штучно сформованими ідентичностями, створеними шляхом поєднання справжніх і вигаданих персональних даних, повторні акаунти, мультиакаунтинг, «нашарування» (шифрування потоків через різні канали). Trulioo вводить біометричну систему, яка аналізує обличчя клієнта на вході, зіставляє з базою вже верифікованих осіб («known faces») і тим самим ідентифікує повторників. Такий підхід допомагає уникнути ситуацій, коли зловмисник реєструється під новою особою, але насправді це той самий суб'єкт. Крім того, система перевіряє документи не лише за даними, які видно людині (ім'я, дата народження), а й метадані файлу: чи документ був змінений, чи фото підроблене, чи існують ознаки маніпуляцій. Це дозволяє значно скоротити кількість ручних перевірок, підвищити точність, а також інтегрувати перевірку особи безпосередньо у мобільний застосунок або вебплатформу, що зменшує відтік доброчесних клієнтів через надмірно складні процедури. У статті наведено, що такі біометричні та поведінкові рішення вже показують значне зниження ручної роботи та покращення операційної ефективності (хоча цифри не деталізовані у великій глибині).

У заключній частині «Формування екосистеми, орієнтованої на довіру, для забезпечення ПВК» висвітлюється ширший контекст: цифрова ідентичність та довіра стають «валютою» цифрової економіки. Trulioo позиціонується не просто як постачальник KYC/KYB-рішення, а як нейтральна інфраструктура центру управління для перевірки, моніторингу і аудиту цифрових суб'єктів (фізичних і юридичних). Платформа акумулює зовнішні сигнали — зокрема реєстраційні дані, поведінкові показники, цифрову активність, історію транзакцій, зміни у структурі власності, санкційні фактори та результати медіааналізу — й об'єднує їх у єдиному середовищі, що забезпечує фінансовим установам та іншим суб'єктам регульованого сектору повну прозорість і підтверджувану відповідність вимогам. У статті наголошується, що регулятори поступово переходять до моделей, у яких оцінка ризику, моніторинг та верифікація здійснюються у режимі реального часу й на безперервній основі, і наведене рішення Trulioo відповідає саме цьому підходу. Зміщується акцент із формального виконання процедур на доказову модель, у межах якої система повинна забезпечувати відстежуваність подій, надання аудиторських журналів та підтверджуваної історії перевірок, щоб рівень довіри був прозорим та придатним для регуляторного контролю. У статті також зазначено, що така модель дає змогу скоротити час і ресурси, необхідні для ручних перевірок, підвищити точність виявлення ризикових суб'єктів і забезпечити кращу видимість цифрових потоків, особливо в умовах транскордонних операцій.

У підсумку, стаття подає Trulioo як технологічний прорив у секторі ПВК/ФТ — компанія демонструє перехід до нового покоління систем цифрової ідентичності, які інтегрують KYC, KYB, біометрику, цифрову аналітику та постійний моніторинг у єдину платформу для управління ризиком. Цей підхід відповідає сучасним викликам: швидкі цифрові платежі, мультиканальні взаємодії, глобальні транзакції, складні корпоративні структури, санкції, розповсюдження ЗМЗ тощо. Стаття не лише описує функції платформи Trulioo, а й розміщує їх у контексті еволюції регуляторного середовища та цифрових кінцевих моделей довіри, що дозволяє зрозуміти, як ідея цифрової ідентичності стає центром антикризових стратегій у фінансовому секторі.

Висновки:

- **Trulioo замінює одноразову ідентифікацію клієнтів моделлю безперервного життєвого циклу цифрової довіри,** у межах якої перевірка здійснюється постійно, а не лише при встановленні ділових відносин.
- **Платформа поєднує KYC, біометричну перевірку документів, KYB та аналіз цифрової поведінки в єдину систему,** що формує комплексну картину ідентичності та ризиків фізичних і юридичних осіб.
- **Перевірка юридичних осіб включає відстеження змін у структурі власності, цифрової присутності та публічної активності,** що дозволяє виявляти розбіжності між задекларованою і фактичною діяльністю.
- **Платформа виконує функцію централізованого центру управління цифровою довірою,** забезпечуючи аудит, моніторинг та фіксацію подій ризику з метою підтверджуваної відповідності регуляторним вимогам.

Ваша думка важлива!

1. Який шлях є реалістичним для України: стати юрисдикцією, що впроваджує токенізацію на практиці та залучає капітал, чи залишитися спостерігачем, який гармонізує правила лише після міжнародних ринків — і які стратегічні наслідки матиме кожен із сценаріїв?
2. Чи є перехід до безперервної перевірки клієнтів у режимі реального часу неминучим кроком для світової системи фінансового моніторингу, і як це співвідноситься з правами на приватність та захист персональних даних — особливо у країнах з воєнним станом?
3. Як держава та приватний сектор можуть побудувати модель співпраці (PPP) у сфері ПВК/ФТ/ФР, у якій фінтех не виступатиме слабкою ланкою, а стане повноцінним партнером у захисті фінансової системи — і які кроки першочергові для України?
4. Чи здатна модель регулювання віртуальних активів ОАЕ — із сильним акцентом на ПВК/ФТ, технологічні інновації та прозорість для інвесторів — стати глобальним стандартом для інших країн, і чи готова Україна адаптувати її елементи у власну нормативну базу?
5. Чи можливо, що в майбутньому токенізовані інструменти з високою ліквідністю та чітким правом власності витіснять стейблкоїни як домінуючий інструмент забезпечення у фінансових операціях, і які регуляторні наслідки це матиме для юрисдикцій, включно з Україною?
6. Як Україні у процесі післявоєнної відбудови запобігти тому, щоб великі інфраструктурні проєкти, ресурси, земля, гуманітарні програми та оборонні закупівлі не стали основними цілями організованої злочинності — і що має бути пріоритетом: інституційні реформи, антикорупційні механізми чи моніторинг ризикових секторів?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-48

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

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