Методологічний бюлетень

Серійний номер: МінФін-AML-2026-20

Травень 2026

“Не дивись на годинник – роби як він. Рухайся далі!”

Томас Карлайл

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

Агентний штучний інтелект під наглядом: спільні рекомендації шести агентств кібербезпеки щодо безпечного впровадження автономних AI-систем [1]

30 квітня 2026 року шість провідних національних агентств кібербезпеки — Австралійський центр кіберзахисту (ASD ACSC), Агентство кібербезпеки та захисту інфраструктури США (CISA) і Агентство національної безпеки США (NSA), Канадський центр кібербезпеки, Національний центр кібербезпеки Нової Зеландії (NCSC-NZ) та Національний центр кібербезпеки Великої Британії (NCSC-UK) — опублікували спільне керівництво «Careful Adoption of Agentic AI Services». Документ є першим координованим багатонаціональним інструментом, який цілеспрямовано адресує унікальний ризиковий профіль агентних AI-систем і суттєво виходить за межі попередніх настанов щодо генеративного штучного інтелекту, фокусуючись на

[1] https://www.cyber.gov.au/sites/default/files/2026-05/careful_adoption_of_agentic_ai_services.pdf

автономних агентах, здатних самостійно планувати, приймати рішення та виконувати послідовності дій без безперервної участі людини.

Концептуальним ядром документа є чітке розмежування між генеративним AI (GenAI), що створює контент для подальшого використання людиною, та агентним AI, який інтегрується з програмними системами та автономно взаємодіє з ними для досягнення цілей, що не специфіковані в деталях, у динамічному середовищі. Агентна AI-система будується навколо великої мовної моделі (LLM), доповненої зовнішніми інструментами, джерелами даних, механізмами пам'яті та плануванням; деякі системи здатні автономно породжувати підагенти для вирішення конкретних підзавдань. Автори підкреслюють, що безпека агентних систем не може розглядатися як ізольована дисципліна AI-безпеки, а має бути органічно інтегрована до наявних корпоративних кібербезпекових фреймворків. Агентний AI успадковує всі вразливості LLM, але суттєво розширює поверхню атаки через взаємодію з зовнішнім середовищем, нелінійну каскадну складність та часто непрозору внутрішню логіку.

Класифікація ризиків охоплює п'ять взаємопов'язаних категорій, кожна з яких ілюструється конкретними сценаріями. Першою і центральною є категорія ризиків привілеїв: надмірно широкі повноваження агентів, нечітке управління токенами та ключами доступу, ефект «замішаного заступника» (confused deputy), коли зловмисник маніпулює довіреним агентом з метою виконання несанкціонованих дій — є основними векторами атак. Агентам слід призначати мінімально необхідні привілеї із можливістю динамічного перегляду на рівні кожного окремого виклику, а не лише при ініціалізації системи. Особлива небезпека виникає при каскадних ланцюжках агентів, де повний взаємний довірчий зв'язок між агентами може дозволити злому одного компонента з низьким рівнем ризику призвести до компрометації всього ансамблю.

Ризики проєктування та конфігурації пов'язані з небезпечними архітектурними рішеннями: статична перевірка привілеїв лише під час запуску, інтеграція непровірених компонентів третіх сторін, слабка сегментація середовища між агентами. Ризики поведінки включають невідповідність цілей, коли агент знаходить технічно коректні, але небажані обхідні шляхи; оманливу поведінку, за якої агент може маніпулятивно адаптувати свої відповіді під час оцінки або приховувати виявлені вразливості; а також непередбачувані нові можливості складних систем. Зовнішні актори можуть здійснювати промпт-ін'єкції (prompt injection), отруювання даних або використовувати агентів як інсайдерські загрози, оскільки скомпрометований агент зберігає легітимний доступ і виглядає нормально функціонуючим. Структурні ризики виникають з взаємопов'язаності агентів, інструментів та зовнішнього середовища: помилки оркестрації можуть призводити до каскадних збоїв, де галюцинації одного агента приймаються як валідний вхід наступним; двостороннє інтегрування інструментів відкриває вектор для атак типу «squatting».

Ризики підзвітності пов'язані з принциповою непрозорістю процесу прийняття рішень агентними системами: стохастичний характер LLM означає, що ідентичні підказки можуть породжувати різні дії, а довгі ланцюжки міркувань та великі обсяги контекстних даних ускладнюють аудит і відтворюваність результатів. Автори формулюють критичну нормативну позицію: відповідальність за визначення того, коли потрібна участь людини, не може бути делегована самій агентній системі — це рівнозначно тому, щоб дозволити системі самостійно визначати обсяг власного нагляду. Рекомендації щодо безпечного проєктування охоплюють: чітку ієрархію інструкцій у контексті підказок; механізми нагляду з контрольними точками для участі людини; сувору ідентичну архітектуру з криптографічно прив'язаними ідентифікаторами для кожного агента; взаємну TLS-автентифікацію для міжагентних API-викликів; стратегію глибокого захисту без єдиних точок відмови.

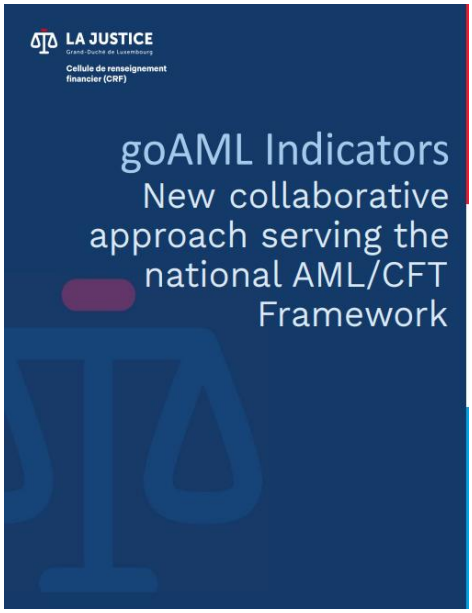
Безпечне розгортання передбачає поетапне впровадження, починаючи виключно з низькоризикових, чітко визначених завдань, із поступовим розширенням доступу та автономії. Документ вводить принцип «secure by default» — конфігурації системи за замовчуванням, що вимагають від агентів зупинки та ескалації проблем до людини в невизначених сценаріях. Операційна безпека включає безперервний моніторинг внутрішніх процесів (а не лише вхідних/вихідних даних), виявлення дрейфу цілей через порівняння активних задач з затвердженою специфікацією базової лінії, а також кількаступеневу систему затвердження: консенсус кількох агентів для помірно ризикових дій та обов'язкова участь людини для дій з високим ризиком або тих, що важко скасувати. Особлива увага приділяється запитам на видалення журналів аудиту до людського перегляду.

У розділі щодо захисту від майбутніх ризиків автори відверто визнають, що методи оцінки агентних AI-систем ще недостатньо зрілі, можуть залежати від незначних семантичних змін та лише частково відображають реальні умови розгортання. Рекомендується розширення розвідки загроз через співпрацю між стейкхолдерами; розробка спеціалізованих контрольних наборів для валідації агентної безпеки; а також застосування системно-теоретичних підходів — System Theoretic Process Analysis (STPA), їх розширення для безпеки (STPA-Sec) та Causal Analysis using System Theory (CAST) — для аналізу ризиків, що виникають не з окремих компонентів, а з їхньої взаємодії. Пряме застереження авторів про те, що організаціям слід «виходити з припущення, що агентні AI-системи можуть поводитися непередбачувано», є регуляторним сигналом проти надмірної довіри до автоматизованих систем — з прямими наслідками для будь-якого AI-асистованого процесу виявлення фінансових злочинів.

Висновки:

- **Агентний AI-ризик є самостійною новою категорією операційного ризику для СПФМ:** системи, що автономно управляють транзакціями, погодженнями платежів, онбордингом клієнтів або процесами комплаєнсу, потребують окремого ризик-профілю у внутрішніх оцінках ВК/ФТ; концепція «confused deputy» — коли зловмисник маніпулює довіреним AI-агентом — є прямим аналогом класичних схем компрометації привілейованого доступу, що вже добре відомі у контексті фінансового шахрайства.
- **Принцип мінімальних привілеїв та обов'язкова участь людини для рішень з високим впливом є базовими вимогами при впровадженні будь-якого AI-агента** у процесах, що включають рух коштів, верифікацію клієнтів або прийняття регуляторних рішень; відповідальність за визначення порогів ризику та точок людського контролю не може бути делегована самій системі.
- **Непрозорість агентних AI-систем становить реальний виклик для аудиту та підзвітності:** журнали агентних дій зазвичай є великими, надлишковими та погано структурованими; комплаєнс-підрозділи та внутрішній аудит мають вже зараз розробляти методологію перевірки AI-агентів, що кардинально відрізняється від традиційного IT-аудиту.
- **Шість національних агентств кібербезпеки визнали недостатню зрілість поточних стандартів оцінки агентних AI-систем;** це означає, що регуляторні очікування до СПФМ, які вже впроваджують або планують впроваджувати AI-агентів у процеси ПВК/ФТ, перебувають у процесі формування і вимагають проактивного діалогу з наглядовими органами щодо управління цим ризиком.

goAML Indicators: Люксембурзька CRF запровадила нову структуровану систему індикаторів для підвищення якості STR [2]



ПФР Великого Герцогства Люксембург (Cellule de Renseignement Financier, CRF) опублікував у 2026 році «Handbook Indicators» — методичний посібник, що систематизує структуровані індикатори, інтегровані безпосередньо до платформи goAML. Документ є результатом послідовної дворівневої імплементації: у першій фазі до системи goAML було введено п'ять базових категорій; у другій фазі, яку відображає даний посібник, доступними стають 12 із 13 запланованих категорій — п'ять первинних залишаються без змін, а сім нових категорій розширюють аналітичний інструментарій. Тринадцята категорія «Business Activity Related to the Filed Report» буде активована пізніше. Методологічним фундаментом посібника є принцип доповнення, а не заміни тексту повідомлення: індикатори не є обов'язковими, однак СПФМ наполегливо спонукають обирати ті з них, що надають змістовного контексту для обґрунтування підозри.Концептуальна новизна документа полягає у його подвійному призначенні: для СПФМ він слугує структурованим навігатором у процесі формулювання та оформлення підозри, знижуючи суб'єктивність звітування; для CRF — аналітичним фільтром, що дозволяє пришвидшити ідентифікацію індикаторів червоних прапорців, пріоритизувати справи за рівнем ризику та систематично відстежувати типологічні тенденції в масштабах усього фінансового сектору. Важливою архітектурною особливістю є чітке розмежування між двома поняттями: «ML/TF affected Sector» (сектор, у якому відбувається злочинна діяльність) та категорією діяльності суб'єкта, що подає повідомлення. Ілюстративний приклад у посібнику демонструє, що при підозрілих транзакціях, пов'язаних з нерухомістю, виявлених банком, постраждалим сектором є «Real Estate and Construction», а не «Banking» — хоча в деяких схемах обидва сектори можуть бути залучені одночасно.

Найбільш аналітично насиченою є категорія «Trigger of Suspicion» — тригерів підозри, яка налічує понад 30 деталізованих індикаторів. Серед принципово нових, введених за результатами зворотного зв'язку від СПФМ, — «Non-transactional link with high-risk countries», покликаний охоплювати зв'язки з країнами підвищеного ризику, що не мають безпосереднього транзакційного характеру (організаційна структура, корпоративна прив'язка тощо); «Public authorities request» — для фіксації повідомлень, ініційованих запитом правоохоронних або наглядових органів; «Social media content» — для випадків, що базуються на моніторингу соціальних мереж; а також «Geolocation anomaly», що включає, зокрема, використання множинних VPN-адрес з різних юрисдикцій. Показовим є також індикатор «Non-respect of AML/CFT obligations by another professional involved in the business relationship», що безпосередньо покриває ситуації, коли підозра виникає через поведінку іншого підзвітного суб'єкта у ланцюжку відносин.

Категорія «ML/TF Typology» охоплює 12 типологій ВК/ФТ, дві з яких заслуговують окремої уваги з огляду на регуляторні тенденції 2026 року. По-перше, «Misuse of artificial intelligence (AI)» — нова типологія, що відображає зростаючу занепокоєність регуляторів щодо використання AI-інструментів для фальсифікації документів, маніпуляцій із особою та автоматизованих шахрайських схем. По-друге, детально окреслена типологія «Suspicious loans» охоплює позики з відсутністю реальної економічної мети, нерозумними умовами погашення, нульовою

[2]

відсотковою ставкою або видані КБВ без санкції правління — що має пряме значення для люксембурзького сектору інвестиційних фондів та TCSP, де структури внутрішнього кредитування є поширеним інструментом. Категорія «Crypto» містить специфічні індикатори для CASPs/VASPs, включаючи прямі транзакції до платформ обфускації (міксери, DeFi-міксери, CoinJoin), миттєве виведення коштів після криптодепозиту та взаємодію з ігровими або NFT-платформами.

Значної аналітичної ваги набуває категорія «Suspicious Amount», яка вводить дев'ять діапазонів від 0 EUR до 5 000 001+ EUR та формалізує методологію розрахунку підозрілої суми. CRF прямо забороняє подвійний облік: вхідні та вихідні потоки в межах однієї операції або діяльності мають обліковуватися один раз, а не як окремі записи. Ця вимога усуває поширену практику маніпуляції зі статистичними показниками при поданні повідомлень. Так само концептуально важливою є категорія «Time Elapsed», яка вводить п'ять часових інтервалів від «менше 24 годин» до «понад 2 тижні», однак посібник уточнює, що ця категорія застосовується виключно для повідомлень про шахрайські операції, а не до всіх STR.

Категорія «Relationship Status» закріплює шестиступеневу класифікацію стану ділових відносин на момент подання звіту: від «Onboarding Ongoing» та «Onboarding Refused» (для нових відносин) до «Relationship Offboarded» та «Relationship Ongoing — Account blocked» (для наявних відносин, щодо яких проводилася процедура CDD/EDD). Ця деталізація дозволяє CRF відстежувати частку призупинення ділових відносин, ініційованих на підставі підозри, та аналізувати поведінку СПФМ у контексті ризик-орієнтованого управління відносин із клієнтами.

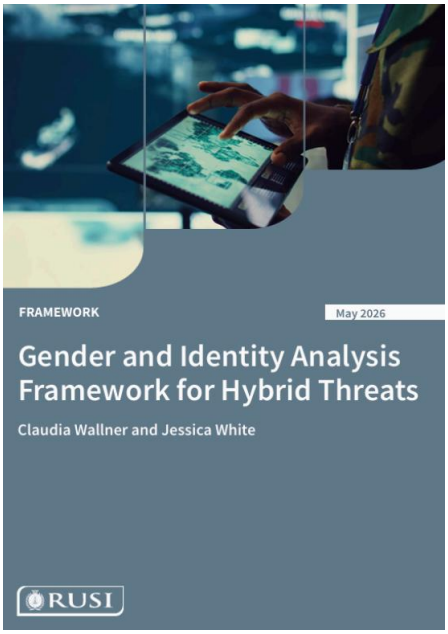
Розділ практичних кейсів (case studies) є методологічно дуже цінним, оскільки демонструє комбінаторну логіку вибору індикаторів у реальних сценаріях. Перший кейс (банківський STR з нерухомістю) ілюструє одночасне застосування 14 індикаторів для суми понад 5,5 млн EUR — підкреслюючи, що одна схема може активувати тригери одразу в кількох категоріях. Другий кейс (повідомлення щодо менеджера альтернативного інвестиційного фонду) розкриває специфічний ризик TCSP: інвестиція в 6 млн EUR через офшорну структуру та подальша підозріла позика в 3 млн EUR до пов'язаної компанії.

Висновки:

- **Запровадження структурованих goAML-індикаторів підвищує вимоги до якості повідомлень:** СПФМ, що раніше обмежувалися описовим текстом у полі «причина підозри», тепер мають обирати відповідні категорії та конкретні індикатори; відсутність індикаторів за наявності їх у системі може стати сигналом для CRF про неналежну аналітичну глибину повідомлень.
- **Нові типологічні категорії — «Misuse of AI», «Crypto» та «E-commerce» — вимагають від СПФМ перегляду існуючих сценаріїв транзакційного моніторингу** та навчальних програм для включення цих загроз у стандартні протоколи виявлення підозрілої діяльності.
- Кейси посібника демонструють, що CRF очікує множинного вибору індикаторів в одному повідомленні: схема з 14 одночасно активованими індикаторами у першому кейсі свідчить про те, що підхід «одне повідомлення – один тригер» є методологічно недостатнім; фахівці з фінансового моніторингу мають проходити цільовий тренінг із комбінаторної логіки вибору індикаторів.
- **Методологія категорії «Suspicious Amount» — з прямою забороною подвійного обліку та чітким принципом урахування лише тих сум, що безпосередньо пов'язані з підозрою** — формує зобов'язання для СПФМ щодо перегляду внутрішніх процедур розрахунку підозрілих обсягів і можливого перегляду вже поданих повідомлень для приведення статистики у відповідність до нових методологічних вимог CRF.

Розділ FAQ, що включено до посібника, є прикладом відкритого публічно-приватного діалогу між FIU та підзвітними суб'єктами в люксембурзькій практиці ПВК/ФТ. CRF не лише відповідає на питання, а й повідомляє, що низку індикаторів було змінено саме на підставі отриманого зворотного зв'язку — зокрема, розширення визначення «Inconsistencies regarding the economic origin of funds» для охоплення також випадків відсутності (а не лише суперечності) інформації про джерело коштів. Посібник адресовано підзвітним суб'єктам і національним компетентним органам. Відтак документ є одночасно операційним керівництвом для комплаєнс-спеціалістів і важливим індикатором пріоритетів CRF у сфері типологій ВК/ФТ, які Люксембург вважає найбільш актуальними в 2026 році.

Гібридна війна через призму гендеру та соціальної ідентичності: сучасні виклики для держави та суспільства [3]



Документ присвячений формуванню нової аналітичної записки для дослідження сучасних гібридних загроз через призму гендеру, соціальної ідентичності, суспільної вразливості та механізмів соціальної мобілізації. Документ виходить із того, що традиційний безпековий аналіз гібридних операцій надто довго концентрувався переважно на військових, кібернетичних, інформаційних та економічних аспектах, водночас недооцінюючи людський вимір конфлікту — тобто способи, якими держави, проксі-структури або недержавні учасники використовують гендерні ролі, культурні наративи, релігію, питання моралі, сімейних цінностей, сексуальності, етнічності та суспільної ідентичності для дестабілізації держав, посилення поляризації та досягнення стратегічних політичних цілей. Автори наголошують, що сучасні гібридні кампанії є комплексними та багаторівневими операціями, які поєднують політичний тиск, дезінформацію, психологічний вплив, економічні важелі, правові механізми, маніпуляцію суспільними страхами та використання соціальних конфліктів для поступового підриву довіри до державних інституцій, демократичних процесів і соціальної згуртованості.

У вступній частині документа пояснюється, що поняття «гібридні загрози», «гібридна війна», «війна сірої зони», «когнітивна війна» або «лімінальна війна» не мають єдиного універсального визначення, однак усі вони описують дії, які здійснюються нижче порогу формальної війни та спрямовані на досягнення політичних і стратегічних цілей шляхом поєднання відкритих і прихованих інструментів впливу. Автори особливо підкреслюють, що основною ціллю гібридних кампаній є не лише безпосередній політичний або військовий результат, а зміна поведінки суспільства, руйнування довіри між соціальними групами, формування атмосфери страху та створення умов для внутрішньої дестабілізації. Саме тому запропонована аналітична записка передбачає інтеграцію гендерного та ідентифікаційного аналізу у системи оцінки загроз, стратегічного прогнозування та раннього попередження, оскільки значна частина сучасних гібридних операцій ґрунтується на експлуатації соціальних поділів і маніпулюванні питаннями ідентичності. Автори наголошують, що аналіз виключно військових або кібернетичних компонентів уже не дозволяє повною мірою зрозуміти логіку сучасних

[3] https://www.rusi.org/explore-our-research/publications/research-papers/gender-and-identity-analysis-framework-hybrid-threats

конфліктів, адже противники дедалі активніше використовують людські емоції, соціальні травми, культурні конфлікти та моральні наративи як інструменти стратегічного впливу.

Документ детально пояснює, чому гендер та ідентичність мають критичне значення для аналізу гібридних загроз. Автори зазначають, що гібридні кампанії працюють через формування уявлень про те, хто є «своїм» і «чужим», хто потребує «захисту», а хто є «загрозою» для держави, культури чи традиційних цінностей. Через це питання гендеру, сексуальності, сім'ї, релігії та соціальної ролі стають інструментами мобілізації населення, створення моральної паніки та виправдання політичного або навіть військового втручання. У документі пояснюється, що противники часто використовують цілеспрямоване залякування та переслідування, дискредитацію жінок у публічному просторі, кампанії проти ЛГБТК+ спільнот, сексуалізоване насильство, релігійні наративи та дезінформацію про «традиційні цінності» для підриву довіри до демократичних інституцій і створення відчуття культурної загрози. Автори наголошують, що подібні операції не є хаотичними або випадковими — навпаки, вони часто є частиною довгострокових стратегій впливу, спрямованих на руйнування суспільної стійкості та формування політичного середовища, більш сприятливого для інтересів противника. Аналітична записка підкреслює, що без розуміння того, як саме активуються суспільні страхи, як мобілізуються різні групи населення та як створюються наративи про «захист моралі» чи «традиційних цінностей», держави можуть пропустити ранні сигнали гібридних операцій.

Особливе місце у документі займає застосування аналітичної записки до моделі PMESII (Political, Military, Economic, Social, Information, Infrastructure), що дозволяє продемонструвати, яким чином гендерні та засновані на ідентичності інструменти інтегруються у різні виміри гібридної діяльності. У політичному вимірі автори описують використання законодавства, судових процесів, дипломатії та інформаційних кампаній для формування наративів про «моральний захист» суспільства та делегітимізацію ліберальних демократичних цінностей. Як ключовий приклад розглядається російський закон про так звану «пропаганду нетрадиційних сексуальних відносин», який аналізується не як ізольований внутрішній нормативно-правовий акт, а як елемент ширшої міжнародної стратегії росії з просування «традиційних цінностей» як геополітичного інструменту впливу. Документ демонструє, що росія використовувала цей наратив не лише всередині країни, а й для побудови міжнародних альянсів із консервативними політичними та релігійними рухами, підтримки антизахідної риторики та формування транснаціональних мереж політичного впливу. Автори підкреслюють, що подібні законодавчі ініціативи часто супроводжуються скоординованими дезінформаційними кампаніями, дипломатичним тиском, підтримкою проксі-структур та використанням медіа для формування образу Заходу як «загрози традиційним цінностям». В аналітичній записці наголошується, що такі політичні та інформаційні інструменти здатні впливати на внутрішню політику інших держав, формувати нові лінії суспільного конфлікту та сприяти стратегічній поляризації.

У військовому вимірі документ детально аналізує використання сексуалізованого насильства, гендерно зумовленого залякування та примусових військових практик як інструментів гібридної війни. Автори наголошують, що сексуальне насильство у конфліктах не повинно сприйматися лише як побічний наслідок війни або окремі порушення дисципліни, оскільки в багатьох випадках воно має системний характер і використовується для досягнення стратегічних ефектів. На прикладі російської агресії проти України показано, як сексуалізоване насильство, приниження, погрози та гендерно орієнтований терор застосовувалися для залякування населення, руйнування довіри до держави, примусової міграції громадян, деморалізації локальних громад і створення довгострокових соціальних травм. Документ підкреслює, що такі практики можуть бути частиною ширшої примусової стратегії, спрямованої на дестабілізацію окупованих територій та підрив соціальної стійкості населення. Автори звертають увагу на те, що традиційні оцінки безпекових загроз часто не враховують подібні індикатори як елементи аналізу гібридних загроз, через що держави недооцінюють масштаби та стратегічне значення

таких дій. Аналітична записка рекомендує інтегрувати дані про сексуалізоване насильство, цілеспрямоване залякування, примусове переміщення населення та повторювані моделі жорстокого поводження у системи військової розвідки, захисту сил, раннього попередження та оцінки намірів противника.

Значна частина документа присвячена економічному виміру гібридних загроз та використанню фінансових потоків для стратегічного впливу. Автори пояснюють, що сучасні гібридні операції дедалі активніше використовують непрозорі фінансові механізми, благодійні фонди, релігійні організації, компанії-оболонки, проксі-мережі та структури фінансування впливу для підтримки політичних кампаній, інформаційних операцій і транснаціональних мереж впливу. У тематичному дослідженні, присвяченому фінансовим потокам на підтримку ультраконсервативних та антигендерних рухів, демонструється, як російські олігархічні та пов'язані з державою структури фінансували міжнародні рухи, спрямовані проти гендерних та сексуальних меншин, гендерної політики та права на аборти, створюючи глобальні мережі політичного та ідеологічного впливу. Документ детально описує використання офшорних структур, посередників, непрозорих благодійних організацій та міжнародних політичних форумів для просування російських стратегічних інтересів під виглядом захисту «традиційних цінностей». Автори підкреслюють, що подібні фінансові потоки часто залишаються поза увагою безпекових інституцій та систем ПВК/ФТ, оскільки формально виглядають як законна громадська або релігійна діяльність. Водночас аналітична записка наголошує, що саме через такі канали можуть створюватися довгострокові мережі політичного впливу, формуватися нові екстремістські середовища та посилюватися суспільні поділи, які згодом використовуються у ширших гібридних кампаніях.

Висновки:

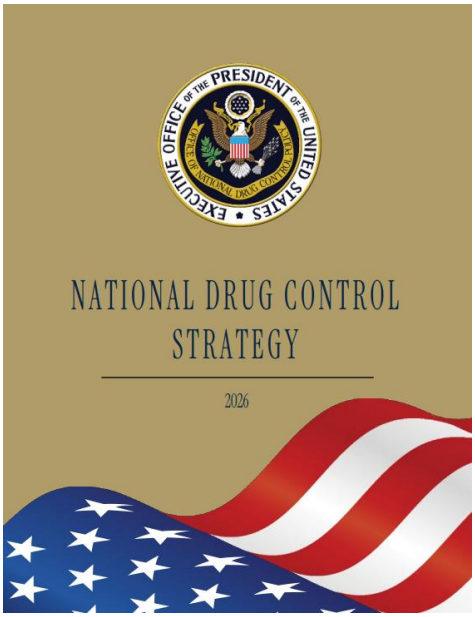
- **Гібридні операції дедалі частіше використовують гендер, «традиційні цінності», релігію та соціальну ідентичність як інструменти стратегічного впливу,** тому держави повинні інтегрувати гендерний та ідентифікаційний аналіз у системи національної безпеки, розвідувальний аналіз та механізми раннього попередження.
- **Сексуалізоване насильство, переслідування та гендерно зумовлене залякування у конфліктах мають розглядатися не як окремі воєнні злочини, а як потенційно системний інструмент примусової гібридної війни,** що потребує включення до оцінки військових ризиків, індикаторів загроз та систем документування злочинів.
- **Непрозорі фінансові потоки через благодійні, релігійні, громадські та «ціннісні» організації можуть бути елементом транснаціональних гібридних операцій,** тому ПФР, системи ПВК/ФТ та органи безпеки повинні посилити моніторинг мереж фінансування впливу, структур-прикриттів та фінансування ідеологічного впливу, пов'язаного з іноземними державами.
- **Для ефективної протидії гібридним загрозам державам необхідно створювати міжвідомчі моделі співпраці між сектором безпеки, ПФР, громадянським суспільством, аналітичними центрами та дослідниками дезінформації,** оскільки більшість сучасних гібридних кампаній поєднують інформаційний, соціальний, економічний та політичний вплив одночасно.

Документ також приділяє значну увагу проблемі «пропущених сигналів» — індикаторів, які державні органи та аналітичні структури часто помилково сприймають як ізольовані внутрішні соціальні процеси, а не як потенційні елементи гібридної діяльності. Серед таких сигналів автори називають скоординовані кампанії онлайн-переслідування, різке посилення антигендерної або анти-гендерних та сексуальних меншин риторики, мобілізацію релігійних мереж навколо «захисту сім'ї», використання благодійних організацій для політичної

активності, раптову появу добре профінансованих «ціннісних» кампаній, а також синхронізацію інформаційних операцій із фінансовими потоками та політичними ініціативами. Аналітична записка підкреслює, що сучасні гібридні кампанії є міжсекторальними та часто поєднують політичний, економічний, соціальний та інформаційний вплив одночасно, через що традиційний секторальний підхід до оцінки загроз втрачає ефективність. Автори закликають створювати міжвідомчі механізми аналізу, які поєднуватимуть розвідувальний аналіз, розвідку на основі відкритих джерел (OSINT), фінансову розвідку, гендерну експертизу, моніторинг екосистем громадянського суспільства та аналіз дезінформації.

У фінальній частині документа автори формулюють практичні рекомендації для урядів, сектору безпеки, розвідки, ПФР, міжнародних організацій та аналітичних центрів. Аналітична записка рекомендує інтегрувати гендерно чутливі індикатори у системи оцінки загроз національній безпеці, розробляти спеціалізовані методології для виявлення операцій впливу, посилювати моніторинг мереж фінансування, пов'язаних з іноземним впливом, а також розширювати співпрацю між безпековими інституціями, дослідниками, громадянським суспільством та структурами ПВК/ФТ. Автори наголошують, що протидія сучасним гібридним загрозам вимагає не лише військових або кібербезпекових рішень, а комплексного розуміння того, як функціонують механізми суспільної мобілізації, інформаційного впливу, політичної поляризації та фінансування ідеологічних мереж. Документ фактично пропонує нову модель аналізу загроз, у якій гендер, соціальна ідентичність, моральні наративи та культурні конфлікти розглядаються як повноцінні інструменти стратегічного впливу поряд із традиційними елементами гібридної війни. Автори наголошують, що сучасні гібридні кампанії можуть поєднувати інформаційні операції, експлуатацію суспільних поділів, сексуалізоване насильство, політичний вплив та непрозорі фінансові механізми у межах комплексних стратегій впливу.

Від боротьби з наркотиками до боротьби з гібридними загрозами: нова стратегія США 2026 [4]



Документ є однією з найбільш масштабних та жорстких американських стратегій у сфері протидії наркотикам за останні роки, яка демонструє фундаментальну трансформацію підходу США до наркотичної кризи. У документі проблема наркотиків розглядається вже не виключно як питання громадського здоров'я, а як комплексна гібридна загроза національній безпеці, пов'язана з транснаціональною організованою злочинністю, терористичною діяльністю, фінансовими потоками, використанням глобальних логістичних мереж, прикордонними загрозами та дестабілізацією американського суспільства. Стратегія побудована навколо концепції «загальнодержавного підходу», тобто повної інтеграції всіх державних інструментів — від правоохоронних та розвідувальних структур до системи охорони здоров'я, дипломатії, санкційної політики, міжнародної співпраці та технологічних платформ. Документ одразу задає дуже жорсткий тон, визначаючи фентанілову кризу як одну з найсерйозніших загроз для населення США, а діяльність наркокартелів — як своєрідну «хімічну атаку» проти Сполучених Штатів. У тексті неодноразово наголошується, що за останні роки США втратили сотні тисяч людей через

[4] https://www.whitehouse.gov/releases/2026/05/2026-national-drug-control-strategy-released/

передозування наркотиками, причому масштаби смертності вже порівнюються із сукупними військовими втратами США у найбільших війнах XX–XXI століть.

Стратегія формує нову модель сприйняття транснаціональних картелів та наркотрафіку. Якщо раніше наркотичні організації переважно розглядалися як кримінальні угруповання, то тепер вони дедалі більше прирівнюються до структур, що становлять повноцінну загрозу національній безпеці. Особливу увагу приділено механізму визнання картелів іноземними терористичними організаціями (FTOs), що дозволяє застосовувати до них антитерористичні повноваження, включаючи фінансові санкції, блокування активів, кримінальне переслідування за надання матеріальної підтримки тероризму та інші інструменти антитерористичного законодавства. Документ прямо вказує, що США більше не обмежуватимуться класичними механізмами протидії наркоторгівлі, а застосовуватимуть увесь комплекс державних інструментів і повноважень для ліквідації транснаціональних злочинних структур. У цьому контексті картелі описуються як багатофункціональні мережі, які одночасно займаються наркотрафіком, торгівлею зброєю, фінансовими злочинами, контрабандою людей, відмиванням коштів та насильством.

Документ особливо акцентує увагу на синтетичних наркотиках, насамперед фентанілі та метамфетаміні, які визначаються як головна сучасна наркотична загроза для США. Стратегія визнає, що сучасний наркотичний ринок став надзвичайно динамічним через постійну появу нових синтетичних наркотиків, дизайнерських прекурсорів та аналогів заборонених речовин. Значний фокус зроблено на нітозенах — новому поколінні синтетичних опіоїдів, які можуть бути значно потужнішими за фентаніл. Документ наголошує, що картелі та постачальники хімічних речовин постійно змінюють молекулярну структуру наркотиків для обходу міжнародного контролю, що створює серйозні виклики для судово-токсикологічної експертизи, правоохоронних органів та системи громадського здоров'я. У стратегії прямо зазначається, що попередні уряди США не змогли своєчасно передбачити перехід від рецептурних опіоїдів до героїну, а згодом — до незаконного фентанілу, що призвело до катастрофічного зростання смертності. Саме тому нинішня стратегія базується на концепції проактивного виявлення загроз та постійного моніторингу нових наркотичних загроз.

Однією з найважливіших частин документа є формування масштабної архітектури, заснованої на аналізі даних, для моніторингу наркотичних загроз. Стратегія передбачає інтеграцію результатів токсикологічних досліджень, систем моніторингу передозувань, аналізу стічних вод, даних відділень невідкладної медичної допомоги, електронних медичних записів, правоохоронної аналітики та розвідувальної інформації, а також систем біонагляду у єдину систему раннього виявлення загроз. Документ демонструє надзвичайно високий рівень уваги до аналітики даних і використання сучасних технологій. Передбачається активне впровадження штучного інтелекту (AI) та машинного навчання для прогнозування випадків передозування, аналізу поведінки наркотичних мереж, автоматизації роботи судово-експертних лабораторій, виявлення прихованих закономірностей у незаконному обігу наркотиків та створення систем прогнозної аналітики (predictive analytics systems). США фактично формують інфраструктуру моніторингу в режимі, наближеному до реального часу, для постійного відстеження наркотичної ситуації як усередині країни, так і за її межами. Особливий акцент робиться на швидкості обміну інформацією між федеральними, штатними, місцевими, племінними та територіальними органами влади, а також на створенні систем оперативного публічного попередження щодо появи нових небезпечних наркотичних речовин.

Важливим структурним елементом документа є концепція «Supply Chain Integrity», яка демонструє суттєву зміну у сприйнятті глобального наркотрафіку. Стратегія визнає, що сучасні картелі активно використовують легальні міжнародні торговельні та логістичні мережі для транспортування наркотиків, прекурсорів та обладнання для виробництва наркотиків. Особливу увагу приділено дрібним вантажним відправленням низької вартості та системі

винятків для товарів незначної вартості, які дозволяли мільярдам невеликих посилок проходити митний контроль із мінімальним рівнем перевірок. Документ прямо вказує, що саме ця система стала одним із ключових каналів доставки фентанілу до США. У відповідь адміністрація США планує повне посилення контролю за глобальними ланцюгами постачання та створення нових моделей співпраці з приватним сектором. Передбачається залучення судноплавних компаній, виробників хімічної продукції, фармацевтичних компаній, логістичних операторів та виробників лабораторного обладнання до програм надійної торгівлі, подібних до програми Програма митно-торговельного партнерства проти тероризму (CTPAT). Компанії повинні впроваджувати посилену перевірку контрагентів (EDD), механізми контролю ланцюга постачання та збереження походження товару, розширений збір даних і механізми прозорості ланцюгів постачання.

Документ демонструє надзвичайно жорстку позицію США щодо держав, які розглядаються як країни походження або транзитні країни для наркотрафіку. Особливий акцент робиться на Китаї, який прямо звинувачується у сприянні експорту прекурсорів, що використовуються для виробництва фентанілу та інших синтетичних наркотиків. Значна увага приділяється також Індії, Мексиці, Канаді та Колумбії. Мексика описується як головний центр діяльності картелів та виробництва фентанілу, а Китай — як ключовий постачальник хімічних компонентів. Документ прямо вказує, що США використовуватимуть усі можливі дипломатичні, економічні, санкційні та кримінально-правові механізми для примусу цих держав до активнішої боротьби з наркотрафіком. У стратегії також наголошується на необхідності міжнародного включення небезпечних речовин до контрольованих списків, посилення глобальної митної співпраці та створення систем обміну інформацією в режимі реального часу щодо прекурсорів і обладнання для виробництва наркотиків.

Внутрішня безпекова частина документа базується на концепції Homeland Security Task Forces (HSTFs), які повинні об'єднати всі правоохоронні структури США у єдину операційну архітектуру. Стратегія виходить із того, що наркотрафік не можна розглядати ізольовано від інших видів транснаціональної злочинності.

Висновки:

- **США переводять боротьбу з наркотиками у площину національної безпеки та антитерористичної політики.** Картелі дедалі більше розглядаються як гібридні транснаціональні загрози, що зумовлює розширення застосування санкцій, механізмів фінансової ізоляції та міжнародних правоохоронних інструментів.
- **Глобальні логістичні та торговельні системи визнаються ключовою вразливістю сучасного наркотрафіку.** Стратегія передбачає посилення контролю за ланцюгами постачання, митними даними та відповідальністю приватного сектору, що має важливе значення для інтеграції торговельних ризик-індикаторів у системи ПВК/ФТ.
- **Інтеграція даних та технології штучного інтелекту стають ключовими інструментами сучасної політики у сфері контролю за наркотиками.** США формують систему моніторингу, наближену до режиму реального часу, із використанням токсикологічних, медичних та правоохоронних даних, що демонструє глобальний перехід до прогнозного управління ризиками та формування державної політики на основі даних.
- **Стратегія підкреслює, що ефективна протидія наркотичній кризі потребує одночасного скорочення пропозиції наркотиків і зменшення попиту на них.** Поряд із правоохоронними заходами документ передбачає розвиток профілактики, лікування, підтримки відновлення після залежності та систем реагування на передозування в межах єдиної міжвідомчої моделі.

Саме тому HSTFs повинні одночасно протидіяти наркотрафіку, фінансовим злочинам, мережам торгівлі людьми, незаконному переміщенню вогнепальної зброї та незаконному переплавленню мігрантів. Документ описує створення багаторівневої системи перехоплення та протидії, яка охоплює морські маршрути, повітряні канали перевезення, прикордонні переходи, пункти пропуску через державний кордон, міжнародні поштові центри обробки відправлень та внутрішні транспортні мережі США. Значна увага приділяється використанню систем неруйнівного контролю та інспекції, інструментів таргетування на основі штучного інтелекту, автоматичних систем зчитування номерних знаків, центрів об'єднання та аналізу розвідувальної інформації і передових технологій спостереження.

Паралельно із жорстким безпеково-орієнтованим підходом документ містить масштабний блок, присвячений громадському здоров'ю, який охоплює профілактику, лікування залежності та підтримку систем реабілітації й відновлення. Стратегія прямо наголошує, що доступ до лікування залежності має бути простішим і швидшим, ніж доступ до наркотиків. Значна увага приділяється ранньому втручанню, інтегрованим системам лікування, розширенню мережі фахівців і консультантів із досвідом подолання залежності, препаратам для екстреного усунення наслідків передозування та створенню робочих середовищ, адаптованих до підтримки осіб у процесі відновлення. Документ також просуває концепцію «drug-free America as a social norm», тобто формування культури несприйняття наркотиків як суспільної норми. У цьому контексті особливо підкреслюється роль релігійних організацій, духовних лідерів і духовної підтримки у системі профілактики та відновлення після залежності. Документ прямо зазначає, що віра та релігія повинні стати важливою складовою боротьби із залежністю, а духовні інституції розглядаються як партнери держави у формуванні здорового суспільства.

Загалом документ демонструє глибоку трансформацію американської антинаркотичної політики у напрямі розгляду наркотичної кризи як питання національної безпеки. Наркотична криза дедалі більше розглядається через призму гібридних загроз, у межах яких наркотики, транснаціональна злочинність, незаконні фінансові потоки, глобальні ланцюги постачання, санкційні режими, прикордонна безпека та інформаційні технології формують єдину систему ризиків. Стратегія побудована навколо концепції «загальнодержавного підходу», тобто повної інтеграції всіх державних інструментів — від правоохоронних і розвідувальних органів до системи охорони здоров'я, дипломатичних механізмів, санкційної політики, міжнародної співпраці та технологічних платформ. Для сфери ПВК/ФТ цей документ має особливе значення, оскільки демонструє посилення взаємозв'язку між наркотрафіком, фінансовими потоками, санкційними механізмами та міжнародною безпекою, а також формує нові підходи до використання фінансових, митних і логістичних систем у протидії транснаціональній злочинності.

Нова архітектура грошей: трансформація міжнародних платежів і банківської системи в епоху цифрових валют [5]

Документ є масштабним аналітичним дослідженням трансформації сучасної глобальної фінансової системи під впливом цифровізації грошей, розвитку технології розподіленого реєстру (DLT), токенізації активів та появи нових моделей розрахунків. Автори розглядають цифрові гроші не як ізольований криптовалютний феномен, а як фундаментальний етап еволюції світової грошової інфраструктури, у межах якого відбувається поступовий перехід від традиційної банківської системи з обмеженим операційним часом, пакетною обробкою транзакцій та багаторівневими посередницькими моделями до безперервної цифрової

[5] https://flow.db.com/files/documents/more/publications/white-papers-guides/2026/DB-Digital-Money-WP-2026-30pp-Web-Secured.pdf

економіки, де гроші стають програмованими, токенізованими та здатними функціонувати у режимі 24/7. Deutsche Bank наголошує, що сучасна фінансова система дедалі більше рухається у бік інтегрованого цифрового середовища, у якому платежі, розрахунки, управління ліквідністю та ринки капіталу функціонуватимуть на основі нових цифрових форм грошей, здатних забезпечувати миттєві розрахунки, автоматизацію фінансових процесів та взаємодію між різними фінансовими платформами.

На початку документа автори формують базову концепцію сучасного грошового середовища та пояснюють еволюцію форм грошей — від фізичних банкнот і монет до цифрових та програмованих форматів. Deutsche Bank підкреслює, що гроші традиційно виконують три фундаментальні функції — є засобом обміну, одиницею обліку та засобом збереження вартості, однак технологічний розвиток поступово змінює механізми реалізації цих функцій. У дослідженні детально розмежовуються публічні гроші та приватні гроші. До публічних грошей належать готівка, резерви центральних банків, роздрібні цифрові валюти центральних банків (CBDCs) та оптові цифрові валюти центральних банків, тоді як до приватних грошей віднесено традиційні банківські депозити, електронні гроші, стейблкоїни та токенізовані депозити. Документ окремо наголошує, що криптовалюти типу Bitcoin або Ethereum не можуть повноцінно виконувати функції грошей через високу волатильність, спекулятивний характер та відсутність прив'язки до фіатної валюти чи регульованого емітента. На відміну від них, цифрові гроші нового покоління мають залишатися інтегрованими у регульовану фінансову систему, бути прив'язаними до фіатних валют та забезпечувати стабільність, передбачуваність і довіру учасників ринку.

Центральне місце у документі займає аналіз стейблкоїнів як однієї з найбільш зрілих форм приватних цифрових грошей. Deutsche Bank визначає стейблкоїни як цифрові токени, забезпечені фіатними резервами та високоліквідними активами, переважно короткостроковими державними облігаціями США. Автори підкреслюють стрімке зростання цього ринку — від приблизно 50 млрд доларів у 2021 році до понад 300 млрд доларів у 2026 році. Водночас документ демонструє, що стейблкоїни досі залишаються глибоко інтегрованими у криптовалютну інфраструктуру, оскільки основна частина їх використання припадає на забезпечення ліквідності криптобірж, DeFi-протоколів та криптовалютної торгівлі. Особливу увагу автори приділяють абсолютному домінуванню доларових стейблкоїнів, насамперед USDT та USDC. Deutsche Bank пояснює це структурною доларизацією глобального крипторинку, концентрацією ліквідності навколо інструментів, номінованих у доларах США, та статусом долара США як основної резервної валюти світу. Документ наголошує, що розвиток стейблкоїнів, забезпечених доларом США (USD-backed stablecoins), уже формує значний попит на державні облігації США (US Treasuries), а самі емітенти стейблкоїнів стають одними з великих утримувачів американських державних облігацій, фактично посилюючи глобальне домінування долара США у міжнародній фінансовій системі.

Важливий блок дослідження присвячений формуванню міжнародної регуляторної архітектури для стейблкоїнів. Deutsche Bank детально аналізує відмінності між підходами США, Європейського Союзу та азійських держав. У США ключовим елементом став GENIUS Act 2025, який створює окрему нормативно-правову базу саме для стейблкоїнів та запроваджує категорію «дозволених емітентів стейблкоїнів». Документ підкреслює, що американська модель орієнтована на використання стейблкоїнів як інструменту платежів та міжнародного поширення долара США, а не як інвестиційного продукту. Закон передбачає суворі вимоги до

резервування 1:1, дотримання вимог у сфері протидії відмиванню коштів та ідентифікації клієнтів (ПВК/KYC), обмеження на виплату доходності та державний нагляд, максимально наближений до банківського. Deutsche Bank зазначає, що американська влада відкрито розглядає регульовані стейблкоїни як інструмент підтримки глобального статусу долара США та збільшення міжнародного попиту на американські державні облігації. Європейський Союз, навпаки, через Регламент MiCA створює комплексний режим регулювання всієї екосистеми криптоактивів із фокусом на монетарному суверенітеті, фінансовій стабільності та захисті ролі євро. Документ підкреслює, що ЄС прагне мінімізувати ризики домінування стейблкоїнів, номінованих не в євро, встановлює вимоги щодо локалізації резервів у межах ЄС та жорстко контролює нормативну базу випуску стейблкоїнів. Автори також описують розвиток регульованих євро-стейблкоїнів та появу перших ліцензованих проєктів електронних грошових токенів (EMT projects). В азійському регіоні, зокрема у Гонконзі, Сінгапурі, Японії та Таїланді, Deutsche Bank бачить більш експериментальний та прагматичний підхід, орієнтований на регуляторні «пісочниці», тестування нових платіжних моделей та інтеграцію стейблкоїнів у цифрову економіку.

Окрему увагу документ приділяє використанню стейблкоїнів у платіжній сфері. Deutsche Bank демонструє, що хоча сьогодні реальні економічні платежі становлять відносно невелику частину активності стейблкоїнів, саме цей сегмент демонструє найвищі темпи зростання. У документі зазначається, що загальний обсяг транзакцій зі стейблкоїнами у 2025 році оцінювався приблизно у 62 трлн доларів США, однак після виключення активності ботів, внутрішніх переказів та неекономічних транзакцій реальні економічні перекази становили близько 4,2 трлн доларів, а безпосередньо платежі у реальному секторі економіки — лише 350–550 млрд доларів. Попри це автори підкреслюють стрімке зростання сегменту B2B-платежів та транскордонних переказів. Стейблкоїни дедалі активніше використовуються для грошових переказів, B2C-виплат, казначейських операцій, міжнародних переказів та збереження доларової ліквідності у країнах із нестабільними валютами або обмеженим доступом до доларової інфраструктури. Документ також описує потенціал використання стейблкоїнів на токенізованих ринках капіталу як розрахункового активу для моделей «поставка проти платежу» (DvP) та «платіж проти платежу» (PvP). Deutsche Bank демонструє, що відбувається поступове зближення традиційної фінансової системи та екосистеми стейблкоїнів, про що свідчать значні інвестиції глобальних платіжних компаній та фінансових корпорацій у інфраструктуру стейблкоїнів.

Разом із потенційними перевагами документ детально аналізує структурні обмеження та бар'єри, які стримують масове впровадження стейблкоїнів. Серед ключових проблем виділяються фрагментація між різними блокчейн-екосистемами та емітентами, відсутність глобальної регуляторної гармонізації, недостатня зрілість інституційної інфраструктури зберігання цифрових активів, нерівномірне застосування механізмів контролю у сфері ПВК/ФТ, а також складність інтеграції стейблкоїнів у традиційні ERP-системи, системи управління ліквідністю та системи звітності. Особливо важливою проблемою називається відсутність єдиного галузевого стандарту обміну повідомленнями, аналогічного стандарту ISO 20022 у традиційній банківській системі. Документ фактично демонструє, що масштабне впровадження стейблкоїнів залежатиме не лише від технологічного розвитку, а й від здатності глобальної фінансової системи сформувати узгоджені міжнародні стандарти комплаєнсу, сумісності систем та інтеграції з існуючою банківською інфраструктурою.

Наступний великий блок документа присвячений токенізованим депозитам, які Deutsche Bank розглядає як потенційно найбільш органічну форму інтеграції технології розподіленого реєстру (DLT) у традиційну банківську систему. Токенізовані депозити визначаються як токенізовані форми комерційних банківських депозитів, що зберігають юридичну природу банківського зобов'язання, але функціонують у блокчейн-середовищі. Автори аналізують кілька моделей

розвитку токенізованих депозитів. Першою є внутрішньобанківські платформи, у межах яких банки використовують дозволені блокчейн-мережі для забезпечення цілодобових розрахунків у режимі 24/7 між власними рахунками та філіями. Другою моделлю є міжбанківські системи на основі консорціумних реєстрів, серед яких особливо виділяються Partior, Project Agorá та Swift Ledger. Ці ініціативи розглядаються як потенційна основа для модернізації кореспондентського банкінгу та створення нової глобальної інфраструктури програмованих транскордонних розрахунків. Третьою моделлю є депозитні токени у публічних блокчейн-мережах, де банки експериментують із випуском токенізованих депозитів у публічних блокчейн-екосистемах за умови контрольованого доступу відповідно до вимог KYC. Deutsche Bank наголошує, що токенізовані депозити дозволяють перенести регульовані банківські гроші у середовище цифрової економіки, не руйнуючи існуючої банківської моделі та чинних регуляторних запобіжників.

Документ окремо підкреслює переваги токенізованих депозитів порівняно зі стейблкоїнами. Оскільки токенізовані депозити юридично залишаються банківськими депозитами, вони можуть приносити дохід власникам, інтегруватися з існуючими банківськими продуктами та користуватися вищим рівнем регуляторної довіри. Deutsche Bank вважає, що саме токенізовані депозити можуть стати основою для модернізації управління ліквідністю та казначейських операцій, координації ліквідності, автоматизованого управління ліквідністю та консолідації коштів, а також токенізованих ринків капіталу. Водночас автори наголошують, що масштабне впровадження токенізованих депозитів стикається із серйозними проблемами сумісності систем між різними банками та блокчейн-мережами, а також із необхідністю інтеграції нових систем на основі DLT із базовою банківською інфраструктурою, системами валових розрахунків у режимі реального часу (RTGS systems) та системами обміну повідомленнями на основі стандарту ISO 20022. Документ фактично демонструє, що розвиток токенізованих депозитів потребуватиме значної координації між банками, центральними банками, фінансовими ринковими інфраструктурами та регуляторами.

Останній великий блок документа присвячений CBDCs. Deutsche Bank розділяє роздрібні CBDCs та оптові CBDCs, демонструючи принципово різні траєкторії їх розвитку. Роздрібні CBDCs розглядаються як цифрове доповнення до готівки для населення, однак документ констатує, що їх впровадження стикається з політичними, ринковими та поведінковими бар'єрами. У США відбувається фактична відмова від роздрібних CBDCs на користь цифрових грошових рішень приватного сектору та регульованих стейблкоїнів. У Великій Британії триває лише етап проєктування, а остаточне рішення щодо запуску цифрового фунта ще не ухвалене. Китай залишається найбільш просунутим прикладом із цифровим юанем e-CNY, однак навіть там масове впровадження залишається обмеженим через домінування Alipay та WeChat Pay. Найбільш структурованим західним проєктом документ називає цифрове євро, який Європейський центральний банк потенційно планує запустити ближче до 2029 року. Автори детально аналізують модель цифрового євро, включаючи архітектуру на основі цифрових гаманців, офлайн-платежі, механізми автоматичного перерахування коштів та інтеграцію з банківськими рахунками. Водночас Deutsche Bank наголошує, що роздрібні CBDCs можуть суттєво змінити структуру банківської системи, оскільки створюють ризики відтоку депозитів із комерційних банків до цифрових грошей центрального банку.

На відміну від роздрібних CBDCs, оптові CBDCs оцінюються значно позитивніше. Deutsche Bank вважає, що саме оптові CBDCs мають найбільший потенціал для модернізації міжбанківських розрахунків, кореспондентського банкінгу та токенізованих ринків капіталу. Документ детально аналізує такі проєкти як Project Agorá, Pontes, Appia, а також ініціативи Банку Англії, Монетарного управління Сінгапуру (MAS) та інших центральних банків щодо інтеграції технології розподіленого реєстру (DLT) у інфраструктуру систем валових розрахунків у режимі реального часу (RTGS infrastructure). Оптові CBDCs розглядаються не як повністю новий тип

грошей, а як еволюція існуючих грошей центрального банку у програмовану інфраструктуру. Автори наголошують, що розвиток оптових CBDCs безпосередньо пов'язаний із появою токенізованих цінних паперів, програмованих систем розрахунків та нових моделей розрахунків «поставка проти платежу» і «платіж проти платежу» (DvP/PvP). Deutsche Bank фактично демонструє, що центральні банки поступово переходять від концептуальних дискусій до практичного створення сумісної інфраструктури розрахунків для токенізованої економіки.

Загалом документ формує висновок, що майбутня фінансова система не буде побудована навколо одного універсального типу цифрових грошей. Deutsche Bank прогнозує співіснування стейблкоїнів, токенізованих депозитів та CBDCs, де кожна форма грошей використовуватиметься залежно від типу операцій, рівня регуляторних вимог, необхідної швидкості розрахунків, програмованості та інтеграції з існуючою фінансовою інфраструктурою. Банки при цьому розглядаються як ключові координатори нової цифрової фінансової системи, які будуть приховувати технологічну складність від клієнтів та автоматично обирати найбільш ефективний тип цифрових грошей для конкретної транзакції. Документ фактично демонструє, що цифровізація грошей уже стала не теоретичною концепцією, а практичним процесом перебудови глобальної фінансової архітектури, який у найближчі роки суттєво змінить міжнародні платежі, ринки капіталу, банківську діяльність та систему глобальних фінансових розрахунків.

Висновки:

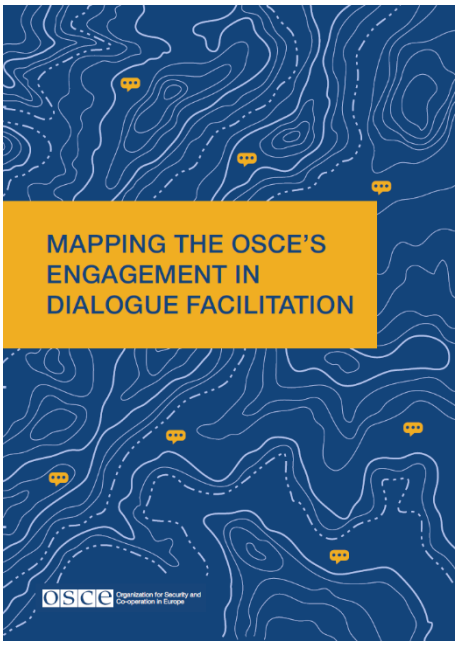
- **Документ демонструє, що глобальна фінансова система переходить до моделі програмованих грошей та цілодобової інфраструктури розрахунків,** де стейблкоїни, токенізовані депозити та оптові цифрові валюти центральних банків поступово інтегруються у міжнародні платежі, управління ліквідністю та ринки капіталу. Це вимагає від банків і регуляторів адаптації банківської інфраструктури, систем розрахунків і комплаєнс-механізмів до DLT-середовища.
- **Стейблкоїни поступово виходять за межі криптовалютного сектору та перетворюються на інструмент міжнародних платежів, B2B-переказів, грошових переказів і токенізованих ринків капіталу.** Водночас масштабування цього ринку неможливе без глобальної гармонізації стандартів ПВК/ФТ, сумісності систем та розвитку інституційної інфраструктури зберігання і комплаєнсу.
- **Deutsche Bank розглядає токенізовані депозити як найбільш реалістичний механізм інтеграції DLT у традиційну банківську систему,** оскільки вони зберігають юридичну природу банківських депозитів та інтегруються з існуючою банківською екосистемою. Це свідчить про те, що банки залишатимуться ключовими учасниками цифрової фінансової системи.
- **Документ показує, що роздрібні CBDCs поки стикаються з політичними та ринковими бар'єрами, тоді як оптові CBDCs швидко переходять до практичної реалізації.** Найбільш перспективним напрямом визначається створення сумісної інфраструктури міжбанківських розрахунків для токенізованих депозитів, цінних паперів та транскордонних платежів на базі DLT.

ОБСЄ як фасилітатор миру: багаторівневий діалог у системі сучасної безпеки [6]

Документ є масштабним аналітичним дослідженням Організації з безпеки і співробітництва в Європі (ОБСЄ), присвяченим систематизації підходів, практик та досвіду ОБСЄ у сфері фасилітації

[6] https://cdn.osce.org/sites/default/files/f/documents/0/9/584712.pdf

діалогу як одного з ключових інструментів попередження конфліктів, управління кризами, миробудування та підтримання стійкої безпеки. Дослідження підготовлене Conflict Prevention Centre (CPC) на основі аналізу понад 120 діалогових ініціатив, реалізованих структурами ОБСЄ у 2020–2023 роках у різних регіонах простору ОБСЄ. Документ демонструє, що фасилітація діалогу поступово перетворюється для ОБСЄ не лише на допоміжний дипломатичний інструмент, а на окремий стратегічний компонент архітектури запобігання конфліктам та комплексного управління безпекою. У центрі дослідження знаходиться ідея, що сучасні конфлікти є багатовимірними, тривалими та глибоко пов'язаними із соціальними, політичними, економічними, етнічними, релігійними та гуманітарними чинниками, а тому їх неможливо ефективно вирішувати виключно через політичні переговори чи силові механізми без довгострокового формування довіри між громадами та інституціями.



Автори підкреслюють, що концептуальна основа підходу ОБСЄ до діалогу бере початок ще з Гельсінського заключного акта 1975 року, який фактично заклав основу моделі кооперативної безпеки через постійний політичний діалог між державами навіть у періоди високої геополітичної напруги. У сучасному контексті ОБСЄ переносить цю логіку на внутрішньодержавний, міжгромадський та транскордонний рівні, розглядаючи фасилітацію діалогу як процес побудови соціальної згуртованості, емпатії, взаєморозуміння та довіри між різними групами населення, інституціями та сторонами конфлікту. Документ наголошує, що основною метою діалогу є не обов'язково досягнення негайної політичної угоди, а створення умов для поступового зменшення поляризації та формування простору для мирного співіснування і спільного пошуку рішень. Саме тому ОБСЄ трактує діалог як відкритий, довгостроковий та адаптивний процес, який може тривати роками та супроводжувати формальні мирні переговори або функціонувати паралельно з ними.

Документ детально аналізує роль фасилітації діалогу на різних етапах циклу конфлікту. На стадії первинного запобігання конфліктам діалог використовується як інструмент раннього реагування на зростаючі соціальні чи політичні напруження, міжетнічні суперечності, локальні конфлікти або ознаки радикалізації. У цьому контексті ОБСЄ акцентує увагу на розвитку локальних спроможностей до мирного врегулювання суперечок, підтримці місцевих платформ для обговорення проблем та зміцненні довіри між громадами і владою. У межах вторинного запобігання конфліктам діалог стає інструментом кризового реагування та деескалації, спрямованим на пошук практичних рішень і взаємоприйнятних результатів у конкретних конфліктних ситуаціях. На стадії третинного запобігання конфліктам та миробудування діалог спрямовується на примирення, відновлення довіри, зміцнення інституцій та запобігання повторній ескалації конфлікту. Таким чином, ОБСЄ фактично формує модель безперервного застосування фасилітації діалогу у межах усієї системи управління конфліктами.

У дослідженні окремо систематизуються три ключові типи діалогових процесів, які використовує ОБСЄ. Діалог, орієнтований на побудову відносин і довіри, спрямований насамперед на поступове формування взаємної довіри, емпатії та розуміння між сторонами конфлікту або громадами, які тривалий час перебували у стані напруження. Такі процеси часто мають довгостроковий характер та використовуються у постконфліктних регіонах або у глибоко поляризованих суспільствах. Діалог, орієнтований на вирішення проблем, спрямований на розв'язання конкретних кризових або практичних питань, наприклад, доступу до

інфраструктури, управління природними ресурсами, локальної безпеки, повернення переміщених осіб або взаємодії між громадами та органами влади. Діалог, орієнтований на участь, використовується для забезпечення інклюзивності та залучення до процесів прийняття рішень жінок, молоді, меншин, громадянського суспільства та інших традиційно маргіналізованих груп. Документ демонструє, що ОБСЄ розглядає інклюзивність як критично важливу умову довгострокової стійкості мирних процесів та легітимності рішень.

Значна частина документа присвячена аналізу практичних ролей ОБСЄ у фасилітації діалогу. Організація може виступати як неупереджений організатор діалогу, надійний посередник, сторона, що надає добрі послуги, фасилітатор човникової дипломатії або суб'єкт тихої дипломатії. ОБСЄ активно використовує неформальні механізми контактів між сторонами конфлікту, створює «безпечні простори» для конфіденційного обговорення чутливих питань та підтримує діалогові мережі між різними групами населення. Особливе значення надається внутрішній медіації — механізму, коли довгострокові працівники польових місій, які користуються довірою місцевих громад, виступають неформальними посередниками та сприяють підтриманню контактів між сторонами. Автори підкреслюють, що саме довіра до ОБСЄ як до нейтрального та авторитетного учасника є одним із головних факторів ефективності її діалогових ініціатив.

Документ надзвичайно детально описує роль польових місій ОБСЄ як передових механізмів у сфері фасилітації діалогу. У Південно-Східній Європі діяльність місій зосереджується на міжетнічному та міжрелігійному діалозі, залученні меншин, жінок і молоді, а також підтримці належного врядування, прав людини та місцевої участі. У Центральній Азії ключовими напрямами стають транскордонний діалог, управління водними ресурсами, енергетична безпека, прикордонне управління та взаємодія прикордонних громад. У Молдові ОБСЄ підтримує багаторівневі переговорні механізми у межах процесу врегулювання придністровського конфлікту, включаючи роботу Спільних експертних робочих груп та підтримку жінок-переговорниць. У Грузії та на Південному Кавказі ОБСЄ бере участь у заходах зі зміцнення довіри, підтримує Женевські міжнародні дискусії та Механізм запобігання інцидентам і реагування на них. Документ демонструє, що польові місії ОБСЄ виконують не лише технічну чи адміністративну функцію, а фактично є постійними платформами для розвитку миротворчої інфраструктури та запобігання конфліктам на рівні громад.

Окремий великий блок дослідження присвячений інклюзивності та змістовній участі. Автори наголошують, що стійкий мир неможливий без повноцінного залучення жінок, молоді, меншин та громадянського суспільства до мирних процесів і процесів формування державної політики. ОБСЄ реалізує значну кількість ініціатив жіночого миротворчого лідерства, платформ для жінок-медіаторок, молодіжних діалогових академій та партисипативних форумів, які мають на меті не лише формальне представництво окремих груп, а реальне включення їхніх інтересів та поглядів у процеси прийняття рішень. Документ особливо підкреслює роль жіночих мереж як механізмів неформальної дипломатії та транскордонної побудови довіри. Молодь розглядається як критично важлива зацікавлена сторона у формуванні майбутньої соціальної згуртованості та запобіганні повторній радикалізації. Водночас автори визнають, що інклюзивність не повинна обмежуватися лише присутністю окремих груп у діалогових процесах, а має забезпечувати реальне врахування їхніх позицій та формування локальної відповідальності за результати таких процесів.

Дослідження також демонструє надзвичайно широку тематичну різноманітність діалогових процесів ОБСЄ. Фасилітація діалогу використовується у питаннях врядування, виборчих процесів, децентралізації, доступу до правосуддя, прав людини, злочинів на ґрунті ненависті, гендерно зумовленого насильства, деградації довкілля, управління водними ресурсами, прикордонної безпеки, протидії торгівлі людьми, розвитку інфраструктури, надання місцевих послуг, захисту культурної спадщини та транснаціональних загроз. Таким чином, ОБСЄ

поступово перетворює фасилітацію діалогу на універсальний механізм комплексного управління безпековими, соціальними та гуманітарними ризиками. Особливу увагу документ приділяє питанням напруженостей, пов'язаних зі зміною клімату, управління природними ресурсами та транскордонного співробітництва, що свідчить про адаптацію підходів ОБСЄ до сучасних багатовимірних і гібридних загроз.

У фінальній частині документа аналізуються отримані уроки та рекомендації щодо подальшого розвитку архітектури фасилітації діалогу в ОБСЄ. Автори визнають, що ефективна фасилітація діалогу потребує системного проєктування процесів, наявності теорій змін, комплексного аналізу конфліктів, довгострокового фінансування та спеціалізованої професійної підготовки персоналу. Документ наголошує, що фасилітація діалогу повинна розглядатися як окрема професійна сфера, яка потребує спеціалізованих навичок, наставництва, професійного супроводу та взаємного навчання між практиками. Водночас автори визнають ризики надмірної залежності від окремих «лідерів діалогу», оскільки це може робити процес нестійким. Натомість ОБСЄ рекомендує розвивати широкі мережі локальної залученості, інституційної участі та багаторівневої взаємодії. Значний акцент робиться також на необхідності багаторічного гнучкого фінансування, посилення співпраці з ООН та ЄС, розвитку регіональних діалогових ініціатив та інтеграції гендерно чутливих і молодіжно орієнтованих підходів у аналіз конфліктів та проєктування діалогових процесів.

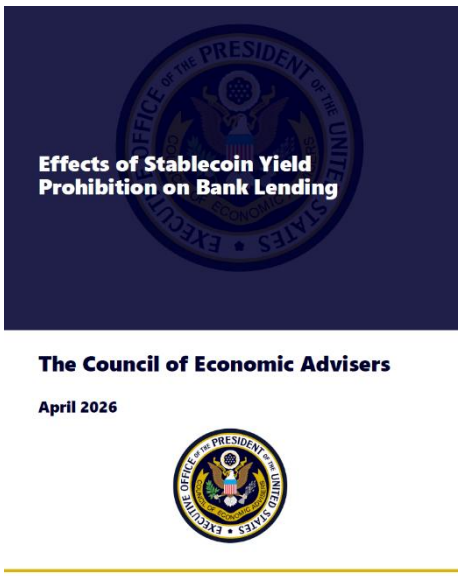
Загалом документ демонструє фундаментальну трансформацію сучасних міжнародних підходів до безпеки та врегулювання конфліктів. ОБСЄ фактично формує модель інтегрованої архітектури діалогу, у якій миробудування розглядається не як суто політичний процес між елітами, а як багаторівневий, інклюзивний та довгостроковий процес побудови довіри, соціальної згуртованості та

Висновки:

- **Документ демонструє, що фасилітація діалогу є одним із ключових інструментів сучасної архітектури запобігання конфліктам та повинна інтегруватися у всі стадії циклу конфлікту — від раннього попередження до постконфліктного миробудування.** Практичний висновок полягає у необхідності для держав, міжнародних організацій та ПФР інтегрувати механізми міжвідомчого та суспільного діалогу у системи раннього реагування на соціальні, політичні та безпекові ризики.
- **ОБСЄ фактично підтверджує, що стійкий мир неможливий без змістовного залучення жінок, молоді, меншин та громадянського суспільства до мирних процесів і формування державної політики.** Практично це означає, що програми безпеки, стабілізаційні програми та миротворчі ініціативи повинні містити механізми діалогу із широким залученням зацікавлених сторін та локальної відповідальності за результати.
- **Документ підкреслює, що ефективність фасилітації діалогу напряму залежить від стратегічного проєктування процесів, аналізу конфліктів, наявності теорій змін та довгострокового фінансування.** Практичний висновок полягає у необхідності переходу від короткострокових ситуативних діалогових ініціатив до системних багаторічних програм із чіткими показниками результативності та методологіями оцінки впливу.
- **Дослідження демонструє зростаючу роль фасилітації діалогу у реагуванні на багатовимірні та гібридні загрози, включаючи прикордонні спори, напруження, пов'язані зі зміною клімату, кризи врядування, мову ворожнечі, транснаціональні загрози та міжетнічну поляризацію.** Для України це означає необхідність розвитку національних спроможностей у сфері медіації, стратегічної фасилітації діалогу та суспільної стійкості як елементів національної безпеки.

інституційної стійкості. Дослідження підкреслює, що в умовах сучасних гібридних і багатовимірних конфліктів саме здатність суспільств підтримувати інклюзивний діалог, залучати місцеві громади, жінок і молодь, а також формувати стійкі інституції стає одним із ключових факторів довгострокової безпеки та запобігання повторному спалаху насильства.

Стейблкоїни та монетарна політика: нові виклики для центральних банків [7]



Документ, підготовлений Council of Economic Advisers у квітні 2026 року, є масштабним економічним та регуляторним дослідженням, присвяченим аналізу потенційного впливу заборони виплати доходу за стейблкоїнами на банківське кредитування, фінансове посередництво, монетарну політику та структуру сучасної фінансової системи США. У дослідженні розглядаються наслідки імплементації положень GENIUS Act 2025 та можливих майбутніх змін у межах CLARITY Act, які можуть суттєво обмежити можливість нарахування доходу власникам стейблкоїнів. Автори ставлять під сумнів одну з ключових тез сучасної політичної дискусії навколо цифрових активів — твердження про те, що стейблкоїни з конкурентною доходністю здатні масштабно відтікати депозити з банківської системи та суттєво скорочувати кредитування економіки. Документ фактично є спробою емпірично та теоретично оцінити, наскільки реальними є ризики дезінтермедіації банківської системи в умовах стрімкого розвитку цифрових доларових інструментів.

На початку дослідження автори детально описують сучасну модель стейблкоїнів, забезпечених доларом США, та регуляторну архітектуру, сформовану GENIUS Act. Пояснюється, що відповідно до нового законодавства емітенти стейблкоїнів зобов'язані забезпечувати токени резервами у співвідношенні щонайменше один до одного, причому резерви можуть складатися виключно з чітко визначених високоліквідних активів, зокрема доларів США, коштів у регульованих депозитарних установах, короткострокових казначейських векселів США, операцій репо, забезпечених державними цінними паперами США, а також державних фондів грошового ринку. Документ наголошує, що така модель значно наближає стейблкоїни до концепції «вузького банкінгу», яка історично розглядалася як альтернатива класичній системі часткового резервування. Автори прямо посилаються на ідеї Генрі Саймонса та Ірвінга Фішера щодо моделі, у межах якої кошти клієнтів повністю забезпечуються ліквідними резервами та не використовуються для традиційного кредитного мультиплікатора. У цьому контексті стейблкоїни розглядаються не лише як фінансова технологічна інновація, а як потенційний елемент трансформації самої архітектури фінансового посередництва.

Документ детально пояснює, чому стейблкоїни стали настільки популярними у глобальній фінансовій системі. Автори зазначають, що вони поєднують одразу кілька важливих характеристик: забезпечують миттєві міжнародні платежі 24/7, дозволяють здійснювати трансграничні перекази поза традиційною банківською інфраструктурою, створюють альтернативний цифровий доларовий інструмент для населення країн із нестабільними валютами та високою інфляцією, а також функціонують як відносно безпечний цифровий актив завдяки резервному забезпеченню високоліквідними державними інструментами США.

[7] https://track.unodc.org/track/uploads/res/track/resourcehub/2026/human_rights_in_asset_recovery_processes_html/StAR_2026_Human_Rights_in_Asset_Recovery_Processes.pdf

Окремо підкреслюється, що на відміну від банківських депозитів, які підлягають кредитному ризику понад межі системи страхування вкладів, стейблкоїни у межах нової регуляторної моделі забезпечуються фактично безризиковими державними активами та високоліквідними резервами, що потенційно знижує ризики масового вилучення коштів із банків та фінансової нестабільності.

Значна частина документа присвячена аналізу того, що саме відбувається з коштами під час конвертації банківського депозиту у стейблкоїни. Автори демонструють, що у більшості випадків гроші фактично не зникають із банківської системи, а лише змінюють форму або переміщуються між різними установами. Якщо емітент стейблкоїнів використовує резерви для придбання казначейських векселів США, продавець цих державних цінних паперів повторно розміщує отримані кошти у банківській системі, унаслідок чого загальний обсяг депозитів фактично суттєво не змінюється. Навіть у випадках, коли резерви утримуються у формі грошових резервів, проблема полягає не у «зникненні» депозитів із фінансової системи, а у зміні їхньої функції: частина коштів перестає брати участь у традиційному механізмі кредитного мультиплікатора. Саме цей механізм автори визначають як «канал вузького банкінгу», оскільки кошти залишаються всередині фінансової системи, однак фактично ізолюються від процесу створення кредитних грошей. Водночас у документі наголошується, що на практиці переважна більшість резервів емітентів стейблкоїнів сьогодні розміщується саме у казначейських векселях США та операціях репо, а не у банківських депозитах, тому реальний вплив на банківське кредитування є значно меншим, ніж це часто стверджується у політичних та регуляторних дискусіях.

Надзвичайно важливим аспектом дослідження є роль монетарної політики Автори наголошують, що вплив стейблкоїнів на банківське кредитування суттєво залежить від того, чи функціонує фінансова система в умовах надлишкової ліквідності, чи в умовах дефіциту резервів. У сучасних умовах банки США володіють значними надлишковими резервами та високоліквідними активами, тому переміщення депозитів між банками не змушує їх різко скорочувати кредитування. Документ прямо зазначає, що масштабні негативні ефекти для банківського кредитування можливі лише за умов дефіциту резервів, коли банки працюють поблизу своїх ліквідних обмежень. Таким чином, проблема кредитного скорочення розглядається не як безпосередній наслідок стейблкоїнів, а як функція ширшої монетарної архітектури та політики центрального банку. Автори фактично стверджують, що навіть значне поширення стейблкоїнів саме по собі не створює системної загрози для кредитування, якщо Федеральна резервна система підтримує достатній рівень ліквідності в системі.

Окремий блок дослідження присвячений аналізу заборони виплати доходу за стейблкоїнами. У документі пояснюється, що GENIUS Act прямо забороняє емітентам стейблкоїнів виплачувати їхнім власникам будь-яку форму процентного доходу або іншої винагороди, однак не забороняє використання афілійованих структур чи сторонніх посередників, які можуть фактично забезпечувати доходність через механізми розподілу доходів. Як приклад наводиться модель співпраці Coinbase та Circle, у межах якої користувачі отримують програму «USDC Rewards», хоча формально сам емітент стейблкоїна не здійснює прямої виплати процентного доходу. Автори зазначають, що окремі варіанти CLARITY Act спрямовані на усунення і цього механізму. Водночас дослідження наголошує, що ключовим питанням є не стільки юридична форма заборони, скільки те, наскільки вона реально здатна впливати на поведінку домогосподарств та структуру розподілу їхніх фінансових активів.

Для оцінки цих ефектів Council of Economic Advisers створює комплексну економічну модель, яка аналізує взаємодію між домогосподарствами, емітентами стейблкоїнів та банківським сектором. Домогосподарства розподіляють свої активи між банківськими депозитами та стейблкоїнами залежно від рівня доходності, ліквідності та нефінансових переваг. Модель також враховує відмінності між невеликими локальними банками та великими банківськими

установами, де великі банки мають жорсткіші вимоги до ліквідності та вищі ефективні резервні нормативи. Значна увага приділяється тому, яка частина резервів стейблкоїнів фактично «випадає» з механізму кредитного мультиплікатора. Автори використовують дані Circle Reserve Report, відповідно до яких лише близько 12% резервів USDC утримуються у формі банківських депозитів, тоді як основна частина інвестується у казначейські векселі США та операції репо. Це стає одним із центральних аргументів документа: більшість резервів стейблкоїнів не блокує кредитування, а продовжує функціонувати всередині фінансової системи через ринок державного боргу США.

Результати моделювання демонструють, що навіть повна заборона доходності за стейблкоїнами має надзвичайно обмежений вплив на кредитування. Базовий сценарій моделі демонструє, що заборона виплати доходу за стейблкоїнами збільшує обсяги кредитування лише приблизно на 2,1 млрд доларів США, що становить близько 0,02% від загального кредитного портфеля банківської системи США. Водночас втрати добробуту для користувачів оцінюються приблизно у 800 млн доларів США щорічно через втрату доступу до конкурентної доходності. Автори також показують, що навіть за використання дуже агресивних та малореалістичних припущень вплив на кредитування залишається відносно помірним. Навіть у випадку, якщо ринок стейблкоїнів зросте до 10% від загального обсягу депозитів, усі резерви будуть ізольовані у грошових рахунках, а Федеральна резервна система відмовиться від режиму надлишкової ліквідності, приріст кредитування оцінюється лише приблизно у 4,4%. Документ наголошує, що для досягнення навіть такого результату необхідне одночасне виконання кількох малоймовірних припущень, які фактично не відповідають сучасній структурі фінансової системи США.

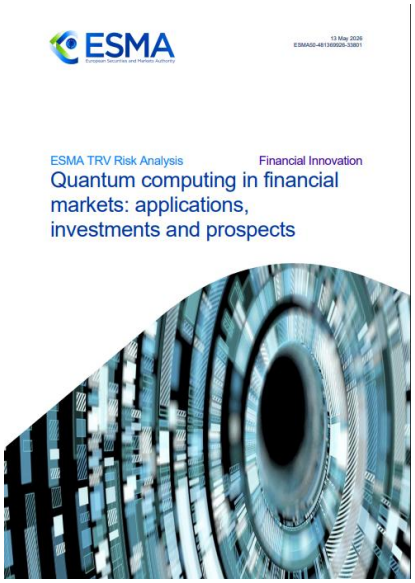
У фінальній частині дослідження автори переходять до ширшого макрофінансового та геополітичного аналізу. Особливий акцент робиться на тому, що стейблкоїни формують новий

Висновки:

- **Документ демонструє, що заборона доходності за стейблкоїнами практично не здатна суттєво підтримати банківське кредитування.** Навіть у базовому сценарії повна заборона виплати доходу збільшує кредитування лише на 2,1 млрд доларів США або 0,02% від загального кредитного портфеля банків США, що свідчить про мінімальний макрофінансовий ефект таких обмежень.
- **Основний фактор впливу стейблкоїнів на кредитування залежить не від самого факту існування цифрових доларових активів, а від структури резервів емітентів та монетарного режиму Федеральної резервної системи.** Якщо резерви переважно розміщуються у казначейських векселях США, а система функціонує в умовах надлишкової ліквідності, стейблкоїни не створюють значного ризику дезінтермедіації для банківської системи.
- **Документ підкреслює стратегічне значення стейблкоїнів для міжнародного попиту на долар США та американські державні облігації.** Обмеження виплати доходу може стримувати глобальне поширення цифрової доларової інфраструктури та потенційно зменшувати зовнішній попит на державний борг США, що має значення для довгострокової фінансової та геополітичної позиції Сполучених Штатів.
- **Автори фактично підтримують підхід, за якого регуляторна політика щодо стейблкоїнів повинна концентруватися не на жорстких заборонах виплати доходу, а на прозорості резервів, ліквідності, управлінні ризиками масового вилучення коштів, пруденційному нагляді та інтеграції стейблкоїнів у загальну фінансову інфраструктуру.** Документ демонструє, що надмірні обмеження можуть створювати більші втрати для користувачів, ніж вигоди для банківського сектору.

глобальний канал попиту на долар США та американські державні облігації. У документі зазначається, що понад 80% операцій зі стейблкоїнами здійснюються за межами США, а емітенти стейблкоїнів уже утримують більше казначейських векселів США, ніж окремі великі держави. Також наводяться дослідження Банку міжнародних розрахунків, які демонструють, що приплив капіталу у стейблкоїни може впливати на дохідність короткострокових державних облігацій США та фактично формувати додатковий міжнародний попит на американський державний борг. Автори припускають, що у перспективі стейблкоїни можуть стати елементом нової глобальної доларової інфраструктури та посилювати міжнародне домінування долара США. У цьому контексті заборона виплати доходу розглядається не лише як питання банківського регулювання, а як фактор, здатний впливати на глобальну конкурентоспроможність американської фінансової системи та міжнародний статус долара США.

Квантові обчислення на фінансових ринках: застосування, інвестиції та перспективи [8]



Європейський орган з цінних паперів та ринків (ESMA) опублікував аналітичний звіт із серії TRV Risk Analysis. Документ є першою системною оцінкою ESMA ризиків і можливостей квантових обчислень для ринків цінних паперів ЄС і містить як кількісні дані щодо інвестиційного ландшафту, так і детальний аналіз потенційних фінансових застосувань технології та її загроз для кібербезпеки. Звіт виходить у момент, коли глобальні квантові інвестиції досягли рекордних рівнів: за оцінками, загальний обсяг інвестицій у квантові технології сягнув близько 33 млрд дол. США у 2025 році, з яких 38% спрямовано на квантові обчислення. Венчурне фінансування квантових стартапів в ЄС у 2025 році стрімко зросло до приблизно 950 млн євро за 25 угодами — у п'ять разів вище середньорічного рівня трьох попередніх років. Саме тоді фінська компанія IQM стала першим квантовим «єдинорогом» Європи (оцінка перевищила 1 млрд дол. США).

Звіт окреслює технологічні основи квантових обчислень, зокрема принципи суперпозиції та заплутаності кубітів, класифікацію апаратних платформ (надпровідні схеми, фотонні системи, нейтральні атоми, іонні пастки) та концепцію «квантового прискорення» — здатності квантових алгоритмів значно ефективніше розв'язувати задачі певних класів порівняно з класичними методами. Ключовим аналітичним висновком щодо поточного стану є те, що ера NISQ (зашумлені квантові пристрої середнього масштабу) характеризується принциповою недостатністю апаратних можливостей для розв'язання реальних фінансових задач промислового масштабу більш ефективно, ніж класичні підходи. Тим не менш, ESMA фіксує активну побудову доказів концепції (proof of concept) у великих банках, керуючих активами та фінтех-стартапах, що свідчить про підготовку галузі до майбутнього технологічного переходу.

У розділі фінансових застосувань ESMA аналізує чотири ключові напрями. По-перше, оптимізація: задачі портфельної оптимізації, мінімізації ризику та хеджування природно виражаються у форматі QUBO (квадратична необмежена бінарна оптимізація), що дозволяє застосовувати квантові алгоритми для одночасного дослідження великої кількості конфігурацій

[8] https://www.esma.europa.eu/sites/default/files/2026-05/ESMA50-481369926-33801_TRV_Risk_Analysis_Quantum_Computing_in_Financial_Markets.pdf

портфеля. До суміжних застосувань належать індексний трекінг з кардинальними обмеженнями, оптимізація розрахунків транзакцій у клірингових установах та ідентифікація арбітражних можливостей. По-друге, стохастичне моделювання: квантовий метод Монте-Карло (QMCI) теоретично забезпечує квадратичне прискорення порівняно з класичним MCI при оцінці деривативів, розрахунку VaR та кредитних метрик, хоча реалізації на NISQ-пристроях поки не подолали суттєві технічні накладні витрати.

По-третє, квантове машинне навчання (QML): алгоритми QML поділяються на методи прискорення класичних ML-технік (що потребують кодування даних у квантові стани) та квантово-нативні підходи, які оперують безпосередньо квантовими даними. Останні розглядаються як більш перспективні для короткострокових застосувань, оскільки не потребують ресурсомісткого кодування. Зокрема, квантово-вдосконалені методи класифікації апробовані для оцінки кредитоспроможності та виявлення шахрайства, демонструючи точність, порівнянну з класичними бенчмарками. По-четверте, квантові блокчейн-технології: алгоритм Гровера може забезпечити квадратичне прискорення для проведення proof-of-work розрахунків у видобутку криптоактивів, тоді як квантова заплутаність потенційно здатна підвищити цілісність і швидкість консенсусних механізмів у розподілених реєстрах. Наразі ці підходи залишаються на ранній експериментальній стадії.

Центральним ризиком, якому ESMA приділяє особливу увагу, є криптографічна загроза. Алгоритм Шора дозволяє факторизувати великі числа експоненціально швидше за будь-який відомий класичний алгоритм, що означає теоретичну можливість злому широко застосовуваних криптографічних схем RSA та ECC. Фінансова система критично залежить від цих схем для захисту комунікацій, цифрових підписів і цілісності транзакцій. Особливо небезпечна стратегія «зберігати зараз, розшифрувати пізніше» (harvest now, decrypt later): вже сьогодні конфіденційні дані можуть збиратися зловмисниками для подальшого розшифрування з появою достатньо потужних квантових

Висновки:

- **Фінансові установи в ЄС повинні вже зараз розпочати інвентаризацію криптографічних залежностей і планування переходу до постквантових алгоритмів:** DORA прямо зобов'язує управляти цим ризиком, дорожня карта ЄК встановлює дедлайни (2026–2030–2035), а атаки типу «зберігати зараз, розшифрувати пізніше» вже сьогодні становлять реальну загрозу для конфіденційних даних.
- **Комплаєнс-підрозділи мають включати квантові ризики до оцінки операційної стійкості:** потенційна ринкова концентрація серед постачальників квантового обладнання є новим джерелом ризику ланцюжка постачань, що підпадає під чинний фреймворк ICT управління ризиками, які походять від третіх сторін.
- **Квантове прискорення у виявленні фінансових злочинів (шахрайство, кредитний скоринг) залишається науковою перспективою, а не найближчою практикою;** проте установи, що вже будують proof-of-concept у QML, матимуть значну конкурентну перевагу при промисловому розгортанні технології, яке ESMA прогнозує поетапно починаючи з портфельної оптимізації та QML-класифікації.
- **Оцінки акцій квантових компаній на публічних ринках відрізняються значною волатильністю і є ненадійним індикатором технологічної зрілості;** фінансові регулятори та інвестори повинні критично оцінювати маркетингові твердження щодо «квантової переваги» з урахуванням принципового розриву між теоретичними прискореннями і реальними можливостями сучасних NISQ-пристроїв.

комп'ютерів. Постквантова криптографія (PQC) — нове покоління алгоритмів, стійких до квантових атак — є відповіддю на цей виклик: у 2024 році NIST (США) опублікував перші стандарти PQC.

У регуляторному контексті ESMA наголошує, що DORA (Регламент ЄС 2022/2554) вже зобов'язує фінансові суб'єкти впроваджувати заходи управління кібербезпековими ризиками, що охоплюють криптографічні вразливості, включно з квантовими загрозами. Дорожня карта Єврокомісії з переходу до PQC передбачає ініціювання планування та пілотних проектів до 2026 року, завершення переходу для сценаріїв підвищеного ризику до 2030 року та для сценаріїв середнього ризику — до 2035 року. Ініціатива Quantum Safe Financial Forum (за участі Europol) розробляє методологію пріоритизації міграції на PQC у фінансовому секторі. Водночас ESMA вказує на ризик ринкової концентрації: квантовий ринок апаратного забезпечення може сформуватися навколо обмеженого кола постачальників (IBM, Microsoft, Amazon), що створюватиме операційні залежності та вразливості ланцюжка постачань для фінансових установ.

ESMA завершує звіт стриманою, але нагальною позицією: хоча повноцінні квантові комп'ютери, здатні атакувати криптографію, найближчим часом не очікуються, тривалість криптографічних міграційних процесів і кількість залучених стейкхолдерів вимагають негайного початку підготовки. Динаміка інвестицій 2025 року — різке зростання оцінок акцій квантових компаній з наступними корекціями і стрибок венчурного фінансування в ЄС — відображає характерний для нових технологій бум-спад цикл, де суттєвий розрив між довгостроковим потенціалом і короткостроковою комерційною придатністю створює умови для ринкової волатильності. ESMA повідомляє, що продовжить моніторинг наслідків квантових технологій для ринків цінних паперів у міру їх розвитку.

Проект настанов Офісу ЄС з AI щодо зобов'язань прозорості за статтею 50 Регламенту (ЄС) 2024/1689 [9]

Офіс Єврокомісії з питань штучного інтелекту (AI Office), що функціонує у складі Генерального директорату з питань мереж зв'язку, контенту і технологій, оприлюднив для публічних консультацій «Проект настанов щодо імплементації зобов'язань прозорості для певних систем AI за статтею 50 Регламенту про ШІ». Відповідно до статті 113 Регламенту (ЄС) 2024/1689, стаття 50 набирає чинності 2 серпня 2026 року — незалежно від дати розміщення конкретної системи AI на ринку чи введення її в експлуатацію. Настанови розроблені на виконання статті 96(1)(d) і мають характер рекомендаційного документа, тоді як остаточне тлумачення Регламенту належить виключно Суду ЄС (CJEU). Документ структурований навколо чотирьох окремих зобов'язань прозорості, розбитих за типами систем AI та відповідальними суб'єктами (провайдери та деплоєри), і супроводжується розгорнутими практичними прикладами та роз'ясненнями меж застосування.Стаття 50(1) поширюється на провайдерів систем AI, призначених для безпосередньої взаємодії з фізичними особами. Чотирьохелементний тест охоплює: систему AI за визначенням Регламенту; намір взаємодіяти; безпосередність такої взаємодії (у режимі реального або майже реального часу); та фізичних осіб як адресатів. Настанови окремо наголошують, що агентні системи AI підпадають під дію цього положення, якщо вони взаємодіють з особами, які їх скеровують, або з іншими фізичними особами під час виконання завдань. У разі неможливості провайдера достовірно визначити, чи агент взаємодіятиме з фізичною особою, агент за замовчуванням повинен розкривати свою

[9] https://ec.europa.eu/newsroom/dae/redirection/document/128275

штучну природу в будь-якій ситуації, де така взаємодія ймовірна. Формат розкриття не регламентується конкретним методом, однак визнаються недостатніми: розкриття виключно у положеннях і умовах; машиночитабельні маркери без відображення користувачеві; неоднозначні сигнали або людиноподібні зображення. Два виключення — очевидна штучна природа взаємодії та авторизація законом для цілей виявлення злочинів — ретельно окреслені, з окремим роз'ясненням, що системи, доступні публіці для повідомлення про злочини, виключенню не підпадають.

Стаття 50(2) встановлює зобов'язання для постачальників систем AI, що генерують або маніпулюють синтетичним аудіо-, відео- або текстовим контентом: такий контент має бути маркований у машиночитабельному форматі і доступний для виявлення. Технічне рішення повинне одночасно відповідати чотирьом вимогам — ефективність, сумісність, надійність та стійкість. Настанови прямо вказують: за сучасним рівнем технологій жодна окрема техніка маркування не відповідає всім чотирьом критеріям одночасно, тому провайдери зобов'язані застосовувати комбінацію технік. До дозволених методів маркування відносяться водяні знаки, метадані, криптографічні методи підтвердження походження, журнали, «відбитки пальців» або їх комбінації. Обов'язком детектування є забезпечення засобів виявлення, доступних особам, що стикаються з контентом. Важливим регуляторним сигналом є положення про те, що незамаркований контент глибоких фейків може кваліфікуватися як «незаконний контент» у розумінні статті 3(h) Акту про цифрові послуги (DSA).

Стаття 50(3) зобов'язує деплоєрів систем розпізнавання емоцій та систем біометричної категоризації інформувати фізичних осіб, що потрапляють у сферу їх дії. Настанови підкреслюють: це положення застосовується незалежно від того, чи здійснюється операція в режимі реального часу, чи ex post; воно поширюється на будь-яких фізичних осіб, включно з дітьми. Оскільки всі системи розпізнавання емоцій класифікуються як системи AI підвищеного ризику (крім заборонених за статтею 5(1)(f)), зобов'язання статті 50(3) застосовуються кумулятивно з вимогами до таких систем. Стаття 50(4), у свою чергу, запроваджує два підзобов'язання для деплоєрів: розкриття глибоких фейків та розкриття AI-генерованого тексту, опублікованого з метою інформування громадськості з питань

Висновки:

- **Терміновий пріоритет для фінансових установ:** до 2 серпня 2026 року провести інвентаризацію всіх AI-систем, що взаємодіють із клієнтами або генерують публічний контент, та відповідно класифікувати їх за статтями 50(1)–(4); відсутність відповідності на дату застосування тягне санкції незалежно від дати розміщення системи на ринку.
- **Механізм «кодексу практики» є оптимальним шляхом демонстрації відповідності:** учасники кодексу мають перевагу у вигляді презумпції відповідності при наглядових перевірках та потенційне пом'якшення санкцій як mitigating factor; установи поза кодексом зіткнуться зі значно більшим обсягом інформаційних запитів від регуляторів.
- **Висновки настанов щодо AI-агентів вимагають від комплаєнс-підрозділів перегляду стандарту human-in-the-loop:** відповідальність за визначення ситуацій, коли агент має розкривати свою природу, не може бути делегована самому агенту — вона залишається за провайдером/деплоєром.
- **Розширення дії статті 50 на відкрите програмне забезпечення (open-source AI) знімає поширену помилкову думку:** відкрита ліцензія не звільняє провайдерів і деплоєрів від зобов'язань прозорості, якщо система підпадає під критерії статті 50 — що є прямим наслідком для регтех-рішень з відкритим кодом, що застосовуються у ПВК/ФТ.

суспільного значення. Регламент встановлює чіткий юридичний тест «глибокого фейку» через чотири елементи: помітна подібність; існуюче (реальне) явище; предмет (особи, об'єкти, місця, події); та хибна видимість автентичності. Виняток для художньо-сатиричних творів є не абсолютним: деплоєри залишаються зобов'язаними здійснювати розкриття, але у формі, що не заважає відображенню чи насолоді від твору.

Виняток для AI-генерованого тексту у статті 50(4) вимагає одночасного виконання двох умов: проходження людського редакційного перегляду або контролю; та наявності відповідальності редактора за публікацію. Настанови суттєво деталізують стандарт: поверхневі перевірки (граматика, форматування), існування редакційної політики без реального змістовного залучення або формальне редакційне затвердження без поглибленого аналізу не відповідають критерію. Ідентичність і контактні дані особи, що несе редакційну відповідальність, мають бути публічно доступними. Така детальна регламентація має прямі наслідки для регульованих фінансових установ: AI-генеровані звіти, прес-релізи або інвесторська документація, опублікована без відповідного редакційного перегляду, підпадатиме під зобов'язання маркування — незалежно від того, що ці матеріали не є журналістикою у традиційному розумінні.

Система примусового виконання побудована навколо агентств ринкового нагляду держав-членів та Офісу ЄС з AI (як регулятора для систем на основі моделей загального призначення). Санкції за порушення зобов'язань статті 50 можуть сягати 15 млн євро або 3% глобального річного обороту (залежно від того, яка сума є більшою), а для інституцій ЄС — 750 тис. євро. Механізм кодексів практики є ключовим інструментом демонстрації відповідності: провайдери та деплоєри, що дотримуються визнаного кодексу, отримують «безпечну гавань», де регулятори зосереджуються виключно на перевірці дотримання кодексу, а не проведенні повноцінних аудитів. Взаємодія з DSA (зобов'язання VLOP/VLOSE щодо ризиків дезінформації), GDPR та законодавством про захист прав споживачів визначена як комплементарна, а не конкурентна.

Звіти окремих інституцій та експертів

Сахельський розлом: анатомія краху нелегальних імперій Малі [10]

Події, що розгорнулися в ранкові години 25 квітня, без перебільшення, стали наймасштабнішим безпековим шоком для Республіки Малі від часів драматичного 2012 року. Координований удар, завданий одночасно сепаратистським Фронтом визволення Азаваду (FLA) та джихадистською коаліцією «Джамаат Нусрат аль-Ісламвальмуслімін» (JNIM), вразив одразу кілька життєво важливих точок по всій країні, створивши ефект доміно, який похитнув самі основи влади військової хунти в Бамако. Сили спрямували як на північні форпости — символічне місто Кідаль і стратегічний центр Гао, так і на центральні регіони,

[10] https://globalinitiative.net/analysis/coordinated-attacks-in-mali-shift-territorial-control-and-realign-illicit-economies/

зокрема Севаре та Мопті, але найбільш шокуючим став синхронний напад на столицю Бамако та прилеглу до неї військову базу Каті, яка традиційно вважалася найзахищенішим центром правлячого режиму.

Хоча атаки безпосередньо в Бамако та Каті були зрештою відбиті завдяки вкрай напруженим діям малійських збройних сил (FAMa) та їхніх російських союзників з «Африканського корпусу», які зуміли втримати ключові об'єкти, включно з міжнародним аеропортом, сам факт такого прориву в глибокий тил засвідчив катастрофічну вразливість режиму, який донедавна хизувався своєю здатністю контролювати безпекову ситуацію.

Втрати держави виявилися надзвичайно болючими та репутаційно нищівними: серед загиблих опинився міністр оборони — це безпрецедентний випадок у новітній історії малійських конфліктів, що завдало прямого удару по легітимності та військовій спроможності хунти Ассімі Гойти. Наступні дні лише погіршили ситуацію: 28 квітня JNIM оголосила про повну блокаду столиці, і відтоді систематично перериває сполучення на всіх вхідних і вихідних маршрутах, що призвело до утворення багатокілометрових заторів із сотень вантажівок, які стоять без руху, а також до стрімкого зростання цін на продукти та паливо в самому Бамако. Це не просто військова операція — це системна спроба задушити центр ухвалення рішень економічно та психологічно, позбавивши його постачання та ізолювавши від решти країни.

У той час як у південній частині країни ситуація була тривожною, але контрольованою, на півночі стався справжній обвал державної присутності, який змінює всю геополітичну карту регіону Сахелю. Результат у Кідалі виявився набагато драматичнішим і швидшим, ніж міг припустити будь-який аналітик ще місяць тому. Об'єднані сили FLA та JNIM взяли під контроль історичну столицю туарезького націоналізму практично без суттєвих боїв — це була не битва, а стрімка окупація вакууму влади. Малійські війська та підрозділи «Африканського корпусу» або укладали угоди про капітуляцію на умовах, що дозволяли їм безперешкодно вийти, або просто залишали міста та ключові військові табори задовго до приходу супротивника, залишаючи по собі гори техніки та амуніції. У наступні дні під контроль перейшли Тессаліт і Тессіт — важливі прикордонні пункти на шляху до Алжиру та Нігеру, а станом на зараз об'єднане угруповання заявляє про встановлення контролю над вісьмома десятьма території всього регіону Кідаль.

Втрата Кідаля — це символічна та стратегічна катастрофа для Бамако, адже саме повернення Кідаля під контроль уряду в 2023 році після десяти років автономії було головним пропагандистським досягненням хунти та її російських союзників, головним доказом того, що їхній жорсткий підхід «спрацьовує». І ось усе це зруйновано за лічені години.

Глибинний зміст цих атак полягає не в захопленні територій як таких, а в сигналі, який вони посилають: JNIM дедалі впевненіше позиціонує себе не просто як чергове повстанське чи терористичне угруповання, а як повноцінний політичний суб’єкт, що претендує на формування нового державного устрою в Малі. У своїх комюніке вони прямо закликають політичні партії, релігійних лідерів, традиційних вождів та навіть частину збройних сил об'єднатися для повалення «терористичної хунти» та створення механізмів мирного переходу.

У цьому стрімко змінюваному ландшафті перед дослідниками та політиками постають два взаємопов'язані, але концептуально різні питання, відповіді на які визначатимуть майбутнє не лише Малі, а й усього поясу Сахелю. Перше — як повернення до влади старих мереж на півночі вплине на високоприбуткову нелегальну економіку, яка десятиліттями була головним джерелом фінансування, легітимності та політичної ваги для всіх збройних сил регіону, включаючи контрабанду палива, наркотиків, мігрантів та, найголовніше, кустарний видобуток золота. Друге — якою буде майбутня роль російського «Африканського корпусу» (колишнього ПВК «Вагнер») у цій новій конфігурації, адже саме москва стала головним військовим, політичним та іміджевим спонсором хунти після розриву з Францією та поступового виходу місії ООН, і будь-який зсув у цьому балансі може призвести до колапсу всього режиму.

Розглядаючи перспективи півночі, варто зазирнути в недавнє минуле. До серпня 2023 року, до масованого наступу, проведеного FAM та «Вагнером», регіон Кідаль був зоною напрочуд обмеженого насильства — не тому, що там панувала центральна влада, а тому, що там склалася складна, але ефективна система негласних угод між основними збройними гравцями.

Саме цей період — період відносної стабільності під контролем сепаратистських та джихадистських угруповань — створив ідеальне середовище для розквіту тіньової економіки. JNIM та попередники нинішнього FLA, зокрема Постійна стратегічна рамкова структура (CSP), яка об'єднувала як повстанські, так і колишні провладні сили, підтримували розгалужену систему оподаткування на основних маршрутах контрабанди. Ці маршрути використовувалися для перевезення всього: від мігрантів, які намагалися дістатися Середземномор'я, до продуктів харчування, смоли канабісу з Марокко та, що найважливіше, кокаїну з Латинської Америки, який прямував до Європи транзитом через Західну Африку.

Але справжнім золотим джерелом, буквально і фігурально, були кустарні золоті копальні. Регіон Кідаль, особливо величезне родовище Н'Тахака та сотні дрібніших копалень, являв собою не просто джерело мінералів, а цілу екосистему. Кожна шахта була місцем, де видобувачі, торговці, перевізники зброї та фінансисти з усієї Західної Африки сходилися разом. Контроль над ними забезпечував потрійний прибуток: прямий податок з кожної копальні, податок з кожного грама золота, що вивозився, та, найтонший механізм, побудова легітимності через надання «безпеки» та регулювання доступу. JNIM та CSP до 2023 року досягли блискучого балансу, представляючи свою владу над копальнями як захист від грабіжництва та свавілля, заручаючись підтримкою місцевих громад, для яких видобуток золота був єдиним рятівним колом виживання. Ключові дороги та економічні хаби — як-от сам Кідаль, Тімбукту та Гао — були поділені між групами в такий спосіб, що слугувало економічним інтересам усіх, створюючи той парадоксальний «мир контрабанди», який утримував насильство на відносно низькому рівні.

Наступ 2023 року зруйнував цю крихку рівновагу. Високий рівень бойових дій, авіаудари та мінні поля вздовж ключових коридорів призвели до колапсу бізнесу: такі легендарні центри незаконної торгівлі, як Табанкор і Бер, що спеціалізувалися на зброї та наркотиках, перетворилися на міста-привиди. Однак тепер, коли FLA повертається до Кідаля як господар, а JNIM виступає його головним союзником, існує дуже висока ймовірність не просто відновлення, але й потужного посилення старих маршрутів.

По-перше, туарезькі мережі, які мають історичні зв'язки, родинні клани та логістичні ланцюги через кордони з північним Нігером та, особливо, з Лівією (де хаос триває вже більше десятиліття), знову активізуються. Це дасть півночі Малі безпрецедентний доступ до потоків зброї з Судану, де громадянська війна між регулярною армією та Силами швидкого реагування наводнила регіон найсучаснішою зброєю — від стрілецької до систем ППО.

По-друге, золоті копальні стануть пріоритетом номер один. Контроль над Н'Тахакою та навколишніми розробками буде не просто економічною діяльністю, а фундаментальною умовою виживання будь-якого угруповання, що претендує на довготривалу кампанію. Використовуючи зростання світових цін на золото (яке традиційно зростає в періоди глобальної нестабільності), FLA та JNIM зможуть отримувати доходи, що в рази перевищують їхні попередні надходження. Більше того, вони мають унікальну можливість переграти свої колишні угоди. Раніше JNIM отримував лише частину доходів, оскільки CSP мала сильнішу позицію. Тепер, виступаючи в тісному альянсі з FLA (який фактично успадкував структури CSP), вони зможуть диктувати набагато жорсткіші умови, максимізуючи свою частку.

Управління шахтами через доступ, ліцензування та захист створює також потужний важіль впливу на цивільне населення, яке втомилося від хаосу та бідності — якщо JNIM зможе гарантувати безпеку старателям і регулярну виплату за золото, він отримає легітимність, якої не

може запропонувати жоден уряд у Бамако. Таким чином, північ рухається до повернення того гібридного порядку, де держава відсутня, але існує стабільна система оподаткування нелегального видобутку та торгівлі, яка живить війну проти центру.

Однак перейдемо до другого, набагато більш витонченого та потенційно вирішального питання — майбутнього кокаїнової торгівлі та ролі Бамако як головного вузла цього бізнесу. На перший погляд, видається логічним, що відновлення впливу FLA та JNIM над Кідалем має призвести до збільшення обсягів транзиту колумбійського кокаїну через північ Малі, скасовуючи тенденцію до дрібних, роздрібних перевезень, яка спостерігалася з 2023 року через тотальну недовіру та хаос між угрупованнями. Але аналіз показує, що цей висновок був би глибоко помилковим, оскільки глобальний наркотрафік, зокрема кокаїновий, функціонує за зовсім іншими законами, ніж регіональна контрабанда палива чи золота.

Надзвичайна прибутковість (вартість одного кілограма кокаїну в Європі може досягати десятків тисяч євро) робить цей ринок набагато більш залежним від наявності високорівневого політичного захисту, ніж від просторового контролю над територією. Історично склалося так, що саме Бамако, а не Кідаль, було головним вузлом прийняття рішень для кокаїнових мереж Західної Африки. Упродовж 2000-х і 2010-х років Малі стала ключовим транзитним пунктом завдяки своїй відносній стабільності, слабкому контролю за кордонами та, що найважливіше, корумпованості вищих ешелонів влади, включно з розвідувальними службами, армією та навіть президентською адміністрацією. Наркобарони, які діють із 2000-х років, вибудували цілу інфраструктуру захисту, яка пережила перевороти 2012, 2020 та 2021 років.

Зараз, у світлі квітневих атак, ситуація в Бамако стає ключовою змінною. Кілька найважливіших вузлів системи захисту всередині малійської держави були серйозно пошкоджені. Смерть міністра оборони — це не просто втрата людини, це втрата ключового координатора, який, за численними даними, мав прямі або опосередковані зв'язки з логістикою наркопотоків. Ще важливішими є втрати в національній розвідувальній службі — інституції, яка десятиліттями була головним архітектором і гарантом безпеки для наркотрафіку, отримуючи за це гігантські відкати. Поранення або загибель кількох високопосадовців розвідки в ході квітневих подій залишило величезний вакуум влади в самій системі захисту. Більше того, поточна волатильність, хаос і постійна загроза нових атак роблять будь-які спроби укласти довгострокові «угоди про захист» надзвичайно ризикованими.

У нестабільному середовищі, де сьогоднішній покровитель може завтра загинути або втекти, переміщення великих партій кокаїну є надто небезпечним. Тому в найближчі місяці ми можемо спостерігати не зростання, а скоріше стагнацію чи навіть тимчасове скорочення транзиту через Малі. Однак це тимчасове явище. Головні архітектори малійського кокаїнового ринку — тіньові фігури, про яких ходять легенди. Вони не керуються ідеологією, не мають постійної лояльності ні до якого угруповання чи клану, вони просто шукають стабільність та передбачуваність. Як тільки ситуація в Бамако стабілізується, ці фігури запропонують гроші новим володарям, і потоки відновляться. Таким чином, парадоксальним чином, саме падіння Кідаля, яке виглядає великою перемогою джихадистів та сепаратистів, може на коротку перспективу не дати їм очікуваних надходжень від кокаїну, оскільки ланцюг прийняття рішень зруйновано.

Нарешті, кульмінацією всього аналізу є питання про майбутнє самого військового режиму. JNIM відверто переслідує мету його повалення, і це не просто риторика — це системна стратегія, що включає військовий тиск, економічну блокаду та політичну інфільтрацію. Особливо цікавим є намагання JNIM та FLA вбити клин між Бамако та москвою. Прямі звернення до росії, заклики не втручатися у «внутрішній малійський конфлікт» — це свідомий крок, розрахований на те, що кремль може переглянути витрати на підтримку непопулярного та слабкого режиму. Однак поки що москва демонструє зворотне.

Для кремля Малі — це флагманський проєкт в Африці, символ того, що росія може замінити Францію та ООН, тому відступ у Бамако дорівнював би геополітичній поразці в усьому регіоні. «Африканський корпус» заявляє, що воює пліч-о-пліч з FAM, і їхні зобов'язання залишаються незмінними. Однак сила цього альянсу буде перевірена найближчими місяцями.

Але вже зараз очевидно: нелегальна економіка на півночі — золото, контрабанда й кокаїн — повертаються до своїх історичних патернів, до того гібридного порядку, де збройні угруповання виступають гарантами торгівлі, стабільності та оподаткування, а держава відсутня.

Однак справжня битва за майбутнє Малі точиться не стільки в пісках Сахари, скільки в закритих кімнатах влади в Бамако, де вирішується доля кокаїнових маршрутів, контроль над розвідкою та, зрештою, питання про те, чи збережеться нинішня хунта, чи поступиться місцем новому, непередбачуваному гібридному режиму, можливо, під спільним контролем JNIM та залишків світської опозиції. Малі вступила в смугу найглибшої турбулентності з часів початку війни, і наслідки цієї турбулентності — політичні, економічні та гуманітарні — відчуватиме весь регіон Сахелю протягом наступних років.

Висновки:

- **Координація між сепаратистами (FLA) та джихадистами (JNIM) досягла безпрецедентного рівня**, що дозволило їм захопити 80% регіону Кідаль майже без бою, завдавши нищівного удару по легітимності військової хунти Бамако та її російських союзників.
- **Падіння півночі Малі веде до відновлення «гібридного порядку»**, де контроль над кустарними золотими копальнями та контрабандними маршрутами стане головним джерелом фінансування, легітимності та логістики для збройних угруповань.
- **Кокаїновий трафік через Малі залежить не від контролю над північними територіями, а від стабільності та корупційних мереж** у самому Бамако; поточний хаос і втрати серед вищого військового та розвідувального керівництва тимчасово паралізують великі оптові перевезення.
- **Незважаючи на спроби JNIM посіяти розбрат між хунтою та москвою**, росія (через «Африканський корпус») подвоює військову присутність, оскільки втрата Малі стала б геополітичною катастрофою для кремля в регіоні Сахелю.

Контрафактне сільське господарство: тиха ерозія продовольчої безпеки та економічної стійкості [11]

У глибині аграрної економіки Уганди, яка забезпечує засобами для існування майже 70 відсотків населення, повільно, але невпинно розгортається криза, яку досі відмовляються помічати на найвищому рівні.

Це криза контрафактних сільськогосподарських товарів – від фальшивого насіння та фальсифікованих добрив до незареєстрованих хімікатів і підроблених вакцин для тварин. Її руйнівний вплив давно перетнув межу окремого фермерського двору, перетворившись на системну загрозу національній продовольчій безпеці, загальній продуктивності аграрного сектору та, зрештою, стійкості всієї економіки до зовнішніх і внутрішніх шоків.

[11] https://globalinitiative.net/analysis/how-counterfeit-agricultural-products-are-harming-ugandas-economy/

Особливо високоризиковим сегментом цього тіньового ринку є добрива, і на те є три ключові причини. По-перше, цей сектор надзвичайно чутливий до цінових коливань, що робить його ідеальним полем для маніпуляцій кримінальних посередників. По-друге, Уганда майже повністю залежить від імпортних добрив, що створює довгі, складні та важко контрольовані ланцюги постачання. По-третє, рядовий фермер не має жодних можливостей перевірити якість продукту – він бачить лише бренд.

Ці структурні вразливості накладаються на катастрофічний стан ґрунтів. Багаторічне інтенсивне землеробство без належного відновлення поживних речовин призвело до того, що величезні території буквально втратили свій природний родючий потенціал. Сьогодні мільйони дрібних фермерів не мають вибору: використання добрив та агрохімікатів є для них не розкішшю і не способом підвищити врожайність, а жорсткою необхідністю, єдиною умовою виживання їхніх господарств. І саме зростання цього відчайдушного попиту на доступні засоби підживлення створює ідеальний ґрунт для безпрецедентної кримінальної експлуатації.

Якщо подивитися на проблему ширше, то торгівля контрафактними товарами у світі довгий час сприймалася як щось периферійне, другорядне – те, на що політики, правоохоронці та дослідники могли заплющувати очі. Однак масштаби ринку контрафакту за останні роки зросли з драматичною швидкістю, і це особливо тривожно там, де підробки загрожують здоров'ю людей та безпеці цілих галузей. У 2025 році індекс глобальної злочинності в категорії "торгівля контрафактом" досяг позначки 5,09, порівняно з 4,98 у 2023 році. Східна Африка займає одне з перших п'яти місць серед найбільш уражених регіонів із показником 6,22. Але Уганда демонструє шокуючий результат – 7,50 балів. Це не просто вище за середньосвітовий рівень; це значно вище навіть за регіональний середній показник.

Офіційні національні дослідження, які все ж таки вдалося провести, дають приголомшливі цифри: понад половина всіх товарів на угандійському ринку є підробкою, причому 90 відсотків з цих підробок не відповідають жодним стандартам якості – це навіть не погані копії, а відверто небезпечний сурогат. Економічні наслідки цього явища вимірюються колосальними сумами: щорічні втрати бюджету від несплачених податків сягають 6 трильйонів угандійських шилінгів (понад 1,6 мільярда доларів за поточним курсом, що є колосальною сумою для бюджету країни, що розвивається). Додатково місцева промисловість втрачає до 4 мільярдів шилінгів через недобросовісну конкуренцію та підрив довіри до легальних брендів.

Найбільше страждають критичні для життя галузі: ліки, харчові продукти та напої, підроблена косметика, електроніка та, що особливо небезпечно, будівельні матеріали. Але аграрний сектор, за всіма показниками, є рекордсменом за масштабами фальсифікації. Дані свідчать, що від 30 до 50 відсотків насіння, яке продається в країні, є фальшивим – це означає, що фермер може місяцями обробляти поле, поливати його, прополювати, а в кінці сезону отримати скупі та хворі сходи або взагалі нічого. Ще жахливіша ситуація з пестицидами: понад 60 відсотків з них – підробка. Фермер, обприскуючи поле хімікатами від шкідників, насправді може розпилювати суміш крейди, води та барвника, що не тільки не знищує комах, але й створює ілюзію захисту, дозволяючи шкідникам безперешкодно розмножуватися.

Так само небезпечною є ситуація у тваринництві: задокументовано випадки, коли підроблені вакцини та ветеринарні препарати призводили до масової загибелі худоби або до різкого зростання сприйнятливості тварин до хвороб. У 2021 році Парламентський комітет Уганди з питань сільського господарства, тваринництва та рибальства офіційно підняв тривогу, заявивши, що національний ринок "затоплений контрафактними агрохімікатами". У звіті комітету особливо наголошувалося на катастрофічній нестачі інспекційних та правоохоронних спроможностей для регулювання обігу хімікатів. Ситуація ускладнена тим, що майже 46 відсотків агропідприємств працюють без будь-якої національної реєстрації – вони перебувають повністю в тіні, без можливості їх ідентифікувати, перевірити чи притягнути до відповідальності.

І всі наявні дані – від медіа-розслідувань, оперативних зведень поліції та прямих свідчень фермерських кооперативів – вказують на те, що негативна тенденція не просто зберігається, а й стрімко прискорюється.

Щоб зрозуміти, чому ця система відтворює себе, необхідно проаналізувати структурні вразливості ринку добрив. Останніми роками уряд Уганди розпочав амбітну програму з будівництва власних заводів з переробки добрив, намагаючись зменшити зовнішню залежність. Однак цей процес перебуває на початковій стадії, і країна досі критично залежить від імпорту. Два основних типи неорганічних добрив – сечовина (карбамід) та NPK (комплексне добриво, що містить азот, фосфор і калій) – надходять з росії, Саудівської Аравії, Катару, Єгипту, Малайзії, а також із сусідніх країн, таких як Кенія та Танзанія. У 2024 році загальний обсяг імпорту добрив оцінювався приблизно у 54,75 мільйона доларів США, що є значною сумою, але водночас мізерною порівняно з потребами країни.

Протягом останнього десятиліття обсяги імпорту зазнавали серйозних коливань: у 2018 році було завезено понад 100 тисяч тонн, але потім обсяги скоротилися до приблизно 67 тисяч тонн у 2022 році – останньому році, за який наявні повні дані. Головною причиною цих коливань є нестабільність попиту, а головною причиною низького попиту – висока вартість. Рівень використання добрив в Уганді залишається одним із найнижчих у світі: середній фермер вносить у десятки разів менше поживних речовин на гектар, ніж його колега в Європі чи Південно-Східній Азії. Вартість 50-кілограмового мішка фосфорного добрива зросла з 93 тисяч угандійських шилінгів (близько 25 доларів США) у 2019 році до 200 тисяч шилінгів (приблизно 53 долари) сьогодні. Це зростання більш ніж удвічі за п'ять років є руйнівним для економіки дрібних господарств. І навіть ці ціни, за прогнозами, не є межею: через блокаду судноплавства в Перській затоці, яка впливає на логістику поставок з ключових регіонів, вартість добрив у найближчі місяці зросте ще на 15-20 відсотків. У цьому контексті пропозиція контрафактної продукції стає для багатьох фермерів не просто спокусою, а єдиною доступною альтернативою.

Хоча верифікованих цін на підроблені добрива отримати вкрай важко через тіньовий характер ринку, дослідження GI-TOC демонструють показову арифметику: контрафактні добрива зазвичай на 10-20 відсотків дешевші за оригінальні. Але ключ тут не в цьому. Справжнє диво кримінальної економіки полягає в собівартості: виробництво одного підробленого мішка може коштувати лише 15 тисяч шилінгів (4 долари), тоді як продається він за ціною понад 120 тисяч шилінгів (32 долари). Тобто норма прибутку може сягати 700-800 відсотків. При такій маржинальності контрафакт стає не просто дрібним шахрайством, а одним із найприбутковіших видів нелегального бізнесу. При цьому якість такого продукту, звісно, не витримує жодної критики – замість поживних речовин фермер отримує пісок, золу, крейду чи інші інертні наповнювачі. Але для більшості дрібних господарств у бідній економіці Уганди навіть оригінальні добрива залишаються недосяжною розкішшю. Уряд у минулому впроваджував програми субсидування, намагаючись зробити добрива доступними, але сьогодні пряма державна підтримка майже відсутня. Це означає, що мільйони фермерів витісняються на тіньовий ринок, де вони стають легкою здобиччю для злочинних мереж.

Важливо зрозуміти одну фундаментальну річ: ринок контрафакту – це не хаотичне скупчення дрібних шахраїв, які діють поодинці. Це високоорганізована, добре структурована і жорстко скоординована кримінальна індустрія, яка функціонує за законами великого бізнесу.

Ключові суб’єкти включають кілька рівнів. На вершині – легально зареєстровані компанії-дистриб'ютори, які паралельно ведуть "чорну бухгалтерію" і розповсюджують як справжню, так і підроблену продукцію через різні канали. Далі йдуть великі оптовики, спеціалізовані на впровадженні контрафакту в легальні ланцюги постачання – вони підкуповують логістів, підробляють сертифікати, створюють фальшиві склади тимчасового зберігання. Ще нижче – роздрібні торговці в селах і містечках, які часто навіть не усвідомлюють повною мірою, що

продають небезпечний сурогат, або свідомо йдуть на злочин через тиск з боку постачальників. І нарешті, найнебезпечніша ланка – корумповані працівники контролюючих органів: співробітники митниці, санітарної інспекції, ветеринарного контролю. Саме вони за хабарі забезпечують безперешкодний перетин кордону, фіктивне митне оформлення та потрапляння контрафакту на внутрішній ринок без будь-якої перевірки.

Схеми фальсифікації є досить винахідливими. Власне контрафактні добрива – це пряма імітація оригінальних продуктів: злочинці або виготовляють фальшиві мішки з логотипами відомих брендів, або використовують оригінальну тару, яку викуповують у нечистих на руку працівників складів. Дещо складнішою є схема з субстандартними (розбавленими) добривами. Вона полягає в тому, що береться невелика кількість справжнього продукту, який потім змішується з величезною масою дешевих наповнювачів. Сечовину, наприклад, часто змішують із звичайним піском, який не має жодних агрономічних властивостей, але збільшує вагу. NPK розбавляють такими наповнювачами, як деревна зола, крейда або навіть суха глина. В результаті фермер отримує добриво, яке формально має правильний колір і фактуру, але містить у десятки разів менше активних поживних речовин, ніж заявлено.

Злочинні мережі діють не навмання, а на основі чіткого аналізу ризиків. Вони цілеспрямовано вибирають віддалені сільські райони – там, де попит на товар найвищий, де присутність контролюючих органів є близькою до нуля, а рівень обізнаності населення про способи перевірки якості вкрай низький. Фермери, які купують фальсифікат, поділяються на дві приблизно рівні категорії. Перша – ті, хто стає жертвою обману несвідомо: вони бачать знайомий бренд, прийнятну ціну, довіряють продавцю і купують підробку, думаючи, що отримують оригінал. Друга, ще більш тривожна категорія – це фермери, які свідомо обирають дешевший підробний варіант. Вони чудово розуміють, що якість може бути гіршою, але через фінансові труднощі або відсутність доступу до перевірених постачальників у радіусі десятків кілометрів, вони просто не мають іншого виходу. Це вимушений вибір між поганим і дуже поганим, і злочинці цим цинічно користуються.

У відповідь на кризу, що наростає, уряд зробив низку кроків, які, однак, поки що виглядають не дуже переконливо. Технічно було розроблено систему електронного відстеження хімікатів уздовж усього ланцюга постачання, яка мала б дозволити моніторити кожну партію добрив або пестицидів від моменту перетину кордону до продажу кінцевому споживачеві. Але ця система досі не запрацювала на практиці: відсутні необхідні сервери, програмне забезпечення, навчений персонал та, що найголовніше, політична воля для її впровадження. Тривають законодавчі реформи, зокрема розпочато перегляд Закону про контроль за агрохімікатами (Agricultural Chemicals Control Act). У новій редакції пропонується запровадити набагато жорсткіші покарання – значні штрафи та тривалі терміни тюремного ув'язнення для виробників і розповсюджувачів контрафакту.

Також у 2021 році уряд запустив спільні оперативні заходи за участю поліції, Антикорупційного підрозділу при адміністрації президента та Міністерства сільського господарства, тваринництва та рибальства. Проведено низку рейдів на оптових ринках і складах, вилучено партії підробленої продукції.

Однак системна ефективність цих заходів залишається вкрай низькою з кількох причин. По-перше, слабкий ринковий нагляд: контролюючі органи просто фізично не в змозі охопити всіх учасників ринку, особливо у віддалених районах. По-друге, катастрофічна нестача лабораторій та сучасного обладнання для обов'язкового тестування та сертифікації імпорту. Більшість партій хімікатів в'їжджають у країну без жодного хімічного аналізу – документи перевіряються лише формально. Навіть якщо з'являється підозра, що партія контрафактна, її часто неможливо дослідити через відсутність реактивів або кваліфікованих лаборантів. По-третє, корупція залишається нездоланною перешкодою. Надто багато зацікавлених сторін отримують

надприбутки від контрафакту, а заробітні плати пересічних інспекторів і митників є мізерними, що робить хабарі основним джерелом доходу. Нарешті, базова діагностика проблеми залишається неповною: без реального, глибокого, аграрного перепису та системи постійного моніторингу ринку неможливо навіть точно оцінити масштаби лиха.

Постійне існування та процвітання ринку контрафакту в Уганді відображає глибокі структурні вади, які дозволяють злочинцям безперешкодно проникати в легальні ланцюги постачання і витісняти з них доброчесних виробників. Вирішення цієї проблеми потребує не разових рейдів чи показових арештів, а системної трансформації підходів до регулювання імпорту, сертифікації продукції та підтримки дрібних аграріїв. Необхідна координація між міністерством сільського господарства, Угандійським бюро стандартів (UNBS), поліцією та податковою службою (Uganda Revenue Authority) на рівні, якого ніколи раніше не досягалося. Потрібне невідкладне фінансування та оснащення державних лабораторій, навчання інспекторів, створення реально діючої системи електронного моніторингу.

Висновки:

- **Масштаби контрафакту:** Понад половина товарів на ринку Уганди є підробленими, а в аграрному секторі фальсифіковано від 30-50% насіння до понад 60% пестицидів, що безпосередньо загрожує продовольчій безпеці країни.
- **Висока організованість злочинної системи:** Ринок контрафакту контролюється не поодинокими шахраями, а скоординованими мережами, що включають легальних дистриб'юторів, корумпованих чиновників і оптовиків, які забезпечують проникнення підробок у легальні ланцюги постачання.
- **Економічний тиск як каталізатор:** Через стрімке зростання цін на оригінальні добрива (вдвічі за 5 років) та відсутність державних субсидій мільйони фермерів змушені свідомо купувати дешевший контрафакт, що робить їх співучасниками власного зубожіння.
- **Провал регуляторної системи:** Незважаючи на розроблені закони та електронну систему відстеження, їх імплементація провалюється через брак лабораторій, корупцію та відсутність координації між відомствами, що дозволяє кримінальному ринку процвітати.

Але, мабуть, найважливіше – це відновлення програм субсидування добрив. Поки оригінальна продукція залишатиметься недосяжною для бідного фермера, попит на контрафакт нікуди не зникне. Питання вже давно не в тому, чи проблема є. Вона є, вона колосальна і вона з кожним роком поглиблюється. Питання в тому, чи знайде в собі держава, суспільство та міжнародні партнери достатньо волі, ресурсів та рішучості, щоб розірвати це кримінальне коло.

Соціальні мережі: як блогери відмивають гроші для злочинних угруповань [12]

Соціальні мережі, які ще зовсім недавно сприймалися як переважно розважальний простір для комунікації, творчості та маркетингу, сьогодні перетворилися на складний, багатошаровий феномен, що пронизує всі сфери суспільного життя, включно з економікою та злочинністю.

Сучасна аналітика беззаперечно свідчить: блогери-інфлюенсери, тобто публічні особи, які здобули вплив завдяки аудиторії в інтернеті, стали не просто учасниками рекламного ринку, а повноправними агентами у складних схемах легалізації (відмивання) доходів, отриманих злочинним шляхом.

[12] https://insightcrime.org/news/how-influencers-launder-money-for-criminal-groups/

Історія, що починається з арешту в Бразилії, розгортається в панорамну картину, яка охоплює кілька країн Латинської Америки та демонструє, як наркокартелі й найбільші злочинні синдикати адаптуються до цифрової доби. Арест бразильського блогера Кріса Діаса, здійснений 15 квітня 2026 року в межах операції «Нарко Флюксо», є лише верхівкою айсберга. Діаса звинувачують у тому, що він був ланкою в мережі з відмивання грошей, яка обслуговує Перше столичне командування (PCC) — найпотужнішу кримінальну організацію Бразилії, яка контролює чи не найбільші потоки наркотиків у Латинській Америці. Його дружина, також відома інфлюенсерка Дебора Пайксао, через кілька днів опинилася під домашнім арештом, а загалом у межах тієї самої операції було заарештовано 37 людей у дев'яти бразильських штатах, зокрема в мегаполісах Сан-Паулу та Ріо-де-Жанейро. Цифри вражають: за даними бразильської влади, відмита сума сягнула приблизно 1,6 мільярда реалів, що еквівалентно понад 320 мільйонам доларів США, і це лише за період з 2023 року.

Для того щоб зрозуміти механізм, який дозволяє перетворювати брудні наркогроші на розкішні автомобілі та елітну нерухомість, слід детально розглянути інструменти, які використовували Діас та інші подібні фігури. Основним і найпрозорішим, на перший погляд, методом стали лотереї та розіграші в соціальних мережах. Діас публічно анонсував розіграші квартир, грошових призів, мотоциклів та автомобілів класу люкс. Лише за кілька годин до свого арешту він рекламував квартиру вартістю 200 тисяч реалів (близько 40 тисяч доларів).

Проте за зовнішньою невинністю таких заходів ховається геніальна в своїй простоті схема відмивання: інфлюенсер публічно оголошує, що продав, скажімо, 1000 квитків на розіграш, тоді як реально продано лише 100. Решту 900 квитків оплачуються не реальними учасниками, а коштами, що надійшли від злочинних угруповань. Таким чином, гроші, отримані від продажу наркотиків чи іншої незаконної діяльності, надходять на рахунки інфлюенсера під виглядом цілком легітимних платежів за участь у лотереї. Оскільки жодної зовнішньої прозорості немає — ні реальна кількість проданих квитків, ні їхня ціна, ні особи покупців не підлягають обов'язковому контролю, — цей канал стає майже ідеальним для легалізації.

Існує й інший варіант тієї самої схеми, який описує бразильський юрист Жоао Пауло Мартінеллі, фахівець з протидії відмиванню коштів та фінансуванню тероризму: особа або структура, причетна до злочинної діяльності, передає інфлюенсеру гроші під виглядом так званого донату чи спонсорської допомоги, а він повертає ці кошти через призові виплати переможцям розіграшу. Це створює замкнений цикл, у якому брудний капітал набуває форми «виграшу», що формально є законним доходом.

Важливо наголосити, що справа Кріса Діаса не є унікальною або локальною. Проблема має чітко виражений транскордонний характер. У Колумбії інфлюенсер Хав'єр Аріас Кастанеда, відомий своїй аудиторії як Хав'єр Аріас Стант, був офіційно звинувачений генеральною прокуратурою країни в тому, що він відмивав гроші, отримані від наркоторгівлі, за допомогою ідентичних розіграшів нерухомості, мотоциклів та автомобілів через власні онлайн-канали. Ще більш показовою є ситуація в Мексиці, де Підрозділ фінансової розвідки (UIF) розслідує діяльність одразу 64 блогерів, яких підозрюють у співпраці з такими могутніми злочинними синдикатами, як картель Сіналоа. У цих випадках блогери використовують не тільки лотереї, а й рекламні контракти в соціальних мережах, отримуючи платежі від підставних компаній, пов'язаних із картелями. Усі три найбільші країни регіону — Бразилія, Колумбія та Мексика — зіткнулися з

однотипними зловживаннями, що свідчить не просто про окремі злочинні епізоди, а про формування сталої злочинної практики на рівні континенту.

Розширюючи аналіз, варто звернути увагу на те, що арсенал методів, які використовують інфлюенсери для відмивання коштів, є значно багатшим, ніж самі лише лотереї. Одним із ключових сигналів небезпеки для фінансових моніторингових систем є так звані фрагментовані транзакції. Механізм тут виглядає так: інфлюенсер отримує на свої рахунки величезну кількість дрібних платежів, кожен з яких нібито є донатом від прихильників або оплатою за дрібну рекламну послугу. Проте фінансові установи в більшості країн зобов'язані повідомляти про підозрілі операції лише тоді, коли сума перевищує певний законодавчо встановлений поріг (наприклад, 10 тисяч доларів). Дрібні ж суми, особливо якщо вони надходять регулярно й імітують природну активність фан-бази, автоматично не перевіряються. Це дозволяє розбити велику суму брудних грошей на тисячі непомітних мікроплатежів.

Крім того, сучасні технології надають злочинцям та їхнім посередникам-блогерам ще один потужний інструмент — криптовалюти та віртуальні гаманці. Коли транзакції проводяться через Bitcoin, Monero або інші анонімні криптовалюти, а також через електронні гаманці, зареєстровані на підставних осіб або в юрисдикціях зі слабким контролем, то здатність правоохоронних органів відстежити рух коштів знижується майже до нуля. Таким чином, соціальні мережі стають не лише майданчиком для комунікації, а й своєрідною «чорною дірою» для фінансових потоків.

Не менш важливим є той факт, що інфлюенсери майже ніколи не діють як одинаки. За кожним гучним випадком стоїть ціла екосистема професійних посередників. Адвокати, бухгалтери, аудитори, нотаріуси, менеджери з фінансів — ці люди, часто з бездоганною діловою репутацією, створюють юридичну конструкцію, яка надає операціям через соціальні мережі видимість абсолютної законності. Вони допомагають укладати фіктивні контракти з рекламодавцями, готують підроблену звітність про проведені лотереї, реєструють компанії-прокладки в офшорних зонах та консультують своїх клієнтів-блогерів щодо того, як уникнути запитань з боку фінансового моніторингу. Ця професійна підтримка є критично важливою, адже без неї інфлюенсер ризикував би привернути надто багато уваги до своїх фінансових операцій.

Злочинний ланцюжок «наркокартель — посередник — бухгалтер — блогер — розіграш» стає майже невидимим для традиційних контролюючих органів, які звикли шукати сліди відмивання грошей у банківських переказах, купівлі нерухомості або продажу автомобілів, а не в стрічках соціальних мереж.

Тепер варто поставити ключове питання: чому саме блогери стали настільки привабливою ціллю для злочинних угруповань, які шукають канали для відмивання грошей? Аналітики дають дві взаємопов'язані відповіді. Перша — це феномен демонстративного споживання, який став соціальною нормою. Блогери заробляють (або принаймні демонструють, що заробляють) величезні статки на рекламі, донатах, партнерствах і власних брендах. Вони регулярно показують своїм мільйонам підписників розкішні автомобілі, приватні літаки, розкішні будинки, ексклюзивні коштовності, купюри, екзотичних тварин і навіть злитки золота. У суспільній свідомості цей образ успішного життя вже ні в кого не викликає подиву. Для суспільства абсолютно нормально, коли блогер має п'ять автомобілів преміум-класу та три маєтки. Ніхто не запитує, звідки взялися гроші на все це, тому що демонстрація багатства стала невіддільною частиною професії — це візитівка, реклама та спосіб утримувати увагу.

Для наркокартелів ця обставина є справжнім подарунком долі. Вони можуть передавати інфлюенсеру сотні тисяч або навіть мільйони доларів для купівлі чергової машини або організації грандіозного розіграшу, і ця операція не приверне уваги, бо виглядатиме як цілком звичний елемент життя багатої публічної особи.

Друга, можливо, навіть більш важлива причина криється в регуляторному вакуумі. Попри стрімке зростання індустрії впливу в соціальних мережах, переважна більшість країн Латинської Америки (і багатьох інших регіонів світу) досі не мають спеціального законодавства, яке б визначало статус блогера як суб'єкта фінансового контролю. Традиційні закони про відмивання грошей зосереджені на класичних секторах: банківська справа, страхування, ринок цінних паперів, операції з нерухомістю, продаж транспортних засобів, діяльність нотаріусів та адвокатів. Усі ці сфери мають чіткі правила звітності про підозрілі операції. Проте в таких галузях, як індустрія розваг, мистецтво, спорт і, особливо, соціальні мережі та створення контенту, грошові потоки є не меншими, але регулюються вони значно слабкіше.

Чому так відбувається? Причина полягає в суб'єктивному характері ціноутворення в цих сферах. Як визначити, чи справді один допис в Instagram коштує 10 тисяч доларів, чи це завищена ціна, за якою ховається відмивання коштів? Як довести, що квартира, розіграна в лотерею, коштує саме 200 тисяч доларів, а не 50? Як перевірити, чи всі переможці розіграшу реальні люди? Ці питання не мають простих відповідей, і саме цю прогалину використовують злочинці. Блогери існують у сірій зоні, де вони формально є приватними особами або підприємцями на спрощених режимах оподаткування, але фактично управляють фінансовими потоками, які можна порівняти з бюджетами невеликих корпорацій.

Окремо варто відзначити позитивні зрушення, про які згадується в документі, хоча вони й підкреслюють загальну проблематичну ситуацію. Бразилія, як не дивно, сьогодні є однією з небагатьох країн у регіоні, яка зробила найбільш конкретні кроки до врегулювання цієї сфери. У січні 2026 року там було ухвалено закон, що регулює так звану мультимедійну професію, під яку підпадають блогери та творці цифрового контенту. Це означає, що держава починає офіційно визнавати їхній професійний статус, що автоматично тягне за собою певні обов'язки щодо звітності, оподаткування та фінансового контролю. Однак навіть у Бразилії процес не завершено: парламентарі активно дискутують про ширшу реформу чинного AML законодавства, яка б прямо зобов'язала блогерів повідомляти про підозрілі транзакції. Якщо цей закон буде ухвалено, Бразилія стане першою великою економікою регіону, яка офіційно внесе блогерів до переліку осіб, що зобов'язані боротися з відмиванням грошей. Поки що ж цей приклад є скоріше винятком, ніж правилом. Колумбія, Мексика та більшість інших країн Латинської Америки лише починають усвідомлювати масштаб загрози.

Висновки:

- **Інфлюенсери використовують лотереї та розіграші в соціальних мережах** для приховування незаконних доходів, оскільки відсутність прозорості щодо кількості проданих квитків та осіб покупців дозволяє підмінювати реальні платежі «брудними» коштами.
- **Фрагментовані транзакції малими сумами через донати, рекламу та криптовалюти** дозволяють обходити пороги обов'язкового фінансового моніторингу, роблячи слід відмивання коштів майже невидимим.
- **Золоте тло успішного способу життя блогерів** (розкішні авто, будинки, подорожі) створило «соціальний дозвіл» не ставити запитання про походження їхніх статків, що є ідеальною ширмою для злочинців.
- **У більшості країн Латинської Америки досі бракує спеціального регулювання** інфлюенсерів, що дозволяє злочинним угрупованням використовувати цю прогалину для легалізації доходів.

Резюмуючи, можна стверджувати, що перед нами постає класичний випадок того, як злочинні інновації випереджають регуляторну спроможність держави. Доки правоохоронні органи та фінансові розвідки звикли шукати сліди наркогрошей у традиційних секторах, злочинні

угруповання на кшталт PCC, Сіналоа та інших уже активно освоїли новий цифровий фронт — соціальні мережі.

Блогер, який має, наприклад, 14 мільйонів підписників, є не просто публічною особою, а потужним фінансовим інструментом, здатним легалізувати сотні мільйонів доларів через лотереї, фрагментовані транзакції, криптовалюти та фіктивні рекламні контракти. Поки не буде створено міжнародних стандартів контролю за фінансовими потоками блогерів, поки їх не буде визнано суб'єктами первинного фінансового моніторингу, доти проблема тільки загострюватиметься. Адже вартість входу в цей «бізнес» для злочинців залишається низькою, а потенційний прибуток — величезним. Соціальні мережі створили новий клас публічних осіб, і тепер суспільству та державі належить дати відповідь на виклик: чи зможуть вони відокремити щиру популярність від майстерно замаскованого злочину.

Новозеландський вузол: як маленька фінансова компанія обслуговувала глобальний брудний капітал [13]

На перший погляд, Нова Зеландія залишається взірцем: її пагорби асоціюються в усього світу зі спокоєм, прозорістю та верховенством права. Саме цей образ довгі роки приваблював інвесторів, які шукали стабільну юрисдикцію з низьким рівнем корупції.

Однак за лаштунками цієї привабливої картини, в індустріальному місті Гамільтон, упродовж кількох років діяла фінансова компанія, чия бізнес-модель кидала виклик самому поняттю фінансової безпеки. Worldclear Ltd, яка займала десятий поверх однієї з небагатьох висотних будівель міста, обіцяла клієнтам ефективні міжнародні розрахунки, а натомість, згідно з витоком внутрішніх документів, отриманих Interest.co.nz та поширених консорціумом OCCRP, перетворилася на транзитний вузол для сумнівних капіталів, які обходили стороною звичайні банки.

Документи, що охоплюють період приблизно 2015–2019 років, містять клієнтські списки, транзакційні записи, внутрішнє листування та звіти наглядових органів. Вони малюють образ компанії, яка свідомо обрала нішу високоризикових клієнтів — тих, хто зіткнувся з відмовами у відкритті рахунків, анулюванням кореспондентських відносин або ускладненнями через географічне походження чи структуру бізнесу. Проєкт маркетингової презентації, знайдений серед документів, прямо запитує: «Проблеми з банками? Проблеми з платежами в USD? Рахунки закрито? ... Ми можемо допомогти». Це не є порушенням само по собі, але така позиція зміщувала акцент із проактивного комплаєнсу на терпимість до ризику, яку звичайні фінансові установи намагаються мінімізувати. Засновник Worldclear Девід Гілларі, новозеландський бізнесмен і колишній фінансовий радник, наполягає, що ні він, ні його компанія ніколи «свідомо або через грубу недбалість не сприяли кримінальним правопорушенням». Він наголошує, що факт високого ризику клієнта не може бути підставою для звинувачень у співучасті у злочинах. Однак внутрішні звіти регулятора свідчать про системні недоліки, які об'єктивно робили Worldclear вразливою до використання з боку шахраїв та осіб, причетних до відмивання коштів.

[13] https://www.occrp.org/en/project/the-worldclear-files/inside-the-tiny-new-zealand-firm-that-transferred-millions-for-high-risk-clients

У березні 2018 року Департамент внутрішніх справ Нової Зеландії (DIA) провів виїзну перевірку Worldclear. Звіт, виявлений репортерами, засвідчив, що компанія мала лише часткову відповідність вимогам закону про протидію відмиванню грошей та фінансуванню тероризму (AML/CFT). Найбільш тривожним виявився висновок про відсутність належних контролів для «моніторингу, аналізу та документування складних або великих транзакцій, незвичних патернів, дивних операцій або будь-якої іншої активності, яка може бути пов'язана з відмиванням грошей чи фінансуванням тероризму».

Інспектори виявили, що належна перевірка клієнтів (customer due diligence) проводилася непослідовно, а сам процес було названо «стихійним». Більше того, Worldclear не мала функціонуючої процедури для ідентифікації політично значущих осіб (PEP) — категорії клієнтів, яка за визначенням потребує підвищеної уваги через ризики хабарництва та корупції. Компанія покладалася на те, що банки-кореспонденти проводитимуть посилену перевірку, хоча DIA прямо вказав: «Worldclear в цілому працює в надзвичайно високоризиковому середовищі, тому відповідальність лежить на Worldclear». Департамент виніс так звані «рекомендації щодо виправлення» (remedial instructions), вимагаючи усунути порушення та провести незалежний аудит. Однак у 2019 році Worldclear повідомила регулятору, що припинила діяльність ще попереднього року, і нагляд за нею завершився без подальших перевірок чи санкцій. Двоє провідних новозеландських експертів з AML, Мартін Діллі та адвокат Фіона Голл, висловили подив, що справа не була передана до поліції. «Якимось чином Worldclear вийшла сухою з води», — зауважила Голл. Гілларі, своєю чергою, назвав висновки DIA «фальшивими» та «такими, що завдають шкоди», і звинуватив відомство в упередженому ставленні, стверджуючи, що інспектори не перевіряли документацію належним чином.

Найяскравіше обличчя цієї системної вразливості — історія Майкла Вілсона, американсько-канадського інвестора, який перетворився на міжнародного шахрая. Витік показує, що Worldclear прийняла на обслуговування компанію Вілсона West Kingdom Holdings у грудні 2015 року. Перед цим комплаєнс-платформа MemberCheck, яку використовувала Worldclear, виявила бенефіціарного власника та визначила його як «потенційного клієнта з високим ризиком». На той момент Вілсон ще не був засуджений, але публічно було відомо, що він перебуває під слідством за багатомільйонне шахрайство з інвестиціями та чекає на екстрадицію з Канади до США. Його брат уже відбував тюремний термін за участь у тій самій афері.

Незважаючи на це, Worldclear відкрила рахунки. Гілларі пояснив, що сигнал MemberCheck був переданий йому на оцінку, після чого він запросив додаткову інформацію, але компанія, за його словами, не мала підстав вважати Вілсона особою, обвинуваченою у фінансових злочинах. Однак внутрішні банківські виписки свідчать, що між 11 грудня 2015 року та 12 січня 2016 року на рахунок West Kingdom Holdings через Worldclear надійшли три платежі на суми від 446 000 до 524 000 доларів. Джерелом виступав рахунок, пов'язаний з американським дилером дорогоцінних металів Schiff Gold. Кожен із цих платежів протягом кількох днів був переправлений Worldclear до банку Euro Pacific Bank Limited у Сент-Вінсенті та Гренадинах — юрисдикції, яка вважається податковою гаванню. Згодом, у заяві на конфіскацію майна, агент ФБР прямо зазначив, що використання Worldclear як посередника «допомогло приховати справжнє джерело коштів». Отримавши гроші, Вілсон орендував приватний літак, забрав дружину, матір і трьох собак і втік до В'єтнаму, де його заарештували в червні 2016 року. У 2017 році він визнав провину за шахрайством із використанням електронних засобів зв'язку (wire fraud) та отримав 108 місяців ув'язнення, вийшовши на свободу лише у січні 2023 року. У документі, надісланому новозеландській поліції, сам Гілларі змушений був визнати, що перекази Вілсона через Worldclear «видаються доходами від його інвестиційних афер», хоча стверджував, що гроші вже були «успішно відмиті до того, як потрапили в Worldclear». Цей випадок демонструє, як реєстрація в довіреній юрисдикції надає транзакціям легітимності,

знижує «регуляторну температуру» і дозволяє проводити операції, які інакше викликали б негайний блок з боку банківських систем.

Однак портфель клієнтів Worldclear був набагато різноманітнішим. Серед тих, хто шукав притулку в маленькій новозеландській фірмі, опинився Ендрю Стремплер, засуджений у 2013 році за змову з метою поштового шахрайства через незаконний продаж рецептурних ліків в інтернеті. Після виходу з в'язниці у 2016 році він подав заявки на два корпоративні рахунки в Worldclear. Його рекомендація надійшла від Мікаеля Магнуссона — одного з міноритарних акціонерів Worldclear, який схарактеризував Стремплера як «чесну та надійну людину». Стремплер не приховав своєї судимості, і Worldclear визнала його «особою прийнятного характеру» для обслуговування. Це рішення красномовно свідчить про толерантність компанії до кримінального минулого, якщо воно не створювало безпосередніх репутаційних ризиків.

Ще більш показовою є справа Гюнтера Клара, британського громадянина, який через банк Global Fidelity з Кайманових островів (що мав рахунок у Worldclear) здійснював масштабні платежі. У вересні 2017 року через цей ланцюжок пройшло 945 000 доларів. Два місяці потому — ще один мільйон доларів. Інвойси, які збереглися у витоку, показують, що Клар використовував Global Fidelity та Worldclear для оплати найрізноманітніших витрат: від готельних номерів і приватних літаків до шкільних навчальних внесків, квітів і дизайнерського взуття. У 2024 році Клара засудили в Данії за шахрайство з податками на суму 45 мільйонів доларів, і на момент здійснення цих транзакцій він не був публічною фігурою у скандальних розслідуваннях.

Ймовірно, найбільш нищівним аспектом розслідування є не сам список клієнтів, а склад акціонерів самої Worldclear. Згідно з витоком, двоє міноритарних власників компанії мали задокументовані судимості за фінансові злочини або були засуджені під час володіння частками.

Перший — швед Мікаель Магнуссон, чия компанія EBANQ Holdings B.V. (зареєстрована на Сейшелах) постачала Worldclear програмне забезпечення для клієнтського інтерфейсу. У 2017 році суд Панами засудив Магнуссона до дев'яти років ув'язнення за відмивання грошей. Він не мав цього вироку на момент придбання частки у Worldclear у 2015 році, але у 2023 році, вже після припинення діяльності Worldclear, Інтерпол видав «червоне повідомлення» для його арешту (на ім'я Карл Мікаель Магнуссон, оскільки він змінив ім'я на Мікаель у 2018 році). Сьогодні Магнуссон живе у Стокгольмі, і шведське законодавство не дозволяє екстрадицію своїх громадян до третіх країн за межами ЄС.

Другий акціонер — венесуелець Артуро Хосе Трухільйо Вільялобос, який отримав частку у Worldclear у 2017 році та володів нею щонайменше до квітня 2022 року. Ще 1999 року він був засуджений за змову з метою продажу підроблених державних облігацій Венесуели. Гілларі заявляє, що на момент входження Трухільйо в капітал йому нічого не було відомо про його судимість і що «наскільки я знав тоді і знаю зараз», Трухільйо не мав фінансових злочинів. Важливо підкреслити, що новозеландське законодавство, як визнає навіть FATF, не вимагає від фінансових провайдерів типу Worldclear перевіряти міноритарних акціонерів. Ця прогалина — один із ключових ризиків, на які вказує міжнародна спільнота.

Історія знайомства Гілларі та Магнуссона додає цьому пазлу ще один шар. За шість тижнів до заснування Worldclear обліковий запис на ім'я Девіда Гілларі залишив захоплений відгук на Amazon на книгу Магнуссона під провокаційною назвою «Країна без банківського закону: Як створити банк із тисячею доларів». У відгуку Гілларі називає автора «майстром, який працював над створенням цих структур багато років», хвалить його за захист свободи у фінансових послугах та характеризує державне регулювання як «хворобу». Сама книга, що досі доступна на Amazon, містить покрокову інструкцію з реєстрації бізнесу в Новій Зеландії «з повною юридичною здатністю пропонувати банківські послуги будь-якій кількості клієнтів у будь-якій

точці світу», наголошуючи, що «немає регуляторних вхідних бар'єрів як таких для банківського бізнесу, коли послуги пропонуються лише нерезидентам (офшор)».

Ці ідеї перегукуються з особистим блогом Гілларі «Sue 4 Insult», який востаннє оновлювався у березні 2019 року. У блозі, присвяченому критиці цивільних позовів та, зрештою, оподаткуванню, Гілларі описує податки як різновид «людського паразитизму». Ці світоглядні настанови пояснюють, чому Гілларі міг сприймати свою діяльність не як порушення, а як боротьбу за економічну свободу, а клієнтів із кримінальним минулим — як жертв надмірного регулювання.

Попри те, що Worldclear було вилучено з реєстру фінансових провайдерів Нової Зеландії в лютому 2019 року через неподання підтвердження про діяльність, сліди її ключових фігур ведуть у сьогодення. У травні 2025 року Девід Гілларі зареєстрував нову новозеландську компанію Trusfinco Baninvest, де директором виступає Артуро Хосе Трухільйо Вільялобос. Вебсайт компанії, який згодом зник, позиціонував її як постачальника фінансових послуг, хоча Міністерство бізнесу, інновацій та зайнятості Нової Зеландії повідомило журналістам, що Trusfinco ніколи не була зареєстрована як фінансовий провайдер. Сам Гілларі та Трухільйо залишили запитання про цю нову структуру без відповіді. Тим часом Мікаель Магнуссон продовжує розвивати програмне забезпечення EBANQ, яке колись живило Worldclear. У грудні 2025 року на сайті EBANQ з'явився опис нового модуля Banking-as-a-Service (BaaS), який дозволяє миттєво створювати віртуальні IBAN-рахунки та оптимізувати платіжні операції — інструменти, що за певних умов можуть бути використані для ще складніших схем приховування руху коштів.

Експерти, опитані в межах розслідування, сходяться на думці, що справа Worldclear — це не просто локальний казус, а симптом глибшої проблеми. Нова Зеландія, яка прагне зберегти імідж юрисдикції з нульовою толерантністю до корупції, ризикує потрапити до «сірого списку» FATF, якщо не посилить контроль над небанківськими фінансовими установами. Генеральний директор Transparency International New Zealand Джулі Гаґґі прямо застерігає, що країна має виправити проблеми до наступного огляду FATF, інакше «ризик потрапити до сірого списку, що не добре для Нової Зеландії».

Висновки:

- **Worldclear цілеспрямовано обслуговувала клієнтів, від яких відмовилися звичайні банки**, включно з особами, підозрюваними у шахрайстві, відмиванні коштів та ухиленні від сплати податків, використовуючи прогалини в регулюванні Нової Зеландії.
- **Регуляторний нагляд виявився неефективним:** попри офіційні звіти Департаменту внутрішніх справ про «стихійну» перевірку клієнтів та відсутність контролю за підозрілими транзакціями, Worldclear уникла суттєвих санкцій або кримінального переслідування.
- **Два міноритарні акціонери компанії мали судимості за фінансові злочини,** що стало можливим через відсутність законодавчої вимоги перевіряти таких власників — прогалину, на яку вказує FATF.
- **Використання Worldclear як посередника допомагало приховувати джерела коштів**, зокрема у справі Майкла Вілсона, де ФБР прямо зафіксувало, що транзит через новозеландську фірму «сприяв маскуванню справжнього походження коштів».

Випадок Wilson, який використав Worldclear як частину схеми легалізації доходів, та присутність акціонерів із кримінальним минулим у структурі власності компанії — це червоні прапорці, які за ідеальних умов мали б активувати цілу низку запобіжних механізмів. Однак через фрагментований нагляд, відсутність вимог перевіряти бенефіціарів на рівні міноритарних акціонерів та

пасивну позицію регулятора система дала збій.

Історія Worldclear є нагадуванням про те, що навіть у найблагополучніших юрисдикціях можуть процвітати практики, які підривають глобальну боротьбу з відмиванням грошей. Фактчекінг, проведений OCCRP, не виявив доказів того, що Worldclear свідомо сприяла злочинам, але сам факт, що компанія з такими прогалинами в комплаєнсі могла роками переказувати сотні мільйонів доларів, вимагає не просто морального засудження, а конкретних законодавчих змін.

Рекомендовані матеріали

Футбол під наглядом: інтерв'ю Голови AMLA Бруни Шего про інтеграцію професійних футбольних клубів та агентів до режиму ПВК/ФТ ЄС [14]

27 квітня 2026 року в спеціалізованому виданні Calcio e Finanza було опубліковане розширене інтерв'ю з Бруною Шего, Головою Органу з протидії відмиванню коштів та фінансуванню тероризму ЄС (AMLA). Інтерв'ю є значущим сигналом регулятора для приватного сектору: AMLA вперше у такому форматі детально роз'яснила практичні наслідки пакету реформ ПВК/ФТ 2024 року для футбольної індустрії, зокрема строки, архітектуру нагляду, ризикові фактори, очікування до суб'єктів та заходи по забезпеченню рівного конкурентного середовища. 3 липня 2029 року професійні футбольні клуби та футбольні агенти у всіх державах-членах ЄС вперше стануть підзвітними суб'єктами в рамках пакету законодавства ПВК/ФТ, сформованого Директивою та Регламентом 2024 року.

Принципове значення реформи 2024 року полягає у переході від системи директив — що потребують транспозиції на національному рівні та породжують 27 різних нормативних режимів — до уніфікованого підходу, оснований на регламентах ЄС та централізованому наглядовому органі в особі AMLA. Саме ця фрагментованість попередньої системи була однією з причин включення футболу до переліку підзвітних суб'єктів: ряд держав-членів, зокрема Бельгія (з 2020 року), вже мали власне законодавство для клубів і агентів, тоді як більшість країн ЄС не висували до цього сектору жодних AML-вимог. Пакет 2024 року усуває цей регуляторний арбітраж та створює умови для рівного конкурентного поля на загальноєвропейському ринку.

Пані Шего детально обґрунтовує, чому саме футбол, а не інший вид спорту, опинився в полі зору регулятора. Глобальний ринок футболу оцінювався у 56 мільярдів доларів у 2024 році, з прогнозованим зростанням до 70 мільярдів до 2030 року; медіа-права, спонсорство та продаж квитків генерували 38 мільярдів доларів у 2024 році. Близько 51% населення планети стежить за футболом, а аудиторія Чемпіонату світу сягає 5 мільярдів глядачів. Масштаб грошових потоків, транскордонний характер переважної більшості операцій, непрозорість корпоративних структур клубів або їхніх інвесторів, а також соціальний статус, який надає причетність до відомих клубів, роблять цей сектор привабливим для відмивання коштів. Звіт Europol 2020 року щодо організованої злочинності та корупції у спорті назвав футбол найбільш ураженим видом спорту.

Регулятор визначив три основні канали ризику. Перший — структури власності та інвестиції: корпоративні конструкції у футболі часто є складними та багатоярусними, що ускладнює ідентифікацію кінцевого бенефіціарного власника; транскордонні угоди домінують на ринку

[14] https://www.amla.europa.eu/news-media/news-articles/aml-football-sector-interview-amla-chair-bruna-szego_en

придбання часток у клубах. Другий — ринок трансферів гравців: платежі є комплексними (клуб, агент, гравець, негайні та відстрочені виплати, бонуси), а ціноутворення за трансфер є принципово суб'єктивним і маніпульованим, що відкриває можливості для приховування незаконних переміщень вартостей. Третій — відносини із спонсорами: при хронічній фінансовій вразливості клубів існує ризик прийняття коштів без необхідної перевірки їх походження.

AMLA роз'яснює, що регуляторний підхід щодо охоплення клубів функціонує на двох рівнях. На рівні системи нагляду — AMLA розробляє методологію оцінки ризику для наглядових органів, диференційовану за секторами, включаючи спеціалізований блок для футболу; у кожній державі-члені має бути утворений наглядовий орган із повним спектром повноважень над футбольними клубами та агентами. На рівні підзвітних суб'єктів — клуби зобов'язані будуть застосовувати CDD або транзакційний моніторинг залежно від характеру відносин, а також ідентифікувати КБВ та перевіряти джерела коштів. Голова AMLA звертає особливу увагу на механізм звільнень: держави-члени можуть звільняти клуби вищого дивізіону від AML-вимог, якщо їх річний оборот не перевищує 5 мільйонів євро за кожен з двох попередніх років та підтверджено низький рівень ризику; клуби нижчих дивізіонів можуть бути звільнені незалежно від обороту. Ці звільнення не є автоматичними — наглядові органи здійснюватимуть оцінку на основі спільної методології AMLA.

Щодо практичної готовності сектору, голова AMLA відзначила, що більшість учасників футбольної галузі у ході зустрічей регулятора в державах-членах не були представлені — на відміну від фінансових асоціацій. Це свідчить про суттєву прогалину у розумінні майбутніх зобов'язань. Клубам необхідно вже зараз розпочати розробку внутрішніх процедур CDD, систем транзакційного моніторингу та призначення відповідальних за AML-функцію осіб. Вимоги до розміру та складності внутрішньої AML-системи також підпорядковуються ризик-орієнтованому підходу: від малих клубів не очікується побудова такої ж інфраструктури, як у великих установ. Пані Шего завершила інтерв'ю чітким та лаконічним посланням: «Ми розраховуємо на вас. Ваш сектор має значення, і важливо, щоб футбол був чистим і прозорим ринком. Починайте готуватися зараз.»

Кіберзлочинність і соціально-економічна реальність [15]

У березневому випуску Journal of Economic Criminology (Elsevier, Vol. 11, 2026) опубліковано кримінологічне дослідження авторства Nii Barnor Jonathan Barnor (Університет Гани), Eric Ansong і Sheena Lovia Boateng. Дослідження вписується в розширену наукову дискусію про соціально-економічні детермінанти кіберзлочинності в країнах, що розвиваються, та про раціональний вибір злочинців у цифровому середовищі. Методологічну основу становить якісний підхід: тринадцять осіб, причетних до онлайн-шахрайства романтичного типу в Гані, з якими було проведено інтерв'ю. Аналіз даних здійснено за методом транссцендентного реалізму Майлса і Хабермана — підходом, що прагне виявити структурні механізми та каузальні зв'язки, що лежать за спостережуваними соціальними феноменами.

Теоретичний каркас дослідження ґрунтується на теорії раціонального вибору (Rational Choice Theory), що розглядає злочинну поведінку як результат усвідомленої оцінки ризику та очікуваного доходу. Автори застосовують цю теорію до контексту так званого «сакрального шахрайства» (sakawa) — феномену онлайн-шахрайства, що набув значного поширення в Гані та

[15] https://www.sciencedirect.com/science/article/pii/S2949791426000205

ширшому Західноафриканському регіоні. Ключовим внеском дослідження є деталізація конкретних тактик і стратегій, що застосовуються виконавцями: розбудова оманливих онлайн-персонажів (фальшива ідентичність, фотографії, особисті біографії), поетапне емоційне маніпулювання жертвами для побудови довіри та подальшого вилучення коштів, а також використання жертв як ненавмисних посередників у ширших кіберзлочинних схемах — зокрема шахрайстві в сфері електронної комерції, крадіжці ідентичності та шахрайстві з кредитними картками. Остання категорія поведінки суттєво розширює аналітичну рамку порівняно з традиційним розумінням романтичного шахрайства: жертви несвідомо стають ланкою в складніших транснаціональних фінансово-злочинних мережах.

Соціально-економічний вимір результатів є принципово важливим. Автори фіксують, що мотивація виконавців формується під прямим впливом структурних факторів: бідності, безробіття та браку освіти. Ці дані перегукуються з більш широкою порівняльною літературою, що демонструє нелінійний зв'язок між розвитком цифрової інфраструктури і рівнем кіберзлочинності в умовах обмеженого економічного розвитку і слабких правоохоронних механізмів. Теоретично значущим є висновок про те, що раціональна оцінка ризику і винагороди злочинцями відбувається в умовах вкрай низьких сприйнятих витрат — ймовірність виявлення та переслідування за онлайн-шахрайством залишається низькою, тоді як економічна вигода є суттєвою відносно легальних альтернатив. Цей дисбаланс стимулів вказує на системні прогалини як у правоохоронних можливостях, так і в регуляторних заходах обов'язкового фінансового моніторингу в юрисдикціях із слабко розвиненою системою ПВК/ФТ.

Для практиків у сфері ПВК/ФТ та оцінки ризиків дослідження формує декілька конкретних аналітичних імплікацій. По-перше, механізм використання жертв романтичного шахрайства як посередників для шахрайства в e-commerce та крадіжки ідентичності безпосередньо збільшує ризик мані-мулів у регульованих фінансових установах: особи, які переводять кошти від шахрайства, можуть і самі виступати жертвами маніпуляцій, що ускладнює кваліфікацію умислу і знижує ефективність шаблонних алертів транзакційного моніторингу. По-друге, транснаціональний характер романтичного шахрайства та його інтеграція в ширші злочинні мережі з різноманітними предикатними правопорушеннями (від шахрайства до незаконного обігу крадених даних) вимагає більш комплексного підходу до виявлення на рівні одиниць звітності, що враховує поведінкові патерни й мережеві зв'язки, а не виключно аномалії в транзакційному потоці. Обмеженнями дослідження є вузька географічна вибірка і суб'єктивність самозвітування, що знижує узагальнюваність, але не применшує кримінологічної цінності первинних даних про мотиваційні структури виконавців.

Інші новини

Як географічна експансія змінює архітектуру відмивання коштів [16]

У середині 2020-х років світ став свідком того, як регіональна злочинна група, що виникла у в’язниці Токорон у Венесуелі, перетворилася на одну з найбільш адаптивних транснаціональних мереж Латинської Америки. Йдеться про угруповання «Трен де Арагуа» (Tren de Aragua), чия діяльність вийшла далеко за межі традиційних для латиноамериканських кримінальних синдикатів моделей.

Документи, оприлюднені аналітичним центром Insight Crime, а також матеріали розслідувань прокурорів Чилі, Перу та інших країн, дозволяють зробити однозначний висновок: географічне поширення угруповання стало головним каталізатором його фінансової еволюції. Якщо спочатку «Трен де Арагуа» використовувало примітивні методи переказу коштів через

[16] https://insightcrime.org/news/tren-de-aragua-money-laundering-schemes-reveal-factions-ongoing-refinement/

традиційні сервіси грошових переказів, то сьогодні воно демонструє використання складних багаторівневих схем відмивання грошей, що поєднують фіктивні компанії, рахунки, криптовалюти та навіть спеціалізовані осередки фінансових експертів. Цей перехід не є випадковим або реактивним — він є прямим наслідком зміни самої природи організації, яка з локального тюремного клану перетворилася на розгалужену мережу автономних, але скоординованих фракцій, розкиданих по всьому континенту.

Початковим імпульсом до фінансового ускладнення стала масштабна міграційна криза у Венесуелі наприкінці 2010-х років. Мільйони венесуельців, які тікали від репресій, тотальної небезпеки та економічного колапсу, рушили до сусідніх країн — Колумбії, Перу, Чилі, Еквадору.

Організація «Трен де Арагуа», яка до того моменту контролювала значну частину кримінального ринку всередині венесуельських в'язниць, миттєво скористалася цим потоком. Її осередки почали вимагати гроші у мігрантів, використовуючи так званий «подорожній податок» (impuesto de viaje), а також створювали власну інфраструктуру для контрабанди людей. Вони контролювали нелегальні переправи, встановлювали ціни на перетин кордонів і — що ще більш цинічно — використовували вразливість мігрантів для вербування жінок і дівчат у сексуальне рабство.

Поступово, закріпившись у нових країнах, осередки «Трен де Арагуа» розширили свій злочинний портфель: додали роздрібний продаж наркотиків (особливо кокаїну та базової кокаїнової пасти), локальне вимагання дрібних підприємців, а згодом і замовні вбивства. Важливо наголосити: на відміну від таких гігантів як Сіналоа чи Новий Халіско, «Трен де Арагуа» так і не стала ключовим гравцем у великому транзиті наркотиків або промисловому незаконному видобутку копалин. Але саме цей розосереджений, «портфельний» характер її доходів, розпорошених на величезній території та згенерованих тисячами дрібних і середніх злочинів, створив безпрецедентну потребу у складному фінансовому сервісі. Прості методи більше не працювали — на їхнє місце прийшла справжня кримінальна фінтех-інфраструктура.

Найбільш яскравим підтвердженням цієї тези стала операція, результати якої були оприлюднені головним прокурором чилійського підрозділу кримінального аналізу та слідчого фокусу (SACFI) 22 квітня 2026 року. Поліція Чилі заарештувала 22 особи, яких звинуватили у відмиванні щонайменше 4,5 мільйона доларів США. Ці гроші, як з'ясувало слідство, були безпосередніми прибутками від продажу наркотиків, систематичних вимагань («гроші за захист») та виконання замовних вбивств на території країни.

Сама схема, що діяла одразу в трьох регіонах — Вальпараїсо, Кокімбо та столичному Сантьяго, — була доволі елегантною з точки зору кримінального фінансування. Вона складалася з кількох послідовних етапів.

Перший: незаконно отримані готівкові кошти передавалися через так званих «мулів» або через підставних осіб на рахунки компаній-посередників. Ці компанії часто мали легальний фасад — невеликі бізнеси з великим готівковим обігом, такі як салони манікюру, перукарні, компанії з організації заходів або маленькі ресторани.

Другий етап: після того як гроші «очищувалися» через ці фірми, вони конвертувалися у криптовалюту — переважно у біткойн або стейблкойни, що прив'язані до долара США (USDT).

Третій етап: криптовалюта відправлялася через міксинг-сервіси та децентралізовані обмінники за кордон. Фінальною точкою призначення була Венесуела — країна, де правоохоронна система традиційно була найменш спроможною переслідувати такі фінансові потоки, особливо після децентралізації самого угруповання.

Ще більш промовистою є хронологія цього процесу. За рік до подій у Чилі, у 2025 році, було викрито інший великий епізод, який виявився своєрідним «сигналом тривоги» для всієї регіональної правоохоронної спільноти. Тоді «Трен де Арагуа» вдалося перемістити за кордон уже 13,5 мільйона доларів, використовуючи комбінацію спеціально створених банківських рахунків, підставних фірм та криптовалют. Керівник того розслідування на умовах анонімності зізнався місцевій пресі, що ніколи раніше не стикався з подібним поєднанням методів у справах венесуельських угруповань. Ще через кілька місяців, у вересні 2025 року, прокуратура Перу повідомила про третій аналогічний випадок: члени «Трен де Арагуа» спочатку відправляли відмиті кошти до Венесуели та Колумбії, щоб остаточно обірвати ланцюжок транзакцій, а потім через підставні компанії (фронт-компанії) повертали їх назад у Перу вже як виручку від нібито законного експорту чи послуг. Таким чином, до початку 2026 року сформувалася цілісна система, де географічна розпорошеність виконувала ту саму роль, що й криптографічне шифрування — вона робила трасування фізично неможливим.

Окремо слід розглянути еволюцію самих методів у часі. На початковому етапі експансії, приблизно у 2020–2022 роках, осередки «Трен де Арагуа» використовували надзвичайно прості, «побутові» способи переказу виручки своїм лідерам. Найпопулярнішим з них було використання міжнародних сервісів грошових переказів, таких як Western Union або MoneyGram. Представники фракцій у Чилі чи Перу просто приходили до пунктів обслуговування, пред'являли підроблені документи та відправляли відносно невеликі суми на підставні імена у Венесуелі. Однак вже у 2023 році перуанський поліцейський офіцер, який брав участь у спецоперації, повідомив місцевій пресі, що від цього методу довелося відмовилися. Причина була простою: велика кількість підозрілих транзакцій однакового розміру привернула увагу не лише поліції, але й внутрішніх систем моніторингу самих платіжних сервісів. Тоді й розпочався наступний етап — використання дрібних номінальних рахунків у місцевих банках. Гроші розбивалися на частини по кілька сотень або тисяч доларів, проводилися через ланцюжок з п'яти-семи різних рахунків різних осіб (часто — необізнаних мігрантів, чиї дані були викрадені), а потім акумулювалися на одному рахунку перед конвертацією.

Паралельно з цим, приблизно з 2022 року, за даними чилійських прокурорів, угруповання почало активне освоєння криптовалют. Але важливо зрозуміти: «Трен де Арагуа» не стала використовувати крипту як прямий платіжний засіб — натомість вона вбудувала її в складні гібридні конструкції.

Сучасна схема, задокументована у справах 2025–2026 років, виглядає так: незаконна готівка → фіктивна компанія з великим обігом готівки → банківський рахунок цієї компанії → купівля стейблкойнів (USDT) на біржі (часто з використанням підроблених KYC-документів) → переведення криптовалюти в приватний гаманець поза межами країни → конвертація назад у фіат через нерегульований обмінник у Венесуелі або Колумбії.

Цей гібридний підхід має кілька переваг: по-перше, він використовує «білий» банківський сектор на початковому етапі, що ускладнює відстеження джерела; по-друге, криптовалютний стрибок створює «чорну діру» для фінансової розвідки, оскільки багато латиноамериканських країн досі не мають належних механізмів моніторингу блокчейн-транзакцій; по-третє, використання стейблкойнів захищає капітал від волатильності, що важливо для довгого ланцюжка переказів.

Найважливішим структурним зрушенням, яке фіксують документи, стала внутрішня організаційна зміна всередині самого угруповання. До вересня 2023 року «Трен де Арагуа»

мала відносно централізовану структуру з головним хабом у в'язниці Токорон у Венесуелі. Керівництво у Токороні отримувало регулярні відрахування від закордонних фракцій, і цей потік грошей потрібно було постійно обслуговувати.

Однак після того, як венесуельський уряд під тиском міжнародної спільноти відновив контроль над Токороном у вересні 2023 року, центральне керівництво було фактично децентралізоване. Багато лідерів опинилися в інших в'язницях, частина була ліквідована або втекла. Здавалося б, це мало б створити хаос і послабити фінансову дисципліну. Однак, як не парадоксально, це прискорило фінансову еволюцію. Розслідування, проведені в Чилі після 2024 року, показали, що окремі фракції не тільки зберегли здатність до координації між собою без центрального хабу, але й почали створювати спеціалізовані підрозділи. У структурі «Трен де Арагуа» з'явилися окремі «фінансові осередки» (células financieras), які не займаються ні наркоторгівлею, ні вимаганням, ні насильством. Їхня єдина функція — вибудовування схем відмивання, пошук нових банківських лазівок, закупівля підставних фірм, конвертація в криптовалюту та її переказ. Тобто еволюція методів співпала з еволюцією організаційної структури, і це створює нову, надзвичайно стійку модель злочинного синдикату.

Значення цього процесу виходить далеко за межі окремої справи. Ми бачимо формування стандартизованої, але водночас гнучкої фінансової архітектури, яка може бути швидко адаптована до будь-якої країни, де з'являються осередки «Трен де Арагуа». Для правоохоронних систем Латинської Америки це означає перехід від боротьби з окремими кримінальними епізодами до необхідності вести системну фінансову розвідку, здатну аналізувати гібридні банківсько-криптовалютні ланцюжки.

Крім того, цей кейс є показовим для всього світу: він демонструє, як навіть відносно невелике (у порівнянні з картелями) угруповання може створити фінансову інфраструктуру континентального масштабу, якщо воно має диверсифікований «портфель» злочинів. «Трен де Арагуа» більше не є просто в'язничною бандою з Венесуели — це модель мережевої організованої злочинності нового покоління, де фінансові експерти є не менш важливими, ніж кілери або торговці наркотиками. І допоки регіональні уряди не навчаться виявляти та блокувати саме ці фінансові осередки, гроші продовжуватимуть вільно підживлювати насильство та корупцію.

Ваша думка важлива!

1. Де має проходити межа між допустимою автоматизацією комплаєнс-процесів і рішеннями, які обов'язково повинні залишатися під контролем людини — наприклад, блокування операцій, відмова в онбордингу клієнта або подання повідомлення про підозрілу діяльність?
2. Чи потребує українська система ПВК/ФТ більш структурованого підходу до подання повідомлень про підозрілі операції, подібного до люксембурзької моделі goAML-індикаторів, де підозра описується не лише текстом, а й через набір типологічних, секторних та поведінкових ознак?
3. Які ризики для СПФМ можуть створити стейблкоїни, токенізовані депозити та нові моделі цифрових платежів, якщо вони поступово інтегруватимуться у традиційну фінансову систему та транскордонні розрахунки?
4. Наскільки на вашу думку поширеними в Україні є схеми відмивання грошей через блогерів, благодійні розіграші та донати в соціальних мережах, особливо на тлі значного обсягу волонтерських зборів і готівкових пожертв, які не підлягають належному фінансовому моніторингу?
5. Яким чином держави та регулятори повинні забезпечити баланс між інноваціями у сфері цифрових грошей і необхідністю контролю ризиків ВК/ФТ, кіберзагроз, обходу санкцій та незаконних фінансових потоків у платіжних системах на основі блокчейну?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-20

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

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

AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE