Методологічний бюлетень

Серійний номер: МінФін-AML-2025-41

Жовтень 2025

“Роби все, що в твоїх силах. Більше не може зробити ніхто”

Джон Вуден

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

Звіт про вирішення ризиків ВК/ФТ в сфері криптоактивів за допомогою нагляду [1]

Представлений документ є комплексним аналітичним звітом Європейської банківської організації (ЕВА), що узагальнює критично важливий досвід, отриманий європейськими наглядовими органами у сфері ПВК/ФТ в секторі послуг з криптоактивами. Звіт охоплює період до та одразу після запровадження в ЄС нового гармонізованого регуляторного режиму, який базується на Регламенті про ринки криптоактивів (MiCA) та посиленому законодавстві з ПВК/ФТ. Його фундаментальна мета — систематизувати та проаналізувати тактики, які використовували деякі учасники ринку для ухилення від нагляду, та на основі цих уроків сформулювати ключові

[1] https://www.eba.europa.eu/sites/default/files/2025-10/6a64efb9-98e9-4e90-a5c5-2704a8ca8ef9/Report%20on%20tackling%20ML%20TF%20risks%20in%20crypto-asset%20services%20through%20supervision.pdf

рекомендації для компетентних органів, щоб забезпечити ефективну та послідовну імплементацію нових правил і запобігти повторенню виявлених ризиків у майбутньому.

У звіті детально висвітлено низку стратегій, до яких вдавалися постачальники послуг з віртуальних активів (VASPs), щоб уникнути регуляторного контролю. Однією з найпоширеніших практик було надання послуг без відповідної ліцензії чи реєстрації, часто з використанням юридичних осіб, зареєстрованих у третіх країнах зі слабким або відсутнім наглядовим режимом, або з іншої країни-члена ЄС без дозволу від приймаючого регулятора. Іншою поширеною тактикою був так званий "форум-шопінг", коли компанії цілеспрямовано шукали юрисдикції, які вони вважали менш суворими щодо вимог до входу на ринок та подальшого нагляду. Зіткнувшись із ретельною перевіркою з боку регулятора, такі компанії часто відкликали свої заявки і намагалися повторити процес в іншій державі-члені. Також зафіксовано випадки недобросовісного використання винятку щодо "зворотної ініціативи" (reverse solicitation), коли компанії стверджували, що клієнти з ЄС зверталися до них за власною ініціативою, хоча насправді велася прихована маркетингова діяльність для обходу регуляторних вимог.

Окрему увагу у звіті приділено серйозним та системним недолікам у внутрішніх системах ПВК/ФТ, виявлених під час інспекцій. Багато компаній надмірно покладалися на групові аутсорсингові моделі, де критичні функції, такі як належна перевірка клієнтів та моніторинг транзакцій, виконувалися головним офісом або іншими структурами групи за межами ЄС. Це призводило до того, що внутрішні політики не були адаптовані до специфічних вимог європейського законодавства, а місцевий менеджмент не мав реального контролю над цими процесами. Було виявлено значні слабкості в базових елементах контролю: неналежна верифікація особи клієнта, відсутність посиленої перевірки високоризикових клієнтів, неефективні інструменти санкційного скринінгу та несвоєчасне оновлення оцінок ризиків у відповідь на появу нових продуктів чи геополітичні зміни. Крім того, наголошується на проблемі нестабільності та недостатнього ресурсного забезпечення функції відповідального спеціаліста з ПВК/ФТ, що виражалося у високій плинності кадрів та призначенні тимчасових або неповністю зайнятих фахівців, що підривало ефективність нагляду.

Ще однією значною вразливістю, яку детально розглядає звіт, є використання непрозорих та надмірно складних корпоративних структур. Такі структури, що включають багатошарові ланцюги власності та використання номінальних акціонерів, ускладнювали для наглядових органів ідентифікацію кінцевих бенефіціарних власників та визначення осіб, які здійснюють фактичний контроль над бізнесом. У деяких випадках одна й та сама компанія надавала суперечливу інформацію про свою структуру різним регуляторам в ЄС. Ця непрозорість посилювалася використанням мультисуб'єктних угод. Наприклад, компанія, яка отримала відмову в ліцензуванні, могла придбати частку в уже ліцензованому VASP (залишаючись трохи нижче порогу кваліфікованої участі) або передати свою клієнтську базу дочірній компанії в іншій юрисдикції, щоб фактично продовжити діяльність і обійти наглядові заходи.

На противагу цим ризикам у звіті описано ключові запобіжники, запроваджені новим законодавчим пакетом. Центральним елементом є створення єдиного загальноєвропейського режиму авторизації та "паспортизації" послуг, який замінює фрагментовані національні підходи і покликаний усунути можливість регуляторного арбітражу. Нова система передбачає, що після отримання авторизації в одній країні-члені, компанія може надавати послуги по всьому ЄС. Водночас, були встановлені жорсткі обмеження на використання "зворотної ініціативи" , посилені вимоги до прозорості бенефіціарної власності, корпоративного управління та ретельної перевірки придатності керівництва ("fit and proper test"). Крім того, значно розширено повноваження наглядових та правозастосовних органів, включно з майбутнім органом з ПВК/ФТ (AMLA), щодо застосування санкцій та виправних заходів.

На завершення звіт наголошує, що успішна імплементація цих інструментів залежить від послідовних та рішучих дій з боку національних компетентних органів. Підкреслюється необхідність проведення ними ретельної та глибокої оцінки компаній, особливо тих, що мають проблемну попередню історію, перш ніж надавати їм авторизацію за MiCA, щоб запобігти поширенню ризиків через механізм "паспортизації". Важливим є впровадження проактивного моніторингу ринку для виявлення неавторизованої діяльності , постійне відстеження нових технологічних ризиків, як-от пов'язаних з DeFi , та посилення транскордонної співпраці та обміну інформацією між регуляторами. Лише спільні та скоординовані зусилля дозволять побудувати надійну систему захисту фінансової системи ЄС від злочинних посягань у сфері криптоактивів.

Висновки:

- **Посилення процесу авторизації як ключового "фільтра" ризиків.** Процес надання авторизації за MiCA не повинен бути формальністю, особливо для компаній, які раніше мали проблеми з дотриманням вимог ПВК/ФТ ("legacy issues"). Національні наглядові органи зобов'язані ретельно перевіряти всю попередню наглядову історію заявника, включно з інформацією від регуляторів інших країн, і відмовляти в авторизації до повного усунення виявлених недоліків. Це критично важливо для запобігання "паспортизації" ризиків по всьому ЄС.
- **Необхідність комплексного нагляду за групами та пов'язаними особами.** Наглядові органи повинні вийти за межі аналізу окремої ліцензованої компанії та проводити цілісну оцінку всієї групи, до якої вона входить. Це включає ідентифікацію та аналіз усіх пов'язаних структур, навіть тих, що зареєстровані за межами ЄС, з метою виявлення прихованих впливів, ризиків від непрозорого аутсорсингу та складних схем власності.
- **Впровадження проактивного моніторингу для виявлення нерегульованої діяльності.** З огляду на спроби компаній працювати "в тіні" або використовувати регуляторні лазівки, компетентні органи мають запровадити стратегії активного ринкового нагляду. Для цього необхідно використовувати сучасні інструменти, такі як аналітика блокчейну, аналіз великих даних та міжнародний обмін розвідувальною інформацією, щоб своєчасно виявляти та припиняти діяльність неавторизованих постачальників послуг.
- **Фокус на якості комплаєнс-функції та управлінні технологічними ризиками.** Наглядовим органам слід приділяти пильну увагу якості комплаєнс-функції в компаніях, перевіряючи її незалежність, достатність ресурсів та компетентність персоналу, особливо в умовах високої плинності кадрів. Компанії також повинні продемонструвати здатність адаптувати свої системи управління ризиками до нових технологій, зокрема розробити чіткі механізми контролю за ризиками, пов'язаними з взаємодією з децентралізованими фінансами (DeFi).

Звіт про підходи компетентних органів до нагляду за діяльністю банків в контексті ПВК/ФТ [2]

Фінальний звіт ЕВА про підходи компетентних органів до нагляду за банками у сфері ПВК/ФТ являє собою важливий звіт, що підсумовує шість років (2018–2024) оцінки ефективності підходів

[2] https://www.eba.europa.eu/sites/default/files/2025-10/1a7ab0a0-6c60-497d-bdb1-cb3b4d507a56/EBA%20Final%20report%20on%20Implementation%20Reviews.pdf

40 національних компетентних органів у боротьбі з ризиками ВК/ФТ у банківському секторі ЄС/ЄЕЗ.

Основна мета цього звіту, полягала у наданні деталізованого, актуального огляду стану нагляду у сфері ПВК/ФТ в ЄС. Цей огляд також слугує основою для майбутнього непрямого нагляду, який здійснюватиме новий Орган ЄС з питань боротьби з відмиванням коштів (AMLA). Правовою основою для цих оглядів було зобов'язання ЕВА забезпечувати ефективні та послідовні наглядові практики та сприяти запобіганню використання фінансової системи ЄС для цілей ВК/ФТ. Оцінка була орієнтованою на виявлення сфер для покращення та підтримку зусиль компетентних органів. Звіт фокусується на прогресі, досягнутому ними у сферах нагляду та співпраці.

Щодо аспектів нагляду ПВК/ФТ, компетентні органи (КО) зробили значні кроки для зміцнення своїх підходів, зокрема, зробивши їх більш ризик-орієнтованими. Більшість КО тепер мають наглядові стратегії, причому 71% тих, хто їх не мав під час огляду, вже запровадили стратегії. КО також посилили свої наглядові плани, приділяючи більше уваги використанню оцінок ризиків на рівні суб'єктів для вибору наглядових інструментів та забезпечуючи координацію планів ПВК/ФТ з пруденційними наглядовими органами. Крім того, усі органи тепер мають наглядовий посібник або працюють над ним, і 81% переглянули свої посібники з огляду на рекомендації ЕВА, щоб забезпечити послідовність застосування інструментів та суджень. КО зробили значний прогрес у більш стратегічному та ефективному використанні наглядових інструментів, відходячи від опори лише на один інструмент, незалежно від наглядових цілей, а 90% компетентних органів з зауваженнями щодо інтрузивності переглянули свій підхід, наприклад, використовуючи аналітичні інструменти. Однак, незважаючи на загальне покращення, для суттєвої меншості КО все ще потрібен більший прогрес у повній відповідності стратегій керівним принципам ЕВА щодо ризик-орієнтованого нагляду, а також у посиленні наглядових посібників.

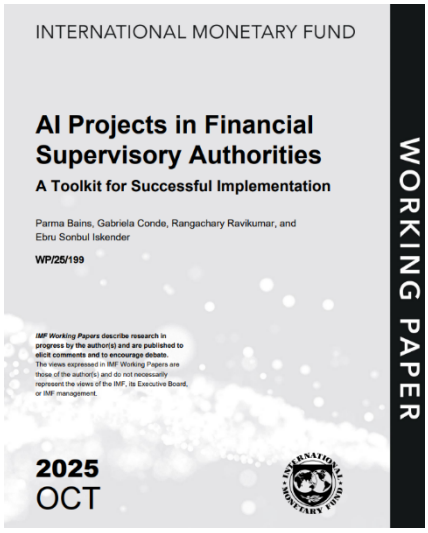
У сфері співпраці КО доклали значних зусиль для зміцнення координації та обміну інформацією. На внутрішньому рівні КО покращили співпрацю з відповідними державними органами, включаючи ПФР та податкові органи, часто формалізуючи її через Меморандуми про взаєморозуміння (МоВ). Однак, майже половина всіх КО все ще недостатньо ефективно використовує наявні канали співпраці на практиці. Співпраця з пруденційними наглядовими органами залишається критичним аспектом: більшість КО, яких критикували за неефективну співпрацю, доклали зусиль для створення ефективних каналів, включаючи уточнення правил співпраці у внутрішніх посібниках або впровадження нових навчальних програм для пруденційних наглядачів. Проте прогрес залишається обмеженим серед майже половини КО. На міжнародному рівні КО досягли значного прогресу у налагодженні ефективної комунікації зі своїми колегами в інших юрисдикціях, зокрема через використання коледжів ПВК/ФТ як ефективного інструменту для обміну інформацією та координації. Проте двостороння співпраця з органами третіх країн все ще є складнішою, навіть якщо КО досягли прогресу і в цій галузі.

Незважаючи на загальне покращення, КО стикалися з низкою викликів, які гальмували зусилля з реформування. До них належать дефіцит персоналу та бюджетні обмеження, особливо з огляду на зростаючу складність ризиків та необхідність нових знань (наприклад, у сфері послуг криптоактивів). Також значні зміни у правовій та інституційній рамці ЄС щодо ПВК/ФТ вимагають перерозподілу ресурсів, іноді затримуючи внутрішні реформи. Геополітична невизначеність і зростаючий спектр обмежувальних заходів ЄС створили додаткову наглядову складність. У висновку, інформація, надана НКО, свідчить про загальне підвищення ефективності нагляду ПВК/ФТ та співпраці, що полегшить впровадження нового пакета ПВК/ФТ та підтримає роботу AMLA.

Висновки:

- **Посилення наглядової документації та інструментів:** НКО повинні забезпечити, щоб їхні наглядові стратегії та посібники були деталізованими, чітко артикулювали покриття ризиків по секторах та містили конкретні вказівки щодо оцінки ефективності контролю банків у сфері ПВК/ФТ, включаючи застосування цільового тестування та надійного відбору проб.
- **Інтеграція ПВК/ФТ у пруденційний нагляд (SREP):** Необхідно інституціоналізувати міцну співпрацю між пруденційними та ПВК/ФТ наглядовими органами, включно з чіткими методологіями для інтеграції ризиків ВК/ФТ у Процес наглядового огляду та оцінки (SREP) та забезпеченням обов'язкового, цільового навчання ПВК/ФТ для пруденційних наглядачів.
- **Формалізація внутрішнього обміну інформацією:** НКО мають підвищити ефективність співпраці з ПФР, податковими та правоохоронними органами шляхом впровадження МоВ, регулярних та структурованих зустрічей на різних рівнях, а також створення специфічних IT-інструментів для систематичного обміну інформацією.
- **Сфокусоване використання ресурсів та міжнародна співпраця:** Необхідно оперативно усунути брак персоналу та бюджетні обмеження. У міжнародному контексті, НКО повинні зміцнювати двосторонню співпрацю та підписання угод (МоВ) з органами третіх країн, забезпечуючи надійний нагляд за іноземними філіями у своїх державах-членах.

Проекти штучного інтелекту в органах фінансового нагляду. Інструментарій для успішного впровадження [3]



Документ є методичним посібником, розробленим фахівцями МВФ для фінансових наглядових органів, що планують упровадження технологій штучного інтелекту (AI) у своїй діяльності. Його головна мета — надати практичний інструментарій для безпечної, ефективної та етичної інтеграції AI у процеси нагляду, забезпечуючи баланс між інноваціями, ризик-менеджментом і стратегічними цілями організації.

Документ підкреслює, що зростаюча цифровізація фінансового сектору — включно з використанням великих даних, хмарних сервісів і генеративних моделей AI (GenAI) — вимагає від наглядових органів постійного оновлення інструментарію. Використання AI може посилити ефективність ризик-орієнтованого нагляду через автоматизацію обробки даних,

[3] https://www.imf.org/en/Publications/WP/Issues/2025/10/03/AI-Projects-in-Financial-Supervisory-Authorities-570625

виявлення підозрілих транзакцій, аналіз корпоративного управління та підвищення якості пруденційного, ПВК/ФТ та поведінкового нагляду. Приклади практичного застосування включають: використання AI Банком Англії для прогнозування фінансових криз, ЄЦБ — для автоматизованого аналізу анкет «fit and proper», та Комісією з цінних паперів Малайзії — для контролю корпоративного управління компаній.

Автори виділяють основні виклики для впровадження AI у державному секторі: обмежені ресурси та фахівці, несумісність застарілих IT-систем, складність закупівельних процедур, ризики дискримінації та відсутність достатньої пояснюваності моделей. Водночас наголошується на потребі побудови AI governance framework — багаторівневої системи управління з чітко визначеними ролями, відповідальністю, механізмами прозорості, контролем етичності та дотриманням законодавства про захист даних (зокрема GDPR). У фокусі — чотири принципи:

- Структура відповідальності (accountability) за результати моделей.
- Людський контроль у контурі рішень (human-in-the-loop).
- Операційне управління з урахуванням життєвого циклу моделей.
- Прозора комунікація із зацікавленими сторонами.

Велика увага приділяється data governance, яка є основою надійності AI. Вона охоплює політики збору, обробки, зберігання, безпеки та знищення даних, вимоги до якості, метаданих і відповідності зовнішнім стандартам (BCBS 239, ISO, GDPR). Також підкреслюється важливість кіберзахисту, управління ризиками третіх сторін (third-party risk management) і використання майбутніх міжнародних стандартів, зокрема ISO/IEC 27090 щодо кібербезпеки в AI.

Документ пропонує методологію CRISP-DM, адаптовану для проєктів AI, із шістьма фазами.

1. Project Foundation (Формування основ проєкту)

Ця фаза визначає стратегічні підвалини всього проєкту.

Команда формулює бізнес-ціль, яка має безпосередньо сприяти ефективності певного аспекту нагляду (наприклад, ліцензування, макропруденційний аналіз). Тут встановлюються ключові показники ефективності (KPI), які дозволять виміряти успіх — наприклад, скорочення часу обробки звітів або підвищення точності виявлення ризиків.

Також здійснюється оцінка ризиків і ресурсів: людських (наявність аналітиків, дата-саєнтистів, IT-фахівців), технічних (інфраструктура, обчислювальні потужності, безпека), та організаційних (готовність керівництва, культура інновацій).

У цій фазі готується детальний проєктний план, який містить:

- чітке визначення проблеми, яку вирішує AI;
- цілі, очікувані результати, метрики успіху;
- аналіз викликів — нестачі даних, кіберризиків, бюрократичних обмежень;
- план комунікації і залучення стейкхолдерів.

Фаза завершується узгодженням проєктного бачення, обсягу, графіку і ресурсів.

2. Data Understanding (Розуміння даних)

Мета цієї фази — визначити, які дані потрібні для розв’язання бізнес-проблеми, оцінити їхню якість, доступність і законність використання.

Аналітики і дата-інженери:

- ідентифікують внутрішні та зовнішні джерела даних (регуляторна звітність, відкриті джерела, публічні реєстри, веб-скрапінг тощо);

- проводять попередній аналіз (EDA): опис структури, розподілу, виявлення пропусків, кореляцій, аномалій;
- оцінюють ризики конфіденційності — особливо при роботі з персональними або чутливими даними (наприклад, використання даних банківських клієнтів).

У документі наголошується, що важливо створювати єдине сховище даних (data repository) для усунення "силоїзації" даних і забезпечення узгодженості та доступності.

Додатково застосовуються інструменти анонімізації, псевдонімізації або data masking для дотримання вимог GDPR та інших регуляторних актів.

Результатом фази є підготовлений опис джерел і характеристик даних, що стануть основою наступних етапів.

3. Data Preparation (Підготовка даних)

Це найтрудомісткіша фаза, у якій відбувається створення "чистого" датасету для побудови моделі.

Дії включають:

- очищення — усунення помилок, дублікатів, пропущених або некоректних значень;
- нормалізацію та уніфікацію форматів (наприклад, дати, валюти, коди країн);
- feature engineering — створення нових змінних із наявних (наприклад, середнє значення по рахунках клієнта, індекси ризику, зв’язки між об’єктами);
- інтеграцію даних із різних джерел для отримання комплексної картини;
- форматування — приведення структури даних до вимог конкретного алгоритму (наприклад, числове кодування категоріальних змінних).

Усі кроки документуються для забезпечення відтворюваності, прозорості та аудиту.

4. Modeling (Побудова та навчання моделей)

На цьому етапі дата-саєнтисти будують моделі AI, здатні вирішувати визначену бізнес-проблему.

Залежно від завдання обираються різні підходи:

- кластеризація — для групування схожих клієнтів або транзакцій;
- регресія — для прогнозів (наприклад, ймовірність дефолту);
- класифікація — для виявлення підозрілих операцій;
- текстовий аналіз (NLP) — для обробки документів або звітів;
- часові ряди — для прогнозування ризиків або трендів.

Моделі тренуються і тестуються на різних підмножинах даних (training / validation / test sets) із використанням методів cross-validation, bootstrap або stratified sampling, щоб уникнути переобучення.

Особлива увага приділяється балансуванню між точністю та пояснюваністю (explainability): надто складні моделі (наприклад, глибокі нейромережі) можуть бути ефективними, але важко інтерпретованими для регулятора.

Також рекомендується будувати "challenger models" — альтернативні моделі для перевірки надійності результатів і виявлення потенційних помилок або упереджень.

5. Evaluation (Оцінювання)

Фаза оцінювання перевіряє, наскільки побудована модель відповідає бізнес-цілям, технічним вимогам і етичним принципам.

Проводиться подвійна перевірка:

1. Технічна — оцінка точності, стабільності, помилки прогнозу за допомогою метрик (accuracy, precision, recall, RMSE тощо).
2. Функціональна / етична — перевірка на відсутність дискримінації, дотримання принципів чесності (fairness) та прозорості.

Для цього використовуються метрики виявлення упередженості: Disparate Impact, Statistical Parity Difference, Equality of Opportunity, Predictive Equality, Calibration тощо. Також застосовуються методи пояснення результатів — LIME, SHAP, Shapley values — для розуміння, які змінні найбільше впливають на рішення моделі.

Рівень деталізації пояснення залежить від аудиторії: технічний персонал потребує глибокого розбору, тоді як керівництву достатньо зрозумілих візуалізацій і ключових висновків.

На завершення ухвалюється рішення: модель схвалюється до впровадження, повертається на доопрацювання або відхиляється.

6. Deployment (Впровадження та моніторинг)

Остання фаза охоплює інтеграцію моделі в наглядову IT-інфраструктуру, перевірку стабільності й створення системи моніторингу.

Основні дії:

- визначення користувачів (інспектори, аналітики, керівники) та сценаріїв використання моделі;
- забезпечення зручного доступу через дашборди, API чи внутрішні портали;
- перевірка інтеграції з іншими наглядовими системами (наприклад, реєстрами, звітними базами, AML-системами);
- розробка плану підтримки та оновлення — моніторинг точності, виявлення деградації моделі, періодичне перенавчання;
- документування всіх кроків, обмежень, припущень та відповідальних осіб.

Для важливих моделей (наприклад, стрес-тестування або прогноз системних ризиків) створюється реєстр моделей (model inventory) з описом призначення, валідації, дати перевірки, ризиків і рішень щодо розгортання.

Також проводиться підсумковий "lessons learned review" — аналіз помилок, успішних рішень і рекомендацій для майбутніх проєктів.

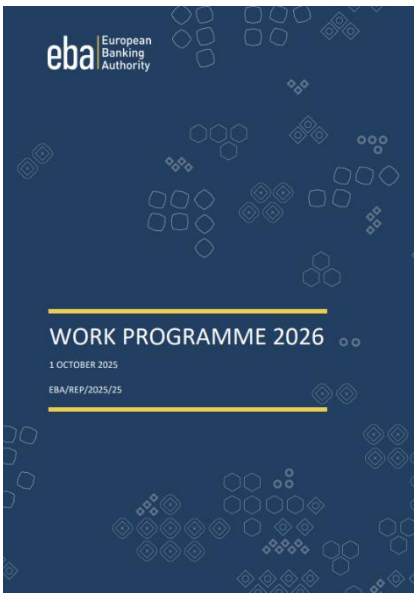
Підкреслено, що управління проєктами AI має бути гнучким, з використанням принципів DevOps / MLOps, які забезпечують безперервне тестування, автоматизацію, контроль якості та швидку адаптацію до змін. Команда проєкту повинна бути мультидисциплінарною — включати бізнес-аналітиків, дата-саєнтистів, інженерів AI, юристів і фахівців з етики.

Висновки:

- **Інституційна готовність:** перед впровадженням AI органи нагляду повинні створити чітку систему AI governance і data governance, що охоплює життєвий цикл моделей, права доступу до даних, аудит, безпеку й етичність.
- **Гнучке управління проєктами:** необхідно переходити від «Waterfall» до Agile / MLOps методологій, які дають змогу поступово вдосконалювати моделі, швидко реагувати на ризики та залучати міжвідомчі команди.
- **Пояснюваність і відсутність упереджень:** усі моделі мають проходити тестування на упередженість, чесність і пояснюваність, із використанням зрозумілих метрик та регулярного моніторингу.
- **Розбудова спроможностей:** пріоритет — розвиток аналітичних компетенцій у персоналу, створення кар'єрних траєкторій для фахівців із даних, модернізація IT-інфраструктури та партнерство з академічними й технологічними інституціями.

Завершальна частина документа наголошує, що запровадження AI сприяє підвищенню ефективності нагляду, покращує управління даними й моделями, а також зміцнює спроможність органів нагляду оцінювати якість управління ризиками в підзвітних установах. Водночас, для досягнення результатів необхідно інвестувати у навчання персоналу, створювати аналітичні кар'єрні шляхи, модернізувати IT-інфраструктуру та забезпечити довіру до рішень AI через прозорість і підзвітність.

Робоча програма EBA 2026: стратегічна трансформація європейського банківського нагляду — від регулятора до технологічного центру фінансової стійкості ЄС [4]



Документ є стратегічним планом діяльності Європейського банківського органу (EBA), який визначає ключові напрями політики, наглядові пріоритети та операційні завдання на 2026 рік у межах Єдиного програмного документа (SPD) на 2026–2028 роки. Його ухвалення знаменує початок нового етапу у функціонуванні EBA після передачі повноважень у сфері протидії відмиванню коштів і фінансуванню тероризму до новоствореного Європейського органу з питань протидії відмиванню коштів (AMLA). Таким чином, 2026 рік стане поворотним моментом для EBA, адже у фокусі залишаться традиційні напрями — розробка регуляторної політики, забезпечення наглядової конвергенції та аналіз фінансових ризиків, але водночас розпочнеться повноцінне виконання нових функцій із нагляду та валідації, передбачених регламентами DORA, MiCA та EMIR 3.

Згідно з програмою, діяльність EBA у 2026 році базуватиметься на трьох стратегічних пріоритетах: розвиток єдиного європейського зводу правил (Single Rulebook), вдосконалення аналітичних і наглядових спроможностей у сфері ризик-менеджменту, а також зміцнення технологічної стійкості та інноваційного потенціалу фінансової системи. У першому напрямі EBA прагне забезпечити простіший, пропорційніший і водночас стійкий до криз регуляторний ландшафт, який сприятиме ефективності єдиного фінансового ринку ЄС. Орган готує масштабне спрощення нормативно-правової бази відповідно до рекомендацій Робочої групи з питань ефективності (TFE), що передбачає зниження регуляторного навантаження, зменшення обсягів звітності щонайменше на 25 %, усунення дублювання вимог і створення єдиного публічного репозиторію даних. Водночас планується поглиблення принципу пропорційності у процесі нагляду через оновлення Керівних настанов з процесу SREP і стимулювання післяфактової конвергенції замість суто попередньої гармонізації норм. Одним із головних напрямів залишиться імплементація Європейського банківського пакету реформ (CRR III/CRD VI), включно з роботою над визначенням вимог до капіталу за кредитними, операційними та ринковими ризиками, а також удосконалення підходів до оцінки ризиків у рамках IRB-моделей. Крім того, EBA активно готуватиметься до впровадження оновленої платіжної архітектури ЄС (PSD3, PSR, FIDA), що об'єднує понад 50 нових мандатів у сфері платіжних послуг, відкритого банкінгу, доступу до фінансових даних і споживчого захисту. Також у 2026 році розпочнеться реалізація Рамкової системи ЄС з управління банківськими кризами та гарантуванням вкладів (CMDI framework) — нового циклу зобов'язань у межах директив BRRD і DGSD, який стосується

[4] https://www.eba.europa.eu/sites/default/files/2025-10/b9fe2713-117b-440f-aae0-bdcb8832c3e0/EBA%20Work%20programme%202026.pdf

раннього втручання, розрахунку внесків до фондів гарантування вкладів і посилення прозорості у сфері врегулювання банків.

Другий пріоритет («Оцінка ризиків») спрямований на зміцнення здатності EBA здійснювати ефективний аналіз, нагляд та оцінку ризиків у банківському секторі. У 2026 році орган готується до масштабної підготовчої фази Загальноєвропейського стрес-тестування банків 2027, яке включатиме нові модулі, зокрема з оцінки кліматичних ризиків (перехідних і фізичних), а також впливу небанківських фінансових установ (NBFI) на стабільність фінансової системи. Заплановано оптимізацію методології, уніфікацію форматів звітності зі стрес-тестами та скорочення витрат на їх проведення шляхом інтеграції з наглядовою звітністю. Значну увагу буде приділено впровадженню нових інституційних функцій — нагляду за критичними ІКТ-провайдерами (CTPP) відповідно до DORA, нагляду за емітентами криптоактивів згідно з MiCA, а також створенню централізованої функції валідації моделей початкової маржі у межах EMIR 3. Ці кроки свідчать про перетворення EBA з регулятора на наднаглядовий технологічний центр ЄС. У сфері кібербезпеки EBA разом з іншими європейськими наглядовими органами (ESMA, EIOPA) розвиватиме пан'європейську систему реагування на кіберінциденти EU-SCICF, що забезпечить координацію у разі системних атак. Паралельно триватиме розвиток єдиної інтегрованої звітності, гармонізованої з ЄЦБ та національними органами, із застосуванням уніфікованих глосаріїв, стандартизованих даних і нової архітектури Data Point Model 2.0 (DPM Studio). Ключовим елементом аналітичної інфраструктури стане платформа EUCLID, яка об'єднає нові набори даних — від ESG та миттєвих платежів до інформації, пов'язаної з DORA і MiCA, що забезпечить більш повне охоплення фінансового сектору.

Третій пріоритет («Інновації») відображає поступ ЄС до цифрової трансформації фінансових послуг і посилення спроможності регуляторів та ринку до технологічних змін. EBA приділяє особливу увагу моніторингу інновацій у сферах штучного інтелекту (AI), машинного навчання, розподілених технологій реєстру (DLT) та криптоактивів, а також розвитку фінансових технологій, що змінюють бізнес-моделі банків. У 2026 році EBA головуватиме у Європейському форумі механізмів сприяння інноваціям (EFIF), забезпечуючи платформу для діалогу між наглядовими органами, технологічними компаніями та фінансовими установами. Орган також братиме активну участь у реалізації AI Act, оцінюючи його вплив на банківський і платіжний сектори, формуючи методології для аналізу ризиків, пов'язаних із використанням моделей загального призначення (GPAI), і вивчаючи залежності між банками та провайдерами AI-рішень. У сфері криптоактивів EBA продовжить моніторинг DeFi-проєктів, моделей під власним брендом та BigTech-компаній, які поступово інтегруються у фінансовий сектор, а також здійснюватиме

Висновки:

- **EBA переходить від створення правил до контролю їх виконання.** Основна увага зміщується з нормативної розробки (післяфактова) до перевірки ефективності нагляду (попередня), що означає посилення контролю за реальними практиками банків і регуляторів у країнах-членах ЄС.
- **Початок нагляду за критичною цифровою інфраструктурою.** Створюється спільна система нагляду ESA за великими IT-постачальниками (CTPP) відповідно до DORA, що зробить фінансову систему ЄС менш вразливою до кібератак і технічних збоїв.
- **Уніфікація даних і прозорість звітності.** Впровадження EUCLID 2.0 і DPM 2.0 забезпечить інтегровану звітність і скорочення дублювання даних на 25%, що зменшить адміністративне навантаження на банки.
- **Регуляторна увага до фінансових інновацій.** Через EFIF і MiCA EBA формує європейську політику цифрового фінансового нагляду — від криптоактивів і DeFi-платформ до застосування штучного інтелекту у фінансових сервісах.

аналітику щодо ролі цифрового євро та комерційних токенів у платіжній екосистемі. Окремий блок присвячено захисту споживачів — боротьбі з надмірною заборгованістю, протидії де-рискінгу та запобіганню шахрайству у платіжних системах. EBA планує розробити дорожню карту для імплементації оновленої Директиви про споживче кредитування (CCD2), удосконалити індикатори роздрібних ризиків, оновити базу національних ініціатив з фінансової освіти та разом з AMLA розробити спільні керівні настанови з питань де-рискінгу до 2027 року.

Організаційно структура EBA у 2026 році охоплюватиме сім основних напрямів діяльності: розробка політики, наглядова конвергенція, аналіз ризиків і фінансової стабільності, безпосередній нагляд, управління даними, врядування та операційна підтримка. Загальний бюджет становитиме приблизно 66,5 млн євро, а чисельність персоналу — 274 особи, з яких частина фінансуватиметься за рахунок внесків галузі (DORA, MiCA, EMIR). Водночас після передачі функцій у сфері ПВК/ФТ EBA втратить 8 штатних посад. Основними пріоритетами залишатимуться впровадження цифрових рішень, зокрема систем EUCLID, EDAP і DPM 2.0, розвиток аналітичних платформ на базі штучного інтелекту, а також посилення кібербезпеки та внутрішнього управління ризиками.

Таким чином, програма EBA на 2026 рік фіксує перехід регулятора до нового рівня функціонування — від законодавчого координатора до багаторівневого наднаглядового органу, який поєднує аналітичну, технологічну та споживчу складові. Вона покликана не лише забезпечити стабільність і цілісність європейської фінансової системи, а й створити більш ефективне, цифрове та інноваційно спроможне середовище, у якому фінансові установи діятимуть у гармонізованому правовому полі з мінімальним адміністративним тиском і водночас підвищеною наглядовою відповідальністю.

Новий підхід DFSA до крипторинку: прозорість, гнучкість та посилений нагляд за стейблкоїнами [5]

Консультаційний документ (CP 168) Управління фінансових послуг Дубаю (DFSA) є одним із найважливіших етапів еволюції нормативного регулювання криптоактивів у межах Міжнародного фінансового центру Дубаю (DIFC). Цей документ представляє системне оновлення регуляторного підходу до діяльності з криптотокенами, спрямоване на досягнення балансу між інноваційним розвитком ринку цифрових активів і забезпеченням фінансової стабільності, захисту інвесторів та дотримання міжнародних стандартів у сфері протидії відмиванню коштів і фінансуванню тероризму (ПВК/ФТ). DFSA у цьому документі пропонує глибоку реформу існуючої системи, засновану на міжнародному досвіді, результатах власного нагляду, попередніх консультаціях (зокрема CP143 від 2022 року, CP150 від 2023 року та CP153 від 2024 року) та активному зворотному зв'язку від учасників ринку.

У преамбулі документу регулятор пояснює, що після двох років дії режиму криптотокенів (запровадженого 2022 року) накопичено достатньо досвіду, щоб здійснити перехід від централізованої моделі, коли DFSA самостійно визнавала ті чи інші токени придатними до

5 https://dfsaen.thomsonreuters.com/sites/default/files/net_file_store/CP_168_Enhancements_to_the_regulation_of_Crypto_okens.pdf

використання, до моделі підзвітності учасників ринку. Відтепер саме ліцензовані фірми нестимуть відповідальність за проведення оцінки придатності криптотокенів, документування цього процесу, постійний моніторинг і публічне розкриття результатів. DFSA залишає за собою наглядові повноваження, але переносить операційну відповідальність на суб'єктів ринку, чим фактично реалізує ризик-орієнтований, пропорційний і гнучкий підхід до регулювання. Такий крок відповідає сучасним тенденціям у Європейському Союзі (після ухвалення Регламенту MiCA), у Великій Британії (модель FCA для криптоактивів) та Сінгапурі (режим MAS для DPTs).

У документі детально описується перехід від режиму «Визнаних криптотокенів» до режиму «Придатних криптотокенів». DFSA більше не створюватиме перелік «визнаних» токенів (за винятком стейблкоїнів), а покладає на кожну компанію обов'язок самостійно визначати, які криптотокени вона вважає придатними для використання у своїй діяльності. Таке рішення має під собою декілька підстав: по-перше, міжнародні регулятори дедалі частіше відходять від централізованих «білих списків» через швидку динаміку ринку, появу нових технологій і високий рівень ризику маніпуляцій; по-друге, DFSA прагне зменшити адміністративне навантаження та забезпечити більшу гнучкість для учасників фінансового ринку DIFC; по-третє, зосередження на підзвітності фірм дає змогу DFSA зосередитись на наглядовій, а не дозвільній функції.

Сама процедура оцінки придатності має ґрунтуватися на п'яти ключових критеріях, визначених у документі: прозорість і корпоративне управління криптотокена (його цілі, структура, засновники); регуляторний статус у інших юрисдикціях і наявність попереднього схвалення з боку інших фінансових регуляторів; розмір, ліквідність і торгову історію ринку цього токена; технологічні параметри (DLT-інфраструктура, безпечність, стійкість); а також відповідність токена чинному законодавству DIFC та вимогам DFSA, зокрема щодо ПВК/ФТ. Компанії повинні документально підтверджувати обґрунтованість свого висновку, постійно моніторити зміни ринку, ризики та інформаційні події, які можуть вплинути на статус токена, і негайно припиняти операції з ним, якщо він більше не відповідає критеріям придатності. Результати оцінки підлягають оприлюдненню на офіційному вебсайті фірми із зазначенням назви, тікера токена та технологічної мережі, на якій він функціонує. Таким чином, DFSA створює саморегулювальний механізм ринкової прозорості, який водночас дозволяє швидко реагувати на динаміку цифрових активів.

Окремий розділ CP168 присвячений фіатним криптотокенам, тобто стейблкоїнам, які мають прив'язку до фіатної валюти. DFSA визнає, що такі токени відіграють дедалі більшу роль у розрахунках, децентралізованих фінансах та транскордонних платежах, але водночас створюють системні ризики — зокрема ризик відтоку капіталу з національних валют, підрив монетарного суверенітету та зростання вразливостей у сфері ПВК/ФТ. Відповідно, DFSA залишає за собою право самостійно визначати, які фіатні токени є придатними до використання у DIFC. Для цього буде оприлюднено офіційне регуляторне роз'яснення із переліком схвалених токенів та критеріями оцінки (зокрема щодо достатності резервів, їхньої ліквідності, диверсифікації, проведення незалежного аудиту, відповідності банків і зберігачів міжнародним стандартам FATF у сфері ПВК). Таким чином, на ринку DIFC запроваджується дворівнева модель: повна децентралізація для звичайних криптотокенів і централізований контроль для стейблкоїнів.

Важливою частиною реформи є також скасування концепції «Визнані юрисдикції» щодо криптоактивів. Це дозволяє суб'єктам ринку залучати партнерів і контрагентів із ширшого кола юрисдикцій, не обмежуючись попередньо визначеним DFSA списком. Регулятор обґрунтовує це тим, що глобальна гармонізація правил (FATF, IOSCO, FSB, ЄС) уможливила відхід від територіальної сегментації.

Ще одне ключове нововведення стосується діяльності інвестиційних фондів. У CP143 DFSA обмежувала участь фондів у крипторинку (наприклад, забороняла куруючому, який

зареєстрований і ліцензований DIFC управляти зовнішніми фондами з криптоактивами та встановлювала ліміт у 30 % загальної вартості активів кваліфікованого інвестиційного фонду). Тепер ці пороги знімаються. Фонди, що діють у DIFC або за його межами, можуть інвестувати у криптотокени без кількісних обмежень, за умови належного проведення оцінки придатності токенів. Це відкриває шлях до інтеграції криптоактивів у структури традиційного управління активами, але зберігає вимоги до прозорості, кастодіальних послуг, обмеження боргового навантаження та належного розкриття ризиків.

DFSA також пропонує зміни до правил ведення бізнесу (COB Rules). Зокрема, вимога надавати документ з основними характеристиками більше не поширюватиметься на тих, хто лише організовує чи надає послуги зі зберігання токенів, адже ця вимога має сенс лише на етапі залучення інвестора, а не при зберіганні. Крім того, регулятор скасовує обмеження на частку криптоактивів, що можуть враховуватися під час визначення статусу професійного клієнта. Це відображає визнання криптоактивів як повноцінного класу активів у приватному банкінгу, дозволяючи клієнтам із великими криптопортфелями відповідати вимогам професійного інвестора.

У частині звітності DFSA запроваджує щомісячний обов'язок подавати звіти про криптотокени через електронний портал протягом 14 днів після закінчення звітного місяця. Звіт повинен містити інформацію про перелік токенів, оцінених як придатні, обсяги операцій, кількість клієнтів, види діяльності та випадки, коли токен було визнано непридатним. Неподання або несвоєчасне подання звіту тягне за собою накладення фіксованого штрафу. Цей механізм створює для DFSA можливість постійного моніторингу ринку, ідентифікації тенденцій, виявлення ризиків фінансової стабільності та забезпечення оперативного наглядового реагування.

Висновки:

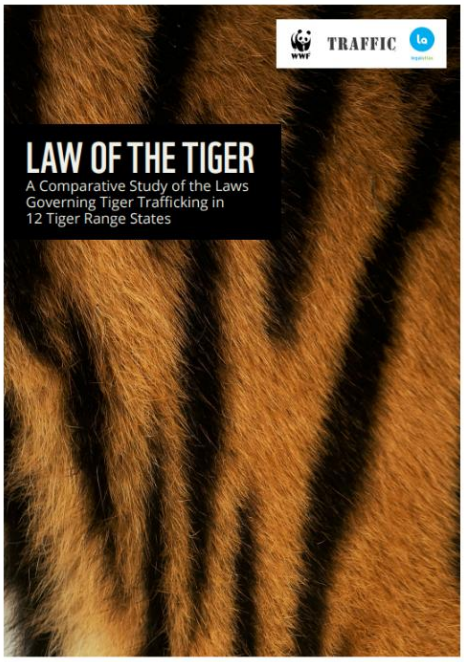
- **Децентралізація регуляторної відповідальності.** DFSA передає суб'єктам ринку обов'язок самостійно визначати придатність токенів (крім стейблкоїнів), водночас вимагаючи документального підтвердження та публічності оцінок.
- **Посилення нагляду за фіатними криптотокенами.** Стейблкоїни залишаються під прямим регуляторним контролем DFSA, із суворими вимогами до резервів, аудиту та відповідності ПВК/ФТ, що відображає глобальний тренд після Звіту Банку міжнародних розрахунків (BIS) 2025 року.
- **Лібералізація фондів і приватного інвестування.** Скасування лімітів на частку криптоактивів у фондах сприятиме притоку інституційних інвесторів, але вимагає зрілих механізмів ризик-менеджменту та контролю за зберіганням активів.
- **Регулярна звітність і підвищена підзвітність.** Запровадження щомісячної звітності дозволить DFSA моніторити ринок у режимі реального часу, швидше виявляти ризики ПВК/ФТ, ринкові зловживання та системні загрози.

Окремий розділ документа визначає перехідні положення. Для токенів, які вже були визнані DFSA (наприклад, Bitcoin, Ethereum, Litecoin), передбачено тримісячний перехідний період, протягом якого вони автоматично вважаються «придатними». Після цього строку компанії повинні провести власну оцінку й оприлюднити результати. У цей час також дозволяється оцінювати нові токени для включення до списку придатних. Після завершення перехідного періоду DFSA видалить свій попередній перелік визнаних токенів із вебсайту, остаточно закріплюючи новий принцип самостійного визначення придатності.

Загалом Консультаційний документ 168 формує нову нормативну філософію DFSA — перехід від жорсткої централізованої моделі до моделі підзвітного саморегулювання, де основну роль відіграють внутрішні системи управління ризиками, політики комплаєнсу та корпоративна відповідальність ліцензованих суб'єктів. DFSA демонструє

готовність підтримувати інновації у сфері цифрових активів, не жертвуючи при цьому ключовими принципами фінансової безпеки, стабільності та захисту інвесторів. Цей документ можна вважати зразком зрілого регуляторного підходу, який об'єднує ризик-орієнтоване регулювання, елементи довіри до професійних учасників ринку та системний контроль за стабільними токенами, що можуть мати макрофінансовий вплив. CP168 також чітко сигналізує прагнення DIFC бути однією з провідних глобальних юрисдикцій для розвитку криптофінансових послуг, створюючи інституційне середовище, яке підтримує інновації в межах прозорих і відповідальних правил гри.

Закон джунглів: глобальна боротьба з торгівлею тиграми [6]



Торгівля тиграми — це не просто кримінальний бізнес, це один із найбільш цинічних проявів глобальної деградації системи охорони дикої природи. Аналітичне дослідження, підготовлене Всесвітнім фондом дикої природи (WWF) та Глобальною мережею моніторингу торгівлі дикою природою (TRAFFIC), показує глибину цієї кризи через правову призму — країни, що мають спільну мету зберегти тигрів, водночас створили різні, часто суперечливі законодавчі режими, які дозволяють злочинним мережам діяти майже безкарно. Цей документ — це не просто юридичний огляд, а діагноз системі, яка мала б захищати символ Азії, але замість цього сприяє його знищенню.

Сьогодні у дикій природі залишилось менше 4 000 тигрів. Проте в неволі, у приватних розплідниках і «сафарі-парках» по всій Азії, утримуються понад 9 000. Ці заклади позиціонують себе як «центри розведення для збереження виду», але насправді виконують функцію прикриття для торгівлі частинами тіла тварин. Кістки, шкіра, зуби, пазурі та навіть кров — усе має ринкову цінність. Попит, головно з боку споживачів у Китаї, В'єтнамі та Лаосі, підтримується століттями усталеною традицією використання частин тигрів у традиційній медицині та як символів багатства й статусу. Але нині це вже не лише культурне питання, а глобальна економіка злочину, у якій задіяні транснаціональні мережі, фінансові посередники та цифрові торгові майданчики.

Законодавства 12 країн ареалу проживання тигра — від Індії до Малайзії — демонструють величезну нерівномірність. У деяких країнах, як-от Індія чи Непал, торгівля, зберігання та транспортування частин тигра криміналізовані максимально жорстко. У той час як в інших, зокрема в Камбоджі, Лаосі чи М'янмі, закони або нечіткі, або майже не застосовуються. Більше того, у низці держав поняття «торгівля дикою природою» обмежується лише фізичною купівлею-продажем, без урахування онлайн-пропозицій, фінансування чи посередництва. Це створює правовий вакуум, у якому злочинці діють через Telegram, WeChat, TikTok або навіть закриті форуми, пропонуючи частини шкіри, кістки й настоянки. Фактично, цифрова економіка стала новим «ринком», де анонімність і криптоплатежі знімають останні бар'єри для торгівлі.

Дослідження показує, що система контролю за розведенням тигрів у неволі — це головний канал легалізації злочину. Формально такі розплідники мають ліцензії, але в реальності облік тварин є фіктивним. Тигри, які гинуть, не фіксуються у звітах; кістки та частини шкіри продаються

6 https://www.traffic.org/site/assets/files/28945/law_of_the_tiger_a_comparative_study_of_the_laws_governing_tiger_trafficking_in_12_tiger_range_states.pdf

через посередників як «відходи», а деякі заклади використовують схрещення з левами чи іншими видами, щоб створити «гібридів». Оскільки більшість країн не мають правового визначення цих гібридів, частини справжніх тигрів відмиваються через такі «підміни». Це класичний механізм — легальна структура, яка функціонує як фасад для незаконного обороту.

Окрему увагу у звіті приділено відсутності ефективної міждержавної координації. Незважаючи на існування CITES, INTERPOL і регіональних платформ, таких як ASEAN-WEN, обмін даними між країнами практично не працює. Кожна держава діє у своїй юрисдикційній бульбашці, тоді як торгівля тиграми має транскордонний характер: браконьєри вбивають тварин у М'янмі, контрабандисти переправляють їхні тіла через Лаос, а в кінці товар потрапляє до Китаю чи В'єтнаму. У результаті злочинці користуються саме різницею між правовими режимами — де за вбивство тигра передбачене довічне ув'язнення, а за його перевезення через кордон — лише адміністративний штраф. Ця асиметрія підриває саму ідею міжнародного правового порядку у сфері охорони дикої природи.

Дослідження також висвітлює драматичну слабкість фінансового аспекту боротьби з браконьєрством. Лише чотири з дванадцяти держав визнають торгівлю дикою природою предикатним злочином для розслідувань AML/CFT. Це означає, що більшість країн навіть не мають законної підстави для відстеження доходів від цього бізнесу, блокування рахунків чи заморожування активів. А тим часом прибутки від торгівлі тиграми оцінюються у сотні мільйонів доларів щороку — це масштаб, співставний із контрабандою наркотиків або зброї. Без фінансового переслідування високопоставлених учасників схеми правоохоронці залишаються на рівні «ловців браконьєрів», не торкаючись головних бенефіціарів.

Не менш важливою є й проблема збереження доказів і управління конфіскованими трофеями. У більшості країн немає централізованих баз даних, що фіксують вилучені об'єкти. Часто шкіра, кістки або препарати просто зберігаються в місцевих відомствах, де згодом «зникають». У деяких державах (як-от В'єтнам чи Камбоджа) чиновники навіть продавали конфіскованих тигрів "для наукових потреб" — фактично повертаючи їх на чорний ринок. Це показує глибину корупційного розладу в природоохоронних структурах, які самі стали частиною злочинного ланцюга.

Однак головний виклик — не лише в законах, а у ставленні до самої проблеми. Торгівля тиграми розглядається переважно як питання екології або гуманності, хоча насправді це високоприбутковий вид організованої злочинності з транснаціональними зв'язками, офшорами, криптовалютами та системною корупцією. Автори звіту наполягають: лише інтеграція природоохоронних злочинів у політику національної безпеки здатна змінити ситуацію. Це означає створення спеціалізованих підрозділів фінансової розвідки, співпрацю митниць, банків і правоохоронців, запровадження ДНК-паспортизації тварин і обов'язкових баз даних їхніх осіб.

Символічно, що «закон тигра» у цьому контексті — це не просто метафора дикої природи, а

Висновки:

- **Необхідно гармонізувати законодавства країн** ареалу проживання тигра, щоб усунути правові прогалини, які дозволяють контрабандистам переміщати трофеї через «слабкі» юрисдикції.
- **Країнам слід визнати злочини проти дикої природи предикатними** для AML/CFT-розслідувань, аби перекрити фінансові потоки, що живлять торгівлю тиграми.
- **Потрібно створити єдину міжнародну базу даних** ДНК-ідентифікації та обліку тигрів, щоб ефективно відстежувати походження вилучених частин і припиняти їхнє «відмивання».
- **Важливо криміналізувати всі форми онлайн-продажів і посередництва**, адже цифрові платформи стали ключовим каналом торгівлі дикими тваринами.

відображення реальності, у якій виживає сильніший — не хижак, а корупційна система. Звіт показує, що боротьба за тигра — це боротьба за правову державу, за цінність життя і верховенство права. Поки ці країни не зможуть створити прозору, координовану й підзвітну систему, тигр залишатиметься символом не сили, а людської жадібності, прикритої бюрократією. І саме це становить ідею цього документу — не просто про охорону природи, а про цивілізаційний вибір між законом і хаосом, між вигодою та збереженням життя на планеті.

Як організована злочинність використовує прямі іноземні інвестиції [7]

Звіт UNODC розкриває тему «стратегічної інфільтрації криміналу у вразливі юрисдикції через прямі іноземні інвестиції». На прикладі автономного регіону Оекусе-Амбено (RAEOA) у Тимор-Лешті UNODC показує, як складна мережа легальних компаній, офшорних структур, гральних операторів та технологічних провайдерів перетворилася на інфраструктуру для кібершахрайства, торгівлі людьми і відмивання коштів, причому все це відбувалося під маскою привабливих та «інноваційних» проєктів. Те, що виглядало як інвестиційний прорив — готелі, технопарки, ліцензійні ігрові платформи, системи цифрової ідентифікації — виявилося ретельно вибудованим фасадом, який приховав транскордонні кримінальні потоки і дозволив міжнародним бандформуванням закріпитися в державних структурах.

Механіка цієї інфільтрації проста у своїй винахідливості й при цьому технологічна: кримінальні суб'єкти використовують легальні інструменти — реєстрацію компаній, право на іноземні інвестиції, програми громадянства в обмін на інвестиції, державні контракти на цифровізацію — щоб отримати контроль над критичною інфраструктурою. Потім через мережу афілійованих підприємств вони маскують джерела прибутків, освоюють платіжні канали, інколи створюють локальні цифрові екосистеми (локальні мобільні мережі, термінали, Starlink-підключення), які використовуються для координації операцій у віддалених таборах Південно-Східної Азії. Фактично, легальність інструментів дає злочинцям імунітет від негайної підозри: договір на запуск системи цифрової ідентифікації або контракт на побудову готельного комплексу сприймаються як іноземні інвестиції, тоді як насправді вони створюють логістичну базу.

Особливе місце у схемі займають «професійні посередники» — юристи, реєстратори компаній, аудиторські фірми, які забезпечують оформлення корпорацій в кількох юрисдикціях, подачу документів на громадянство, відкриття рахунків і легалізацію угод. Вони або свідомо, або з необережності створюють «корпоративні лабіринти», через які гроші проходять поза контролем національних систем фінансового моніторингу.

Ще одна ключова ризикова ланка — програми «паспортів за інвестиції» і загалом слабке регулювання громадянства та віз. UNODC виявив, що багато ключових фігурантів мали декілька паспортів, іноді отриманих легально через відповідні програми, іноді — внаслідок корупційних схем. Наявність кількох паспортів дозволяє фізичним особам уникати екстрадиції, відкривати рахунки в різних юрисдикціях і швидко переміщувати бізнес у відповідь на міжнародний тиск.

7 https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Alert_Strategic_infiltration_of_vulnerable_jurisdictions_through_criminal_foreign_direct_investments.pdf

Тобто той самий механізм, який повинен залучати інвестиції і таланти, став інструментом «юрисдикційного шопінгу» для криміналу.

Природна слабкість невеликих держав — обмежені людські ресурси, малий регуляторний потенціал, корупційні ризики — у поєднанні з надмірною відкритістю інвестиційних режимів створюють «точку входу» для транснаціональних злочинних мереж. UNODC звертає увагу на те, що інфільтрація не обмежується економікою: кримінальні діяння швидко трансформуються у політичний вплив — через лобіювання, підкуп, маніпуляції громадською думкою й навіть участь у формуванні державних ІТ-проєктів. Коли особи із сумнівним минулим очолюють системи цифрової ідентифікації або відповідають за національні бази даних, ризики витоку персональних даних, їхнього використання для операцій з відмивання або для зовнішнього впливу стають системними.

Глобальна картина показує, що кейс RAEOA — не унікальний: аналогічні сценарії спостерігалися у портових зонах Камбоджі, М'янми та Філіппін, де гральний бізнес, нерухомість і ІТ-проєкти служили ширмою для формування скам-економік. Коли такі схеми закріплюються, процес розплутування вимагає не лише силових заходів, а й масштабних політичних рішень: перегляду інвестиційних правил, систем ліцензування, податкових стимулів і міжнародної співпраці. Адже при наявності транскордонних корпоративних зв'язків і офшорних рахунків один лише локальний арешт активів дає мало результату без узгоджених дій у країнах, де прокладено маршрут «відмивання».

UNODC робить наступний висновок: відповіді мають бути комплексними. Проводити лише операції з арешту обладнання чи закриття готелів — корисно, але цього недостатньо. Необхідно терміново переглянути нормативні рамки, зокрема: посилити процедури due diligence для інвесторів, запровадити обов'язкові перевірки походження коштів для великих інвестиційних проєктів; ввести більш жорсткі вимоги до прозорості бенефіціарів та адміністрування корпорацій; обмежити можливості для мультигромадянства осіб, підозрюваних у фінансових злочинах; інтегрувати природоохоронні, антикорупційні й фінансові органи у швидкісні міжвідомчі механізми реагування; і, нарешті, створити технічні платформи для миттєвого обміну фінансовими й розвідувальними даними між країнами регіону.

Висновки:

- **Державам із вразливими інституціями необхідно створити механізми перевірки походження капіталу** перед наданням дозволів на прямі іноземні інвестиції, щоб запобігти кримінальному впливу на економіку.
- **Необхідно запровадити спільні міждержавні бази даних для перевірки інвесторів і бенефіціарів**, які були помічені у фінансових злочинах, з метою попередження повторного входження на інші ринки.
- **Урядам слід інтегрувати фінансову розвідку, антикорупційні та інші служби в єдину систему** моніторингу, щоб виявляти схеми відмивання коштів і цифрового шахрайства на ранніх етапах.
- **Потрібно обмежити програми "громадянства за інвестиції"** для осіб із високим ризиком, створивши міжнародні стандарти перевірки репутації інвесторів та джерел їхнього капіталу.

Для малих держав, що прагнуть іноземних інвестицій, це означає болючу дилему: як залишатися відкритими для капіталу і одночасно не допустити перетворення власної економіки на притулок для криміналу. Відповідь — у розділенні ризиків: введенні «червоних ліній» для категорій інвесторів, що не пройшли незалежну перевірку; в обмеженні доступу до критичної інфраструктури; у запровадженні міжнародних гарантій і партнерств, які дозволять малим країнам отримати технічну і правову підтримку при перевірці складних структур. Без такого підходу легкий шлях до економічного розвитку може перетворитися на шлях до втрати суверенітету.

В кінці, UNODC попереджає: кримінальні інвестиції — це не «економічний подарунок», а стратегічний виклик, який ставить під загрозу державність. Якщо міжнародна спільнота не розробить нових інструментів контролю і не підтримає вразливі юрисдикції у підвищенні їхньої інституційної стійкості, ми будемо свідками нових економічних зон, що служать базою для глобальних злочинних імперій, а не для розвитку громад і націй.

Прозорість під загрозою: як ЄС балансує між приватністю та антикорупцією у нових правилах бенефіціарної власності [8]

Звіт Transparency International розкриває те як Європейський Союз, попри багаторічні декларації про відкритість, фактично опинився у стані регресу щодо прозорості корпоративної власності.

Цей документ аналізує, що сталося після рішення Суду ЄС у листопаді 2022 року, яким було скасовано публічний доступ до реєстрів бенефіціарних власників — колосальний відступ від принципів, які роками формували європейську антикорупційну архітектуру. Transparency International провела практичний експеримент у 14 державах ЄС, перевіривши, наскільки реально діє новий механізм доступу на підставі так званого “легітимного інтересу”. Результати показали: на практиці цей інструмент майже не працює, а більшість держав або навмисно обмежують доступ, або створюють такі складні процедури, що відлякують навіть фахові організації.

Контекст цієї проблеми сягає корінням у розвиток антикорупційного законодавства ЄС. Після ухвалення четвертої (AMLD4) і п’ятої (AMLD5) директив боротьби з відмиванням коштів, бенефіціарні реєстри стали головним інструментом запобігання зловживанням корпоративними структурами — саме вони дозволяли громадськості, журналістам, слідчим і фінансовим установам ідентифікувати реальних власників компаній. Публічність таких реєстрів допомогла розкрити сотні справ, зокрема у межах “Panama Papers” і “Pandora Papers”, де складні мережі трастів і офшорних структур приховували політиків, корупціонерів і олігархів. Але рішення Суду ЄС, прийняте на тлі позову люксембурзьких компаній, фактично перекреслило ці досягнення — тепер доступ можливий лише для тих, хто доведе “легітимний інтерес”, тобто обґрунтує, що отримання інформації безпосередньо пов’язане з діяльністю у сфері запобігання злочинам чи відмиванню коштів.

Transparency International вирішила перевірити, як цей механізм функціонує на практиці. Організація подала офіційні запити до 14 держав ЄС, від Ірландії до Фінляндії, представляючись як антикорупційна неурядова організація, яка діє у суспільному інтересі. Результат виявився красномовним: у більшості випадків доступ було відмовлено або відкладено на невизначений термін, а деякі країни навіть не відповіли на запити протягом шести місяців.

Угорщина, Ірландія, Австрія й Італія встановили такі вузькі критерії, що навіть професійні журналісти-розслідувачі не могли пройти процедуру доведення свого статусу. У низці випадків, як-от в Ірландії, Transparency International отримала відмову з аргументацією, що “запит не доводить безпосереднього інтересу заявника до конкретної компанії”. Таким чином, країни ЄС створили штучний бюрократичний фільтр, який суперечить суті самої ідеї “легітимного інтересу” — зробити прозорість доступною для тих, хто працює на суспільне благо.

[8] https://www.transparency.org/en/news/countdown-to-new-eu-beneficial-ownership-rules?utm_source=linkedin&utm_medium=social&utm_campaign=regional%2CWEEU%2Cdirtymoney

Окремий розділ звіту описує технічні та адміністративні бар'єри, які створюють ефект "прихованого неприйняття". У багатьох країнах (зокрема, в Іспанії, Нідерландах, Хорватії) доступ до реєстру можливий лише через національну систему електронної ідентифікації (eID), якою можуть користуватись лише громадяни або резиденти цих держав. Це фактично відсікає міжнародні організації, незалежних дослідників і закордонних журналістів. Додаткові проблеми створюють мовні бар'єри: чимало реєстрів доступні лише державною мовою, без перекладів чи англомовного інтерфейсу. А у деяких державах, як-от у Греції чи Іспанії, електронні платформи взагалі не функціонували на момент тестування.

Transparency International також фіксує суттєві фінансові бар'єри. Восьмеро з чотирнадцяти досліджених країн стягують плату за доступ до даних, причому суми коливаються від символічних кількох євро до понад двохсот. Наприклад, у Фінляндії журналісти повинні укласти контракт на річний доступ із фіксованою оплатою понад 200 євро, тоді як у Бельгії та Франції інформація надається безкоштовно. Це створює ситуацію, коли великі комерційні структури можуть дозволити собі регулярний моніторинг, а громадські організації — ні.

Ще більш проблематичним виявилось тлумачення поняття "легітимного інтересу". У деяких державах воно зведене до юридичних осіб, які мають процесуальний статус сторони у справі (наприклад, правоохоронні органи чи адвокати). Інші трактують це поняття ширше, включаючи журналістів або громадські організації. Проте відсутність уніфікованого стандарту робить ситуацію правовим хаосом. Наприклад, у Франції журналіст може отримати дані на підставі членства у профільній асоціації, тоді як в Угорщині чи Ірландії навіть міжнародна організація з бездоганною репутацією має подавати детальні докази зв'язку із запитуваною компанією.

Transparency International наголошує, що нове законодавство ЄС —AMLD6 — може виправити ситуацію, але лише за умови чіткої імплементації. Ця директива вимагає, щоб журналісти, громадські організації, науковці та активісти, які займаються антикорупційною діяльністю, мали спрощений і гарантований доступ до даних після одноразової верифікації статусу. Фактично це спроба відновити баланс між приватністю та прозорістю після рішення Суду ЄС. Однак Transparency International застерігає: без політичної волі держав-членів і жорсткого нагляду Єврокомісії нові норми ризикують залишитись "мертвими".

Організація пропонує конкретні заходи: уніфікувати критерії "легітимного інтересу", створити централізовану систему електронного запиту для всієї Європи, дозволити альтернативні способи ідентифікації для користувачів поза межами ЄС і зобов'язати країни регулярно звітувати про кількість відмов у доступі. Transparency International також наголошує, що втрата прозорості у сфері бенефіціарної власності несе не лише антикорупційні, але й геополітичні ризики: саме через компанії-прокладки Росія, Іран і Китай обходять санкції, скуповують

Висновки:

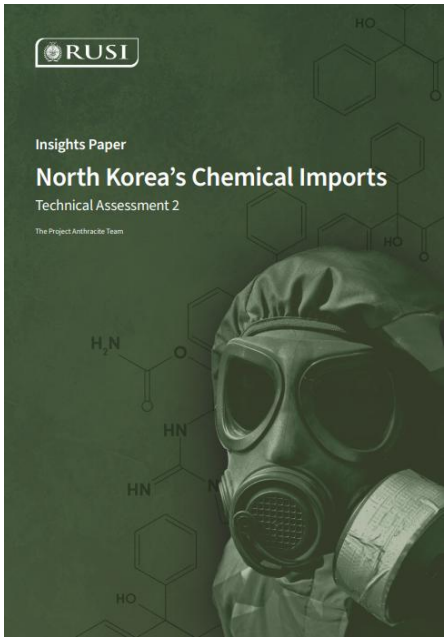
- **ЄС має терміново уніфікувати визначення "легітимного інтересу"** та створити єдиний електронний механізм доступу до реєстрів бенефіціарів, щоб уникнути фрагментації та зловживань на національному рівні.
- **Державам-членам необхідно запровадити спрощену процедуру верифікації** для журналістів, науковців і громадських організацій, які працюють у сфері антикорупції, без вимоги постійного доведення їхнього інтересу.
- **Єврокомісії слід контролювати виконання AMLD6** та зобов'язати країни регулярно звітувати про кількість відмов у доступі до реєстрів, щоб виявляти системні перешкоди прозорості.
- **Країнам ЄС варто усунути фінансові, технічні й мовні бар'єри**, забезпечивши безкоштовний і багатомовний доступ до даних про бенефіціарів як інструмент захисту суспільних інтересів і запобігання санкційним обходам.

нерухомість у ЄС і фінансують політичні мережі впливу. Без прозорих реєстрів Європа втрачає здатність виявляти ці ризики у зародку.

Якщо нові правила не забезпечать реального, уніфікованого та оперативного доступу до даних про бенефіціарів, то боротьба з корупцією, відмиванням коштів і ухиленням від санкцій опиниться під загрозою.

Звіти окремих інституцій та експертів

Технічна оцінка імпорту хімічних речовин Північною Кореєю [9]



Представлений документ є технічною оцінкою імпорту хімічних речовин та обладнання до Північної Кореї, підготовленою командою Project Anthracite (RUSI), з метою аналізу даних торгівлі, які можуть мати відношення до програми хімічної зброї КНДР. Слід одразу наголосити, що автори зазначають неможливість достовірно встановити кінцеве використання проаналізованих товарів. Звіт охоплює період з січня 2015 року по грудень 2024 року і ґрунтується на так званих "дзеркальних імпортних даних", оскільки Північна Корея не публікує власні торгові записи. Це означає, що надані цифри є мінімальними показниками, і існує висока ймовірність того, що дані могли бути відредаговані, приховані або некоректно відображені країнами-експортерами.

Згідно з агрегованими даними, за вказаний період Північна Корея імпортувала щонайменше 667 820 тонн хімічних речовин та 2 124 тонни відповідного обладнання, які можуть мати відношення до виробництва хімічної зброї. Зокрема, було імпортовано 15 861 тонну неорганічних хімікатів (HS Глава 28), 651 959 тонн органічних хімікатів (HS Глава 29) та 2 124 тонни обладнання (HS 8419). Методологія аналізу ґрунтувалася на номенклатурі Всесвітньої митної організації (ВМО) 2022 року, зосередившись на кодах, які включають хімікати подвійного використання, прекурсори, перелічені у Конвенції про хімічну зброю (CWC), а також устаткування, необхідне для процесів, що передбачають зміну температури (HS 8419), яке є ключовим для виробництва бойових хімічних речовин. Важливою методологічною проблемою є те, що HS-коди не містять інформації про матеріали конструкції обладнання, що ускладнює визначення відповідності обмеженням, які фокусуються на корозійностійких матеріалах.

Серед імпорту були ідентифіковані три хімічні речовини, що викликають особливе занепокоєння. По-перше, це фосфору трихлорид (Phosphorus trichloride), імпортований з Індії в обсязі 168 тонн у період 2015–2017 років. Ця речовина включена до Списку CWC і її експорт до КНДР був заборонений ще у 2006 році Резолюцією Ради Безпеки ООН 1718 (РБ ООН 1718). По-друге, було ідентифіковано імпорт з Китаю 2,5 тонн фториду натрію (Sodium fluoride), який є прекурсором у контрольному списку і може бути використаний у виробництві нервово-паралітичних речовин G-серії, таких як зарин і зоман. По-третє, імпорт з Китаю дисульфату натрію (Disodium sulfate) в обсязі 8 203 тонни, який хоча і не є безпосереднім прекурсором, може бути легко перетворений на сульфід натрію, відомий як прекурсор шкірно-наривних речовин.

[9] https://static.rusi.org/north-koreas-technical-imports-assessment-2.pdf

Загальний аналіз демонструє суттєву залежність КНДР від китайського імпорту: Китай є найбільш комплексним постачальником, експортувавши понад 171 170 тонн хімікатів та обладнання за 93 різними HS8-кодами. Ввезення обладнання (HS 8419) з Китаю, що включало стерилізатори, сушарки, ректифікаційні колони та теплообмінні агрегати, суттєво зменшилося після 2017 року. Це може бути пов'язано з ініціативою Кім Чен Ина щодо розвитку «хімічної промисловості С1» або введенням Китаєм невідомих обмежень на експорт промислового обладнання.

Аналіз торгових шляхів виявив використання певних юридичних осіб. Наприклад, російські поставки неорганічних хімікатів і обладнання часто здійснювалися через спільне російсько-північнокорейське підприємство JV RasonConTrans, яке має виключення із санкцій РБ ООН. Також відзначається участь компаній White Stone JVC та TLC VL Logistic LLC. Серед північнокорейських вантажоодержувачів, яким постачалася російська оцтова кислота, була Puhung Trading Company, яку Японія включила до Списку іноземних користувачів через підозри у зв'язках з ризиками розповсюдження біологічної, хімічної та ядерної зброї.

Примітним є імпорт КНДР базових хімікатів, таких як бікарбонат натрію (харчова сода) та оцтова кислота. Враховуючи наявність у КНДР сировини та потужностей для виробництва цих речовин, їх імпорт може свідчити про значні вузькі місця, обмеженість потужностей, або нездатність виробляти хімікати необхідної якості (наприклад, харчового ґатунку). Це вказує на потенційну системну вразливість або невідповідність у хімічній промисловості режиму. Обмеження аналізу, пов'язані з двоїстим

Висновки:

- **Пряме порушення санкцій та високий ризик прекурсорів:** Виявлення імпорту фосфору трихлориду (заборонений РБ ООН 1718) та значних обсягів фториду натрію та дисульфату натрію вимагає негайного посилення фінансового та торговельного моніторингу, особливо щодо китайських та індійських експортних потоків за відповідними HS-кодами (281213, 282619, 283311), оскільки це свідчить про доведену здатність КНДР обходити існуючі контрольні механізми.
- **Пріоритетність моніторингу обладнання подвійного використання (HS 8419):** Неможливість визначення порушень контролю за експортом обладнання (наприклад, теплообмінників, дистиляційних установок) через відсутність інформації про корозійностійкі матеріали в HS-кодах (8419) вимагає від операторів комплаєнсу вжиття заходів щодо поглибленої перевірки кінцевого використання та матеріалів конструкції для будь-яких поставок, що підпадають під цю главу, незалежно від країни походження.
- **Ідентифікація та посилений контроль торгових посередників:** Спеціалістам необхідно сфокусуватись на компаніях, які забезпечують повторювані поставки та логістику для КНДР, таких як JV RasonConTrans, TLC VL Logistic LLC, а також на північнокорейських кінцевих вантажоодержувачах з ризиком розповсюдження, як Puhung Trading Company. Торговельні моделі у російських та індійських постачальників можуть бути індикатором спеціалізованих, але фрагментованих мереж закупівель, що потребує уваги при мережевому аналізі.
- **Використання даних про внутрішні слабкі місця для аналізу ризиків:** Імпорт КНДР базових хімікатів, таких як бікарбонат натрію та оцтова кислота, вказує на ймовірні системні «вузькі місця» або проблеми з якістю у їхній хімічній промисловості. Ця інформація повинна бути використана для моделювання їхніх виробничих потреб та прогнозування майбутніх закупівельних пріоритетів, а також для пріоритетного моніторингу тих іноземних постачальників, які можуть заповнювати ці критичні внутрішні прогалини.

призначенням HS-кодів та відсутністю детальних даних про постачання, особливо щодо матеріалів конструкції, підкреслюють необхідність подальшої верифікації, зокрема за допомогою супутникових зображень нових або реконструйованих хімічних об'єктів для зіставлення з даними про імпорт обладнання.

Глобальні платежі без кордонів: як технології, стандарти та співпраця формують фінансову екосистему 2026 року [10]

Документ є масштабним аналітичним звітом, підготовленим спеціально до конференції Sibos 2025 у Франкфурті, присвяченим глибинній трансформації системи міжнародних платежів, яка відбувається під впливом технологічних інновацій, нових регуляторних підходів, загострення ризиків кіберзлочинності та посилення глобальної конкуренції між банками, фінтех-компаніями і технологічними гігантами. Звіт позиціонується як стратегічний дороговказ для фінансових інституцій, регуляторів і постачальників технологій, які прагнуть досягнути інтегрованої, швидкої, безпечної та прозорої інфраструктури міжнародних платежів до 2026 року і далі.

Вступне слово голови стратегії SWIFT Джонатана Еренфельда задає головний тон усього звіту — це пошук рівноваги між інноваціями та довірою, між технологічною швидкістю та фінансовою стабільністю, між фрагментацією та глобальною взаємопов’язаністю. Він підкреслює, що світова фінансова система опинилася на роздоріжжі: політична поляризація, зростання регіональної самостійності, поява нових цифрових валют і штучного інтелекту створюють ризики дезінтеграції, проте водночас відкривають можливість створення більш гнучкої, взаємопов’язаної і стійкої фінансової екосистеми. Еренфельд визначає головну ідею конференції Sibos 2025 — подолання фрагментації через силу колективної взаємодії, технологічного партнерства і спільних стандартів, що дозволяють перетворити потік розрізнених інновацій на цілісний інструмент розвитку світових фінансів.

Основна аналітична частина звіту пояснює, що трансформація міжнароднхих платежів є результатом кількох взаємопов’язаних факторів: глобального переходу до миттєвих платежів, посилення вимог до фінансової безпеки та комплаєнсу у сфері ПВК/ФТ, упровадження технологій штучного інтелекту, блокчейну, API та цифрових валют, а також радикального оновлення нормативних рамок, серед яких ключову роль відіграють Дорожня карта G20 щодо вдосконалення міжнародних платежів, PSD3, MiCA, FiDA, PSR та EUDI Regulation. Звіт створено на основі експертних інтерв’ю з представниками провідних банків (HSBC, JPMorgan, ING, Standard Chartered, Société Générale, RBI, BNY Mellon, FCA, NAB, ZA Bank тощо), що дозволяє сформувати цілісне бачення розвитку платіжної екосистеми в найближчі роки.

Автори детально описують, як міжнародні платежі перетворюються із громіздкої, фрагментованої системи кореспондентських банківських ланцюгів у гнучку, технологічно з’єднану мережу, що функціонує на базі ISO 20022, хмарних технологій, DLT і відкритих API. Філ Бруно (ACI Worldwide) підкреслює, що завдання майбутнього полягає не лише у прискоренні переказів, а у збереженні довіри та фінансової цілісності. Сучасні міжнародні розрахунки відзначаються високою вартістю, низькою прозорістю й ризиком порушення вимог у сфері ПВК/санкційного контролю. Індустрія шукає шляхів зменшити тертя у транзакціях, не жертвуючи надійністю. За його прогнозом, у найближчі 15–20 років світ перейде до «мережі мереж», де

[10] https://www.finextra.com/researcharticle/356/the-future-of-cross-border-payments-2026-strategies-for-success

національні та регіональні платіжні системи будуть взаємопов'язані через спільні стандарти та взаємну довіру, а цифрові валюти — як приватні стейблкоїни, так і державні CBDC — відіграватимуть ключову роль у миттєвому міжнародному клірингу без проміжних ланок.

Важливою темою є виклики впровадження миттєвих платежів. Автори підкреслюють, що швидкість транзакцій — це не просто технологічна перевага, а вимога часу, продиктована цифровими очікуваннями клієнтів і зростаючим попитом на цілодобову ліквідність. Проте головною загрозою залишається фрагментація між країнами і платформами. Успіх залежить від гармонізації регуляторних підходів, стандартизації форматів даних і розвитку хмарних інфраструктур. Експерти відзначають, що партнерство між банками, фінтехами та регуляторами стає більш цінним, ніж конкуренція, адже лише через спільну розробку стандартів можна забезпечити взаємодію між національними системами. Значну увагу приділено управлінню ліквідністю у режимі реального часу: стейблкоїни, цифрові валюти центральних банків та алгоритмічні рішення на базі AI розглядаються як інструменти оптимізації казначейських операцій та підвищення стійкості до ризиків.

Окремий великий розділ присвячено темі фінансових злочинів і кібербезпеки. Звіт констатує, що швидкість цифрових платежів створює нові вразливості. Шахрайство типу APP (Authorised Push Payment), фішинг, діпфейки, використання штучних ідентичностей і криптозлочинність зростають у геометричній прогресії. Експерти з провідних банків (Standard Chartered, J.P. Morgan, Société Générale, FV Bank, NAB, ZA Bank) підкреслюють, що традиційні «правила та фільтри» більше не працюють, натомість ефективними стають адаптивні моделі AI, які вчаться на потоках транзакцій у реальному часі. У звіті описано зсув до нової парадигми — «забезпечення дотримання вимогза принципом вбудованого дизайну», коли ПВК, санкційний моніторинг і виявлення аномалій вбудовуються безпосередньо у продуктові архітектури банківських систем. Ключовим стає колективний підхід: обмін даними між банками, регуляторами, телекомунікаційними та технологічними компаніями, спільні бази даних шахрайських операцій і стандарти кіберзахисту. Автори називають це «екосистемною відповідальністю», де безпека більше не є питанням окремої установи, а стає колективним обов'язком.

Дуже значний аналітичний обсяг присвячено пост-ISO 20022 світу, у якому злиття технологій AI, DLT, токенізації, API та відкритих стандартів створює принципово нову платіжну архітектуру. ISO 20022 постає як «універсальна мова» для передачі багатих, структурованих даних, що забезпечує автоматизацію комплаєнсу, моніторинг ризиків і операційну прозорість. Звіт пояснює, що міграція до цього стандарту — не просто технічне оновлення, а фундаментальна зміна способу взаємодії банків, фінтехів і регуляторів. На цій основі вибудовується інфраструктура «розумних платежів», де штучний інтелект забезпечує динамічну маршрутизацію, попередження шахрайства, автоматичне узгодження й миттєве дотримання регуляторних вимог, а токенізовані депозити, стейблкоїни та CBDC створюють основу для миттєвого клірингу без посередників. Таким чином, майбутнє визначається не швидкістю трансакцій, а розумом і довірою системи.

Регуляторний блок звіту є одним із найінформативніших. Він аналізує прогрес виконання Дорожньої карти G20 щодо вдосконалення міжнародних платежів, де до 2027 року передбачено скорочення вартості переказів до 1–3%, забезпечення доступності щонайменше однієї інфраструктури для кожного користувача і миттєву доступність коштів у 75% трансакцій протягом години. Проте автори зазначають, що темпи реалізації цілей поки не задовільні. Водночас у ЄС триває формування нової нормативної екосистеми: PSD3 і PSR створюють умови для безпечної відкритості даних і прозорості платежів, FiDA розширює обмін фінансовою інформацією між банками і третіми сторонами, MiCA встановлює правові рамки для ринку криптоактивів і стейблкоїнів, а EUDI Regulation запроваджує загальноєвропейську цифрову ідентичність, що стане ключовим елементом уніфікованої аутентифікації. У поєднанні ці

документи формують фундамент відкритої фінансової екосистеми, у якій клієнт отримує повний контроль над даними, а регулятори — єдині стандарти безпеки та звітності.

Фінальна частина звіту, підготовлена Volante Technologies, окреслює технологічний горизонт 2026 року і після нього. Вона показує, що майбутнє міжнародних платежів лежить у переході від застарілої кореспондентської моделі до хмарно-нативних, API-орієнтованих платформ, які забезпечують цілодобову взаємодію між RTGS, ACH, миттєвими платіжними системами та токенізованими мережами. Така модель дає змогу знизити операційні витрати на третину, підвищити рівень автоматизації (STP) до 85% і скоротити потребу в ностро-рахунках на 40–60%. Автори підкреслюють, що перехід до хмарно-нативної архітектури — це не лише питання ефективності, а й умова виживання у світі, де дані, прозорість і швидкість стають головними конкурентними перевагами.

Висновки:

- **Інтероперабельність і спільні стандарти — критичні для зниження фрагментації.** Необхідно створити «мережу мереж» із повною сумісністю ISO 20022, API та хмарних платформ.
- **AI, блокчейн і цифрові валюти змінюють природу комплаєнсу й ризик-менеджменту.** Штучний інтелект забезпечить миттєвий аналіз транзакцій, а токенізовані депозити — автоматизоване розрахування між юрисдикціями.
- **Регуляторна конвергенція (PSD3, MiCA, FiDA, G20 Roadmap) формує основу для відкритих фінансів.** Вона відкриває шлях до прозорих, безпечних і дешевших міжнародних платежів та до гармонізації ПВК/KYC-підходів.
- **Безпека — наріжний камінь розвитку.** Галузь переходить від реактивного підходу до «проактивного втручання», коли фінансові установи прогнозують і блокують шахрайство ще до його реалізації, через спільні аналітичні й технологічні платформи.

У цілому звіт Finextra формує цілісну картину глобальної еволюції платіжної індустрії, де технології, регуляції та колаборація стають трьома опорами майбутнього. Його центральне послання полягає в тому, що майбутнє міжнародних платежів — це не просто технологічна інновація, а системна інтеграція, яка поєднує швидкість, безпеку, довіру та інклюзивність. Тільки шляхом гармонізації стандартів, узгодження регуляторних режимів, розвитку цифрових валют і побудови довіри між державами, банками й технологічними компаніями можливо створити нову архітектуру глобальних фінансів, де кордони перестають бути бар'єром, а стають лише технічним параметром у системі миттєвого, прозорого й безпечного руху капіталу.

Контроль за товарами подвійного призначення: практичні настанови для запобігання фінансуванню розповсюдження [11]

Документ є аналітичним звітом, спрямованим на формування узгодженого бачення ролі децентралізованих фінансів (DeFi) у майбутній фінансовій системі Великої Британії. Його мета — запропонувати практичні рекомендації для розробки пропорційного, технологічно нейтрального та конкурентоспроможного регуляторного підходу до DeFi, який дозволить країні зберегти статус міжнародного лідера у сфері інновацій та фінансової стабільності. Звіт підготовлений як внесок до поточного процесу осмислення цього питання британським регулятором — Управління з питань фінансової поведінки (FCA, Велика Британія).

11 https://static1.squarespace.com/static/651bea53fe849553fe8a19d0/t/68d661e13b51d039b8e3fe1e/1758880225517/UKCBC+DeFi+Report+%284%29.pdf

У вступній частині документ підкреслює, що DeFi — це не фінансовий посередник у традиційному розумінні, а програмна інфраструктура з відкритим кодом, яка дозволяє користувачам здійснювати транзакції без контролю чи втручання третіх сторін. Така структура радикально змінює характер взаємодії між користувачами та фінансовими продуктами, що потребує переосмислення ризиків і підходів до їхнього пом'якшення. Автори зазначають, що розподілені технології (DLT) відкривають можливості для підвищення ефективності, прозорості, конкуренції та підзвітності у фінансовій системі. У той час як токенізація та DLT уже активно впроваджуються у традиційних фінансових послугах, DeFi залишається сприйнятим як периферійне явище, хоча фактично має потенціал стати каталізатором розширення доступу до фінансових продуктів та послуг. Документ наголошує, що DeFi не слід розглядати як заміну існуючої системи, а радше як інноваційне доповнення, яке надає користувачам — як роздрібним, так і інституційним — ширший вибір способів взаємодії з ринком: через традиційні інституції, DeFi-протоколи або комбіновані рішення.

Звіт детально описує технологічну архітектуру DeFi, який складається з трьох рівнів: блокчейн-рівня, де фіксуються й фіналізуються транзакції; рівня протоколів і активів, що працює на основі смартконтрактів; та рівня користувацьких інтерфейсів, які забезпечують зручність взаємодії без передачі контролю над активами. На відміну від централізованих систем, де транзакції відбуваються через посередників, у DeFi усі операції відбуваються безпосередньо між учасниками, що зменшує ризик контрагента, усуває необхідність у традиційних клірингових етапах і дозволяє здійснювати миттєві розрахунки. Особливу увагу приділено феномену самостійного зберігання, який дає користувачам повний контроль над своїми активами через приватні ключі, та моделі P2P, яка зменшує потребу у довірених посередниках.

Документ подає глибокий опис ключових застосувань DeFi, серед яких позики та запозичення, flash loans (миттєві позики без застави, які виконуються в межах однієї транзакції), децентралізовані біржі (DEX), деривативи, синтетичні активи та ринки прогнозів, де користувачі можуть робити прогнози щодо майбутніх подій. Такі інструменти забезпечують новий рівень ринкової ефективності, зокрема завдяки арбітражним можливостям і ліквідності, але водночас створюють нові виклики — зокрема ризики маніпуляцій, вразливості смартконтрактів і проблеми розуміння складних продуктів з боку користувачів. Окремо розглянуто роль оракулів — механізмів, які забезпечують зв'язок блокчейна з реальним світом шляхом надання перевірених даних для виконання смартконтрактів, наприклад, у прогнозних ринках або страхових продуктах.

Звіт окреслює основні риси «справді децентралізованих» протоколів, які відрізняють їх від централізованих систем. Серед таких рис — автономність, відсутність людського втручання, відкритий вихідний код, прозорість і нейтральність, децентралізоване управління, відсутність кастодіальної функції, атомарність розрахунків і можливість сумісності. Саме ці параметри, на думку UKCBC, повинні бути використані як об'єктивні критерії при визначенні рівня децентралізації та розробці регуляторної рамки. Це дозволить відрізняти справжні децентралізовані протоколи від тих, які лише частково відповідають цьому визначенню, запобігаючи регуляторному арбітражу, коли централізовані послуги маскуються під децентралізовані для уникнення контролю.

Автори визнають, що попри переваги DeFi, існують суттєві ризики, які необхідно врегулювати або мінімізувати шляхом саморегулювання та співпраці індустрії з державними органами.

Серед них — вразливості коду, шахрайські схеми, людські помилки, ризик втрати доступу до активів, а також сплутування користувачами централізованих і децентралізованих сервісів, коли вони взаємодіють через спільні платформи. UKCBC пропонує не переносити на DeFi підходи, характерні для традиційних фінансових установ, оскільки це призведе до непропорційного регулювання і пригальмує інновації. Замість цього доцільно створити нову методологію оцінки рівня контролю у DeFi, базовану на технічних і організаційних параметрах системи.

Окремий розділ документа присвячено порівнянню міжнародних підходів до регулювання DeFi. Європейський Союз через регламент MiCA залишив поза межами регуляторного периметра послуги, що надаються «повністю децентралізованим чином без посередників», однак відсутність чітких визначень спричинила фрагментацію між країнами-членами. У США прийнятий Палатою представників Закон про чіткість регулювання ринку цифрових активів (CLARITY Act) запровадив чіткі стандарти децентралізації, базовані на понятті контролю, що дозволяє звільняти справді децентралізовані протоколи від регуляторних вимог. Франція, у свою чергу, розвиває модель добровільних стандартів аудиту смартконтрактів у співпраці з галуззю. Велика Британія наразі дотримується проміжного підходу — DeFi поки що перебуває поза регуляторним периметром, але уряд і FCA визнають нагальну потребу у створенні єдиного об'єктивного підходу до оцінки «контролю», щоб визначити, які проєкти можна вважати дійсно децентралізованими.

У завершальній частині UKCBC висуває п'ять ключових рекомендацій для політиків. По-перше, регулювання має бути технологічно нейтральним і застосовуватись лише до посередників фінансових послуг, а не до самих програмних протоколів. По-друге, необхідно розробити детальні критерії «контролю», що дозволять ідентифікувати «справді децентралізовані» системи, зокрема за ознаками автономності, відкритості коду та відсутності централізованого управління. По-третє, слід дозволити взаємодію централізованих посередників із децентралізованими протоколами без втрати статусу децентралізації, забезпечивши при цьому прозорість і захист користувачів. По-четверте, Велика Британія повинна узгоджувати свої підходи з іншими передовими юрисдикціями — насамперед США та ЄС — задля стимулювання ліквідності, міжнародної координації та підвищення ефективності нагляду. По-п'яте, необхідно оновити податкову систему щодо DeFi, створивши спеціальний податковий механізм, який спростить звітність і застосовуватиме принцип «без прибутку / без збитку» для транзакцій у DeFi-протоколах, що зробить британську юрисдикцію привабливішою для інвесторів.

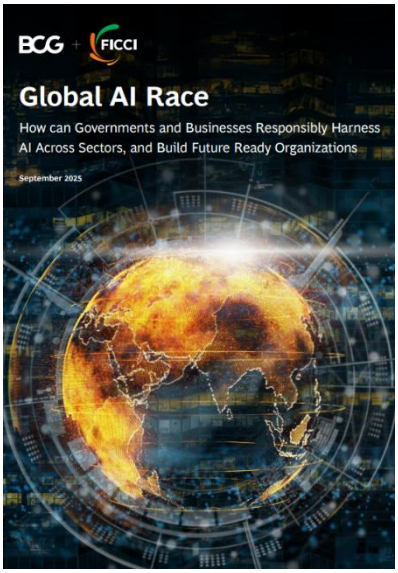
Загалом документ окреслює DeFi як стратегічну можливість для Великої Британії, що здатна зробити фінансову систему більш відкритою, ефективною та інноваційною. Водночас він закликає до збалансованого підходу, який поєднає правову визначеність, захист споживачів і стимулювання технологічного розвитку. За логікою UKCBC, майбутнє фінансових ринків полягає не у виборі між

Висновки:

- **Необхідно закріпити принцип технологічної нейтральності** — регулювання має охоплювати фінансових посередників, а не розробників чи програмний код DeFi-протоколів.
- **Варто розробити об'єктивні критерії «контролю» для визначення рівня децентралізації,** що стане базою для правової визначеності та пропорційного нагляду.
- **Потрібно забезпечити сумісність і взаємодію CeFi та DeFi,** створивши механізми прозорості та запобігання плутанині між регульованими і нерегульованими сервісами.
- **Британська політика має бути узгоджена з міжнародними стандартами (США, ЄС, IOSCO, FSB) та супроводжуватись оновленням податкового режиму** для стимулювання інновацій та інвестицій у DeFi.

централізацією та децентралізацією, а у формуванні єдиного гнучкого ландшафту, де традиційні фінансові інституції, DeFi-протоколи та користувачі зможуть співіснувати у безпечному, прозорому й конкурентному середовищі.

AI-революція: виклики, що формують нову економічну архітектуру людства [12]



Аналітичний звіт, підготовлений Boston Consulting Group (BCG) спільно з Federation of Indian Chambers of Commerce and Industry (FICCI) у вересні 2025 року, є масштабним дослідженням про глобальні тенденції розвитку штучного інтелекту (AI) як визначального чинника економічного, технологічного та політичного домінування у XXI столітті. Документ розкриває, як країни та бізнеси можуть відповідально використовувати AI для зростання, продуктивності, інновацій та суспільного добробуту, і водночас попереджає про небезпеку формування глибокої «AI-нерівності», що загрожує посиленням дисбалансів між розвиненими та тими, що розвиваються, економіками.

Звіт починається з окреслення масштабів глобального впливу AI, який, за прогнозами, до 2030 року забезпечить понад 15,7 трильйона доларів США додаткового внеску у світову економіку. Це не лише технологічна революція, а нова економічна епоха, у якій інтелектуальні системи стають стратегічними активами держав і корпорацій. Уже сьогодні AI скорочує цикл наукових досліджень із років до місяців, підвищує ефективність виробництва, збільшує врожайність сільського господарства, персоналізує освіту та оптимізує медичну діагностику. Водночас концентрація технологічного потенціалу у кількох країнах — насамперед у США та Китаї — створює структурну асиметрію, коли решта світу опиняється у ролі споживачів, а не творців інновацій. Ця ситуація формує те, що автори звіту називають «глобальними перегонами AI», які розгортаються у чотирьох взаємопов'язаних вимірах: обчислювальна потужність, дані, моделі та кадровий потенціал.

У розділі, присвяченому «Глобальним вимірам перегони AI», зазначено, що обчислювальні потужності — це фундамент, від якого залежить уся система. Попит на комп'ютні ресурси подвоюється кожні п'ять місяців, а розробка передових моделей потребує сотень мільйонів доларів інвестицій у GPU та ценрів обробки даних. Доступ до таких ресурсів є надзвичайно нерівномірним, адже понад 90% високопродуктивних чипів виробляється на Тайвані, що створює геополітичні ризики. Дані, хоча й доступні у величезних обсягах, залишаються фрагментованими, неякісними та локалізованими через політики конфіденційності й національні обмеження, такі як GDPR у ЄС чи CCPA у США, що ускладнює створення глобальних моделей. Моделі, зокрема базові системи, стають новим полем конкуренції між пропрієтарними розробками та відкритим кодом: у 2024 році з'явилося 167 великих моделей, а відкриті системи, такі як європейська Mistral або арабська Falcon, вже майже не поступаються за ефективністю закритим продуктам. Усе це підсилюється критичною нерівномірністю у розподілі кадрового потенціалу — одна третина усіх фахівців у сфері AI працює у США, тоді як більшість країн борються із «відпливом мізків». Китай, водночас, утвердився як лідер за кількістю наукових публікацій і цитувань у сфері AI, тоді як ЄС, Індія, Ізраїль, Сінгапур і ОАЕ намагаються формувати власні центри інновацій через державні програми, регуляторні пісочниці та цільові інвестиційні фонди.

[12] https://web-assets.bcg.com/9b/33/15438ea347878a0f5ce03d2dcae6/global-ai-race.pdf

Автори документа підкреслюють, що така ситуація призводить до «AI-прірви», коли 70% країн світу залишаються нижче базових порогів зрілості в дослідженнях, навичках та екосистемному розвитку. На рівні бізнесу, попри масові експерименти, лише близько 26% компаній спромоглися перейти від пілотних проєктів до масштабного використання AI. У результаті формується цикл, у якому великі економіки та корпорації нарощують перевагу, а країни, що розвиваються, залишаються у залежності від імпортних технологій. Висвітлюється також секторальний дисбаланс: фінансові технології та охорона здоров'я мають рівень впровадження AI понад 60%, тоді як освіта, сільське господарство та енергетика — менше 25%. Розподіл інвестицій у AI в Індії, як приклад, демонструє, що лише менше 10% коштів спрямовується на соціально значущі сектори, тоді як левова частка фінансує фінтех та сектор охорони здоров'я.

Другий розділ присвячено проблемі переходу «від пілотів до реального впливу». Зазначається, що попри мільярдні інвестиції, 95% стартапів у сфері AI зазнають невдачі, а лише 11% компаній отримують значну віддачу від технології. Причинами цього є не лише технічні бар'єри, а й людський чинник — відсутність лідерства, стратегічного бачення, системної культури даних та узгоджених процесів. У більшості випадків компанії зосереджуються на алгоритмах, ігноруючи управління змінами, навчання персоналу, етичні стандарти та інтеграцію AI в операційні процеси. Досвід провідних корпорацій, таких як J.P. Morgan, L'Oréal, Amazon або Uber Freight, показує, що реальна цінність виникає тоді, коли технології інтегруються в бізнес-модель, а не використовуються як допоміжний інструмент. Успішні компанії вкладають до 70% зусиль не у технології, а у трансформацію людей і процесів, створюючи середовище, де ШІ доповнює людські навички.

Далі звіт переходить до аналізу ролі держави у формуванні життєздатної екосистеми. Автори окреслюють концепцію RISE (дослідження, інвестиції, навчання та етика) — стратегічну модель державного втручання, необхідну для забезпечення стійкого розвитку AI. Держави повинні одночасно стимулювати дослідження та інновації, розбудовувати цифрову інфраструктуру, розвивати людський капітал і впроваджувати етичне регулювання. Приклади таких ініціатив включають державну програму IndiaAI Mission, яка об'єднує понад 10 мільйонів рупій для розвитку потужностей обчислень, майбутніх навичок і безпечного застосування AI; програму «AI на благо усім» у Бразилії з бюджетом 4 млрд доларів; ініціативу Основи AI у Фінляндії, яка навчила понад мільйон громадян основам AI; та прийняття Європейського акту про штучний інтелект (EU AI Act, 2024) — першої у світі законодавчої рамки, що систематизує регулювання ризиків і визначає категорії безпечного застосування. Водночас у документі наголошується на потребі міжнародної координації — через фінансові механізми на кшталт InvestAI Partnership в ЄС, ініціативи ООН AI Hub for Sustainable Development, або двосторонніх угод між урядами та технологічними гігантами.

Висновки:

- **Подолати «AI нерівності» через RISE.** Держави мають інвестувати в чотири напрямки — дослідження, інфраструктуру, навчання та етику, щоб уникнути залежності від закордонних технологій і створити власні центри інновацій.
- **Масштабування, а не експерименти.** Бізнесу слід переходити від пілотів до реального впливу — обирати обмежену кількість стратегічних кейсів, інтегрувати AI у ключові процеси й розвивати культуру експериментування.
- **Інвестиції у людей — ключ до рентабельності інвестицій (ROI).** 70% успіху в AI визначається не алгоритмами, а готовністю персоналу, лідерства та процесів; системне підвищення кваліфікації є умовою масштабування.
- **Етичне регулювання = довіра = стійкість.** Запровадження чітких рамок відповідального AI (на кшталт EU AI Act) є не лише нормативною вимогою, а й передумовою інвестицій та громадської законності AI.

Звіт також зосереджується на проблемі довіри до AI. Автори відзначають, що 77% американців не довіряють бізнесу у сфері відповідального використання AI, а понад 60% побоюються дезінформації, діпфейків і порушення приватності. Етичне врядування, прозорість алгоритмів, пояснюваність рішень і системи сертифікації виступають не лише моральною вимогою, а й економічною передумовою для зростання. Відповідальне впровадження стає конкурентною перевагою, яка формує нову культуру співіснування технологій і суспільства.

Завершується документ закликом до колективної дії. На думку авторів, AI не має стати гонкою за перевагою — це має бути спільне прагнення до прогресу, у якому держави інвестують у базову інфраструктуру та довіру, бізнес переходить від пілотів до системного впровадження, а міжнародні організації сприяють вирівнюванню можливостей. Тільки за умови скоординованих дій — через об'єднання наукових ресурсів, обмін даними, спільне навчання й розробку етичних стандартів — людство зможе перетворити штучний інтелект із чинника геополітичної конкуренції на рушійну силу інклюзивного зростання, сталого розвитку та соціальної рівноваги. Звіт BCG та FICCI є, по суті, маніфестом нового світового підходу до AI: від технологічної елітарності — до відповідальної спільної епохи, де інновації поєднуються з етикою, а продуктивність — із людяністю.

Інтернет-рабство XXI століття: як технології створили новий ринок експлуатації [13]

Розслідування Reuters викриває одну з найжахливіших сторін сучасного злочинного світу — перетворення торгівлі людьми на транснаціональний бізнес, який поєднує жорстоку фізичну експлуатацію з високотехнологічними шахрайськими схемами.

Історії людей, що вирушили до Таїланду у пошуках роботи чи відпочинку, а зрештою опинилися у трудовому рабстві на території М'янми, є лише частиною величезної злочинної системи. У ній злочинці, бізнесмени, корумповані чиновники й військові діють як єдиний організм, керуючи "фабриками" фінансового шахрайства, замаскованими під IT-компанії.

У центрі цієї системи — табори на півночі М'янми, у зонах, що контролюються місцевими військовими, які мають тісні зв'язки з китайськими мафіозними структурами. За високими мурами та під контролем озброєної охорони утримуються тисячі людей із різних країн — Африки, Південної та Південно-Східної Азії, навіть Європи. Їх заманюють через онлайн-оголошення про роботу в "інтернет-компаніях" або "криптопроєктах" у Таїланді, пропонуючи зарплати у кілька тисяч доларів. Проте після прибуття документи відбирають, людей перевозять через кордон — часто за прямої участі корумпованих тайських прикордонників — і вони опиняються в замкнених комплексах, де немає ані прав, ані зв'язку із зовнішнім світом.

Жертв змушують працювати у "кіберцентрах", що функціонують як фабрики інтернет-шахрайства. Під загрозою побиття чи тортур їх навчають видавати себе за інвесторів, бізнесменів або коханців у мережі, щоб виманювати гроші з жертв у різних країнах. Ці люди проводять до 18 годин за комп'ютером, виконуючи щоденні "норми" — залучити певну суму чи кількість нових "інвесторів". Тих, хто не досягає результатів, карають: б'ють електрошокерами, саджають у камери без води, змушують стояти на колінах або працювати без сну. Свідки

[13] https://www.reuters.com/graphics/SOUTHEASTASIA-SCAMS/mypmxwdwwvr/

розповідають, що деяких в'язнів продавали з "компанії" до "компанії" — як товар, змінюючи власників за кілька тисяч доларів.

Після військового перевороту у М'янмі 2021 року влада втратила контроль над прикордонними регіонами, і саме в цьому вакуумі виникла ця злочинна інфраструктура. Місцеві етнічні армії, які воюють із центральним урядом, уклали угоди з китайськими кримінальними угрупованнями, дозволяючи їм будувати "бізнес-зони" для шахрайства, торгівлі людьми й зброєю. Уряд М'янми публічно заперечує участь у схемі, однак міжнародні розслідування показують, що багато чиновників отримують частку прибутків, забезпечуючи прикриття. Корупція в Таїланді й Камбоджі — ще один ключовий елемент системи: прикордонники й поліцейські не лише "закривають очі" на перевезення жертв, а й іноді самі беруть участь у їхньому "відборі".

Механізм схеми збудований із хірургічною точністю. На першому етапі — вербування через соцмережі та фейкові рекрутингові сайти, де обіцяють роботу, наприклад, "менеджера з криптоінвестицій". Далі — транзит через легальні авіарейси до Бангкока, потім — перевезення до прикордонного міста Месай, де туристів зустрічають "працівники компанії". Звідти людей нелегально переправляють через річку Меконг до М'янми, де вони фактично зникають. У таборах їх змушують відкривати акаунти на криптобіржах, використовувати підроблені профілі у Facebook, Tinder, LinkedIn, WhatsApp і Telegram. Це перетворює трудових рабів на "операторів" у глобальній схемі відмивання грошей і фінансових афер.

Найстрашніше, що більшість урядів регіону не поспішають визнавати масштаби проблеми. Камбоджа, Лаос, М'янма та навіть частково Таїланд зволікають із розслідуваннями, прикриваючись "внутрішніми питаннями суверенітету". Попри це, міжнародні організації, такі як ООН, Інтерпол та Global Initiative, фіксують уже понад 300 000 осіб, втягнутих у ці схеми. Для багатьох звільнених "порятунок" стає лише ілюзією: частину жертв відправляють у тимчасові табори, якими керують ті самі угруповання, і вони знову опиняються у рабстві під іншим прикриттям.

Ця історія — не просто трагедія окремих людей, а симптом глибшої системної кризи. Вона демонструє, як злочинність, корупція, війна та цифрові технології утворили новий симбіоз, у якому людина перетворюється на ресурс — на "інструмент прибутку". Фінансові потоки, що проходять через криптовалютні платформи, вже не можна відокремити від торгівлі людьми: прибутки від шахрайства конвертуються у зброю, нерухомість, підкуп політиків і розширення впливу кримінальних мереж. Це нова форма економіки насильства — цифровий рабовласницький капіталізм, що живе за законами темряви.

Для міжнародної спільноти цей кейс має стати приводом для рішучих дій. Необхідно не лише переслідувати виконавців, а й руйнувати фінансові механізми, які підживлюють цю індустрію. Криптопровайдери, банки, платіжні системи та уряди мають створити глобальний механізм фінансової прозорості у кіберпросторі — із зобов'язанням виявляти та блокувати транзакції, що можуть бути пов'язані з

Висновки:

- **Необхідно інтегрувати боротьбу з торгівлею людьми у глобальну стратегію** кібербезпеки, адже сучасне рабство перемістилося у цифровий простір.
- **Міжнародні фінансові регулятори повинні встановити жорсткий моніторинг** криптовалютних транзакцій, пов'язаних із підозрілими онлайн-проєктами та шахрайськими платформами.
- **Країнам регіону слід посилити антикорупційні механізми** в міграційних і прикордонних службах, які часто виступають співучасниками схем торгівлі людьми.
- **Потрібно створити міжнародну систему швидкого реагування** для виявлення, евакуації та реабілітації жертв цифрового рабства.

експлуатацією людей. Без контролю над цими потоками жодна кількість поліцейських рейдів не зупинить індустрію, яка перетворює довірливих шукачів роботи на невільників цифрової доби.

Рекомендовані матеріали та події

Криптоактиви в Україні: ризики, можливості та гібридна війна [14]

Основний зміст дискусії на тему "Криптоактиви в Україні: ризики, можливості та гібридна війна", яку було організовано Центром фінансової доброчесності (CFI), розкриває двоїсту природу криптоактивів для України. З одного боку, вони стали потужним інструментом для підтримки країни в умовах повномасштабної агресії, дозволивши швидко та ефективно залучати міжнародні донати на військові та гуманітарні потреби. З іншого боку, існує глибоке розуміння того, що сфера віртуальних активів несе значні ризики ВК/ФТ, які потребують негайного та ефективного регулювання. Експерти наголошують, що ризики, пов'язані з віртуальними активами в Україні, можна поділити на дві категорії: загальні, які притаманні багатьом країнам, та специфічні, зумовлені саме українським контекстом. До загальних ризиків належать непрозорість походження коштів та загроза втрати контролю над активами. Специфічні ж ризики безпосередньо пов'язані з гібридною війною: використання позабіржових (OTC) сервісів для обходу обмежень на рух капіталу, ухилення від санкцій та фінансування військових дій з боку агресора. Україна також розглядається як транзитний вузол для криптовалютних потоків, що використовуються в політичних операціях та елементах гібридної війни.

Центральною темою обговорення стало питання законодавчого регулювання ринку. Було зазначено, що спроби врегулювати цю сферу тривають ще з 2018 року, а ухвалений у лютому 2022 року Закон "Про віртуальні активи" досі не набрав чинності. Значна увага приділялася законопроєкту №10225-д, який має на меті імплементувати в українське законодавство стандарти європейського Регламенту про ринки криптоактивів (MiCA). Цей крок є критично важливим для гармонізації українських норм з європейськими, що сприятиме залученню інвестицій та легалізації діяльності криптобірж. Водночас залишається невирішеним ключове питання — призначення відповідальних регуляторів, що створює невизначеність для ринку. Пропонується модель подвійного регулювання, де Національний банк України наглядатиме за обігом стейблкойнів (ARTs та EMTs), а НКЦПФР — за всіма іншими постачальниками послуг у сфері віртуальних активів. Проте такий підхід несе ризик регуляторного арбітражу, коли компанії можуть використовувати прогалини або неузгодженості в політиках двох регуляторів.

Важливим аспектом, на якому зосередились учасники, є необхідність зміцнення державно-приватного партнерства (PPP) у боротьбі з фінансовими злочинами. Ефективна співпраця між державними органами та приватним сектором, чітке визначення ключових стейкхолдерів та усунення прогалин в обміні інформацією є вирішальними для створення спільних механізмів управління ризиками. Було підкреслено, що Україні необхідно не лише розробити законодавчу базу, а й посилити інституційну спроможність, зокрема через навчання слідчих та прокурорів, та активно використовувати наявні аналітичні інструменти для нагляду, в тому числі за неліцензованими крипто-платформами. Незважаючи на те, що Україна добре розуміє ризики ВК/ФТ, її геополітичне становище та триваюча війна роблять її особливо вразливою. Тому

[14] https://cfi-ua.org/crypto-assets-in-ukraine-risks-opportunities-and-hybrid-warfare/

ефективне та збалансоване регулювання ринку віртуальних активів стає дедалі нагальнішим завданням, яке вимагає рішучих дій, а не очікування ідеальних рішень.

Саміт SIFMANet 2025 [15]

Мережа SIFMANet (Sanctions and Illicit Finance Monitoring and Analysis Network) функціонує під егідою RUSI, зокрема через Центр фінансів і безпеки (Centre for Finance & Security, CFS). Її мета — об'єднати дослідницькі інституції, урядові структури, академічні кола та приватний сектор з метою підсилення спроможностей ЄС і окермих держав у протидії незаконним фінансовим потокам, вдосконалення санкційної політики та закриття "дірок" у механізмах обходу санкцій. Саміт 2025 року стане черговим майданчиком для обміну досвідом, вироблення рекомендацій і стимулювання координації між зацікавленими сторонами.

Саміт відбудеться 4 грудня 2025 року в Брюсселі. Формат — очно (in person). Час: 08:30 – 20:00 GMT. Подія буде складатися з комбінації форм: закриті воркшопи для експертів та публічна панельна дискусія, відкрита для ширшої аудиторії. У програмі заплановано ранкову дискусію, два тематичні воркшопи, сесію "coffee chat/insider view", панельне засідання з публічним форматом, а після — нетворкінг.

Захід є безоплатним. Запит на реєстрацію потрібно подати до 22 жовтня 2025 року для розгляду заявки. Підтвердження учасникам надішлють після закінчення терміну реєстрації. У процесі реєстрації потрібно обрати, чи зацікавлені ви у повному дні з воркшопами або лише у публічній панельній частині. Слід врахувати, що лише заявки від експертів розглядатимуться для участі у закритих воркшопах / повному дні.

Саміт охоплює кілька взаємопов'язаних тем, з акцентом на актуальні виклики санкційної політики й практики її реалізації:

1. **Скасування санкцій / "offramps":** як практично здійснювати зняття санкцій, які уроки дали попередні кейси, і як невизначеність щодо можливого скасування впливає на політичні рішення й на поведінку приватного сектору.
2. **Контргібридні дії росії:** як через санкції протидіяти "гібридним інструментам" - тіньовому флоту, саботажу в роботі критичної інфраструктури, кібернападам - та синхронізувати санкційні заходи з іншими інструментами оборони й безпеки.
3. **Санкції проти транснаціональної злочинності:** організована злочинність, кіберзлочинність, незаконна міграція - наскільки дієвими можуть бути тематичні санкційні режими і як їх адаптувати до динамічних мереж злочинців.
4. **Процес оскарження санкцій та прозорість:** внутрішній погляд представників осіб, які були внесені до санкційних списків, на механізми побудови кейсів, виклики дотримання права на захист, і уроки для політиків із цих процесів.
5. **Криптовалюти та обхід санкцій поза фінансовою системою:** як криптоактиви використовуються для закупівлі пріоритетного обладнання та компонентів, які формально не проходять через банківські системи, що ускладнює контроль; які моделі

[15] https://my.rusi.org/events/sifmanet-summit-2025.html

зловживань вже виявлено, які інструменти розслідування використовуються та які політики потрібні, щоб закрити ці лазівки.

6. **Синергія санкцій з іншими політичними та безпековими інструментами**, та роль координації між наглядовими органами, урядами, приватним сектором і міжнародними організаціями.

SIFMANet Summit 2025 адресовано широкому колу зацікавлених сторін:

- Урядовцям (державні служби, міністерства зовнішніх справ, фінансів та безпеки), які відповідають за вигляд санкцій, їхнє застосування та моніторинг.
- Практикам у сфері фінансового розслідування (фінансові розслідувачі, служби фінансового моніторингу, правоохоронні органи), котрі займаються виявленням обходу санкцій, оцінкою ризиків та співпрацею з міжнародними партнерами.
- Експертам з прав людини, правовим аналітикам і адвокатам, які представляють інтереси осіб, які підпадають під санкції, чи аналізують законність санкційних процедур.
- Спеціалістам із технологій, зокрема у сфері криптовалют, блокчейну, OSINT (open-source intelligence), кібербезпеки — з погляду виявлення нових схем обходу санкцій.
- Аналітикам, дослідникам, академічним установам, громадським організаціям, які працюють у сфері санкційної політики, міжнародного права, безпеки та фінансового контролю.
- Представникам приватного сектору — фінансовим установам, компаніям з ланцюгів постачання, консалтинговим фірмам — які хочуть зрозуміти, як санкційні режими змінюватимуться й як це вплине на їхню діяльність або відповідність регуляторним вимогам.

Учасники отримають можливість: поділитися досвідом, почути інсайди щодо процесу формування та оскарження санкцій, працювати у вузьких форматах з іншими експертами, налагодити міжнародні контакти й отримати свіжі дані щодо інструментів контролю криптовалют, нових методів обходу санкцій, а також практичних підходів до адаптації санкційної політики у мінливому середовищі.

Інші новини

Порт крові: як інвестиції, глобальна торгівля й корупція відкрили ворота наркокартелям Еквадору [16]

Порт Посорха (Posorja) — символ глибокої суперечності між розвитком і руйнуванням, між модернізацією та розпадом державного контролю. Те, що мало стати вітриною економічного відродження Еквадору, перетворилося на один із найнебезпечніших вузлів міжнародного наркобізнесу. Коли в 2019 році відкрився новий глибоководний порт, уряд рекламував його як стратегічний інфраструктурний проєкт, що створить тисячі робочих місць і зробить країну ключовим торговельним центром Тихоокеанського узбережжя. Але вже за кілька років цей мегапроєкт,

[16] https://www.occrp.org/en/feature/stained-with-blood-new-port-brings-violent-drug-cartels-to-ecuador-fishing-town

збудований за участю міжнародної компанії DP World, став центром насильства, мафіозних війн і гігантської корупції.

Сьогодні Посорха стала головним каналом транспортування кокаїну з Андських країн до Європи. Через порт щорічно проходить понад 1,5 млн контейнерів, і частина з них заповнена не лише морепродуктами, бананами чи кавою, а й ретельно замаскованими партіями наркотиків. За даними європейських митних агентств, з 2022 року частка вилучень кокаїну, відправленого саме з Посорхи, зросла на понад 300%. Партії, які раніше йшли через старий маршрут Гуаякіль — Панама — Роттердам, тепер стартують із новітнього, високотехнологічного терміналу, який позиціонувався як «найбезпечніший у регіоні». Але саме його сучасність — високі швидкості перевалки, автоматизація, велика кількість субпідрядників — і створила ідеальні умови для злочинних мереж, які швидко пристосовуються до будь-яких технологічних систем.

Розслідування OCCRP показало, що вже на ранніх етапах експлуатації порту до його роботи почали інтегруватися угруповання, пов'язані з колумбійськими, мексиканськими та албанськими наркокартелями. Їхня логіка проста: великі інвестиції у порт, нова економічна зона, відносна віддаленість від основних митних і поліцейських управлінь — ідеальне середовище для прихованого контролю над логістичними процесами. Усе це збіглося з внутрішньою слабкістю державних структур. Поки уряд зосереджувався на презентації порту як «вітрини відкритого Еквадору», злочинні організації вже розбудовували паралельну інфраструктуру — сховища, склади, фіктивні логістичні компанії, а головне — розгалужену мережу впливу серед місцевого персоналу.

Сьогодні тут ніхто не довіряє поліції. Працівники порту розповідають, що перевірки безпеки часто проводяться формально, а деякі сканери просто не працюють. У судах свідчать вантажники, яких примушували перевантажувати контейнери під загрозою насильства. Багатьох поліцейських змушують закривати очі на «дрібні неточності в документах». І якщо хтось намагається чинити опір — його доля відома наперед. За останні два роки тут було вбито понад 200 осіб, з них понад два десятки — працівники охорони та поліції. Місцеві рибалки розповідають, що море тепер належить не їм, а мафії: картелі використовують їхні човни для транспортування товару, а у випадку відмови — викрадають або вбивають.

Економічна модель злочину побудована з точністю до інженерного розрахунку. Використовуючи легальні експортні товари — морепродукти, банани, квіти, рибу — картелі вмонтовують наркотики в стінки контейнерів, упаковки або замінюють частину вантажу на кокаїн у вакуумній тарі. Завдяки надвеликому обсягу перевезень (у середньому 5 000 контейнерів на день) фізично перевірити кожен неможливо. Навіть із сучасними системами сканування, контроль вибірковий — а корупційний тиск на персонал робить ці перевірки ще менш ефективними. У деяких випадках наркотики виявляють не в Еквадорі, а вже в європейських портах, що свідчить про масштабність та організованість каналів.

Водночас Посорха — це не лише порт, а й соціальна трагедія. Місцеве населення опинилося в повній економічній залежності від цієї злочинної системи. Тисячі людей працюють у суміжних галузях — охорона, транспорт, ремонт, обслуговування. Будь-яка спроба відмовитись від співпраці з мафією означає втрату роботи і ризик для життя. «Картелі не приховують свою присутність, — розповідає місцевий житель. — Вони фінансують школи, дають роботу, платять за свята. Уряд — далеко, а вони — поруч». Така ситуація створює ідеальний ґрунт для мафіозної стабільності, коли злочинна структура замінює державу, підкупляючи лояльність населення дрібними благами.

Злочинне насильство стало частиною щоденної реальності: вибухи на вулицях, викрадення, розправи — це звичний фон міста. Тіла нерідко знаходять просто біля порту або в морі, а слідство майже ніколи не доходить до суду. Навіть після того, як уряд направив до регіону

спеціальні підрозділи армії, ситуація не змінилася — злочинні структури мають кращу розвідку, фінансування й підтримку серед населення.

Посорха сьогодні — це мікромодель того, як міжнародна злочинність інтегрується в офіційну економіку. Порт, побудований для торгівлі, став логістичним центром глобальної мафії, а корпорації, що інвестували в розвиток, — мимовільними співучасниками її розширення. Це не лише проблема Еквадору: аналогічні процеси спостерігаються в інших країнах Латинської Америки, Африки та навіть Європи, де великі інфраструктурні проєкти стають об'єктами кримінальної експансії.

Аналітики підкреслюють, що такий стан справ — це не збій системи, а закономірний наслідок моделі глобалізації, у якій капітал рухається швидше, ніж контроль. Без посилення фінансового моніторингу, без належної перевірки інвестицій, без справжньої боротьби з корупцією будь-який великий проєкт може стати порталом для криміналу. І поки міжнародні компанії хизуються «успішними історіями розвитку», тисячі місцевих жителів гинуть, стаючи колатеральною жертвою глобального наркобізнесу. Посорха вже не просто порт — це географічна точка, де зустрілися гроші, насилля і безкарність, створивши нову столицю контрабанди XXI століття.

Swift AI: штучний інтелект проти фінансового шахрайства [17]

Аналітична стаття від Swift демонструє приклад того, як фінансовий сектор намагається перейти від реактивного до превентивного підходу у боротьбі з шахрайством, використовуючи штучний інтелект (AI) і технології спільного обміну даними.

Swift, глобальний фінансовий кооператив, що забезпечує обмін повідомленнями між понад 11 500 фінансовими установами у більш ніж 200 країнах, у партнерстві з 13 провідними банками та технологічними компаніями, провів масштабні експерименти з аналізу 10 мільйонів транзакцій. Результати перевершили очікування: ефективність виявлення шахрайських операцій удвічі перевищила показники систем, які працюють на ізольованих масивах даних.

Ключова інновація полягає у використанні технологій збереження конфіденційності (Privacy-Enhancing Technologies, PETs) та навчання (Federated Learning). Це дозволяє банкам спільно тренувати алгоритми штучного інтелекту, не передаючи чутливі дані клієнтів. Інакше кажучи, замість того, щоб збирати всю інформацію в єдину базу, система «відвідує» кожен банк, навчаючись локально. Таким чином, досягається синергія між приватністю і колективною безпекою — банки спільно покращують виявлення шахрайства, не порушуючи законодавства про захист персональних даних. Це фундаментальний прорив у фінансовій кібербезпеці: тепер кооперація між установами можлива без ризику витоку або втручання в комерційну таємницю.

У ході тестування Swift довів, що така модель не лише зберігає конфіденційність, але й радикально скорочує час реагування. Під час симуляцій банки могли виявляти підозрілі транзакції у реальному часі, обмінюватися підтвердженнями щодо підозрілих рахунків і блокувати шахрайські перекази ще до їх виконання. Це означає, що глобальна фінансова система вперше отримує інструмент, здатний реагувати на шахрайство у хвилини, а не у години чи дні, як це відбувається нині.

Рейчел Леві, керівник підрозділу штучного інтелекту Swift, підкреслила, що головна сила цього підходу — у колективності: «Єдина індустріальна система захисту завжди буде ефективнішою

[17] https://www.swift.com/news-events/press-releases/swift-ai-innovation-creates-blueprint-banks-stop-fraud-faster-through-cross-border-collaboration

за ізольовані оборонні стратегії окремих банків». І справді, за оцінками Swift, у 2023 році фінансовий сектор втратив від шахрайства близько 485 млрд доларів, і більшість цих збитків припали саме на міжнародні перекази. Завдяки створенню спільного аналітичного середовища можна скоротити ці втрати на десятки відсотків, підвищивши довіру до транскордонних платежів.

Експерименти Swift також стали своєрідною «лабораторією майбутнього» для фінансової аналітики. Компанія розвиває понад 50 окремих кейсів використання AI у пілотних проєктах та реальних операціях — від виявлення відмивання коштів до оптимізації мережевих розрахунків. У рамках цих ініціатив Swift уже запустив AI-enhanced Payments Controls Service, який допомагає невеликим і середнім банкам точніше визначати ризикові транзакції. Це особливо важливо для установ, які не мають потужних власних відділів фінансового моніторингу, але стають частиною глобального ланцюга транскордонних переказів.

Інтерес до таких рішень пояснюється зростанням масштабів кіберзлочинності. За даними консалтингових агентств, обсяг шахрайських схем у глобальному фінансовому секторі зростає щорічно на 15–20%. Зловмисники дедалі частіше використовують автоматизацію, DeepFake-технології, викрадені ідентифікаційні дані та фішингові кампанії для проникнення у системи. Традиційні методи протидії — реактивні, повільні та ізольовані — не витримують темпу цифрової епохи. Саме тому ініціатива Swift може стати новим стандартом безпеки, який поєднує технологічну швидкість і міжбанківську довіру.

Особливу увагу Swift приділяє питанню довіри до обміну даними. Ключова ідея полягає в тому, щоб замінити обмін “сирими” даними обміном аналітичними результатами, що створюються локально. Такий підхід забезпечує баланс між комплаєнсом, інновацією та кіберзахистом. Водночас успішне впровадження потребує створення єдиної нормативної бази для регулювання транскордонного обміну результатами роботи AI, що стане серйозним викликом для регуляторів.

Результати пілотного проекту переконливі: учасники відзначають подвоєння ефективності виявлення шахрайства, зменшення кількості хибних спрацьовувань і покращення оперативності між фінансовими центрами. Зараз Swift планує другу фазу, під час якої технологію протестують уже на реальних транзакційних даних. Мета — продемонструвати практичний ефект на рівні світової фінансової системи й створити дорожню карту для масштабного впровадження.

Таким чином, Swift створює не просто інструмент, а нову парадигму колективного захисту фінансової системи. У світі, де злочини відбуваються за секунди, а гроші рухаються миттєво, ізольовані підходи втрачають сенс. Лише глобальна взаємодія, підтримана AI та прозорими стандартами конфіденційності, здатна дати відповідь на виклик XXI століття — цифрове шахрайство, яке не визнає кордонів.

Ваша думка важлива!

1. Які практичні нефінансові індикатори (крім традиційного санкційного скринінгу) можуть використовувати СПФМ, що працюють у сфері торгівлі, для ідентифікації високоризикових транзакцій за обладнанням, яке потенційно може бути використане для ФР?
2. Як відсутність прозорого та миттєвого доступу до даних про КБВ може ускладнювати щоденну роботу СПФМ з верифікації клієнтів (CDD/EDD), особливо в контексті виявлення обходу санкцій чи складних транскордонних схем?
3. UNODC попереджає про «стратегічну інфільтрацію» злочинності, коли мафіозні структури використовують державні контракти чи ліцензовані фірми як фасад для кібершахрайства та торгівлі людьми. Які ключові ризик-індикатори у діяльності, пов'язаній з інвестиціями, або у корпоративному управлінні нових клієнтів (особливо у сферах IT, нерухомості чи грального бізнесу), повинні насторожувати СПФМ щодо ймовірності такої кримінальної інфільтрації?
4. Чи може Україна, в умовах післявоєнного економічного відновлення, стати мішенню для кримінальних схем з прямими іноземними інвестиціями, і як цьому запобігти під час залучення іноземних інвесторів?
5. Враховуючи необхідність захисту даних клієнтів (GDPR) і збереження комерційної таємниці, які регуляторні кроки або стандарти обміну даними необхідні в Україні, щоб забезпечити безпечну та ефективну кооперацію між фінансовими установами у використанні AI для боротьби з шахрайством та ВК/ФТ?
6. Яким чином Україна може інтегрувати принцип «технологічної нейтральності» у своє фінансове регулювання, щоб не стримувати розвиток DeFi та токенізації, водночас забезпечуючи контроль за ризиками відмивання коштів і шахрайства?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-41

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

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