# Методологічний бюлетень

Серійний номер: МінФін-AML-2026-04

Січень 2026


*“Ким би ви не були, будьте кращими!”*

сентенція XIX століття

**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

### Стратегічний злам у боротьбі з транснаціональною корупцією: аналіз Антикорупційної стратегії Великої Британії 2025 [1]

Опублікована у грудні 2025 року та введена в дію на початку 2026 року, «Антикорупційна стратегія Великої Британії 2025» є фундаментальним програмним документом, що визначає архітектуру фінансової безпеки однієї з ключових світових юрисдикцій на наступну п’ятирічку. Документ, що складається зі 123 конкретних зобов'язань, виходить далеко за межі декларативних заяв, пропонуючи радикальну перебудову інституційних механізмів нагляду, правоохоронної діяльності та міжнародної співпраці.

Аналіз цього документа є критично важливим для українських суб'єктів державного та приватного сектору, оскільки Велика Британія залишається одним із центрів тяжіння для капіталів, а також стратегічним партнером України у питаннях санкційного тиску на державу-агресора та повернення виведених активів. Зміни в британському регуляторному ландшафті неминуче вплинуть на стандарти комплаєнсу українських експортерів, банків та фінансових установ, що мають кореспондентські відносини з британськими контрагентами.

[1] https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2025/uk-anti-corruption-strategy-2025-accessible

## Контекст та передумови: Від визнання проблеми до системних дій

Стратегія 2025 року базується на відвертому визнанні того факту, що корупція становить пряму загрозу національній безпеці, економічному зростанню та демократичним інститутам Сполученого Королівства. Уряд констатує, що 68% британців стурбовані впливом іноземних корумпованих акторів на національну безпеку, а 59% — їхнім впливом на ринок нерухомості, що робить боротьбу з «брудними грошима» питанням соціальної стабільності.

Документ з'явився на тлі зростаючої критики ролі Лондона як глобального хабу для відмивання коштів («London Laundromat») та необхідності адаптації до нових геополітичних реалій, де корупція використовується авторитарними режимами як інструмент гібридної війни. Стратегія інтегрує уроки, отримані під час запровадження санкцій проти російських олігархів, та спрямована на усунення системних прогалин, що дозволяли клептократам використовувати британську правову та фінансову систему для легалізації статків.

## Архітектура стратегії: Три стовпи оборони

Структурно документ поділений на три взаємопов'язані стовпи, кожен з яких адресований конкретному аспекту проблеми:

**Стовп 1: Боротьба з корумпованими акторами та їхніми коштами.** Цей напрямок фокусується на посиленні репресивного апарату та механізмів притягнення до відповідальності. Ключовою новацією є суттєве розширення повноважень та фінансування нового **Підрозділу боротьби з внутрішньою корупцією (Domestic Corruption Unit — DCU)** у складі поліції Лондонського Сіті. Це свідчить про зміну парадигми: Британія більше не розглядає корупцію виключно як проблему «третіх країн», а визнає наявність внутрішніх загроз.

Стратегія передбачає широке впровадження **штучного інтелекту** для аналізу великих масивів фінансових даних з метою прискорення розслідувань шахрайства та хабарництва. Це відповідь на проблему ресурсомісткості традиційних фінансових розслідувань, які часто тривають роками. Використання ШІ дозволить правоохоронцям виявляти складні патерни відмивання коштів, які неможливо помітити при ручному аналізі.

Особлива увага приділяється механізму повернення активів. Уряд зобов'язується надавати посилену підтримку постраждалим країнам у відстеженні та репатріації викрадених коштів, що є прямим сигналом для України щодо можливості активізації співпраці у цій сфері.

**Стовп 2: Усунення вразливостей Великої Британії.** Цей стовп містить найбільш революційні зміни в регуляторній архітектурі. Уряд визнає, що ефективна боротьба з відмиванням коштів неможлива без жорсткого контролю над **«професійними пособниками»** — юристами, бухгалтерами, агентами з нерухомості та провайдерами корпоративних послуг, які створюють та обслуговують схеми приховування активів.

Центральним елементом реформи є консолідація нагляду. Наразі у Британії існує фрагментована система з 22 професійних органів-наглядачів (OPBAS), що створює ризики непослідовного застосування стандартів та конфлікту інтересів. Стратегія анонсує передачу наглядових функцій у сфері ПВК/ФТ для всього сектору професійних послуг єдиному регулятору — **Управлінню з фінансового нагляду (FCA)** або новоствореному органу. Це означатиме уніфікацію стандартів, підвищення штрафних санкцій та кінець епохи «м'якого» саморегулювання для юридичних та консалтингових фірм.

Також передбачено створення **Комісії з етики та доброчесності** для нагляду за стандартами поведінки в публічному секторі, що є реакцією на внутрішні політичні скандали. Це посилює інституційну спроможність держави протистояти корупційному впливу зсередини.

**Стовп 3: Побудова глобальної стійкості.** Британія прагне відновити своє лідерство у встановленні глобальних антикорупційних стандартів. Стратегія анонсує проведення у 2026

році **Саміту з протидії незаконним фінансам**, який має стати майданчиком для координації зусиль з партнерами по G7, ЄС та країнами Глобального Півдня.

Критично важливим елементом є тиск на Заморські території та Коронні володіння щодо впровадження **публічних реєстрів бенефіціарної власності**. Британія фактично ставить ультиматум своїм офшорним сателітам: ера фінансової таємниці завершується, і прозорість стає умовою доступу до британської фінансової системи. Це має колосальне значення для глобальної боротьби з відмиванням коштів, оскільки саме ці юрисдикції (БВО, Кайманові острови тощо) історично використовувалися для створення непрозорих корпоративних структур.

### Економічний та правовий аналіз наслідків

Реалізація Стратегії 2025 призведе до суттєвого зростання вартості комплаєнсу (compliance costs) для бізнесу, що оперує у британській юрисдикції. Посилення відповідальності за «нездатність запобігти шахрайству», запроваджене Законом про економічні злочини та корпоративну прозорість 2023 року (ECCTA), у поєднанні з новими ініціативами Стратегії, створює безпрецедентний тиск на корпоративний сектор.

Компанії будуть змушені інвестувати у складні системи моніторингу транзакцій та перевірки контрагентів, щоб уникнути кримінальної відповідальності. Водночас, централізація нагляду під егідою FCA може спростити взаємодію з регулятором для сумлінних гравців, усунувши нерівні умови гри, коли менш принципові конкуренти користувалися слабкістю нагляду з боку професійних асоціацій.

Особливий акцент на прозорості політичного фінансування та захисті інституцій від «відмивання репутації» через благодійні внески свідчить про намір уряду перекрити канали впливу клептократичних режимів на суспільну думку та політичні рішення у Великій Британії.

**Висновки:**

- **Зміна парадигми нагляду:** Перехід від фрагментованого саморегулювання до централізованого державного нагляду (через FCA) за сектором професійних послуг (юристи, бухгалтери) є історичним зрушенням, що значно підвищить ефективність системи ПВК/ФТ та усуне можливості для регуляторного арбітражу.
- **Технологізація боротьби:** Інституціоналізація використання штучного інтелекту в розслідуваннях корупційних злочинів сигналізує про перехід до data-driven підходу в правоохоронній діяльності, що вимагатиме від бізнесу впровадження дзеркальних технологічних рішень для внутрішнього контролю.
- **Глобальна прозорість як зброя:** Вимога до Заморських територій щодо відкриття реєстрів КБВ є стратегічним кроком, що руйнує традиційну модель офшорної таємності та відкриває нові можливості для транскордонних розслідувань та повернення активів, зокрема для України.
- **Відповідальність «пособників»:** Стратегія чітко визначає «професійних посередників» як ключову ланку в ланцюгах відмивання коштів, що призведе до підвищення ризиків для консультантів, які працюють з високоризиковими клієнтами, та зміни стандартів надання послуг.
- **Внутрішня гігієна:** Створення Комісії з етики та доброчесності та посилення контролю за фінансуванням політики демонструє розуміння того, що боротьба з транснаціональною корупцією неможлива без забезпечення доброчесності власних державних інституцій.

## Точка неповернення: Глобальний звіт PwC про регулювання криптоактивів 2026 [2]


Звіт PwC є фундаментальним дослідженням, що фіксує тектонічні зрушення у світовій фінансовій системі. Головна теза документа — світ пройшов «точку неповернення» у питанні інтеграції цифрових активів. Якщо раніше криптоіндустрія існувала паралельно з традиційними фінансами, то у 2026 році вона стає їх невід'ємною, «бекендовою» частиною.

Для українського регуляторного середовища, яке перебуває на етапі імплементації європейського регламенту MiCA, висновки PwC є дорожньою картою, що вказує на майбутні виклики та необхідні кроки для збереження конкурентоспроможності національного фінансового ринку.

### Еволюція регуляторного ландшафту: Від теорії до практики

Звіт виділяє 2026 рік як період переходу від нормотворчості до жорсткого нагляду та правозастосування. У Європейському Союзі завершується перехідний період імплементації MiCA, і регулятори (EBA, ESMA) переходять до фази активного моніторингу дотримання вимог. Це означає, що час для адаптації вичерпано: компанії повинні демонструвати повну операційну відповідність стандартам капіталу, управління ліквідністю та захисту прав споживачів.

PwC відзначає, що регулювання стає більш гранулярним та спеціалізованим. Замість загальних правил для «криптоактивів», юрисдикції розробляють специфічні режими для стейблкоїнів, токенізованих депозитів, NFT та DeFi-протоколів. Це вимагає від учасників ринку глибокої юридичної експертизи та побудови складних матриць комплаєнсу.

### Феномен стейблкоїнів: Системна інтеграція

Окремий фокус звіту — регулювання стейблкоїнів, ринкова капіталізація яких перевищила 300 мільярдів доларів США, причому 99% з них прив'язані до долара США. PwC констатує, що стейблкоїни перестали бути просто інструментом для торгівлі на біржах; вони перетворилися на інфраструктурний елемент глобальних платежів.

Регулятори провідних країн (США, ЄС, Сінгапур, Японія) досягли консенсусу щодо необхідності регулювання емітентів стейблкоїнів за стандартами, наближеними до банківських. Ключові вимоги включають:

- **Резервування:** 100% забезпечення високоліквідними активами, сегрегованими від власних коштів емітента.
- **Право вимоги:** Гарантоване право власника токена на погашення за номіналом (redemption at par) у будь-який момент.
- **Операційна стійкість:** Вимоги до кібербезпеки та безперервності діяльності (у ЄС — в рамках акту DORA).

Звіт підкреслює, що регуляторна невизначеність у США щодо федерального законодавства про стейблкоїни створює ризики для доларової гегемонії, оскільки інші юрисдикції (зокрема ЄС та ОАЕ) створюють прозорі правила гри, залучаючи емітентів.

### «Travel Rule» та прозорість транзакцій

Імплементація «Travel Rule» FATF (вимога щодо передачі інформації про відправника та отримувача при переказах віртуальних активів) стала глобальним стандартом де-факто. Звіт

[2] https://www.pwc.de/de/unterlagen/pwc-global-crypto-regulation-report-2026.pdf

наводить статистику, згідно з якою більшість розвинених юрисдикцій вже впровадили цю вимогу в національне законодавство.

Для VASP (провайдерів послуг з віртуальними активами) це створює технологічний виклик: необхідність інтеграції з протоколами обміну даними та забезпечення сумісності різних стандартів. PwC зазначає, що неспроможність виконувати Travel Rule стає критичним бар'єром для доступу до банківського обслуговування та ліквідності. Компанії, які ігнорують цю вимогу, витісняються в «сіру зону» з обмеженими можливостями розвитку.

**Висновки:**

- **Геополітика стейблкоїнів:** Регулювання стейблкоїнів стає питанням монетарного суверенітету. Юрисдикції змагаються за право встановлювати стандарти для цифрових грошей, розуміючи, що це визначатиме архітектуру майбутніх фінансових потоків.
- **Завершення епохи «Дикого Заходу»:** Консолідація нагляду та впровадження жорстких пруденційних норм для крипто-посередників (бірж, кастодіанів) призведе до очищення ринку від слабких гравців та домінування інституційних платформ.
- **Технологічна конвергенція:** Межа між традиційними (TradFi) та децентралізованими фінансами (DeFi) стирається. Успішними будуть моделі, що поєднують надійність та комплаєнс банків з ефективністю та прозорістю блокчейну.
- **Дані як актив:** Здатність збирати, верифікувати та безпечно передавати дані про клієнтів та транзакції (відповідно до Travel Rule) стає ключовою конкурентною перевагою та умовою виживання для VASP.

### Інституційна незворотність та токенізація

Найважливішим аналітичним висновком звіту є теза про **інституційну незворотність** прийняття криптоактивів. Традиційні фінансові установи (банки, asset managers) вже інтегрували блокчейн-технології у свої бек-офісні системи для токенізації активів, управління заставою та транскордонних розрахунків. Ця інтеграція часто є невидимою для клієнта, але вона фундаментально змінює архітектуру фінансового ринку.

Токенізація реальних активів (RWA — Real World Assets) розглядається як головний драйвер зростання на найближче десятиліття. Регулятори адаптують правила, щоб дозволити використання токенізованих активів як застави (collateral) в операціях РЕПО та деривативах, що відкриває шлях до трильйонних ринків.

## TCSP під мікроскопом: Секторальна оцінка ризиків CSSF 2026 [3]


Оновлена Секторальна оцінка ризиків 2026 року, підготовлена Комісією з нагляду за фінансовим сектором Люксембургу (CSSF), є зразковим аналітичним документом, що демонструє еволюцію наглядового підходу до сектору постачальників послуг трастам та компаніям (TCSP). Враховуючи статус Люксембургу як одного з найбільших фінансових хабів Європи, цей звіт задає стандарти для ідентифікації та оцінки ризиків у сфері управління корпоративними правами та трастами.

Для України цей досвід є особливо релевантним у контексті євроінтеграції та необхідності посилення контролю за професійними посередниками (юристами, аудиторами), які надають послуги зі створення та управління компаніями.

[3] https://www.cssf.lu/wp-content/uploads/ML_TF_risk_assessment_TCSP.pdf

### Методологічна досконалість: Від загального до конкретного

CSSF відмовилася від узагальненого підходу, застосувавши детальну сегментацію діяльності TCSP. Аналіз базується на трьох чітких таксономіях:

1. **Реєстрація компаній (Incorporation):** Оцінка ризиків на етапі створення юридичної особи.
2. **Надання послуг управління (Management):** Ризики, пов'язані з наданням номінальних директорів та секретарів.
3. **Доміциляція (Domiciliation):** Ризики надання юридичної адреси та офісу.

Оцінка здійснюється за двоступеневою моделлю: спочатку визначається **притаманний ризик** на основі аналізу загроз та вразливостей без урахування контролів, а потім — **залишковий ризик (Residual Risk)** після застосування пом'якшувальних заходів. Використовується чотирирівнева шкала оцінки (Low, Medium-Low, Medium-High, High), що дозволяє більш точно калібрувати наглядові дії.

Джерельна база дослідження включає дані FATF, національної фінансової розвідки (CRF), результати наглядових перевірок та інформацію від приватного сектору через механізми державно-приватного партнерства (PPP). Такий мультиджерельний підхід забезпечує об'єктивність та повноту картини ризиків.

### Аналіз ризикового профілю TCSP

**1. Високий ризик відмивання коштів (ВК).** Звіт підтверджує, що сектор TCSP залишається зоною **Високого** притаманного ризику відмивання коштів. Це зумовлено самою природою послуг, які дозволяють створювати складні, багатошарові корпоративні структури, що можуть використовуватися для приховування реальних бенефіціарів. Значна частка клієнтів (61%) має бенефіціарних власників з-поза меж ЄС, що додає географічні ризики. Проте, завдяки впровадженню жорстких вимог до ідентифікації клієнтів та постійному нагляду, **залишковий ризик** вдалося знизити до рівня **Середній**. Це свідчить про ефективність побудованої системи захисту, яка здатна нівелювати значну частину загроз.

**2. Специфіка ризику фінансування тероризму (ФТ).** Важливим висновком є оцінка ризику фінансування тероризму як **Середнього** (притаманний) та **Низького** (залишковий). CSSF аргументовано доводить, що послуги TCSP є менш привабливими для терористів порівняно з відмивачами коштів. Терористичне фінансування часто оперує невеликими сумами та потребує швидкості та дешевизни переказів (наприклад, через системи Hawala або P2P-перекази), тоді як створення та утримання корпоративних структур у Люксембургу є дорогим та довготривалим процесом.

**Висновки:**

- **Ефективність нагляду:** Досвід Люксембургу доводить, що навіть у високоризиковому секторі можливо досягти прийнятного рівня залишкового ризику завдяки комбінації жорсткого регулювання та технологічного комплаєнсу.
- **Диференціація ризиків:** Важливо розрізняти ризики відмивання коштів та фінансування тероризму. Універсальні підходи («one size fits all») є неефективними та призводять до нераціонального використання ресурсів.
- **Прозорість структур:** Сектор TCSP залишається гейткіпером фінансової системи. Його здатність ідентифікувати кінцевих бенефіціарних власників є критичною для запобігання використанню корпоративних оболонок у злочинних цілях.
- **Роль даних:** Наявність якісної статистики та зворотного зв'язку від ринку (через опитувальники та PPP) є фундаментом для адекватної оцінки ризиків регулятором.

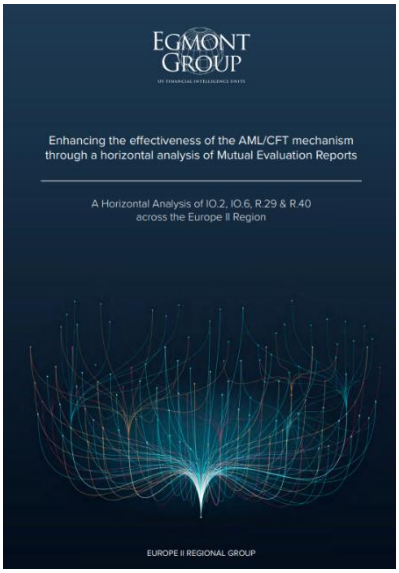
**3. Еволюція «поличних» компаній (Shelf Companies).** Тематичний огляд показав, що ринок Люксембургу трансформувався: лише 5% спеціалізованих провайдерів займаються продажем готових «поличних» компаній. Це знижує ризик використання анонімних структур, які були створені заздалегідь («vintage companies») для надання видимості легальної діяльності. Більшість послуг надається під конкретні потреби клієнта з повним проходженням процедур KYC/CDD на етапі створення.

### Регуляторні очікування та наслідки

Звіт встановлює чіткі імперативи для учасників ринку:

- **Інтеграція оцінки:** Провайдери зобов'язані інкорпорувати висновки секторальної оцінки ризиків у свої власні моделі оцінки ризиків (EWRA). Ігнорування національних та секторальних оцінок розглядатиметься як суттєве порушення.
- **Управління ризиком:** Вимагається формалізація «ризик-апетиту» на рівні керівних органів. Провайдери повинні чітко визначити, з якими типами клієнтів та юрисдикцій вони готові працювати, а які виходять за межі їх апетиту до ризику.
- **Якість даних:** Наголос робиться на необхідності збору та верифікації даних про бенефіціарів та структуру власності. Формального підходу до ведення реєстрів вже недостатньо; регулятор вимагає розуміння економічної суті транзакцій.

## Ефективність ПВК/ФТ на практиці: уроки горизонтального аналізу FATF та роль фінансової розвідки в регіоні Europe II [4]




Документ є ґрунтовним аналітичним дослідженням, спрямованим на оцінку та підвищення ефективності систем ПВК/ФТ у державах регіону Europe II шляхом горизонтального аналізу результатів п’ятого раунду взаємних оцінок FATF та MONEYVAL. Його центральним фокусом є практична результативність діяльності підрозділів фінансової розвідки (ПФР) у двох ключових вимірах: міжнародне співробітництво (Immediate Outcome 2) та використання фінансової розвідки (Immediate Outcome 6), а також роль і реалізація Рекомендацій FATF 29 і 40, які формують інституційну та операційну основу для функціонування ПФР і транскордонної взаємодії

Документ виходить із фундаментальної ідеї сучасної методології FATF, відповідно до якої формальна наявність законів, процедур і інституцій не є достатньою умовою ефективності. Визначальним чинником є те, яким чином ці елементи працюють на практиці, чи трансформується фінансова інформація у реальні розслідування, кримінальні переслідування та конфіскацію активів, а також чи здатні національні органи діяти скоординовано у транснаціональному середовищі. Саме тому дослідження має горизонтальний характер і не оцінює окремі країни, а виявляє системні закономірності, повторювані сильні та слабкі сторони, які впливають на рівень ефективності в усьому регіоні.

У частині, присвяченій міжнародному співробітництву в межах IO.2, аналіз показує загалом позитивну картину для регіону Europe II. Більшість юрисдикцій досягли суттєвого рівня ефективності, а випадки низької ефективності відсутні. Це свідчить про те, що базові механізми

[4] https://egmontgroup.org/wp-content/uploads/2026/01/EUII-Group-Horizontal-Analysis-of-IO2-and-IO6-Final-version.pdf

міжнародної взаємодії, зокрема участь у мережі Егмонтської групи, використання Egmont Secure Web та укладення меморандумів про взаєморозуміння, у цілому функціонують. Водночас документ чітко демонструє, що навіть за формально достатніх інструментів ключовою проблемою залишається характер використання цих механізмів. У юрисдикціях із помірною ефективністю міжнародне співробітництво часто має реактивний характер, зосереджений на відповідях на запити, а не на проактивному обміні інформацією. Типовими слабкими місцями є затримки у відповідях на іноземні запити, відсутність чітких процедур пріоритизації, низька кількість спонтанних розкриттів та обмежені правові можливості для обміну інформацією з органами, які не є ПФР. У більш ефективних системах ці недоліки поступово трансформуються у сильні сторони, що проявляється у швидкому реагуванні, активному ініціюванні співпраці, системному обміні фінансовою розвідкою та реальній участі у транскордонному трасуванні й заморожуванні активів.

Найбільш критичні виклики, зафіксовані в документі, стосуються використання фінансової розвідки в межах IO.6. Аналіз демонструє, що саме ця сфера є «вузьким місцем» для більшості юрисдикцій Europe II, оскільки переважна частина з них отримала лише помірний або низький рівень ефективності. Центральною проблемою виступає розрив між потенціалом фінансової розвідки та її фактичним застосуванням у діяльності правоохоронних органів. У країнах з низькою ефективністю фінансова розвідка часто має обмежену аналітичну глибину, значною мірою через низьку якість звітів про підозрілі операції, які подаються з оборонною метою, а також через дефіцит людських, фінансових та технологічних ресурсів. У таких умовах матеріали ПФР рідко стають підставою для ініціювання повноцінних розслідувань ВК/ФТ, а паралельні фінансові розслідування, особливо щодо іноземних предикатних злочинів, практично не застосовуються.

**Висновки:**

- **Регулярне та пріоритетне використання матеріалів ПФР правоохоронними органами є ключовим фактором високої оцінки IO.6.** Без інституційного закріплення обов'язкового розгляду та використання аналітичних продуктів ПФР у розслідуваннях ефективність системи залишається обмеженою, незалежно від формальної відповідності стандартам.
- **Проактивне міжнародне співробітництво (спонтанні розкриття, швидка реакція, пріоритизація ризиків) є визначальною ознакою високої ефективності IO.2.** Юрисдикції, які обмежуються реактивними відповідями на запити, системно втрачають можливості для виявлення та припинення транскордонних схем ВК/ФТ.
- **Якість STR, особливо з боку ВНУП, прямо впливає на здатність ПФР генерувати аналітичні продукти, придатні для використання у фінансових розслідуваннях.** Практичні результати досягаються лише за умови цільового навчання, зворотного зв'язку та секторальних аналізів ризиків, а не шляхом нарощування кількості звітів.
- **Інвестиції в ресурси, IT-доступ і стратегічну аналітику ПФР мають мультиплікативний ефект для всієї системи ПВК/ФТ.** Доступ до реєстрів, зниження плинності кадрів, збереження напрацьованих підходів і методик роботи та розвиток стратегічного аналізу напряму корелюють з переходом від помірної до суттєвої та високої ефективності.

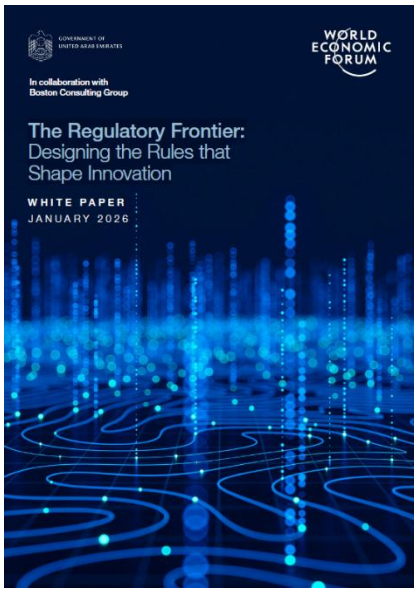
Для юрисдикцій із помірним рівнем ефективності характерні часткові зрушення: фінансова розвідка використовується для формування слідів розслідувань і підтримки кримінальних проваджень, однак залишається нестабільною з точки зору системності. Документ підкреслює, що проблеми якості та кількості STR зберігаються, особливо у секторах ВНУП, де рівень обізнаності та комплаєнсу часто є недостатнім. Додатковим стримувальним фактором виступають правові та процедурні бар'єри, зокрема високі пороги доступу до інформації або надмірна

орієнтація на предикатні злочини замість автономного переслідування ВК/ФТ. Навіть у юрисдикціях із суттєвим та високим рівнем ефективності документ не фіксує повної відсутності проблем, звертаючи увагу на потребу подальшого розвитку стратегічного аналізу, удосконалення зворотного зв'язку між ПФР, правоохоронними органами та суб'єктами фінансового моніторингу, а також забезпечення стабільного доступу до ключових державних реєстрів і баз даних.

Окрему аналітичну цінність документа становить його методологічний підхід. Автори детально описують процес якісного контент-аналізу ключових висновків і рекомендацій MERs, що дозволяє мінімізувати суб'єктивність і забезпечити порівнюваність результатів. Водночас прямо визнається, що навіть за такого підходу результати відображають насамперед системні тенденції п'ятого раунду оцінювання і мають бути інтерпретовані з урахуванням змін, закладених у методології шостого раунду FATF, зокрема посилення фокусу на ризик-орієнтований підхід та фінансову інклюзію.

У підсумку документ формує чітке концептуальне повідомлення: ефективність систем ПВК/ФТ визначається не рівнем технічної відповідності стандартам FATF, а здатністю ПФР бути активним, ресурсно забезпеченим і інтегрованим учасником національної та міжнародної екосистеми ПВК/ФТ. Саме регулярне використання фінансової розвідки правоохоронними органами, проактивне міжнародне співробітництво та інвестиції в аналітичну спроможність ПФР розглядаються як ключові умови переходу від формального виконання стандартів до реальних, вимірюваних результатів у боротьбі з фінансовими злочинами.

## Регулювання як інструмент конкурентної переваги в умовах технологічної трансформації [5]




Документ є концептуальним і водночас прикладним аналітичним дослідженням, у якому регулювання розглядається не як допоміжний інструмент стримування ризиків, а як повноцінний фактор формування інноваційної економіки, конкурентоспроможності держав і довіри суспільства. Центральна ідея документа полягає в тому, що в умовах прискореного технологічного розвитку класичні, статичні регуляторні моделі більше не відповідають реаліям ринку, а здатність держави проєктувати регулювання стає такою ж стратегічною навичкою, як і здатність створювати самі технології

Автори виходять з тези, що регулювання перестало бути реактивним механізмом, який «наздоганяє» інновації після появи ризиків або криз. Натомість воно дедалі частіше виконує роль інфраструктури, яка визначає швидкість масштабування нових рішень, напрями руху капіталу та те, які юрисдикції стають глобальними стандартами для інших. У цьому контексті регуляторні рішення прямо впливають на економічну стійкість, інвестиційну привабливість і геополітичну вагу держав. Документ підкреслює, що надмірно повільне або надто жорстке регулювання так само небезпечне, як і його відсутність: перше

5 https://reports.weforum.org/docs/WEF_The_Regulatory_Frontier_Designing_the_Rules_that_Shape_Innovation_2025.pdf

консервує ринки та витісняє інновації в інші юрисдикції, друге породжує недовіру, суспільний спротив і подальші заборони.

Аналітичне ядро документа побудоване навколо п'яти взаємопов'язаних доменів регуляторного дизайну, які разом утворюють цілісну «архітектуру» сучасного регулювання. Перший домен стосується визначення регуляторних меж і показує, що традиційні інституційні підходи, орієнтовані на тип суб'єкта, більше не працюють у середовищі, де технологічні компанії виконують фінансові, медичні чи інфраструктурні функції, не будучи класичними установами відповідних секторів. Як альтернатива пропонується діяльнісний і ризик-орієнтований підхід, за якого регулюється не статус організації, а характер дій і потенційний рівень шкоди. Це дозволяє одночасно забезпечувати захист суспільних інтересів і не блокувати експериментальні або низькоризикові інновації, підтримуючи довіру до регулятора як до раціонального архітектора ринку.

Другий домен присвячений регуляторному навчанню й еволюції правил на основі доказів. Документ розглядає регуляторні «пісочниці», спільне проєктування правил із бізнесом та міжнародні мережі регуляторів не як допоміжні інструменти, а як фундамент сучасного нагляду. Регулювання в цій логіці є живою системою, яка змінюється разом із технологіями, спираючись на емпіричні дані, результати пілотних проєктів і реальну поведінку ринку. Особливо наголошується, що відсутність чітких механізмів зворотного зв'язку перетворює інноваційні інструменти регулювання на формальність, унаслідок чого зміни відбуваються запізно і під тиском криз, а не завчасно й усвідомлено.

Третій домен аналізує дизайн доступу до ринку як критичний фактор трансформації інновацій у масове впровадження. Автори показують, що класичні ліцензійні режими, побудовані за принципом повної заборони або повного дозволу, не відповідають природі технологій, які розвиваються поступово й потребують перевірки в реальних умовах. Поетапні та умовні дозволи, відкриті технічні стандарти й інтероперабельність розглядаються як засоби забезпечення одночасно швидкості входу на ринок і збереження довіри. У цьому контексті регулятор виступає не лише арбітром, а й активним гарантом публічних інтересів, забезпечуючи рівні та недискримінаційні умови доступу до ринку і відповідаючи за те, щоб відкриті системи не були захоплені домінантними учасниками.

Четвертий домен розкриває ситуації, у яких регулятор виходить за межі нормотворчості та бере на себе роль створення спільної інфраструктури. Коли ринок не здатний самостійно забезпечити базові цифрові «рейки» — у сфері платежів, обміну даними або цифрової ідентифікації — держава може

**Висновки:**

- **Регулювання слід проєктувати як адаптивну систему, а не як статичний набір норм:** безперервні механізми навчання (пісочниці, спільне проєктування, обмін даними) мають бути інституціоналізовані, інакше правила неминуче відставатимуть від технологій.
- **Діяльнісний і ризик-орієнтований підхід до меж регулювання є критичним для міжсекторальних інновацій:** він дозволяє уникнути як «регуляторних прогалин», так і надмірного тиску на експерименти, зберігаючи довіру до ринку.
- **Поетапний доступ до ринку та відкриті стандарти мають замінити бінарні режими ліцензування:** це прискорює масштабування інновацій без втрати регуляторного контролю та знижує ризик концентрації ринку навколо домінантних цифрових суб'єктів, що здійснюють контроль доступу до ринку.
- **Країни та регулятори, які першими створюють узгоджені та передбачувані регуляторні рамки, формують глобальні стандарти:** регуляторна ясність стає інструментом конкурентної переваги, залучення капіталу та міжнародного впливу.

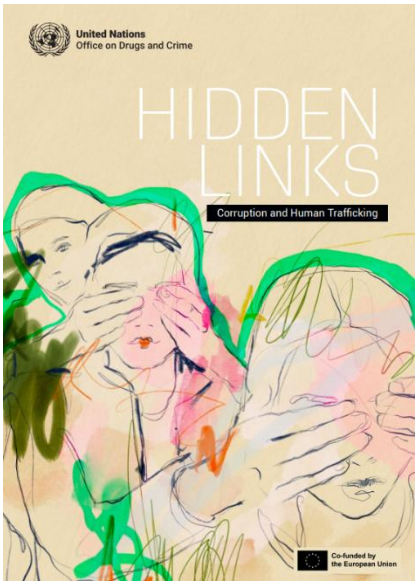
виступати як платформа, що знижує бар'єри входу та забезпечує масштабування. Водночас документ чітко фіксує ризики такого підходу: політизацію, витіснення приватних інвестицій і втрату нейтральності. Тому ключовим чинником успіху визнається не стільки технічний дизайн, скільки прозоре управління, підзвітність і чітке розмежування ролей регулятора як оператора й наглядового органу.

П'ятий домен зосереджений на адаптивності права та збереженні його легітимності в умовах постійних технологічних змін. Документ аргументує, що принципо-орієнтоване законодавство, технологічна нейтральність і моделі безперервної авторизації дозволяють поєднати правову визначеність для бізнесу з можливістю оновлення стандартів без постійного переписування законів. Втрата цієї здатності до адаптації розглядається як одна з головних загроз довірі, оскільки формально гнучкі, але фактично застарілі норми створюють правову невизначеність і фрагментацію ринків.

На основі поєднання п'яти доменів документ описує три типові регуляторні траєкторії: адаптивну, системну та конвергентну. Вони відображають різні стратегічні вибори держав залежно від інституційної спроможності, рівня ризику та потреби в міжнародній інтеграції. При цьому підкреслюється, що жодна з траєкторій не є універсальною або постійною, а ключовим фактором успіху стає узгодженість між доменами регулювання та здатність переходити від однієї моделі до іншої в міру зміни контексту.

Завершуючи аналіз, документ позиціонує регулювання як публічне благо і форму стратегічної сили. Регуляторні рамки, створені раніше за інших і сприйняті як легітимні та ефективні, перетворюються на глобальні еталони, впливаючи на міжнародні ринки та стандарти. Для регуляторів це означає потребу в розвитку форсайту, технічної експертизи та постійного діалогу з ринком, а для бізнесу — необхідність сприймати регулювання не як витрати на відповідність, а як частину продукту, довіри й довгострокової конкурентної стратегії.

## Приховані зв'язки безкарності: як корупція живить торгівлю людьми і підриває верховенство права [6]




Аналітичний звіт, підготовлений УНЗ ООН, є масштабним і концептуально цілісним дослідженням, яке розкриває корупцію не як супутнє або другорядне явище у сфері торгівлі людьми, а як один із її фундаментальних структурних елементів. Документ послідовно доводить, що у сучасних умовах торгівля людьми функціонує як форма організованої злочинності, яка глибоко вбудована у державні та напівдержавні інституційні процеси, а тому її відтворення на практиці неможливе без системної участі або толерування з боку корумпованих посадових осіб. Центральна ідея звіту полягає в тому, що корупція і торгівля людьми формують замкнений взаємопідсилювальний цикл: корупція створює умови для безперешкодного здійснення експлуатації, а доходи від цієї експлуатації використовуються для подальшого підриву інституційної доброчесності та забезпечення безкарності.

Звіт ґрунтується на винятково широкій емпіричній базі, яка включає аналіз понад 120 кейсів із майже 80 юрисдикцій, використання міжнародних і національних судових баз даних, матеріалів правоохоронних органів, медіа-розслідувань, а також системні консультації з прокурорами,

[6] https://www.unodc.org/documents/human-trafficking/2025/Publications/Corruption_and_TIP.pdf

слідчими, суддями, представниками міжнародних організацій, громадянського суспільства та журналістами. Така методологія дозволяє авторам вийти за межі поодиноких прикладів і реконструювати стійкі типології корупційної поведінки, виявити ролі різних категорій акторів і простежити, як подібні моделі повторюються у різних регіонах незалежно від рівня економічного розвитку чи формальної якості законодавства.

Концептуально звіт побудований навколо аналізу корупції на всіх етапах ланцюга торгівлі людьми, що дозволяє розглядати її не фрагментарно, а як наскрізний механізм забезпечення злочинної діяльності. На етапі вербування корупція постає як інструмент зловживання державними процедурами у сферах працевлаштування, соціального захисту, освіти, охорони здоров'я та опіки над дітьми. Документально зафіксовано, що посадові особи можуть як пасивно ігнорувати ознаки експлуатації або незаконної діяльності рекрутингових структур, так і активно сприяти їй шляхом видачі дозволів, фальсифікації документів, приховування порушень або прямої участі у торгівлі людьми. Особлива увага приділяється ситуаціям, коли корупція поєднується з експлуатацією вразливих груп — дітей, мігрантів, біженців, жінок, осіб у крайній бідності або соціальній ізоляції, — де владні повноваження посадових осіб використовуються для посилення контролю над жертвами та зменшення ймовірності їхнього звернення по допомогу.

На стадії переміщення, транзиту та приховування жертв корупція набуває системного характеру і стає ключовим чинником масштабованості торгівлі людьми. Звіт детально демонструє, як через хабарництво, зловживання службовим становищем і багаторівневу змову з посадовими особами міграційних, прикордонних, консульських і правоохоронних органів створюються «безпечні маршрути» для переміщення жертв як у межах держав, так і через міжнародні кордони. Корупція у сфері документування та прикордонного контролю дозволяє учасникам злочинних мереж з торгівлі людьми не лише переміщувати людей, а й легалізовувати їх перебування у країнах призначення, що істотно ускладнює подальше виявлення експлуатації. Важливим аспектом аналізу є роль приватного сектору — транспортних операторів, посередників, роботодавців, — які за умов слабкого нагляду або корупційного прикриття інтегруються у злочинні ланцюги і фактично виконують функцію інфраструктурного забезпечення торгівлі людьми.

На етапі експлуатації корупція виконує функцію довгострокового «захисного механізму», який дозволяє злочинним схемам існувати роками без істотного ризику викриття. Звіт охоплює різні форми експлуатації — примусову працю, сексуальну експлуатацію, вилучення органів, примусову жебрацьку діяльність, примусову злочинність та сучасні форми онлайн-експлуатації, зокрема шахрайські кол-центри. У документі показано, що посадові особи можуть діяти як пасивні «гаранти безкарності», які ігнорують порушення або попереджають учасників злочинних мереж з торгівлі людьми про перевірки, так і як активні учасники злочинів, безпосередньо отримуючи вигоду від експлуатації. Особливо наголошується на феномені «подвійної віктимізації», коли жертви стикаються не лише з насильством і примусом з боку учасників злочинних мереж з торгівлі людьми, а й з вимаганням хабарів, сексуальною експлуатацією або погрозами з боку представників державної влади, що остаточно руйнує довіру до інституцій захисту.

Системно важливою частиною звіту є аналіз корупції як перешкоди кримінальному правосуддю та антитрафікінговим зусиллям. УНЗ ООН демонструє, що навіть у випадках виявлення торгівлі людьми корупція на рівні поліції, прокуратури, судів і пенітенціарних органів призводить до витоку оперативної інформації, знищення або фальсифікації доказів, тиску на потерпілих і свідків, маніпуляцій із кваліфікацією злочинів і зосередження на другорядних епізодах хабарництва замість викриття системної змови. У результаті кількість притягнутих до відповідальності посадових осіб залишається непропорційно низькою, а відсутність повних і

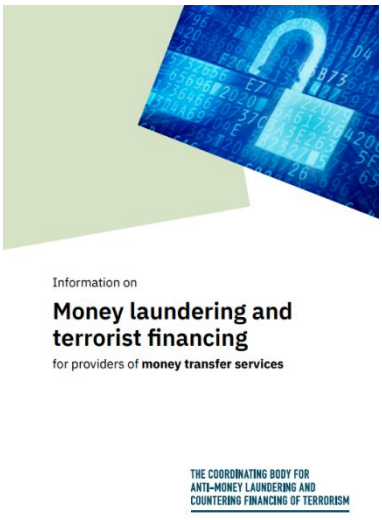
**Висновки:**

- **Корупція є системним і всеосяжним чинником торгівлі людьми та присутня на всіх етапах ланцюга —** від вербування і переміщення жертв до експлуатації та блокування кримінального правосуддя.
- **До корупційного сприяння торгівлі людьми залучене широке коло учасників,** включно з посадовими особами міграційних, прикордонних, правоохоронних, судових, соціальних і медичних установ, а також приватними суб'єктами, які діють у змові з організованими злочинними мережами.
- **Корупція істотно посилює шкоду для жертв торгівлі людьми,** призводячи до подвійної віктимізації, зниження рівня повідомлень про злочини та підриву довіри до державних інституцій.
- **Відсутність систематичного обліку, аналізу та переслідування корупційної складової у справах про торгівлю людьми сприяє безкарності та приховує реальні масштаби проблеми,** що унеможливлює формування ефективної політики протидії.

зіставних даних приховує реальні масштаби проблеми та підриває можливість формування доказової державної політики.

Узагальнюючи, звіт робить принциповий висновок, що корупція і торгівля людьми утворюють стійкий взаємопідсилювальний механізм, який підриває інституційну спроможність держав, еродує верховенство права і системно позбавляє жертв доступу до захисту та справедливості. УНЗ ООН наголошує, що ізольований підхід до протидії торгівлі людьми без одночасного, цілеспрямованого подолання корупції є концептуально хибним і практично неефективним. Натомість документ обґрунтовує необхідність інтегрованого підходу, який поєднує антикорупційні стратегії та заходи із запобігання та протидії торгівлі людьми, він базується на ризик-орієнтованому аналізі, інституційній доброчесності, захисті викривачів і потерпілих, цифровізації процедур, міжвідомчій та міжнародній координації як ключових передумов реального розриву механізму, в межах якого корупція сприяє торгівлі людьми, а доходи від торгівлі людьми живлять подальше корумпування.

## Грошові перекази та протидія злочинності: аналіз вимог шведського регулювання щодо запобігання відмиванню коштів та фінансуванню тероризму [7]




Швеція, яка посідає одне з провідних місць у світі за рівнем розвитку цифрової економіки та проникнення безготівкових платежів зіткнулася з парадоксальним викликом: відмова банків від масових готівкових операцій створила потужний стимул для злочинних угруповань переорієнтуватися на альтернативні фінансові сервіси, зокрема на мережі грошових переказів. Цей феномен став каталізатором для формування в країні одного з найбільш деталізованих та жорстких регуляторних ландшафтів у сфері протидії відмиванню коштів (AML) та фінансуванню тероризму (CFT) спеціально для цього сектора.

Документ, розроблений Координаційним органом, що об'єднує 17 ключових державних інституцій на чолі з Поліцією Швеції, є стратегічним інструментом трансформації ролі провайдера

[7] https://polisen.se/siteassets/dokument/om-polisen/penningtvatt/penningoverforaren_a5_2025_uk_ta.pdf/download/?v=cb6c43540263d028e17f51dc680e8a13

грошових переказів із пасивного виконавця операцій у активного захисника фінансової цілісності держави.

Важливо усвідомити, що сама природа бізнесу грошових переказів містить низку вбудованих вразливостей, які документ детально викладає. По-перше, це високий рівень анонімності або псевдонімності: отримувачу в багатьох випадках не потрібно мати банківський рахунок, а ідентифікація особи, яка фізично отримує кошти в країні-одержувачі, часто є неможливою або ненадійною. По-друге, значна частка операцій здійснюється готівкою, що ускладнює відстеження цифрового сліду. По-третє, глобальна мережа агентств дозволяє миттєво переміщати кошти через кордони, у тому числі в юрисдикції зі слабким наглядом або зони конфліктів. Саме ці характеристики, що роблять сервіс зручним для легальних користувачів, одночасно перетворюють його на ідеальний інструмент для легалізації прибутків від наркоторгівлі, торгівлі людьми, шахрайства та для фінансування терористичної діяльності. Документ прямо зазначає, що злочинці активно експлуатують цей канал, щоб розмити зв'язок між кримінальним джерелом коштів і їх остаточним використанням у легальній економіці, а також для трансферу коштів терористичним організаціям.

Відповідь регулятора на ці загрози – це не просто набір заборон, а комплексна філософія управління ризиками, вбудована в законодавчу площину. Її фундаментом слугує Закон про протидію відмиванню коштів та фінансуванню тероризму (2017:630), який імплементує стандарти FATF (Фінансової групи з протидії відмиванню коштів) та директиви ЄС. Однак справжню глибину підходу розкривають супутні норми, такі як регламент ЄС 2023/1113, що встановлює жорсткі вимоги щодо супровідної інформації (originator and beneficiary information) для всіх трансферів коштів, фактично усуваючи можливість абсолютно анонімних міжнародних переказів.

Ключовим елементом, що свідчить про закріплення нового статусу галузі, є обов'язкове ліцензування всіх провайдерів платіжних послуг з 1 липня 2025 року. Це історичний крок, який ліквідує режим винятків та формалізує галузь, зобов'язуючи всіх операторів, крім тих, хто надає лише інформаційні послуги про рахунки, пройти жорстку перевірку на відповідність вимогам AML/CFT. Невиконання цієї вимоги до кінця 2025 року призведе до припинення діяльності. Окремо акцентується увага на явищі «хавала» – неформальних альтернативних систем переказів, що існують поза традиційною банківською системою. Шведський регулятор закриває можливу лазівку, прямо заявляючи, що для надання таких послуг також потрібна ліцензія, що фактично означає спробу легалізувати та взяти під нагляд навіть тіньові канали.

Серцевиною практичної реалізації цих правил є концепція ризик-орієнтованого підходу. Це не кліше, а конкретна обов'язкова процедура, яка покладає на керівництво компанії відповідальність не лише за виконання інструкцій, але й за постійний аналітичний процес. Кожен провайдер зобов'язаний розробити, документально оформити та регулярно оновлювати Загальну оцінку ризиків для свого бізнесу. Цей внутрішній документ має бути глибоким аналізом, що враховує всі аспекти: від специфіки продуктів (наприклад, перекази готівкою в певні країни) та характеристик клієнтської бази (наявність нерезидентів, студентів, трудових мігрантів) до географії роботи агентів та можливостей нових технологій. Особливо сувора вимога стосується оцінки ризиків, пов'язаних із мережею агентів. Провайдер несе повну відповідальність за дії свого агента, тому він повинен чітко ідентифікувати, чи знаходиться агент у географічній зоні, визначеній Поліцією Швеції як «вразлива територія», які існують процедури контролю на місцях та наскільки ефективним є навчання персоналу агента. Загальна оцінка ризиків не є статичним звітом – це динамічна основа для всіх подальших дій компанії.

Саме на фундаменті цієї оцінки будуються всі внутрішні процедури та настанови, які документ вимагає впровадити. Центральне місце серед них займають процедури ідентифікації клієнта (KYC), які виходять далеко за межі перевірки паспорта. KYC в шведській інтерпретації – це

цілісний процес встановлення та підтвердження ідентичності клієнта, бенефіціарного власника (у випадку компаній), з'ясування джерела коштів та мети передбачуваних бізнес-відносин. Провайдер повинен чітко розуміти, чому клієнт відкриває рахунок або регулярно користується послугами, які суми очікуються і яка їх природа. Для разових транзакцій або серій пов'язаних транзакцій на суму від 1000 євро (еквівалент) такі заходи є обов'язковими. Документ наголошує на важливості виявлення осіб, що мають політично значуще становище (PEP), та застосування до них посилених заходів перевірки. Критично важливим є твердження про те, що якщо інформації, отриманої від клієнта, недостатньо для оцінки ризику AML/CFT, компанія не має права встановлювати або продовжувати бізнес-відносини. Це перетворює KYC з формальності на реальний бар'єр для входу.

Процедура моніторингу представлена як безперервний, активний процес аналітики, а не пасивне спостереження. Мета – виявлення будь-яких відхилень від нормального, зрозумілого шаблону поведінки клієнта. Це означає аналіз частоти, сум, валют, географії, типу одержувачів, а також порівняння транзакцій з відомою інформацією про фінансовий стан і бізнес-профіль клієнта. Документ прямо вказує, що інтенсивність моніторингу повинна бути прямо пропорційною ризиковості клієнта, визначеної під час оцінки. Для клієнтів з високим ризиком моніторинг має бути постійним і глибоким. Однак найбільш значущим елементом всієї системи, вершиною айсберга контролю, є обов'язок негайного звітування до ПФР при виникненні будь-яких обґрунтованих підозр. Документ чітко розмежовує поняття: для повідомлення не потрібні докази злочину, достатньо розумних підстав вважати, що операція пов'язана з відмиванням коштів або фінансуванням тероризму. Це ключовий момент, який знімає з працівників компанії обов'язок розслідування та переносить акцент на спостереження та інтуїцію, підкріплену знанням «червоних прапорців».

Особливу глибину документ набуває в частині, присвяченій фінансуванню тероризму. Тут автор проводить важливу концептуальну відмінність: якщо для відмивання ключовим є кримінальне походження активів, то для фінансування тероризму критичним є їхнє майбутнє призначення. Це означає, що терористична діяльність може фінансуватися зовсім невеликими сумами легально зароблених коштів, що робить традиційні індикатори відмивання неефективними. Документ підкреслює, що запобігання передачі навіть мінімальних сум у високоризикові регіони або конфліктні зони є критично важливим для підриву фінансового потенціалу терористичних організацій, оскільки вони живляться саме такими дрібними трансферами для оплати проживання, транспортних витрат, комунікації та тренувань своїх членів.

Система відповідальності за невиконання вимог є багаторівневою та суворою. З одного боку, Фінансова

Висновки:

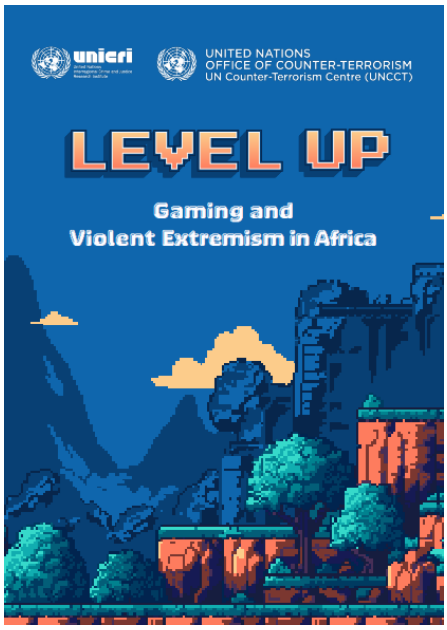
- **Шведська модель регулювання ґрунтується на превентивному, ризик-орієнтованому підході,** де провайдери грошових переказів несуть пряму відповідальність за активне виявлення, аналіз та протидію загрозам відмивання коштів і фінансування тероризму через власні сервіси, а не лише за формальне виконання правил.
- **Документ підкреслює критичну роль постійного моніторингу та звітування про будь-які обґрунтовані підозри до ПФР —** без необхідності надавати докази злочину.
- **Особлива увага приділяється вразливості неформальних систем переказів та обов'язковому ліцензуванню всіх операторів**, що свідчить про прагнення держави взяти під контроль усі канали руху коштів, включаючи тіньові.
- **Відділення фінансування тероризму як окремої загрози з акцентом на призначення коштів (а не їхнє походження)** вказує на необхідність спеціальної пильності щодо навіть дрібних транзакцій у конфліктні регіони.

інспекція (FI) має широкий спектр заходів адміністративного впливу: від обов'язкових наказів про усунення порушень до накладення штрафів (санкцій) та остаточного відкликання ліцензії, що рівнозначно закриттю бізнесу. З іншого боку, існує жорстка кримінальна відповідальність. Документ детально пояснює склад злочину комерційного відмивання коштів, який може бути інкримінований самому провайдеру або його співробітникам. Примітно, що для кваліфікації дій за цією статтею не обов'язково доводити кримінальне походження коштів. Достатньо довести, що підприємство або фізична особа, діючи в рамках бізнесу, свідомо пішли на невиправданий ризик, взявши участь у операції, метою якої могло бути приховання походження коштів. Це розширює поле відповідальності.

Окремо варто відзначити культурно-організаційні вимоги, висунуті до компаній. Це не лише створення процедур, але й реальної системи їх впровадження. Документ зобов'язує провести оцінку доброчесності (suitability assessment) всіх працівників та підрядників, чиї обов'язки важливі для AML/CFT, а також забезпечити їхню постійну освіту. Навчання має бути не формальним, а практично орієнтованим, включаючи знання нормативної бази, розуміння внутрішньої оцінки ризиків, процедур компанії та вміння розпізнавати «червоні прапорці». Для іноземних агентів відповідальність за їхнє навчання покладається на головного провайдера.

Отже, документ демонструє, як держава може трансформувати приватний бізнес у ефективну лінію оборони національної безпеки, перекладаючи макро-загрози на мову конкретних дій на мікрорівні. Успіх цієї моделі залежить від синергії між правовим регулюванням, чіткими діями наглядових органів, а також від реальної зміни корпоративної культури в компаніях, які повинні усвідомити свою роль не лише як постачальників послуг, але й як гарантів фінансової чистоти.

## Геймінг та екстремізм в Африці: глибинна аналітика нової цифрової загрози [8]




Дослідження, спільно підготоване Міжрегіональним дослідницьким інститутом ООН з проблем злочинності та правосуддя (UNICRI) та Офісом Контртероризму ООН (UNOCT), є ґрунтовним стратегічним документом, що прориває крізь поверхневі дискусії про вплив відеоігор. Воно розкриває складну панораму найдинамічнішого цифрового ринку світу — геймінгу — у перетині з найбільш гострою безпековою проблемою африканського континенту — екстремізмом.

Ця праця, створена за підтримки та експертизи Мережі досліджень екстремізму та геймінгу (EGRN), не лише діагностує реальність, але й виступає в ролі превентивного навігатора, будуючи сценарії майбутніх загроз та пропонуючи конкретні, практичні механізми захисту цифрових просторів, які вже за кілька років стануть домом для майбутніх мільйонів геймерів.

Африка переживає не просто цифрову трансформацію, а справжню демографічно-технологічну революцію, драйвером якої стало масове проникнення смартфонів, що змінило саму природу комунікації та дозвілля. За прогнозами GSMA, до 2030 року 751 мільйон жителів Африки на південь від Сахари буде володіти мобільними пристроями, причому 87% із них — саме смартфонами. Ця технологічна хвиля безпосередньо формує геймінговий ландшафт, трансформуючи мільйони пристроїв у ігрові. У 2024 році 32 мільйони африканців стали новими

[8] https://unicri.org/sites/default/files/2025-11/Level%20Up%20%E2%80%93%20Gaming%20and%20Violent%20Extremism%20in%20Africa%202025_0.pdf

геймерами, збільшивши загальну аудиторію до приблизно 349 мільйонів осіб, що становить майже десяту частину всіх геймерів планети. Аналітики вже окреслили тренд формулюваннями на кшталт «наступний мільярд геймерів буде африканським». Фінансові показники підтверджують цей бум: ринок ігор в Африці оцінювався у 1.8 мільярда доларів США у 2024 році, демонструючи річне зростання у 12.4% — темпи, що в шість разів перевищують світові, де зростання сповільнилось до 2.1%. Локальні ігрові студії стрімко розвиваються: з 2023 по 2024 рік кількість студій у Західній Африці зросла майже вп'ятеро, у Південній — у сім разів.

Ключовою, визначальною особливістю континенту є абсолютна гегемонія мобільного геймінгу: 92% опитаних геймерів у ключових ринках (Єгипті, Кенії, Нігерії та ПАР) грають саме на смартфонах. Це не просто розвага, а соціальна екосистема, що формує нові форми ідентичності та спілкування. З 17 найпопулярніших на континенті ігор 13 мають мультиплеєрний режим, а 11 — функцію внутрішньоігрового чату, перетворюючи такі хіти як PUBG Mobile, Call of Duty Mobile чи навіть Yalla Ludo у повноцінні соціальні мережі з інтегрованим голосовим спілкуванням.

Паралельно існують «офлайн-хаби» — ігрові центри та кібер-кафе, які залишаються доступними соціальними просторами, особливо для молоді, що не має власних потужних пристроїв. Ці центри часто є гендерно-гомогенними, з чоловічими домінуючими спільнотами, де проводяться локальні турніри та вирощується місцева кіберспортивна сцена. У таких просторах формуються потужні соціальні зв'язки, але, як зазначає дослідження, саме вони можуть стати вразливими для вербувальної діяльності. Гендерний аспект виявляється критично важливим: поширення мізогінії в ігровій культурі не лише завдає шкоди, але й, як показують дослідження, є потужним корелятом підтримки насильницького екстремізму, створюючи ґрунт для радикалізації.

Саме ця соціальна взаємопов'язаність, стрімке зростання аудиторії та наявність незахищених соціальних вузлів роблять геймінгові простори потенційно вразливими для експлуатації з боку терористичних та насильницьких екстремістських угруповань, які особливо активні в регіонах Сахелю, Східної Африки та Африканського Рогу. Хоча на момент дослідження зафіксовано небагато випадків прямого використання ігрових платформ африканськими терористичними групами (відомо лише про використання офлайн-ігор Боко Харам для тренування дітей-солдатів), автори, адаптуючи світовий досвід експлуатації ігор групами від ІДІЛ до неонацистів, будують шість реалістичних сценаріїв загроз, спеціально адаптованих до місцевих умов.

Перший сценарій — створення власних ігор та модифікацій. Такі групи, як JNIM у Сахелі, можуть, натхненні державними стратегіями підтримки геймінгу, розробляти ідеологізовані модифікації для популярних шутерів або створювати цілі ігрові світи на платформах на кшталт Roblox, інтегруючи наративи про боротьбу з «західним імперіалізмом. Ризик оцінюється як середньо-низький, проте вразливість велика через брак регулювання.

Другий сценарій — експлуатація офлайн-геймінг середовищ. Тут акцентується увага на таких групах, як Аш-Шабаб, які можуть використовувати ігрові кафе в Сомалі та Кенії або навіть громадські місця, де молодь грає на телефонах для встановлення першого контакту. Вербувальник може працювати в кафе або просто приєднатися до гри, використовуючи соціальні зв'язки та токсичну атмосферу, що іноді панує в таких чоловічих колективах, для «вирощування» кандидатів. Ризик цього сценарію оцінюється як високий, оскільки практичних бар'єрів для такого вербування немає, а вразливість очевидна.

Третій сценарій — вербування та комунікація в іграх. Він передбачає використання внутрішньо-ігрових чатів у популярних мобільних шутерах (PUBG Mobile, Free Fire, Call of Duty Mobile) групами на кшталт Ісламської Держави у Західній Африці (ISWAP) або JNIM для первинного контакту. Набираючи гравців у публічних іграх, фільтрованих за локальною мовою, вербувальники можуть потім переносити спілкування в зашифровані месенджери (Telegram, Signal) для подальшої радикалізації. Критичною проблемою є лінгвістична різноманітність

Африки: навіть такі поширені мови як амхарська погано охоплені модераційними алгоритмами платформ, що робить чати вільними для пропаганди. Ризик — середньо-високий через низький бар'єр входу для терористів та значну вразливість.

Четвертий сценарій — гейміфікація терористичного контенту. Це запозичення ігрової естетики для популяризації реального насильства. Сюди відносяться трансляції атак з коментарями як на кіберспортивних турнірах, створення «таблиць лідерів» у Telegram за кількістю жертв, відтворення реальних терактів у віртуальних середовищах (як Minecraft) для тренування або пропаганди. Досвід атак у Крайстчерчі та Буффало доводить ефективність такого підходу для залучення уваги. Ризик оцінюється як високий, оскільки нормалізація насильства через ігрову призму може знизити психологічні бар'єри для участі в тероризмі.

П'ятий сценарій — використання ігрових посилань та естетики для пропаганди. Відрізняється від першого тим, що акцент робиться не на геймплеї, а на створенні контенту для соцмереж. Групи можуть використовувати генеративний ШІ, інструменти з Minecraft або Roblox для створення пропагандистських мемів, аніме-стилізованих роликів або кліпів, що імітують геймплей, для поширення через TikTok, Instagram Reels та Telegram. Мета — вірусне поширення ідеології серед молоді. Ризик також високий через низький бар'єр створення та високий потенціал.

Шостий сценарій — фінансування тероризму та відмивання коштів. Він розглядає можливість використання внутрішньоігрових мікроплатежів, торгівлі віртуальними предметами (скінами), криптовалютних шлюзів або перепродажу ігрових ключів через треті сторони (типу Kinguin) для відмивання коштів, особливо коли традиційні фінансові канали перебувають під тиском. Проте, ризик оцінюється як низький, оскільки групи поки що мають простіші альтернативи фінансування (вимагання, «податки», контрабанда).

Дослідження виявляє не просто окремі загрози, а системні, структурні прогалини, які роблять всю африканську екосистему вразливою. Насамперед, це глибокий мовний розрив. Модераційні інструменти та алгоритми провідних глобальних платформ (від Meta до Google) практично не адаптовані до лінгвістичного ландшафту Африки. Відсутність класифікаторів, лексиконів та навчальних даних для таких мов як хауса, суахілі, амхарська чи сомалійська означає, що пропаганда, координація та вербування в текстових та голосових чатах можуть відбуватися абсолютно непомітно для автоматичних систем захисту.

По-друге, існує значний регуляторний та наглядовий вакуум навколо офлайн-просторів. Ігрові кафе, що є критично важливими соціальними вузлами, часто працюють без базових норм безпеки: відсутні вікові обмеження, навіть елементарні перевірки, немає підготовки персоналу щодо виявлення тривожних ознак, відсутня навіть інформація про лінії підтримки для жертв переслідувань.

По-третє, спостерігається дефіцит знань та спеціалізованих інструментів у правоохоронних органах. Поліція та спецслужби в більшості країн континенту не мають технічних можливостей, протоколів або навіть базового розуміння того, як здійснювати моніторинг, розслідування та збір доказів у середовищах голосових та текстових чатів популярних ігор, які за шифруванням та анонімністю часто не поступаються месенджерам.

На етапі Запобігання (Prevent) пропонується чотири ключові ініціативи. По-перше, створити «Африканський хаб безпеки в геймінгу» на базі держав чи структури ООН. Його завдання — бути центром компетенції: проводити щорічні навчання, а також фінансувати переклад стандартів безпеки та модерації на ключові африканські мови. По-друге, запровадити добровільну сертифікацію безпеки для ігрових кафе. По-третє, боротися з мізогінією як шляхом до екстремізму.

На етапі Виявлення (Detect) акцент робиться на людях та технологіях. Головна пропозиція — масштабне розгортання програми «Довірених модераторів спільноти» (ТСМ). Їх навчать розпізнавати не лише явну пропаганду, але й тривожні поведінкові патерни, пов'язані з вербуванням та радикалізацією. Для них створять легкий механізм звітування — через мобільний портал або чат-бот у WhatsApp, — який одночасно надсилає сигнал і в службу безпеки платформи, і в національний кіберпідрозділ.

На етапі Реагування (React) пропозиції зосереджені на допомогі постраждалим та втручанні в кризи. Ключовим є створення мережі направлень до психосоціальних служб. Коли ТСМ виявляє особу, яка може бути жертвою переслідування або демонструє ознаки радикалізації, він може анонімно ініціювати сигнал через спеціальну систему. Ця система має забезпечити, щоб регіональна неурядова організація з підтримки виходила на контакт протягом 24 годин. У регіонах, де таких організацій немає, система має надавати безкоштовні онлайн-ресурси з де-ескалації, самодопомоги або кризового консультування. Це замикає ланцюжок: від виявлення загрози до надання реальної допомоги людині, яка потрапила в ризиковану ситуацію.

Головний стратегічний висновок дослідження полягає в тому, що Африка, на відміну від Європи чи Північної Америки, де експлуатація геймінгу екстремістами вже стала реальністю, має унікальне, але вузьке вікно можливостей для проактивних дій. Є можливість вбудувати безпеку, стійкість та норми інклюзивності в геймінг-екосистему ще до того, як загрози стануть масштабними та системними. Це вікно обумовлене трьома факторами: стрімким, але ще не завершеним зростанням аудиторії; наявністю живої та інноваційної індустрії; та тим, що терористичні групи ще не перенесли свою вербувальну машину в цифрові ігрові простори континенту масово.

Проте, це вікно може швидко зачинитися. Демографічна динаміка, активність груп у Сахелі та Східній Африці, а також транскордонна природа геймінгу роблять питання надзвичайно актуальним. Захист — це не лише питання контртероризму, але й фундаментальна інвестиція в безпечний цифровий розвиток, захист прав мільйонів молодих людей, соціальну згуртованість та інклюзивність.

Висновки:

- **Африка стає епіцентром геймінг-революції,** де стрімке зростання мобільного геймінгу та соціально взаємопов’язаних ігор створює нові цифрові спільноти, але також і вразливості для вербування та радикалізації з боку терористичних угруповань, особливо в регіонах, уражених конфліктами.
- **Геймінг може стати новим фронтом терористичної діяльності через шість реалістичних сценаріїв:** від створення ідеологізованих модифікацій ігор та вербування в чатах до гейміфікації насильства та використання ігрової естетики в пропаганді.
- **Протидія вимагає проактивних, багатосторонніх рішень,** заснованих на принципах «запобігання, виявлення, реагування», включаючи розвиток локальних ініціатив, створення мережі довірених модераторів, адаптацію технологій модерації під локальні мови та налагодження взаємодії між державою, ігровою індустрією та громадянським суспільством.

Запропонований підхід, що поєднує зусилля держави, міжнародних організацій, бізнесу та громадянського суспільства з чітким дотриманням прав людини на приватність та свободу слова, може стати моделлю не лише для Африки, але й для інших регіонів, що розвиваються. Бездіяльність зараз, ігнорування цього, може призвести до того, що через кілька років соціальні зв'язки майбутнього будуть відбуватися не в безпечних і інклюзивних спільнотах, а в середовищах, де процвітають вербування, пропаганда насильства та радикалізація з усіма їхніми трагічними наслідками в реальному світі. Час діяти заздалегідь — зараз.

## Звіти окремих інституцій та експертів

### Механіка стабільності: Аналіз інструментарію стейблкоїнів від Wharton [9]

У січні 2026 року Wharton Blockchain and Digital Asset Project (BDAP) оприлюднив звіт, який пропонує глибокий академічний та ринковий аналіз екосистеми стейблкоїнів. Цей документ є спробою систематизувати знання про новий клас активів, що стрімко трансформує глобальну фінансову архітектуру, та надати регуляторам і учасникам ринку концептуальну рамку для розуміння ризиків і можливостей.

Для спільноти ПВК/ФТ цей звіт є цінним ресурсом, оскільки він деконструює економічну природу стейблкоїнів, виходячи за межі поверхневого розуміння їх як «криптовалют» і розглядаючи їх як інструменти грошового ринку нового покоління.

#### Стейблкоїни як міст ліквідності та розрахунків

Wharton визначає стейблкоїни як фундаментальний компонент екосистеми цифрових активів, що виконує функцію критичного моста між традиційними фінансами (TradFi) та ринками на основі блокчейну. Звіт акцентує на тому, що стейблкоїни забезпечують **фіналізацію розрахунків** у режимі 24/7/365, що є недосяжним для існуючих банківських систем (SWIFT, ACH), які залежать від банківських годин та кореспондентських ланцюжків.

Аналіз показує, що стейблкоїни еволюціонували від інструменту для арбітражу на криптобіржах до засобу транскордонних переказів та збереження вартості в країнах з високою інфляцією. Це створює нові виклики для фінансового моніторингу, оскільки потоки вартості стають швидшими, децентралізованими та глобальними за замовчуванням.

#### Регуляторні інновації та дилема ідентифікації

Центральною темою звіту є проблема застосування традиційних процедур **KYC** у децентралізованих системах. Автори аргументують, що класичні вимоги до ідентифікації є погано сумісними з архітектурою Web3, де користувачі оперують через некастодіальні гаманці (self-hosted wallets).

Як альтернативу, Wharton пропонує концепцію **децентралізованої ідентифікації (Decentralized ID)** та

**Висновки:**

- **Нова інфраструктура ринку:** Стейблкоїни слід розглядати не як спекулятивний актив, а як новий варіант платежів, що конкурує з картковими мережами та банківськими переказами.
- **Інновації в Compliance:** Майбутнє фінансового моніторингу у Web3 лежить у площині криптографічних доказів та децентралізованої ідентифікації, а не в механічному перенесенні паперових процедур у блокчейн.
- **Приватність vs Прозорість:** Звіт підкреслює необхідність гнучких механізмів контролю приватності, які дозволяють користувачам захищати свої дані, водночас забезпечуючи можливість аудиту та розслідувань у випадках зловживань.
- **Системна важливість:** Зі зростанням капіталізації стейблкоїнів вони стають системно важливими для стабільності традиційних фінансових ринків (через резерви в казначейських облігаціях), що вимагає відповідного пруденційного нагляду.

[9] https://bdap.wharton.upenn.edu/wp-content/uploads/2026/01/Stablecoin-Toolkit.pdf

використання **соціальних графів (social graphs)**. Цей підхід передбачає створення перевірених цифрових ідентифікаторів, які дозволяють підтвердити легітимність користувача без розкриття його персональних даних кожному контрагенту. Це дозволяє досягти балансу між приватністю (privacy) та підзвітністю (accountability), що є ключовим для відповідності вимогам ПВК/ФТ.

### Взаємодія TradFi та DeFi

Звіт розглядає сценарії взаємодії традиційних фінансів та децентралізованих протоколів. Рекомендується розвивати інструменти для управління схваленням транзакцій та покращення розкриття ризиків. Автори визнають, що TradFi та DeFi можуть існувати як паралельні системи, але вони потребують чітких "шлюзів" (bridges) та стандартів управління (governance standards) для забезпечення безпечної взаємодії. Особливий наголос робиться на тому, що регулювання повинно бути технологічно нейтральним і фокусуватися на економічній суті операцій, а не на програмному коді.

## Глобальний зсув у регулюванні криптоактивів: стейблкоїни, інституціоналізація ринку та нові виклики ПВК/ФТ у 2025 році [10]


Аналітичний звіт, підготовлений компанією Elliptic, є ґрунтовним і багатовимірним дослідженням еволюції глобального регулювання криптоактивів, яке фіксує 2025 рік як точку якісного зламу у сприйнятті, правовому оформленні та інституційному вбудовуванні криптоактивів у світову фінансову систему. Документ виходить за межі простого опису регуляторних змін і пропонує цілісну аналітичну картину того, як криптоактиви — насамперед стейблкоїни — стали об'єктом стратегічної уваги держав, центральних банків, органів фінансового нагляду та міжнародних стандартотворчих інституцій у контексті фінансової стабільності, платіжного суверенітету та протидії фінансовим злочинам.

У вступній частині звіту підкреслюється, що 2025 рік ознаменувався відмовою багатьох провідних юрисдикцій від підходів, заснованих на вибірковому правозастосуванні, регуляторній невизначеності та домінуванні санкційних і кримінальних інструментів. Натомість регулювання криптоактивів дедалі більше оформлюється як повноцінна галузь фінансового права з чітко визначеними ролями регуляторів, прозорими вимогами до учасників ринку та передбачуваними правилами доступу. У цьому контексті криптоактиви розглядаються не лише як джерело ризиків, а й як потенційний драйвер інновацій, конкуренції та модернізації фінансових ринків, за умови їх належної інтеграції у регуляторні рамки.

Особливе місце у звіті займає аналіз трансформації регуляторної політики США, яка у 2025 році стала ключовим каталізатором глобальних змін. Ухвалення GENIUS Act розглядається як історичний момент, що вперше закріпив на федеральному рівні комплексний режим регулювання стабільних криптоактивів, визначивши вимоги до резервного покриття, ліквідності, викупу, корпоративного управління та нагляду за емітентами. Водночас цей закон став інструментом повернення США у центр глобальної криптоінноваційної екосистеми, створивши умови, за яких конкуренція між учасниками ринку переміщується з площини регуляторного арбітражу у площину надійності, масштабованості та відповідності стандартам

[10] https://www.elliptic.co/resources/global-crypto-regulation-review-2025

фінансової доброчесності. Звіт наголошує, що не менш важливим був і перегляд позиції американських регуляторів щодо ролі банків, які у 2025 році фактично отримали можливість повноцінно взаємодіяти з криптоактивами, надаючи кастодіальні, платіжні та інфраструктурні послуги, що радикально підвищило рівень інституційної легітимності ринку.

На глобальному рівні звіт детально аналізує реакцію міжнародних стандартотворчих органів на стрімке зростання ролі стейблкоїнів у платіжних системах. Рада з фінансової стабільності у 2025 році зосередила увагу на фрагментованості імплементації своїх рекомендацій, підкреслюючи, що нерівномірне впровадження стандартів створює серйозні ризики регуляторного арбітражу та ускладнює ефективний нагляд за транснаціональними крипторинками. FATF, у свою чергу, зафіксувала, що стейблкоїни дедалі частіше використовуються у схемах відмивання коштів, фінансування тероризму, кіберзлочинності та обходу санкцій, що перетворює їх на пріоритетний об'єкт уваги для фінансових розвідок і наглядових органів. Звіт наголошує, що формальна імплементація стандартів ПВК/ФТ більше не є достатньою, а ключовим викликом стає операційна спроможність держав і приватного сектору забезпечувати ефективний моніторинг транзакцій, обмін інформацією та використання аналітичних інструментів на блокчейні.

Регіональний розріз звіту демонструє, що, попри спільні глобальні тенденції, підходи до регулювання залишаються значною мірою зумовленими політичними, економічними та геостратегічними факторами. В Європейському Союзі 2025 рік став першим роком повномасштабного застосування Регламенту MiCA, який створив єдину правову рамку для ринку криптоактивів і значно підвищив рівень правової визначеності для учасників. Водночас документ підкреслює внутрішні напруження, пов'язані з різними підходами держав-членів до перехідних положень, ліцензування та наглядової практики, що стимулює дискусії про посилення ролі наднаціональних органів і необхідність подальшого нормативного врегулювання децентралізованих фінансових моделей, які залишилися поза межами первинного регламенту.

**Висновки:**

- **У 2025 році більшість ключових юрисдикцій перейшли від правоохоронно-орієнтованого підходу до комплексних законодавчих режимів регулювання криптоактивів,** що забезпечують більшу правову визначеність і передбачуваність для ринку.
- **Стейблкоїни стали центральним фокусом глобального регулювання** через їх зростаючу роль у платіжних системах і транскордонних операціях, що призвело до впровадження спеціалізованих регуляторних рамок.
- **У 2025 році відбулося суттєве розширення участі традиційних фінансових установ у крипторинку** внаслідок зняття регуляторних обмежень і надання банкам дозволів на надання криптопослуг.
- **Регулятори та міжнародні органи у звіті відзначають, що нерівномірна імплементація глобальних стандартів у сфері криптоактивів створює ризики регуляторного арбітражу та ускладнює ефективний нагляд,** зокрема у частині ПВК/ФТ і Travel Rule.

У регіоні Азійсько-Тихоокеанського простору звіт описує високу поляризацію регуляторних стратегій, де окремі юрисдикції, такі як Гонконг, виступають флагманами інноваційного, але жорстко контрольованого підходу, поєднуючи високі стандарти ПВК/ФТ із використанням регуляторних пісочниць і активною інтеграцією банківського сектору. Інші країни регіону демонструють більш обережні або рестриктивні підходи, зумовлені занепокоєннями щодо фінансової стабільності або необхідністю виконання рекомендацій FATF для виходу з-під посиленого моніторингу. Водночас у звіті простежується чітка тенденція використання регулювання криптоактивів як інструменту геоекономічної конкуренції та елемента платіжного суверенітету, зокрема у контексті розвитку альтернативних

платіжних інфраструктур і зменшення залежності від домінування доларово-орієнтованих стейблкоїнів.

Узагальнюючи, документ формує розширене аналітичне бачення 2025 року як етапу глибокого інституційного дозрівання криптоекосистеми, коли регулювання перестало виконувати виключно стримувальну функцію і трансформувалося у механізм стратегічного управління розвитком фінансових інновацій. Водночас звіт чітко підкреслює, що подальша еволюція крипторинку буде залежати від здатності держав забезпечити баланс між інноваціями та фінансовою безпекою, ефективно імплементувати стандарти ПВК/ФТ, посилити міжнародну координацію та запобігти фрагментації глобального регуляторного простору, оскільки без цього криптоактиви можуть стати не інструментом розвитку, а джерелом системних ризиків для міжнародної фінансової системи.

## Афера за тиждень: ідеальна схема кіберзлочинності [11]


У світі, де цифрові взаємодії все частіше замінюють живі контакти, злочинці вдосконалили мистецтво обману до рівня тонкого психологічного конструкту, що базується на наукових підходах до маніпуляції свідомістю. Ексклюзивні матеріали результатів поліцейських рейдів на території Філіппін, отримані Reuters, відкривають завісу над одним із найбільш розповсюджених та руйнівних видів кіберзлочинності сьогодення — схемою, відомою як «pig-butchering». Цей термін точно відображає суть процесу: жертву годують увагою та емоційною підтримкою, створюючи ілюзію близькості та довіри, а потім ведуть на фінансовий «забій». Знайдені посібники китайською та англійською мовами — це не просто набори порад, це детальні стратегічні дорожні карти, розраховані на впровадження повномасштабного обман. Вони розкривають, як технології, глибинне розуміння людської психіки та організація праці перетворюють злочин на високоприбуткову індустрію.

Серцевиною механізму афери є ретельно сконструйована легенда — фальшива особистість, створена для максимальної привабливості для конкретної цільової аудиторії. Аналіз посібників показує, що злочинці проводять справжнє маркетингове дослідження, визначаючи архетипи, які викликають найбільшу довіру. Для жінок, як пояснює психолог Мартіна Дав, що вивчала матеріали, найефективнішими є образи успішних професіоналів — лікарів, юристів, військових чи інженерів, що поєднують статус із видимою стабільністю та емоційною стриманістю. Для чоловіків сценарії часто передбачають створення жіночого образу, який активно використовує мову емоційного підключення, духовного спілкування та ніжної турботи. Ці персонажі не статичні; вони динамічно адаптуються до відповідей жертви, створюючи враження справжньої взаємності та розуміння «на рівні душі».

Перший контакт, описаний у посібниках, може здатися невинним — стандартне привітання від невідомого номера. Однак за цим стоїть ціла система фільтрації. Перші години спілкування присвячені не просто знайомству, а швидкій психологічній діагностиці. Шахрай за шаблоном з'ясовує ключові моменти: чи переживала людина фінансові труднощі чи розлучення, чи мріє про швидке покращення життя, чи відчуває самотність. Кожна «так» у відповіді — це червоний прапорець, що позначає потенційно вразливу точку для подальшого впливу. Посібник містить

[11] https://www.reuters.com/graphics/SOUTHEASTASIA-SCAMS/MANUALS/klpyjlqelvg/

точні фрази, які, прикидаючись байдужим інтересом, витягують з людини інформацію, що робить її психологічно відкритою для подальших дій злочинця.

Наступний етап — інтенсивне «затоплення» позитивними емоціями. Це не просто компліменти; це структурована програма щоденного емоційного супроводу. Жертва отримує ранкові привітання, добраніч, питання про самопочуття, спільне обговорення книг чи фільмів, випадково знайдених «спільних» інтересів. Психологічна мета — викликати в мозку жертви асоціативний ланцюжок: спілкування з цією особою = отримання позитивних емоцій = залежність від цього спілкування. В одному з найбільш маніпулятивних моментів посібник рекомендує давати жертві невеликі, нібито незначні прохання («переглянь цю статтю та скажи свою думку», «нагадай мені зателефонувати завтра о 10»). Це класична техніка перевірки: виконання маленького прохання підвищує ймовірність згоди на більш значні дії в майбутньому, наприклад, на фінансову операцію.

Другий-третій день за планом вже включають перший голосовий дзвінок або спілкування через відеозв'язок (часто з використанням технологій Deepfake або попередньо записаних матеріалів). Тут сценарій прописує не лише теми для розмови, а й емоційний контекст: потрібно ділитися особистими, трохи меланхолійними спогадами, створюючи атмосферу виняткової довіри. Паралельно, дуже обережно, вводиться тема фінансів. Зазвичай це розповіді про власні успішні інвестиції, про «чудову можливість», якою злочинець нібито ділиться виключно через особливі почуття. Мова йде не про пряме прохання грошей, а про створення образу людини, яка розуміється на зростанні капіталу і щедро ділиться знаннями.

Четвертий-п'ятий дні — фаза «романтичного закріплення». Відносини формалізуються: пара називає себе закоханою, обговорюються плани на спільне майбутнє. Це критичний момент для створення когнітивного дисонансу у майбутньої жертви: як можна сумніватися в щирості людини, з якою у тебе стільки спільних планів і почуттів? Одночасно посилюється тиск на ізоляцію: зловмисник може ненав'язливо критикувати друзів або родичів жертви, які виявляють скепсис, натякаючи, що «тільки вони двоє розуміють одне одного по-справжньому». У цей же час починається підготовка до фінансової транзакції. Жертві демонструють (через підроблені скріншоти або доступ до фейкового кабінету) «прибутки» самого шахрая або інших «клієнтів».

Шостий-сьомий день — кульмінація. Жертві пропонують зробити перший, часто невеликий внесок на фейкову торгову платформу, яка імітує торгівлю нафтою, криптовалютою або акціями. Інтерфейс платформи професійний, цифри на рахунку зростають, що створює повну ілюзію успіху. Після цього включається фінальний механізм тиску: потрібно внести більшу суму, щоб «отримати доступ до преміум-сегменту», «сплатити податок на велику виплату» або, «оплатити екстрений внесок для виводу мільйонів». Важливо, що на цій стадії з жертвою часто починає працювати інший член злочинної групи, який видає себе за фінансового менеджера або технічного спеціаліста, надаючи процесу видимість легальності та професійної підтримки.

Окремою темою є соціально-економічний контекст, у якому існують ці схеми. Як повідомляє Reuters, значна частина таких афер керується з комплексів у Південно-Східній Азії, де тисячі людей, часто самі ставши жертвами торгівлі людьми, примусово працюють за конвеєрною системою. Вони живуть в ізоляції, працюють по 12-14 годин на день, відпрацьовуючи чіткі сценарії. Це перетворює кібершахрайство не просто на злочин, а на глобальну гуманітарну та правову проблему, де експлуатація одних жертв веде до руйнації життя інших.

Роль технологій у цих схемах не можна переоцінити. Штучний інтелект використовується для масового створення правдоподібних профілів у соціальних мережах, генерації індивідуалізованих листів, імітації голосів під час коротких розмов. Криптовалютні гаманці та миттєві транзакції ускладнюють відстеження коштів, а використання зашифрованих месенджерів — розслідування. Це перетворює боротьбу з такими аферами на постійні перегони озброєнь між правоохоронцями та злочинцями.

Захист від таких складних схем вимагає не обережності, а просвіти. Необхідно розуміти, що реальні романтичні стосунки розвиваються поступово, включаючи зустрічі в реальному житті, а не лише інтенсивне листування. Будь-які розмови про інвестиції з особисто незнайомою людиною, яка з'явилася в житті онлайн, повинні сприйматися як червоний прапор. Критично важливо обговорювати такі «знайомства» з друзями та родичами — зовнішній погляд часто помічає невідповідності, невидимі для того, хто знаходиться в емоційному полі впливу. Фінансові установи та платформи знайомств, зі свого боку, повинні впроваджувати більш складні системи верифікації користувачів та активно попереджати про ризики.

**Висновки:**

- **Сучасне кібершахрайство набуло форми структурованої психологічної війни,** де злочинці використовують детально розписані сценарії для маніпулювання жертвами через створення фальшивих емоційних зв'язків, що ведуть до фінансових втрат за короткий термін.
- **Методика «pig-butchering» базується на поетапному впливі:** від створення фейкової привабливої особистості та інтенсивного емоційного захоплення до введення теми інвестицій та фінансового шантажу з використанням фейкових платформ.
- **Ці схеми часто є частиною масштабних транснаціональних злочинних операцій,** що базуються в Південно-Східній Азії, де працівники можуть бути жертвами торгівлі людьми, а технології значно підвищують ефективність та складність викриття афер.

Отже, це більше ніж просто шахрайство. Такі схеми показують, як прагнення до близькості, розуміння та фінансової стабільності можуть бути перетворені на руйнівний інструмент. Боротьба з цим явищем вимагає комплексного підходу: посилення міжнародного співробітництва правоохоронних органів, суворішого регулювання криптоплатформ, а також глибинної психологічної просвіти громадськості. Тільки усвідомлюючи складність та масштаби маніпуляцій, людина може побудувати емоційний та цифровий імунітет, здатний протистояти навіть найвитонченішій архітектурі обману.

## Тіні в раю: як Палау стала вузлом глобальної мережі кібершахрайства [12]

Детальне розслідування, проведене OCCRP на основі масиву конфіденційних документів, розкриває тривожну реальність, приховану за ідилічним фасадом Палау — невеликої тихоокеанської острівної держави, відомої своєю незайманою природою. Виявлені матеріали не просто документують існування двох масштабних шахрайських центрів у готелях Cocoro та Beluu Sea View Resort, але й демонструють складний симбіоз між транснаціональною організованою злочинністю та впливовими місцевими елітами. Ця історія виходить за межі окремих злочинів, перетворюючись на вивчення системної вразливості держав з обмеженими ресурсами перед глобальними злочинними мережами, що шукають безпечні гавані для своєї діяльності. Файли включають оперативні звіти силових відомств Палау, аналіз конфіскованої цифрової техніки, дані корпоративного реєстру та фінансові

[12] https://www.occrp.org/en/investigation/foreign-workers-local-sponsors-inside-palaus-hotel-scam-centers

розслідування, що разом формують переконливу картину індустрії, яка працює на межі легальності та повної злочинності.

Серцевину цієї операції становили десятки іноземних працівників, переважно громадян Китаю, В'єтнаму та Малайзії, які прибували в Палау за привабливими офіційними запрошеннями на посади водіїв або інспекторів. Реальність, однак, була далекою від цих описів. Вони опинялися в переповнених, брудних кімнатах, де місяцями та роками не бачили сонячного світла, живучи та працюючи в одній будівлі. Їхня робота полягала у використанні складних, заздалегідь підготовлених скриптів для залучення жертв через онлайн-платформи, що пропонували азартні ігри та криптовалютні інвестиції. Свідчення, записані після рейдів у січні 2026 року, розповідають про умови, що межують з примусовою працею: контроль пересування, обмеження зв'язку з зовнішнім світом та постійний моніторинг. За словами Ерін Вест, засновниці організації Operation Shamrock, таке повне ув'язнення працівників на тривалі періоди є ознакою кричущого порушення прав людини і повністю відповідає шаблонам, що спостерігаються в аналогічних центрах по всій Південно-Східній Азії.

Проте найбільш показовим аспектом цієї схеми є механізм її легалізації та прикриття. Аналіз документів виявив, що практично всі працівники цих центрів мали абсолютно законні робочі візи, спонсоровані місцевими будівельними або IT-компаніями. Власниками цих компаній, як показав корпоративний реєстр Палау, виступали дві впливові фігури: Венс Полікарп, власник готелю Cocoro та колишній член наглядової ради органу, що регулює банківську діяльність у країні, та Еліас Камсек Чин, колишній віце-президент Палау. Саме ці структури, формально зайняті будівництвом або технологіями, служили каналом для масового в'їзду іноземців, яких потім використовувалися в злочинній діяльності. Звіт спеціалістів, найнятих силовиками Палау, прямо вказує, що операція в Cocoro Hotel керувалася «витонченою системою управління персоналом» і функціонувала як «структурована транснаціональна злочинна організація під прикриттям» цих легальних підприємств. Хоча прямі докази особистої причетності Полікарпа або Чина до шахрайства відсутні, створена ними система спонсорства та прикриття була життєво необхідною для існування центру, що безперешкодно працював понад два роки в країні з населенням одного невеликого міста.

Технологічна складова операції була високопрофесійною та спеціалізованою. На конфіскованих комп'ютерах знайшли цілий арсенал інструментів для онлайн-шахрайства. Серед них — повноцінна платформа для проведення онлайн-лотереї «6688 Caipiao», орієнтована виключно на китайськомовних користувачів, з рекламними баннерами, що обіцяли удачу та легкі гроші. Більш детальні файли містили покрокові інструкції для операторів щодо психологічного маніпулювання жертвами: від початкового залучення за допомогою щедрих, але фіктивних бонусів до емоційного тиску та вимагання все більших сум. За словами автора звіту, злочинці мали повний контроль над цими сайтами, що дозволяло їм маніпулювати балансами рахунків, створювати ілюзію виграшів та приховувати програші, систематично спустошуючи гаманці жертв.

Окремої уваги заслуговує криптовалютна складова схеми. За даними Фінансової розвідувальної служби Палау, аналіз блокчейну виявив «витончену та скоординовану схему криптовалютного шахрайства». Злочинці завантажували цифрові токени, які насправді не мали жодної цінності, в гаманці мільйонів користувачів популярної платформи, створюючи видимість активів. Прибуток від усієї діяльності, за оцінками Джей Хантера Ансона, керівника з інформаційної безпеки Міністерства фінансів Палау, досягав щонайменше 200 тисяч доларів на місяць лише з одного центру. Ці кошти, ймовірно, відмивалися та виводилися через складні ланцюжки криптотранзакцій, що ускладнювало їхнє відстеження.

Глибинна проблема, на яку вказують усі джерела, полягає в системній неспроможності Палау протистояти такому рівню загрози. У країні повністю відсутнє спеціальне законодавство про

кіберзлочинність, а правоохоронні органи не мають ні технічної експертизи, ні фінансових ресурсів для розслідування складних міжнародних схем. Наслідком цього стала фактична безкарність: затриманих під час рейдів іноземних працівників просто депортували, оскільки не існувало ні правових підстав, ні можливостей для їхнього судового переслідування. Як зазначає Ансон, діяльність шахрайських центрів у Палау не лише не згасає, але й стає «все гіршою та сміливішою», оскільки організатори розуміють свою практичну безпечність. Це створює замкнене коло: відсутність успішних справ не дає розвиватися експертизі, а відсутність експертизи унеможливлює розкриття справ.

Контекст цієї ситуації є суто глобальним. Палау — не унікальний випадок, а ланка в ланцюзі. Дослідження Управління ООН з наркотиків та злочинності (UNODC) фіксує поширення подібних «шахрайських композитів» з Південно-Східної Азії до таких віддалених регіонів, як Східний Тимор або грузинське місто Батумі. Санкції США та Великої Британії, спрямовані наприкінці 2025 року проти камбоджійського конгломерату Huione Group, пов'язаного з відмиванням коштів від «pig-butchering», а також проти низки осіб, пов'язаних з проектами в Палау, чітко вказують на інтеграцію острівної держави в міжнародну злочинну інфраструктуру. Китайські транснаціональні злочинні угруповання, що стоять за більшістю таких операцій, демонструють вражаючу адаптивність, швидко переносячи свої активи та персонал у нові юрисдикції зі слабшим контролем у відповідь на тиск у традиційних центрах, таких як Камбоджа або М'янма.

Висновки:

- **Слабке законодавство та відсутність спеціалізованих інструментів боротьби роблять держави вразливими.** У Палау повністю відсутнє законодавство про кіберзлочинність, а правоохоронні органи не мають ресурсів для розслідування міжнародних схем, що призводить до депортації злочинців замість їхнього судового переслідування.
- **Легалізація злочинної діяльності часто відбувається через спонсорство впливових місцевих фігур.** Робочі візи для працівників шахрайських центрів оформлювалися через компанії, пов'язані з колишнім віце-президентом та членами наглядових органів, що створювало видимість законності та ускладнювало виявлення.
- **Глобальний тиск лише зміщує активність шахрайських центрів, а не ліквідує їх.** Санкції та рейди в одних країнах призводять до швидкого перенесення операцій в інші юрисдикції зі слабким контролем, таких як Палау.

Таким чином, поєднання факторів — відсутність нормативної бази, обмежені можливості правоохоронних органів, наявність впливових локальних фігур, готових надавати прикриття (свідомо чи ні), а також стратегічне розташування — перетворило Палау на вразливу точку в глобальній мережі. Подолання цієї загрози вимагає не просто разових поліцейських рейдів, а комплексної багаторівневої стратегії. На національному рівні необхідне термінове ухвалення законів про кіберзлочинність, створення спеціалізованих підрозділів та посилення фінансового нагляду. На регіональному та міжнародному рівнях критично важливою є поглиблена координація між правоохоронними органами, обмін розвідувальною інформацією та спільні операції, спрямовані на розрив ланцюжків фінансування та спонсорства. Без цих кроків Палау та подібні їй юрисдикції залишатимуться не просто місцем злочинів, а стратегічними плацдармами, з яких глобальна індустрія шахрайства продовжуватиме свій рух, підриваючи безпеку та економіку в усьому світі.

# Інші новини

## VoidLink: Нова ера гібридних кіберзагроз на перетині ШІ та хмарних технологій [13]

У січні 2026 року дослідники Check Point Research та Sysdig оприлюднили деталі про новий, безпрецедентний за своєю складністю тип шкідливого програмного забезпечення для Linux-систем — VoidLink. Ця загроза знаменує перехід кіберзлочинності на якісно новий рівень, де поєднуються хмарна орієнтованість, глибока системна інтеграція та генеративний штучний інтелект як інструмент розробки.

### Технічна анатомія: Невидимість та адаптивність

VoidLink — це модульний фреймворк, написаний мовою програмування Zig. Вибір цієї мови забезпечує високу продуктивність, компактність коду та, що найважливіше, ускладнює аналіз традиційними інструментами, які заточені під C/C++ або Go.

### Ключові технічні інновації:

1. **Компіляція руткітів на сервері (Server-Side Rootkit Compilation — SRC):** Це революційна технологія у світі шкідливого ПЗ. Замість того, щоб містити в собі універсальний набір модулів ядра (що збільшує розмір файлу та ризик збоїв), VoidLink сканує систему жертви, визначає версію ядра Linux та відправляє ці дані на свій командний сервер (C2). Сервер "на льоту" компілює унікальний модуль (LKM або eBPF), ідеально підігнаний під конкретну систему, і відправляє його назад. Це забезпечує максимальну стабільність роботи та невидимість для систем захисту.
2. **Хмарна свідомість:** VoidLink "розуміє", де він знаходиться. Він розпізнає середовища AWS, Azure, Google Cloud, а також контейнери Docker та кластери Kubernetes. Його мета — не просто заразити сервер, а викрасти специфічні хмарні облікові дані (IAM tokens, API keys), що відкриває доступ до управління всією хмарною інфраструктурою жертви.
3. **Адаптивна скритність:** Шкідливе ПЗ розраховує "рівень ризику" оточення, виявляючи наявність EDR-систем (Endpoint Detection and Response). Залежно від цього рівня, воно змінює свою поведінку: від агресивного сканування до повного "заморожування" активності, щоб уникнути виявлення.

### Роль ШІ: Демократизація створення кіберзброї

Найбільш тривожним аспектом VoidLink є докази його створення за допомогою **генеративного штучного інтелекту**. Дослідники Check Point виявили артефакти (плани спринтів, структуру коду, коментарі), які вказують на те, що складний фреймворк, який зазвичай потребує роботи команди професіоналів протягом місяців, був створений, ймовірно, однією особою за допомогою просунутого AI-агента менш ніж за тиждень.

Це підтверджує, що ШІ радикально знижує поріг входу в створення складної кіберзброї. Тепер зловмисник-одинак може генерувати код рівня державних спецслужб (nation-state level), автоматизувати тестування та масштабувати розробку з неймовірною швидкістю.

### Опис загрози

[13] https://arstechnica.com/security/2026/01/never-before-seen-linux-malware-is-far-more-advanced-than-typical/

VoidLink представляє собою складну екосистему, що включає завантажувачі, імплантати, модулі комунікації (HTTP/2, WebSocket, DNS tunneling) та засоби антифорензики (очищення логів, перезапис видалених файлів). Він орієнтований на тривалу присутність у критичній інфраструктурі, шпигунство та викрадення даних, а не на швидке руйнування чи шифрування (як у програм-вимагачів). Його здатність ховатися на рівні ядра (використовуючи технологію eBPF) робить його майже невидимим для стандартних засобів моніторингу операційної системи. Поява такого інструменту вимагає перегляду підходів до захисту хмарних середовищ та моніторингу цілісності runtime-процесів.

## Цифрова павутина обману: як фейкові інвестиційні платформи слугують глобальним мережам шахраїв [14]


У світі, де фінансові можливості нібито доступні кожному, а цифрові технології стирають кордони, виникає парадоксальна загроза: чим простіше стає інвестувати, тим складніше відрізнити чесну пропозицію від витонченої пастки.

Розслідування «Scam Empire», проведене журналістами OCCRP, розкрило безпрецедентну за масштабами та організацією шахрайську мережу, яка протягом майже чотирьох років діяла на глобальному рівні, маніпулюючи довірою тисяч людей з різних куточків планети. Завдяки аналізу внутрішніх документів, витоку даних із кол-центрів та кропіткій роботі з корпоративними реєстрами, вдалося не лише виявити 81 інвестиційну платформу, що були частиною єдиного механізму, але й простежити їхній штучно створений зв'язок із престижними юрисдикціями, відсутність будь-якого реального регулювання та систематичне використання психологічних технік для маніпуляції жертвами. Ця мережа не була зборищем різнорідних проектів; вона була чітко структурованою імперією обману, де кожен елемент, від дизайну вебсайтів до сценаріїв телефонних розмов, був продуманий для максимізації прибутку шахраїв і повного позбавлення інвесторів їхніх заощаджень. Складність її виявлення полягала саме в імітації конкурентного середовища: кожна платформа мала унікальне ім'я, кольорову гаму, невеликі відмінності в переліку активів для торгівлі, що створювало повну ілюзію вибору для потенційного клієнта, який, обираючи між, наприклад, Finbok та Fintrexcap, насправді обирав лише різні двері в одну й ту саму кімнату, де його гроші мали безповоротно зникнути.

Справжнім нервом цієї імперії були кол-центри, розташовані в країнах із порівняно ліберальним законодавством у сфері телекомунікацій та фінансових послуг, таких як Ізраїль, Кіпр, Болгарія та Іспанія. Саме звідти оператори, які часто володіли кількома мовами, використовуючи складні психологічні методики. Вони працювали за детальними скриптами, які передбачали етапи від першого «теплого» контакту, де клієнту представлялися персональним аналітиком або фінансовим радником, до фінальної стадії активного тиску, коли потрібно було переконати жертву вкласти останні кошти під час «виключної ринкової можливості». Важливо розуміти, що ці люди не були аматорами; вони пройшли навчання, мали доступ до актуальної інформації про фінансові ринки (що додавало їхнім словам довіри) і вміло експлуатували емоції: жадібність, страх втратити шанс, бажання швидкої фінансової незалежності. Особливу увагу вони приділяли новачкам, які не мали досвіду та могли повірити в казкові умови. Платформи пропонували так

[14] https://www.occrp.org/en/project/scam-empire/these-81-investment-platforms-were-part-of-a-scam-network-heres-what-we-learned-about-them

звані «бонуси за реєстрацію», які насправді були класичним гачком — отримавши «подарунок» у вигляді бонусних коштів на рахунок, людина психологічно починала відчувати себе зобов'язаною і більш схильною вкладати власні кошти. Персональні «консультації» також були частиною вистави: «аналітик» міг протягом тижнів створювати враження успішної торгівлі, надаючи сфабриковані звіти про прибуток, поки не наставав момент для великого «інвестування», після якого зв'язок обривався, а платформа «зникала» або перейменовувалася.

Одним із найбільш вражаючих аспектів цієї схеми була система адміністрування та відмивання грошей. Всі платформи, незважаючи на зовнішню автономність, керувалися з єдиного центру. Внутрішня бухгалтерія велася в загальних електронних таблицях, де були детально розписані операції, «клієнтські» рахунки та рух коштів між різними брендами. Це дозволяло керівникам мережі в реальному часі моніторити ефективність кожної платформи, визначати, які з них привертають більше вкладень, і оперативно перерозподіляти ресурси. Прибутки від афери не залишалися на рахунках платформ; вони миттєво перенаправлялися через складну павутину офшорних компаній, зареєстрованих у юрисдикціях з мінімальним фінансовим наглядом. Ці фірми, часто засновані на підставних особах або викрадених документах, виконували роль пралень: кошти змішувалися, переказувалися між рахунками, іноді конвертувалися в криптовалюту, що робило їхнє фінальне відстеження майже неможливим для правоохоронних органів окремих країн. Таким чином, мережа була не лише інструментом для виманювання грошей, але й цілісною фінансовою інфраструктурою, орієнтованою на безпеку та прибутковість злочинної діяльності.

Детальний аналіз контактної інформації, зазначеної на сайтах платформ, виявив ще один шар обману. З 81 проекту 68 вказали фізичні адреси, створюючи враження наявності офісів у реальному світі. Проте жодна з цих адрес не відповідала місцю реальної операційної діяльності. Натомість платформи масово використовували адреси престижних бізнес-центрів у Лондоні, Франкфурті, Цюриху, Торонто або навіть на Канарських островах. Це була свідома стратегія, спрямована на експлуатацію стереотипів про надійність західних фінансових інститутів. Інвестор, особливо з країн, що розвиваються, бачачи британську чи швейцарську адресу, автоматично асоціював платформу з стабільністю, чесністю та високими стандартами регулювання. Насправді ці адреси часто були просто поштовими скринями, послуги яких надавалися віддалено, а іноді й взагалі вигаданими. Розслідування показало, що навіть ті, хто в корпоративних документах фігурував як генеральний директор британської компанії, могли фізично знаходитися в офісі кол-центру в Софії, віддаючи накази та отримуючи звіти через зашифровані канали зв'язку.

Для додаткової легітимізації шахраї вдавалися до відверто кримінальних методів, таких як підробка ліцензій та спонсорських угод. Кілька платформ на своїх сайтах розмістили скани документів, нібито виданих «Mwali International Services Authority» або «Anjouan Offshore Financial Authority». Для недосвідченого ока це виглядало як офіційні дозволи на фінансову діяльність. Однак, як підтвердив Центральний банк Коморських Островів, ці установи не мають жодного відношення до державних органів країни та не володіють повноваженнями ліцензування. Вони є вигаданими утвореннями, створеними саме для обслуговування потреб шахраїв. Аналогічно, на деяких сайтах з'являлися логотипи відомих автомобільних або спортивних брендів, супроводжувані написом «офіційний спонсор». Наприклад, були випадки використання логотипу BMW без жодних на те прав. Метою було створити підсвідомий зв'язок між платформою і світовим брендом, що символізує успіх, якість та надійність. Така практика не лише вводила в оману клієнтів, але й завдавала репутаційної шкоди самим брендам.

Реакція національних фінансових регуляторів стала важливим індикатором масштабу проблеми, але також продемонструвала обмеженість їхніх можливостей у боротьбі з транснаціональною злочинністю. Такі організації, як FINMA у Швейцарії, FCA у Великій Британії та комісії з цінних паперів різних провінцій у Канаді, включили більшість із 81 платформи до

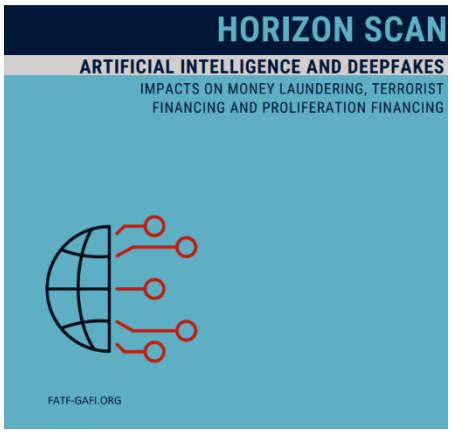
своїх попереджувальних списків як несанкціоновані. Ці попередження публікувалися на офіційних сайтах, про них могли повідомляти ЗМІ. Однак, як показало розслідування, для шахрайської мережі це було лише сигналом до оперативної перебудови. Як тільки конкретний бренд отримував «зайву увагу», його починали поступово «згортати»: припиняли активну рекламу, обмежували функціонал сайту, а потім і закривали його. Паралельно в межах тієї ж системи запускалася абсолютно нова платформа з іншим ім'ям, але тими самими шаблонами сайту, схожим дизайном і часто навіть тими ж самими «аналітиками» за телефонами. Дані з внутрішніх таблиць показали чіткий графік: після публікації регуляторного попередження надходження на рахунок «проблемного» бренду різко падали практично до нуля, а новий бренд за кілька місяців виходив на попередні обсяги вкладень. Це була безкінечна «гра в кота й мишу».

Журналістські запити до формальних власників цих компаній, виявлених у реєстрах, у більшості випадків закінчилися безрезультатно або отриманням заперечень. Люди, чиї імена фігурували в документах, стверджували, що їхні паспортні дані були використані без їхнього відома, що вони нічого не знають про діяльність платформ, і посилалися на інших осіб, нібито відповідальних. Це класичне прикриття для складних шахрайських схем, де справжні бенефіціари залишаються в тіні, а на передній лінії знаходяться підставні особи, часто зі складних соціально-економічних умов, які погоджуються на таку роль за невелику винагороду.

Підсумовуючи, розкрита мережа є яскравим прикладом того, як сучасні технології, глобалізація фінансових потоків та людські слабкості можуть бути об'єднані в потужний механіст для злочинного збагачення. Вона демонструє, що традиційні підходи до регулювання, заточені під національні юрисдикції, неефективні проти транснаціональних, швидких та технологічно оснащених угруповань. Боротьба з такими явищами вимагає не лише міжнародної координації правоохоронних органів і регуляторів, але й активної просвітницької роботи серед потенційних інвесторів, які повинні розуміти, що надмірно привабливі, позбавлені ризику обіцянки швидкого багатства в цифровому світі майже завжди є ознакою обману.

## Для загального розвитку

### AI-трансформація фінансової злочинності: нові ризики для системи ПВК/ФТ/ФР у світлі аналізу FATF [15]




Документ, підготовлений FATF, є стратегічним аналітичним дослідженням, спрямованим на випереджальне осмислення того, як розвиток штучного інтелекту, зокрема технологій діпфейків та генеративних моделей, трансформує ландшафт ризиків відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення. Документ розроблений у межах поетапного підходу FATF до нових і перспективних технологій і має на меті не лише зафіксувати вже наявні зловживання, але й окреслити майбутні сценарії ризиків, які можуть мати системний характер для глобальної архітектури ПВК/ФТ/ФР. Він адресований широкому колу суб'єктів – національним органам влади, фінансовим установам, постачальникам послуг, пов'язаних з віртуальними активами, визначеним нефінансовим установам та професіям, підрозділам

[15] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Horizon%20Scan%20AI%20and%20Deepfakes.pdf.coredownload.inline.pdf

фінансової розвідки і правоохоронним органам, – і покликаний стимулювати як регуляторні, так і операційні відповіді на нові загрози.

У вступній частині FATF підкреслює подвійний характер штучного інтелекту: з одного боку, він відкриває значні можливості для підвищення ефективності комплаєнсу, нагляду, фінансових розслідувань і аналітики, а з іншого – стає потужним інструментом у руках злочинців, терористичних мереж і суб'єктів, які обходять санкційні режими. Саме ця асиметрія розвитку – коли технології поширюються швидше, ніж оновлюються контрольні та наглядові механізми, – формує ключовий ризиковий фон, на якому побудовано весь аналіз. Документ ґрунтується, зокрема, на обговореннях під час робочих груп і Пленарного засідання FATF у червні 2025 року та поєднує емпіричні кейси з концептуальним прогнозуванням.

Перша частина дослідження зосереджена на діпфейках як найбільш зрілому та вже широко застосовуваному прояві зловживання AI у фінансовій злочинності. FATF детально описує, як синтетичні відео-, аудіо- та візуальні матеріали використовуються для переконливої імітації реальних осіб, подій і документів, що дозволяє обходити ключові превентивні бар'єри, передбачені Рекомендаціями FATF, насамперед у сфері належної перевірки клієнтів і дистанційної ідентифікації. Наголошується, що діпфейки суттєво підривають довіру до біометричних систем, відео-KYC та цифрових ідентифікаційних рішень, які раніше розглядалися як підвищення стандартів безпеки. Особливо небезпечним визнається те, що створення дипфейків перестало бути високовартісною або технічно складною діяльністю: сьогодні такі інструменти доступні практично будь-кому, що призводить до масштабування шахрайських схем і зростання кількості злочинів.

Документ докладно аналізує, яким чином діпфейки використовуються як низькокваліфікованими правопорушниками, так і професійними організованими злочинними групами. У першому випадку вони полегшують фішинг, споживче шахрайство, романтичні та інвестиційні схеми, у другому – стають частиною складних багаторівневих операцій, пов'язаних з відмиванням коштів, маніпуляціями на фінансових ринках і транскордонними потоками віртуальних активів. FATF підкреслює, що AI створює так званий «мультиплікатор злочинності», дозволяючи автоматизувати та масштабувати злочинні процеси, водночас зменшуючи потребу в людських ресурсах.

Через серію практичних кейсів документ демонструє реальні приклади використання діпфейків для обходу CDD, створення синтетичних або «гібридних» ідентичностей, а також для здійснення масштабних шахрайських операцій, включно з фальшивими відеоконференціями із «керівниками» міжнародних компаній і використанням підроблених медіаматеріалів для інвестиційних шахрайств. Важливий акцент зроблено на тому, що навіть найбільш просунуті автоматизовані системи не здатні повністю замінити людську експертизу, а виявлення таких схем часто стає можливим завдяки поєднанню аналітичної роботи фінансових розвідок, інформації від фінансових установ та міжвідомчої співпраці.

Окремо FATF розглядає належні практики реагування, підкреслюючи необхідність застосування багаторівневих моделей захисту, які поєднують технологічні інструменти виявлення синтетичних медіаматеріалів, розширені перевірки фактичної присутності та автентичності особи, багатофакторну перевірку достовірності доступу, а також посилені процедури моніторингу фінансових операцій. Документ звертає увагу на важливість інституційного навчання, створення спеціалізованих кіберпідрозділів, підготовки слідчих і прокурорів, а також розвитку державно-приватних партнерств як критично важливих елементів стійкості системи ПВК/ФТ.

Друга частина дослідження виходить за межі технологій створення синтетичних медіаматеріалів і має характер стратегічного огляду перспектив, присвяченого майбутнім ризикам, пов'язаним із генеративним штучним інтелектом, прогнозними аналітичними

моделями та автономними інтелектуальними системами. FATF описує потенційні сценарії, у яких злочинці можуть використовувати машинне навчання для імітації легітимної фінансової поведінки, створення синтетичних транзакційних патернів, що «зливаються» з нормальними потоками, або для повністю автоматизованого управління схемами відмивання коштів. Особливо небезпечними визнаються сценарії, у яких AI-агенти здатні в реальному часі адаптуватися до контрольних механізмів, аналізувати регуляторні матеріали та типології й цілеспрямовано обходити виявлені слабкі місця.

Документ також приділяє значну увагу використанню AI для професійного сприяння фінансуванню тероризму та обходу санкцій, зокрема через створення фіктивної торговельної документації, оболонкових компаній, синтетичних ланцюгів постачання та складних схем торговельного відмивання коштів. На цьому тлі FATF підкреслює, що AI ускладнює не лише виявлення та припинення злочинів, але й подальше розслідування, арешт активів і судове переслідування, зважаючи на проблеми доказовості, обсяги синтетичних даних і «непрозорість» алгоритмічних рішень.

У регуляторному вимірі документ констатує відсутність єдиного глобального підходу до регулювання AI та наголошує на важливості Рекомендації 15 FATF щодо нових технологій як базового інструменту для ризик-орієнтованого підходу. FATF розглядає цей стандарт як платформу для подальшої міжнародної координації, що має забезпечити баланс між використанням переваг AI та мінімізацією його системних ризиків.

Узагальнюючи, документ формує чітке стратегічне бачення: штучний інтелект і діпфейки вже стали чинником структурної трансформації фінансової злочинності, а не тимчасовим або периферійним ризиком. Відповідь на ці виклики потребує безперервного аналізу ризиків, адаптації наглядових і операційних механізмів, інвестицій у технології та людський капітал, а також посилення міжнародної та міжсекторальної співпраці з метою збереження цілісності глобальної фінансової системи.

**Висновки:**

- **CDD та цифрова ідентифікація потребують негайного перегляду:** фінансові установи та ВНУП мають перейти від формального використання біометрії до багаторівневих, динамічних моделей перевірки, що враховують ризики діпфейків і синтетичних ідентичностей.
- **AI стає інструментом як злочинців, так і захисту:** ефективна протидія можлива лише за умови активного впровадження AI в транзакційний моніторинг, виявлення аномалій та контент-верифікацію, а не лише шляхом регуляторних заборон.
- **Автоматизовані схеми відмивання коштів є найближчим системним ризиком:** регулятори та ПФР мають завчасно готуватися до появи інтелектуальних агентів AI, здатних здійснювати повністю автономні операції з ВК/ФТ/ФР, шляхом розвитку мережевої аналітики, пояснюваних моделей штучного інтелекту та моделей ухвалення рішень із обов'язковою участю людини.
- **Без міжсекторальної співпраці система ПВК/ФТ не витримає:** стійкість до AI-загроз залежить від глибоких державно-приватних партнерств, обміну типологіями, спільних навчань і формування пулу спеціалізованих експертів для розслідувань і судового переслідування.

## Ваша думка важлива!

1. Зважаючи на те, що діпфейки та 'синтетичні ідентичності' нівелюють ефективність традиційної біометрії, яким чином, на вашу думку, має трансформуватися архітектура процедур належної перевірки (CDD) у найближчі роки? Які саме параметри 'динамічної перевірки' або поведінкового аналізу ви вважаєте пріоритетними для впровадження, щоб відрізнити реального клієнта від цифрового клону?
2. Як Україні слід адаптувати національну систему ПВК/ФТ/ФР до зростаючого використання діпфейків і генеративного штучного інтелекту, зважаючи на високу частку дистанційних фінансових послуг, воєнний контекст та обмежені інституційні ресурси?
3. Враховуючи глобальний тренд на інтеграцію стейблкоїнів у традиційний банкінг та пропозиції Wharton щодо переходу на криптографічні докази, як ви бачите практичну реалізацію цих підходів в українському правовому полі? Які існують сценарії адаптації вимоги Travel Rule, щоб вони не заблокували розвиток DeFi-сектору, але зберегли прозорість потоків?
4. Наскільки інтеграція банківського сектору з криптоінфраструктурою є необхідною умовою для фінансової стійкості та прозорості ринку в Україні, і які ризики виникають, якщо банки залишаються осторонь крипторинку на тлі його інституціоналізації в США та ЄС?
5. Звіт FATF прямо вказує, що кількість повідомлень (STR) не дорівнює якості розслідувань. Що саме має змінитися у механізмі зворотного зв'язку між ПФР, правоохоронцями та приватним сектором, аби такий формат співпраці був би найбільш продуктивним?
6. Чи достатньо ефективна українська регуляторна система для виявлення та блокування транснаціональних фінансових афер, що маскуються під легальні інвестиційні платформи? Як війна та економічна нестабільність в Україні впливають на вразливість громадян до фінансового шахрайства, і чи може це стати приводом для посилення національної політики кібербезпеки та фінансового захисту населення?
7. Чи потребує Україна спеціалізованої стратегії або нормативної бази для захисту цифрових ігрових просторів від зовнішніх деструктивних впливів, і яку роль у цьому могли б відіграти держава, ігрова індустрія та волонтерські спільноти?

## Контактуйте щодо цього документу з Міністерством фінансів України:


- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-04


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

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