Методологічний бюлетень

Серійний номер: МінФін-AML-2026-01

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.

Ключові події 2025 року

Включення Росії до списку високоризикових третіх країн Європейського Союзу [1]

У грудні 2025 року Європейська Комісія ухвалила історичне рішення, закріпивши статус Російської Федерації як юрисдикції з високим рівнем ризику у сфері відмивання коштів та фінансування тероризму. Процес, що передував цьому рішенню, був тривалим і складним. Після призупинення членства Росії у Групі з розробки фінансових заходів боротьби з відмиванням коштів (FATF) у лютому 2023 року, європейські регулятори розпочали власну технічну оцінку ризиків, що походять від російської фінансової системи. У липні 2025 року був прийнятий

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2910

Делегований Регламент (ЄС) 2025/1393, який зобов'язав Комісію завершити перегляд третіх країн, чиє членство у FATF призупинено, але які ще не були включені до списків FATF.

Технічна оцінка Комісії підтвердила, що Росія має стратегічні недоліки у своєму національному режимі AML/CFT, які становлять суттєву загрозу для фінансової системи Європейського Союзу. У своєму прес-релізі від 3 грудня 2025 року Комісія наголосила, що російська правова та інституційна рамка не забезпечує достатньої прозорості та співпраці у розслідуванні фінансових злочинів, особливо в контексті обходу міжнародних санкцій.

Важливо зазначити, що це рішення є автономним кроком ЄС, який виходить за межі рекомендацій FATF. Хоча FATF продовжувала утримуватися від включення Росії до свого "Чорного списку" через відсутність повного консенсусу серед країн-членів, Європейський Союз використав своє суверенне право захищати власний внутрішній ринок. Регламент набуває чинності після періоду розгляду Європейським Парламентом та Радою ЄС, який зазвичай триває один місяць з можливістю продовження ще на один місяць.

Включення до списку високоризикових країн має фундаментально іншу природу, ніж санкційні обмеження. Якщо санкції зазвичай є адресними (спрямованими на конкретних осіб, сектори або товари), то статус "High-Risk Third Country" стигматизує всю юрисдикцію як токсичну для фінансових операцій.

Автоматичне застосування посиленої перевірки (EDD). Відповідно до статті 18a Директиви (ЄС) 2015/849 (4-та Директива AML), підзвітні суб'єкти (obliged entities) у всіх країнах-членах ЄС повинні автоматично застосовувати заходи посиленої належної перевірки до будь-яких ділових відносин або транзакцій, що залучають контрагентів з високоризикових країн. Це означає, що європейські банки більше не можуть покладатися на стандартні процедури при роботі з будь-якими російськими клієнтами або операціями, навіть якщо вони не підпадають під прямі санкції.

Операційна ізоляція. На практиці це може призвести до масового закриття кореспондентських рахунків та розриву ділових відносин (de-risking). Витрати на проведення EDD для кожної транзакції з російським елементом стають високими, і фінансовим установам може бути економічно невигідно підтримувати такі зв'язки. Це рішення фактично завершує процес фінансової ізоляції Росії від європейського ринку, перекриваючи канали, які могли використовуватися для "сірого" імпорту або виведення капіталу.

Вплив на треті країни. Рішення ЄС також надсилає потужний сигнал країнам, які продовжують активну співпрацю з РФ (наприклад, Туреччина, ОАЕ, країни Центральної Азії). Європейські фінансові інституції будуть змушені переглядати свої відносини з банками в цих юрисдикціях, якщо виявлять, що через них проходять російські кошти, оскільки це створює ризик "зараження" європейської фінансової системи.

Економічна блокада — Санкційна політика ЄС [2]

2025 рік продемонстрував рішучість Європейського Союзу не просто продовжувати санкційний тиск, а кардинально змінювати його якість. Прийняття чотирьох пакетів санкцій (з 16-го по 19-й) засвідчило перехід від стратегії "виснаження" до стратегії "задушення" ключових технологічних та логістичних артерій російської економіки.

[2] https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-packages-sanctions-since-february-2022/

16-й пакет санкцій (Лютий 2025): Удар по "Тіньовому флоту"

Приурочений до третьої річниці повномасштабного вторгнення, цей пакет сфокусувався на ліквідації механізмів обходу нафтового ембарго.

- **Блокада суден:** До санкційного списку було внесено **74 нових судна**, що ідентифіковані як частина "тіньового флоту" РФ. Загальна кількість заблокованих суден досягла 153. Цим суднам заборонено захід у порти ЄС, отримання страхових та технічних послуг.
- **Транспортна ізоляція:** Введено заборону для російських осіб володіти часткою понад 25% у європейських транспортних компаніях. Це закрило популярну схему створення фіктивних автоперевізників у Польщі та Балтії для обходу заборони на в'їзд вантажівок.

17-й пакет санкцій (Червень 2025): Боротьба з обходом

Цей пакет став логічним продовженням попереднього, розширивши список суден "тіньового флоту" ще на **189 одиниць**. Також було посилено експортний контроль щодо компаній з третіх країн (Китай, Туреччина, ОАЕ), які допомагають РФ отримувати товари подвійного призначення. Введено додаткові обмеження для енергетичного сектору.

18-й пакет санкцій (Липень 2025): Технологічний та фінансовий нокдаун

Прийнятий 18 липня 2025 року, цей пакет став одним із найболючіших для фінансової інфраструктури агресора.

- **Зниження Price Cap:** ЄС узгодив з G7 зниження цінової стелі на російську нафту з $60 до **$47.60** за барель. Це рішення, що набуло чинності у вересні 2025 року, має на меті критично знизити рентабельність російського нафтовидобутку.
- **Банківське ПЗ:** Вперше введено повну заборону на продаж, постачання та оновлення спеціалізованого банківського програмного забезпечення для уряду РФ та російських компаній. Це удар по серцю російського фінтеху, який залежав від західних рішень.
- **Заборона Nord Stream:** Повна заборона на будь-які транзакції, пов'язані з "Північним потоком 1" та "2", що унеможливлює навіть теоретичне їх відновлення.

19-й пакет санкцій (Жовтень 2025): Енергетичне ембарго та крипто-блокада

Прийнятий 23 жовтня 2025 року, цей пакет закрив останні великі лазівки.

- **LNG Ban:** Введено повну заборону на імпорт російського скрапленого природного газу (LNG). Враховуючи залежність деяких країн, встановлено перехідний період для довгострокових контрактів до січня 2027 року, а для короткострокових (spot) — 6 місяців.
- **Перші крипто-санкції:** ЄС вперше ввів прямі санкції проти конкретного криптоактиву — стейблкоїна **A7A5**, прив'язаного до рубля, та його емітентів (A7 LLC). Це безпрецедентний крок, що визнає криптоактиви об'єктом санкційного права на рівні з фіатними валютами.

- **Анти-інновації:** Заборона на надання послуг у сфері штучного інтелекту (AI) та квантових обчислень.

Кумулятивний ефект пакетів 2025 року призвів до системної деградації можливостей РФ вести зовнішньоекономічну діяльність.

Руйнування логістики нафтоекспорту: Внесення понад 500 суден (сумарно) до чорних списків створило кризу у морських перевезеннях. Глобальні страховики (P&I Clubs) масово відмовляють у покритті суден, що перевозять російську нафту, навіть якщо вона продається нижче price cap, через ризик вторинних санкцій. Це змушує РФ використовувати старий, аварійно небезпечний флот і платити величезні премії за ризик, що "з'їдає" прибуток від експорту.

Технологічна деградація банківського сектору: Заборона на банківське ПЗ (18-й пакет) має відкладений, але руйнівний ефект. Російські банки втрачають доступ до оновлень систем безпеки, комплаєнсу та управління ризиками. Це підвищує вразливість до кібератак та ускладнює інтеграцію з платіжними системами навіть "дружніх" країн, які працюють на міжнародних стандартах (ISO 20022).

Блокування альтернативних розрахунків: Санкції проти SPFS (російський аналог SWIFT) та стейблкоїна A7A5 (19-й пакет) руйнують стратегію побудови паралельної фінансової системи. Китайські та індійські банки, побоюючись втрати доступу до ринку ЄС, почали масово відмовлятися від роботи через SPFS, що призвело до затримок платежів на 3-4 тижні навіть у нацвалютах.

Робота фахівця з комплаєнсу у 2025 році вимагає переходу від формальної перевірки списків до глибокого розслідування (Enhanced Due Diligence).

Скринінг суден

Це новий "must-have" для фахівців у сфері торгового фінансування (Trade Finance). Необхідно інтегрувати автоматизовані системи перевірки номерів IMO. Кожен коносамент (Bill of Lading), що стосується нафти, нафтопродуктів або добрив, має перевірятися на предмет перевезення судном із санкційного списку. Також слід аналізувати історію маршруту судна: наявність відключень AIS (транспондерів) у відкритому морі є "червоним прапорцем" щодо перевантаження вантажу (STS transfer) з підсанкційного судна.

Програмне забезпечення як ризик

При обслуговуванні IT-компаній, що працюють на експорт, необхідно ретельно перевіряти кінцевих користувачів. Експорт ПЗ для фінансового сектору, хмарних рішень або AI до країн Центральної Азії (Казахстан, Киргизстан) вимагає додаткового підтвердження, що продукт не буде реекспортовано до РФ. Порушення заборони на експорт ПЗ (18-й пакет) несе такі ж ризики, як і експорт зброї.

Крипто-комплаєнс та A7A5

Фахівці повинні налаштувати свої системи блокчейн-аналітики на виявлення транзакцій, пов'язаних з токеном A7A5. Оскільки цей стейблкоїн використовувався для розрахунків за паралельний імпорт, його поява у ланцюжку транзакцій клієнта є прямим доказом порушення санкційного режиму. Будь-які вхідні платежі від платіжних систем, що працюють з цим токеном, підлягають блокуванню.

Операція «Мідас» [3]

У листопаді 2025 року Національне антикорупційне бюро України (НАБУ) та Спеціалізована антикорупційна прокуратура (САП) провели масштабну спецоперацію під кодовою назвою «Мідас». Розслідування, що тривало 15 місяців, викрило діяльність злочинної організації, яка систематично отримувала неправомірну вигоду від підрядників державного підприємства «Енергоатом».

Схема полягала у створенні штучних перешкод для підрядників (так званий «шлагбаум»): блокуванні платежів за виконані роботи або виключенні з переліку постачальників. Для розблокування оплат компанії змушені були платити «відкати» у розмірі 10-15% від суми контракту. Кошти легалізувалися через мережу компаній та «бек-офіс» у центрі Києва. Загалом задокументовано відмивання близько 100 мільйонів доларів США.

Низці осіб було оголошено підозри, серед яких - бізнесмени Тимур Міндіч та Олександр Цукерман, колишній радник міністра енергетики Ігор Миронюк, виконавчий директор з фізичного захисту та безпеки «Енергоатому» Дмитро Басов, а також працівники «бек-офісу».

Внаслідок операції було затримано 5 осіб. Суд обрав запобіжні заходи, зокрема тримання під вартою з альтернативою застави у розмірі 126 млн грн для колишнього радника міністра та 40 млн грн для посадовця «Енергоатому».

Ця справа є важливим сигналом для суб'єктів первинного фінансового моніторингу. **Практичні рекомендації та фокус уваги:**

1. **Моніторинг операцій з держпідприємствами:** Особливу увагу слід приділяти клієнтам-постачальникам стратегічних державних підприємств. Різке збільшення обсягів переказів на користь третіх осіб (консалтинг, маркетингові послуги тощо) після отримання державних коштів може свідчити про сплату «відкатів».
2. **Аналіз зв'язків (PEP):** Необхідно ретельно перевіряти ділові зв'язки клієнтів з політично значущими особами (PEP) та їхнім оточенням. У справі «Мідас» ключову роль відігравали «неофіційні радники» та посередники.
3. **Виявлення схем легалізації:** Схема включала використання «бек-офісів» та конвертацію коштів у готівку або криптовалюту. Фахівці повинні звертати увагу на нетипові операції з готівкою та перекази на криптогаманці.

Запуск роботи наднаціонального органу з ПВК/ФТ — AMLA: Нова ера централізованого нагляду в ЄС [4]

Європейський Союз у межах масштабного «AML-пакету» завершив у 2024 році підготовку до запуску нового наднаціонального регулятора – **Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)**. Уже 1 липня 2025 року ця агенція офіційно

[3] https://nabu.gov.ua/news/operatciia-midas-vykryto-vysokorivnevu-zlochynnu-organizatciiu-shcho-diiala-u-sferi-energetyky/
[4] https://www.amlintelligence.com/2025/07/official-amla-begins-operations-today-july-1/

розпочала свою діяльність, розмістившись у Франкфурті-на-Майні. AMLA стала першим центральним органом ЄС, відповідальним за нагляд та координацію в сфері AML/CFT на рівні Союзу. В її мандат входить прямий нагляд за найбільш ризикованими фінансовими установами ЄС (планується, що з 2026–2027 рр. AMLA визначить близько 40 таких суб'єктів і з 2028-го перебере їх на прямий контроль від національних регуляторів). Крім того, AMLA має повноваження видавати загальноєвропейські нормативно-правові акти (стандарти, технічні регламенти) та координувати обмін інформацією між фінрозвідками різних країн. Її створення – частина пакету, що включає також новий Регламент ЄС 2024/1620, прийнятий 31 травня 2024 року, який безпосередньо встановлює правила функціонування AMLA.

Запуск AMLA ознаменував **переломний момент** у підході ЄС до боротьби з фінансовими злочинами. Раніше нагляд за AML здійснювався лише національними регуляторами, що призводило до різного рівня ефективності та скандалів (як-от кейси Danske Bank, Wirecard тощо). Тепер же Євросоюз матиме **єдиний центр** прийняття рішень у цій сфері. Короткостроково, у 2025–2026 рр., AMLA займатиметься формуванням штату, методології та відбором піднаглядних установ. Проте вже сам факт її існування тисне на банки: очікується, що навіть до початку прямих перевірок компанії добровільно підвищать рівень відповідності, щоб не потрапити до списку «проблемних». AMLA отримає інструменти для транснаціональних розслідувань – зможе збирати дані, проводити **спільні інспекції** та накладати штрафи на порушників у межах усього ЄС. Це вирівняє практику: слабші ланки (де регулювання було м'яким) змушені будуть підтягнутися до рівня найсильніших. У глобальному вимірі поява AMLA підвищує вимоги і до партнерів ЄС. Країни-кандидати (як Україна) мають адаптувати своє законодавство, щоб відповідати новим регламентам ЄС. Також посилиться взаємодія ЄС зі США/Великобританією: AMLA стане контактним центром для міжнародних ініціатив.

Для українських фінансових установ і регуляторів увага до AMLA – це погляд у майбутнє. Банкам, що працюють з європейськими партнерами, слід врахувати: згодом правила гри будуть визначатися в Брюсселі/Франкфурті, а не тільки національними банками окремих країн ЄС. Це означає можливе **посилення вимог** до клієнтів-нерезидентів з України: європейські банки під оком AMLA будуть більш ретельно перевіряти українські компанії, особливо щодо бенефіціарів та джерел коштів. Українським фахівцям із комплаєнсу варто вже зараз ознайомитися з положеннями AML-пакету ЄС, оскільки Україна, прагнучи до членства, імплементує ці норми. Суб'єкти державного фінансового моніторингу з часом мають налагодити співпрацю з AMLA: обмін даними, методиками, участь у спільних тренінгах.

Регулювання віртуальних активів в Україні: Стратегічний вибір та баталії довкола законопроєкту № 10225-д [5]

Історія легалізації віртуальних активів (ВА) в Україні — це драма, що розгорталася протягом кількох років. Прийнятий ще у лютому 2022 року профільний закон так і не набрав чинності через відсутність змін до Податкового кодексу. Цей "законодавчий лімб" створив парадоксальну ситуацію: Україна стабільно входила до топ-країн за рівнем прийняття

[5] https://ips.ligazakon.net/document/ji12722i

криптовалют населенням, але весь цей ринок залишався у "сірій зоні", генеруючи мільярдні обороти поза фіскальним контролем та створюючи колосальні ризики для фінансового моніторингу.

2025 рік міг стати вирішальним. На порядку денному стояло завдання не просто прийняти податковий закон, а обрати модель розвитку: ліберальну, орієнтовану на перетворення країни на "крипто-офшор" (позиція Мінцифри), або консервативну, гармонізовану з європейським регламентом MiCA (Markets in Crypto-Assets), на чому наполягали МВФ та Національний банк України.

Ключовою подією року стало голосування у Верховній Раді України **3 вересня 2025 року**. Парламент 246 голосами підтримав у першому читанні законопроєкт № 10225-д «Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні».

Цей документ став результатом складного компромісу між різними групами впливу. На відміну від попередніх версій, доопрацьований законопроєкт ("д") врахував ключові вимоги міжнародних партнерів, зокрема МВФ, щодо недопущення розмивання податкової бази та захисту монетарного суверенітету.

Одним із найгостріших питань 2025 року була дискусія "Хто буде регулятором?". Міністерство цифрової трансформації тривалий час претендувало на роль ключового регулятора, аргументуючи це необхідністю підтримки інновацій. Однак, з огляду на позицію НБУ щодо ризиків доларизації економіки через стейблкоїни, у 2025 році було затверджено модель подвійного нагляду:

1. **Національний банк України (НБУ):** Отримує повноваження регулювати оборот віртуальних активів, що забезпечені валютними цінностями (токени електронних грошей, EMT). Це логічно, оскільки такі активи (наприклад, USDT, USDC) фактично виконують функцію грошей і прямо впливають на монетарну стабільність.
2. **Національна комісія з цінних паперів та фондового ринку (НКЦПФР):** Стає регулятором для всіх інших видів віртуальних активів (asset-referenced tokens, utility tokens) та відповідає за ліцензування та нагляд за постачальниками послуг, пов'язаних з віртуальними активами (VASP – Virtual Asset Service Providers).

Попри позитив, ставка 18% + 5% викликає занепокоєння учасників ринку. В умовах глобальної конкуренції юрисдикцій, трейдери можуть обрати зміну податкового резидентства на користь країн з більш лояльним режимом (ОАЕ, Сальвадор, Португалія). Це створює ризик, що Україна отримає регулювання, але втратить значну частину активних гравців ринку.

Що це означає для фахівців у сфері фінансового моніторингу

Для суб'єктів первинного фінансового моніторингу події 2025 року вимагають певної перебудови підходів до роботи з клієнтами, що володіють віртуальними активами.

Фахівці більше не можуть просто відмовляти в обслуговуванні клієнтам через наявність операцій з криптовалютою. Натомість, вони повинні розробити складні матриці оцінки ризиків:

- Source of Wealth (SoW) / Source of Funds (SoF): Головним викликом стане верифікація джерел походження ВА. Якщо клієнт декларує дохід від "раннього інвестування в Bitcoin", фахівець має вимагати не просто скріншот балансу, а криптографічно підтверджену історію транзакцій, що доводить володіння адресою в минулому.
- Робота з VASP: При обслуговуванні криптобірж як корпоративних клієнтів, банки повинні будуть проводити аудит їхніх AML-процедур. Чи використовує біржа інструменти блокчейн-аналітики? Чи дотримується вона "Travel Rule"? Відсутність позитивних відповідей на ці питання зробить обслуговування VASP неможливим.

Фахівці з фінмоніторингу повинні самі опанувати інструменти блокчейн-аналітики. Поняття "чистоти гаманця" стає таким же важливим, як і кредитна історія. Особливу увагу слід звертати на взаємодію клієнта з міксерами (Tornado Cash), даркнет-маркетплейсами або підсанкційними особами (наприклад, Garantex). Використання технологій обфускації транзакцій після набрання чинності законом буде розглядатися як спроба відмивання коштів.

Глобальний "Шок TD Bank": Рекордні штрафи та визнання провини у відмиванні коштів [6]

Однією з найбільш резонансних подій, що сколихнула глобальний фінансовий світ і мала безпосередній вплив на стандарти комплаєнсу у 2025 році, стала справа TD Bank. Хоча основні юридичні дії розгорнулися у жовтні 2024 року, повний масштаб наслідків, включаючи виплату штрафів, впровадження зовнішнього моніторингу та перегляд стратегій іншими гравцями ринку, припав саме на 2025 рік.

TD Bank (Toronto-Dominion Bank) став першим національним банком в історії США, який визнав себе винним у змові з метою відмивання грошей. Банк погодився виплатити сукупний штраф у розмірі 3,09 мільярда доларів США регуляторам, включаючи Міністерство юстиції (DOJ), Мережу боротьби з фінансовими злочинами (FinCEN) та Управління контролера грошового обігу (OCC).

Розслідування виявило шокуючі факти: протягом майже десятиліття (2014–2023) банк не оновлював свої системи моніторингу транзакцій, керуючись парадигмою "плоских витрат" (flat cost paradigm). Це призвело до того, що 92% обсягу транзакцій з 2018 по 2024 рік залишалися без належного моніторингу. Через рахунки банку було відмито понад 670 мільйонів доларів наркокартелів та інших злочинних угруповань. Співробітники банку не лише ігнорували "червоні прапорці", але й активно сприяли злочинцям, отримуючи хабарі у вигляді подарункових карток.

Справа TD Bank створила новий прецедент у регуляторній практиці — накладення "стелі активів" (asset cap). Окрім фінансових стягнень, регулятори заборонили банку відкривати нові філії або розширювати свої активи у США до повного усунення недоліків. Для глобального банку це є найтяжчим покаранням, оскільки воно зупиняє розвиток бізнесу та дає перевагу конкурентам.

Крім того, банку було призначено зовнішнього незалежного спостерігача (independent monitor) строком на чотири роки. Ця особа має необмежений доступ до внутрішніх документів банку та

[6] https://www.justice.gov/criminal/case/united-states-america-v-td-bank-na

звітує безпосередньо уряду, що фактично означає втрату банком суверенітету над власною функцією комплаєнсу.

Для глобального ринку це стало сигналом, що економія на AML-системах є найдорожчою помилкою, яку може зробити фінансова установа. У 2025 році спостерігалося різке зростання інвестицій у RegTech та оновлення застарілих систем моніторингу в банках по всьому світу.

Рекордні штрафи для криптовалютних компаній [7]

2025 рік став історичним у сфері міжнародного правозастосування AML/CFT, продемонструвавши **зсув фокусу** з традиційних банків на фінтех і криптоіндустрію. Під прицілом опинилися криптовалютні біржі, платіжні платформи та небанківські посередники. Сумарно у 2025 році штрафи за недотримання AML для різних суб'єктів у США перевищили $1,1 млрд, і **найбільша частка припала саме на криптообмінники – понад $927 млн** (близько 85% всіх стягнень). Серед покараних – такі гіганти як *BitMEX*, *KuCoin*, *OKX*, які були оштрафовані Мін'юстом США за умисне невпровадження належних KYC/AML-програм і відмивання коштів через їхні платформи (окремо KuCoin сплатив $297 млн штрафу, OKX – $504 млн). Одночасно регулятори приділили увагу й секторам переказів, цінних паперів та казино (разом ~15% штрафів). Щодо санкційного комплаєнсу, найбільшим випадком стало стягнення $216 млн з інвесткомпанії GVA Capital (США) за управління грошима підсанкційного російського олігарха в обхід санкцій. **Нова риса 2025 року** – поява перших в історії **спільних дій кількох регуляторів штатів** проти однієї компанії. У січні регулятори 8 штатів разом уклали мирову угоду з компанією *Block, Inc.* (власник Cash App) на $80 млн штрафу за виявлені недоліки програми фінмоніторингу. А в липні п'ять штатів спільно оштрафували компанію *Wise US* (платіжний сервіс) на $4,2 млн за проблеми з поданням повідомлень про підозрілу діяльність і збоями у моніторингу транзакцій. Така координація регуляторів стала сигналом про новий підхід до нагляду у фінансовому секторі США.

Ці тенденції свідчать про **еволюцію ризиків** та адаптацію контролюючих органів. Переорієнтація на криптобіржі означає, що регулятори більше не вважають їх «сірою зоною» – навпаки, 2025 року криптоіндустрію поставили в один ряд з банками щодо відповідальності. Для глобального ринку це призвело до підвищення стандартів: великі біржі вимушені впроваджувати процедури ідентифікації клієнтів, моніторингу транзакцій та блокування коштів, пов'язаних з відмиванням, щоб уникнути багатомільйонних санкцій. Факт відсутності великої кількості штрафів для банків можна частково пояснити тим, що банки інвестували значні ресурси в AML-системи після хвилі скандалів 2010-х – і тепер ці інвестиції дали результат. Але можливо, це й **тиша перед бурею**: регулятори перевіряють нові сектори, тоді як банки все одно залишаються під постійним наглядом. Спільні дії регуляторів штатів сигналізують про **посилення координації**: різні органи об'єднуються, щоб охоплювати великі міжнародні платформи, таким чином уникаючи ситуації, коли компанія «грає на різниці» між вимогами різних штатів чи країн. Така модель, ймовірно, стане прикладом і для інших юрисдикцій – можливо, у ЄС регулятори також проводитимуть

[7] https://finintegrity.org/aml-cft-and-sanctions-enforcement-actions-in-2025/#:~:text=This%20will%20likely%20go%20down,corporates%20involved%20in%20trade%20transactions

спільні перевірки під егідою AMLA. В підсумку, 2025-й дав зрозуміти: **нові технології – нові штрафи**, і compliance має йти в ногу із розвитком фінансових послуг.

Українським фінансовим установам і регуляторам слід врахувати світові уроки. По-перше, якщо в структурі бізнесу банку чи фінкомпанії є взаємодія з криптовалютами (напряму чи опосередковано), потрібно негайно зміцнити цей напрям: впровадити процедури **AML для віртуальних активів** (Travel Rule, моніторинг адрес гаманців, санкційні списки для крипто), навчити персонал виявляти транзакції, пов'язані з обмінниками, міксерами тощо. Досвід США показує, що такі транзакції більше не залишаються непоміченими – і хоча в Україні поки нема мільйонних штрафів, цього не варто чекати, краще діяти на упередження. По-друге, фінмоніторинг підзвітних небанківських установ (платіжні сервіси, системи переказів) має бути не менш суворим, ніж у банках. NBFI мають оновити свої програми підозрілих операцій: випадок Wise US демонструє, що **неподання своєчасно SAR/STR** та технічні збої в моніторингу – серйозне порушення, за яке настає покарання. Український регулятор (НБУ) вже в 2025 почав штрафувати небанківський сектор, і світовий тренд підтверджує цю лінію. По-третє, варто звернути увагу на **міжвідомчу співпрацю**. Хоча в Україні різні регулятори часом діють окремо, приклад штатів США може спонукати до більш тісної координації всередині країни. Для працівників з фінмоніторингу це означає готовність відповідати одночасно вимогам кількох органів.

Боротьба проти анонімності (Tornado Cash, Samourai Wallet, Bitcoin Fog): Прецедент відповідальності розробників коду

2025 рік став роком, коли правоохоронна система США за підтримки глобальних партнерів остаточно зруйнувала популярний у криптоспільноті наратив "Code is Free Speech" (Код — це свобода слова). Серія судових вироків створила залізобетонний прецедент: розробники програмного забезпечення, що сприяє анонімізації фінансових потоків, несуть повну кримінальну відповідальність за дії користувачів їхнього софту.

Tornado Cash: Справа Романа Сторма [8]

У серпні 2025 року суд присяжних Південного округу Нью-Йорка виніс історичний вердикт у справі **Романа Сторма**, співзасновника децентралізованого міксера Tornado Cash. Сторм був визнаний винним у змові з метою ведення неліцензованого бізнесу з переказу грошей.

Це рішення стало шоком для індустрії, оскільки Tornado Cash позиціонувався як децентралізований протокол (smart contract), який працює автономно. Однак прокуратура довела, що розробники отримували прибуток через токени TORN, підтримували інтерфейс сайту (UI) та свідомо ігнорували факти використання сервісу хакерами (зокрема, Lazarus Group). Хоча присяжні не змогли досягти одностайності щодо звинувачень у відмиванні коштів та порушенні санкцій (що призвело до часткового "глухого кута" у цих пунктах), сам факт криміналізації розробки коду для переказу коштів створив новий правовий стандарт.

[8] https://www.justice.gov/usao-sdny/pr/founder-tornado-cash-crypto-mixing-service-convicted-knowingly-transmitting-criminal

Важливим юридичним нюансом стала паралельна справа у П'ятому апеляційному суді США, де розглядалося питання, чи є смарт-контракти "власністю", яку можна санкціонувати. Рішення суду про те, що незмінні смарт-контракти *не є* власністю у розумінні закону IEEPA, створило колізію, але не врятувало Сторма від кримінальної відповідальності за ведення бізнесу.

Samourai Wallet: Вирок за "Privacy as a Service" [9]

У листопаді 2025 року завершилася справа проти засновників біткоїн-міксера Samourai Wallet. **Кеонн Родрігес** (CEO) був засуджений до 5 років позбавлення волі, а **Вільям Хілл** (CTO) — до 4 років. Окрім тюремних строків, суд ухвалив рішення про конфіскацію активів на суму понад **$237 млн**.

Слідство довело, що Samourai Wallet був не просто інструментом приватності, а цілеспрямовано рекламувався як засіб для обходу санкцій та відмивання коштів з даркнету. Функції "Whirlpool" та "Ricochet" були прямо націлені на розрив ланцюжка транзакцій для обману біржових систем AML. Вирок показав, що надання послуг мобільного міксування (CoinJoin) без процедур KYC є тяжким злочином.

Bitcoin Fog: Легітимізація блокчейн-аналітики [10]

Хоча основний вирок оператору Bitcoin Fog **Роману Стерлінгову** (12,5 років в'язниці) був винесений раніше, у 2025 році відбулася ключова апеляційна стадія, яка закріпила статус блокчейн-аналітики. Суд відхилив спроби захисту визнати методи компанії Chainalysis (зокрема, евристики кластеризації та інструмент Chainalysis Reactor) "ненауковими". Це рішення створило прецедент: звіти аналітичних компаній тепер є допустимими та надійними доказами у суді на рівні з ДНК-експертизою.

Загалом, події 2025 року призвели до екзистенційної кризи сектору Privacy Tech.

1. **Розширення визначення VASP:** Тепер під визначення "money transmitter" підпадають не лише кастодіальні гаманці чи біржі, а й розробники некастодіального софту, якщо вони зберігають будь-який контроль над протоколом (наприклад, через ключі адміністратора, DAO-голосування або контроль над інтерфейсом) та отримують вигоду.
2. **Токсичність міксерів:** Використання будь-яких сервісів міксування (навіть з легальною метою) тепер автоматично маркує кошти як "High Risk" або "Illicit". Жодна регульована біржа не прийме такі кошти без ризику втрати ліцензії.
3. **Масовий Delisting:** Біржі почали масово делістити анонімні монети (Privacy Coins: Monero, Zcash, Dash) та токени, пов'язані з міксерами, щоб уникнути звинувачень у сприянні анонімності.

Для українських та світових фахівців ці події означають необхідність впровадження "нульової толерантності" до анонімізації. Системи моніторингу повинні бути налаштовані на виявлення патернів міксування.

- **Пряма взаємодія:** Будь-які транзакції з адресами, маркованими як Tornado Cash, Samourai Whirlpool, Wasabi CoinJoin, підлягають негайному блокуванню та звітуванню (SAR/STR).
- **Непряма взаємодія (Hops):** Слід аналізувати глибину зв'язків. Зазвичай ризиковими вважаються кошти, що пройшли через міксер менше ніж 5-10 "хопів" (кроків) тому.

[9] https://www.irs.gov/compliance/criminal-investigation/founders-of-samourai-wallet-cryptocurrency-mixing-service-sentenced-to-five-and-four-years-in-prison
[10] https://www.chainalysis.com/blog/bitcoin-fog-daubert-hearing-chainalysis/

- **Peeling Chains:** Фахівці повинні вміти розпізнавати техніку "очищення" (peeling chains), яку часто використовують після міксерів для дроблення сум.

Необхідно чітко розмежовувати прозорі DeFi-протоколи (наприклад, Uniswap, де транзакції прозорі) та протоколи з обфускацією. Клієнт, що активно користується DEX, не обов'язково є злочинцем, але клієнт, що користується Tornado Cash, з точки зору регулятора 2025 року, є особою, що вчиняє спробу відмивання коштів, доки не доведено зворотне.

При встановленні ділових відносин з криптобіржею, банк повинен вимагати підтвердження, що біржа має політику блокування коштів з міксерів. Якщо VASP дозволяє ввід коштів з Tornado Cash, такий партнер є токсичним для банку.

Безпрецедентні заходи НБУ: посилення нагляду і рекордні штрафи

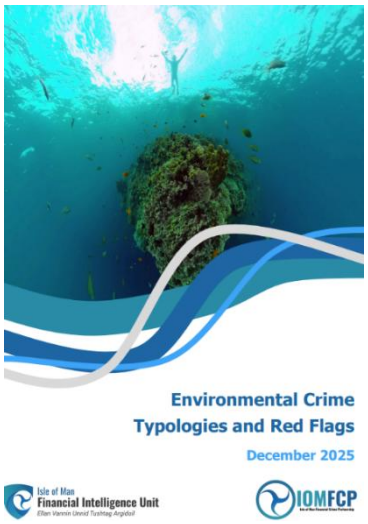
Національний банк України різко посилив контроль за дотриманням вимог фінансового моніторингу в 2025 році, що вилилося у значне зростання кількості санкцій до банків і фінансових установ. У травні НБУ оштрафував 2 банки і 6 небанківських установ за порушення в сфері фінмоніторингу, а вже в липні застосував рекордні заходи – штрафи отримали 2 банки і 21 небанківська організація. Найгучнішим інцидентом стали дії проти платіжної компанії **«НоваПей»**: її оштрафовано на 90 млн грн за недотримання правил фінмоніторингу.

Активізація наглядових дій НБУ суттєво підвищила роль відповідності (compliance) у фінансовому секторі. Великі штрафи і публічність цих кейсів сигналізують усім гравцям ринку про **нульову толерантність** до нехтування AML/CFT-нормами. Це спонукало банки та небанківські установи терміново переглянути свої процедури: посилити моніторинг транзакцій, навчити персонал ознакам підозрілих операцій і забезпечити належне документування дій фінансового моніторингу. На макрорівні такі заходи покращують імідж України в очах міжнародних партнерів (зважаючи на вимоги MONEYVAL), але і вказують на проблемні місця – наприклад, недоліки у внутрішньому контролі деяких фінансових компаній. Регулярні порушення, які фіксував НБУ, спонукали до тіснішої координації між регуляторами та правоохоронцями, що підвищує ефективність виявлення складних схем.

Для відповідальних за фінмоніторинг осіб в українських установах такі прецеденти – серйозне попередження. **Ризик-апетит** фінансових установ має бути знижений: операції, раніше сприймані як допустимі, тепер можуть призвести до штрафів. Комплаєнс-фахівцям слід ретельно перевіряти високоризикові операції (великі готівкові транзакції, перекази за кордон, роботу з PEP тощо) і без зволікань подавати повідомлення про підозри. Особливу увагу слід приділити сегменту небанківських платіжних установ, який продемонстрував вразливість – випадок з NovaPay свідчить про необхідність посилення контролю в компаніях FinTech-сектору. Внутрішні аудити та стрес-тести систем фінмоніторингу наразі є обов’язковими заходами, аби виявити і усунути недоліки до приходу перевірки НБУ.

Звіти міжнародних організацій та окремих юрисдикцій

Екологічні злочини як предикатні злочини у сфері відмивання коштів: типології, фінансові ризики та індикатори виявлення [11]



Документ, підготовлений Фінансовою розвідкою острова Мен, є комплексним аналітичним і практично орієнтованим дослідженням, присвяченим екологічним злочинам як повноцінному та системно недооціненому джерелу доходів від відмивання коштів і суміжних фінансових правопорушень. У його основі лежить усвідомлення того, що сучасна екологічна злочинність давно перестала бути локальною проблемою охорони довкілля і перетворилася на транснаціональний кримінально-економічний феномен, який генерує значні, стійкі та повторювані фінансові потоки, що активно інтегруються у формальну фінансову систему через банки, трастові та корпоративні структури, страхові та інвестиційні продукти, а також ринок нерухомості

У вступі документ чітко визначає свою роль у межах міжнародної системи протидії відмиванню коштів і фінансуванню тероризму, прямо пов'язуючи його підготовку з виконанням Рекомендації 29 FATF, яка покладає на фінансові розвідки обов'язок не лише реагувати на підозрілі повідомлення, але й проактивно формувати аналітичні продукти, що підвищують спроможність регульованого сектору виявляти нові та еволюціонуючі загрози. Документ також позиціонується як внесок у роботу Егмонтської групи щодо ролі ПФР у боротьбі з екологічною злочинністю, що відображає зміну міжнародної парадигми, відповідно до якої незаконна вирубка лісів, незаконний вилов риби, торгівля дикими тваринами, незаконний видобуток корисних копалин і серйозні форми забруднення довкілля розглядаються як складові глобальної організованої злочинності з безпосереднім фінансовим виміром.

Розкриваючи зміст поняття екологічних злочинів, автори свідомо відходять від вузьких юридичних дефініцій і застосовують широке функціональне тлумачення, яке охоплює не лише самі протиправні дії проти довкілля, а й пов'язані з ними фінансові та економічні правопорушення. Екологічні злочини у документі описуються як діяльність, що базується на незаконній експлуатації природних ресурсів, системному обході регуляторних вимог, використанні корупційних зв'язків і слабкості контролю у вразливих юрисдикціях. Наведені оцінки глобальних масштабів такої злочинності, що вимірюються сотнями мільярдів доларів США на рік, використовуються для аргументації тези про її високу привабливість для організованих злочинних мереж і здатність конкурувати за прибутковістю з традиційними кримінальними ринками.

Окремий розділ присвячений специфіці острова Мен як міжнародного фінансового центру та біосферного резервату ЮНЕСКО, що створює подвійний контекст відповідальності. З одного боку, документ визнає, що більшість екологічних предикатних злочинів фізично вчиняються за межами юрисдикції острова, проте з іншого — наголошує, що саме міжнародні фінансові центри з розвиненою інфраструктурою корпоративних і трастових послуг є ключовими вузлами для легалізації доходів, отриманих від таких злочинів. У цьому контексті екологічна злочинність розглядається як реальна загроза фінансовій цілісності та репутації юрисдикції, а не як абстрактна зовнішня проблема.

Важливим аналітичним елементом документа є результати опитування регульованого сектору, які виконують функцію емпіричного підтвердження існуючих прогалин у сприйнятті ризиків.

[11] https://www.fiu.im/media/1251/environmental-crime-typology-december-2025.pdf

Дані опитування демонструють, що значна частина фінансових установ, ВНУП та інших суб'єктів майже не розглядають екологічні злочини як потенційне джерело доходів від відмивання коштів, мають обмежене або поверхневе розуміння їх типів і механізмів, не проводять спеціалізованого навчання персоналу та не використовують окремі індикатори або типології для їх виявлення. У документі ці результати інтерпретуються як системна вразливість фінансового сектору, яка створює сприятливе середовище для використання його інфраструктури злочинними мережами.

Центральне місце у документі займає детальний виклад типологій екологічних злочинів із внутрішнім та міжнародним предикатним складником, які подані у формі реалістичних сценаріїв, заснованих на аналізі SAR, міжнародному обміні інформацією та OSINT. Через ці сценарії послідовно демонструється, як доходи від незаконного вилову, знищення природних середовищ, незаконної вирубки лісів, незаконного видобутку корисних копалин і торгівлі дикими тваринами проходять класичні стадії відмивання коштів — від первинного розміщення через складні етапи розшарування до остаточної інтеграції у формальну економіку. Особливу увагу приділено використанню офшорних компаній, складних корпоративних структур, фіктивних консультаційних і інвестиційних схем, схем зворотного кредитування, страхових продуктів і операцій з нерухомістю, а також ролі професійних посередників, номінальних власників і політично значущих осіб у приховуванні реального бенефіціарного контролю.

Документ постійно підкреслює практичний вимір наведених типологій, фокусуючись на тих фінансових і поведінкових ознаках, які можуть бути виявлені у процесі належної перевірки клієнтів, посиленої перевірки клієнта та транзакційного моніторингу. Невідповідність між заявленими доходами і стилем життя, непрозорі джерела статків, економічно необґрунтовані фінансові рішення, ранній викуп довгострокових продуктів, платежі до юрисдикцій з підвищеними екологічними та корупційними ризиками і використання третіх осіб для приховування контролю розглядаються не ізольовано, а як сукупні сигнали, здатні вказувати на зв'язок із екологічною злочинністю.

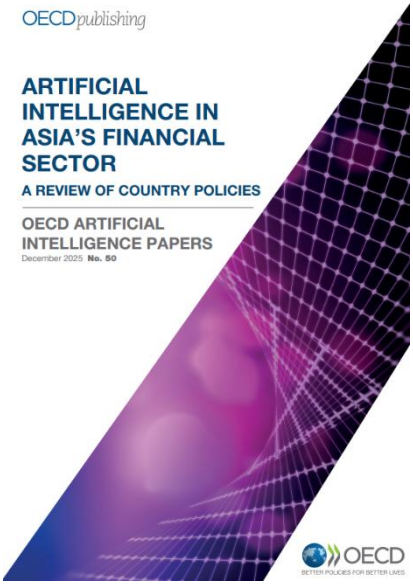
Висновки:

- **Екологічні злочини мають бути системно інтегровані в ризик-орієнтовані моделі ВК/ФТ.** Фінансові установи та ВНУП мають прямо включати злочини проти довкілля як окрему категорію предикатних злочинів у свої оцінки ризиків, сценарії моніторингу та внутрішні політики, а не розглядати їх як маргінальну або суто екологічну проблему.
- **Типології та червоні прапорці у сфері екологічних злочинів повинні використовуватися на практиці, а не декларативно** Наведені в документі сценарії (офшорні структури, механізми зворотного кредитування, достроковий викуп інвестицій, PEP з використанням підставних осіб, непрозоре фінансування будівництва) мають бути трансформовані у конкретні правила транзакційного моніторингу та тригери для EDD.
- **Навчання та підвищення обізнаності є критичним слабким місцем регульованого сектору.** Результати опитування демонструють необхідність цільового навчання з фокусом саме на екологічні злочини як джерело нелегальних доходів, а не формального включення теми злочинів проти довкілля до загальних тренінгів у сфері ПВК/ФТ.
- **Міжнародна співпраця та OSINT є ключовими для розкриття схем у сфері злочинів проти довкілля.** Більшість типологій мають транскордонний характер, тому ефективна ідентифікація потребує активного використання OSINT, міжнародного обміну через Егмонтську групу та взаємодії з ініціативами на кшталт Project Anton.

Завершальна частина документа інтегрує міжнародний вимір через опис Project Anton як прикладу сучасної публічно-приватної ініціативи, спрямованої на підрив фінансових основ незаконної торгівлі об'єктами дикої природи. Цей розділ логічно підсилює загальний меседж документа про те, що ефективна протидія екологічним злочинам можлива лише за умови тісної координації між фінансовими установами, фінансовими розвідками, правоохоронними органами та природоохоронними структурами, а також активного використання типологій, аналітичних інструментів і міжнародного обміну інформацією.

У цілому документ формує цілісне, глибоке та прикладне бачення екологічних злочинів як серйозної фінансово-кримінальної загрози, демонструючи, що їх ігнорування у системах протидії відмиванню коштів створює не лише репутаційні й регуляторні ризики, але й реальні прогалини у глобальній архітектурі фінансової безпеки, якими активно користуються організовані злочинні мережі

Штучний інтелект у фінансовому секторі Азії: масштаби впровадження, ризики та регуляторні підходи [12]



Документ OECD є комплексним аналітичним дослідженням, присвяченим системному аналізу використання штучного інтелекту у фінансовому секторі Азії та підходів державної політики й регулювання, що формуються у відповідь на стрімке поширення AI-технологій. Звіт охоплює 19 азійських юрисдикцій і ґрунтується на спеціальному опитуванні OECD щодо політик у сфері AI у фінансах, проведеному на початку 2025 року, а також на аналізі чинних нормативних актів, стратегій, рекомендацій і саморегуляторних ініціатив.

У документі штучний інтелект розглядається не як ізольоване технологічне явище, а як структурний фактор трансформації фінансових ринків, який впливає на всі ключові сегменти фінансової діяльності — від банкінгу та страхування до ринків капіталу, фінансових технологій і наглядових функцій регуляторів. OECD підкреслює, що в більшості азійських країн фінансові установи вже активно експериментують з AI або впроваджують його в операційну діяльність, хоча інтенсивність і зрілість такого використання суттєво відрізняються. Банківський сектор залишається головним провідником AI-інновацій, однак дедалі активніше AI застосовується небанківськими фінансовими установами, страховими компаніями та FinTech-провайдерами, особливо в економіках із розвиненими цифровими екосистемами та високим рівнем проникнення мобільних фінансових послуг.

Особлива увага у звіті приділяється прикладним сценаріям використання AI. Найбільш поширеним напрямом є кредитування, зокрема автоматизація кредитного скорингу, ухвалення кредитних рішень та управління кредитними портфелями. OECD наголошує, що AI-моделі дозволяють фінансовим установам працювати з альтернативними джерелами даних і обслуговувати так званих клієнтів із обмеженою або відсутньою кредитною історією — мікро-, малі та середні підприємства й фізичних осіб без повноцінної кредитної історії, що особливо актуально для країн із високим рівнем фінансової інклюзії, яка ще формується. Паралельно активно розвиваються AI-рішення для дистанційного онбордингу клієнтів і електронної

[12] https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/artificial-intelligence-in-asia-s-financial-sector_b8532d0b/3385bbd8-en.pdf

ідентифікації, включно з біометричними технологіями, розпізнаванням облич, перевірок ознак присутності живої особи та автоматизованого зіставлення даних із державними реєстрами.

Значний блок документа присвячено використанню AI у сфері протидії фінансовим злочинам, зокрема для виявлення шахрайства, моніторингу транзакцій, а також у процесах протидії відмиванню коштів і фінансуванню тероризму. OECD відзначає, що застосування машинного навчання дозволяє підвищити точність виявлення підозрілих операцій і зменшити кількість хибнопозитивних спрацювань, водночас наголошуючи, що ці переваги супроводжуються новими ризиками, пов'язаними з непрозорістю моделей, залежністю від якості даних і сторонніх технологічних провайдерів. Окремо підкреслюється зростання ролі генеративних AI, які використовується як інструмент підтримки роботи фахівців — аналітиків, фахівців з дотримання вимог законодавства, спеціалістів з управління ризиками, — але водночас створюють додаткові загрози, зокрема через генерування недостовірного або оманливого контенту, синтетичні аудіо- та відеоматеріали, а також можливості масштабованого автоматизованого шахрайства.

Поряд із вигодами від впровадження AI документ детально аналізує ризики, які виникають у фінансовому секторі. До найбільш значущих регулятори азійських країн відносять кіберризики, ризики маніпулювання ринками, модельні та управлінські ризики, упередженість і дискримінацію в автоматизованих рішеннях, проблеми захисту персональних даних і конфіденційної інформації, а також системні ризики, пов'язані з однотипним використанням схожих AI-моделей великою кількістю учасників ринку. OECD звертає увагу на те, що в окремих юрисдикціях ці ризики ще не формалізовані на рівні офіційних оцінок, що свідчить про нерівномірну регуляторну готовність регіону до масштабного AI-впровадження.

Висновки:

- **AI у фінансовому секторі Азії вже є системною реальністю, а не експериментом,** особливо в кредитуванні, e-KYC та ПВК/ФТ; регуляторам доцільно переходити від загального спостереження до структурованого збору даних про AI-використання.
- **Технологічно нейтральне фінансове регулювання залишається ефективною основою,** але воно має бути доповнене AI-специфічними наглядовими очікуваннями щодо пояснюваності, управління моделями та сторонніми провайдерами.
- **Генеративний AI істотно підвищує профіль ризику,** зокрема у сфері шахрайства, маніпуляцій із використанням синтетичних аудіо- та відеоматеріалів і непрозорих рішень, що потребує пріоритетного включення цих ризиків до рамок операційної та кіберстійкості.
- **Найбільш життєздатною моделлю AI-врядування є багаторівневий підхід,** який поєднує чинне фінансове законодавство, гнучкі керівні настанови щодо застосування штучного інтелекту, саморегулювання та інноваційні регуляторніпісочниці, узгоджені з Принципами OECD.

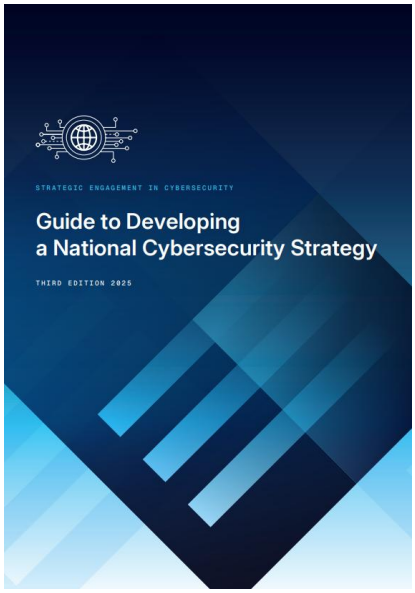
Центральною темою звіту є аналіз політичних і регуляторних підходів до AI у фінансовому секторі. OECD фіксує значну різноманітність моделей регулювання — від обов'язкових законів і міжсекторальних актів до м'якого права, принципів, рекомендацій і кодексів поведінки. Водночас ключовим об'єднувальним елементом для більшості країн є застосування технологічно нейтрального фінансового регулювання, відповідно до якого чинні вимоги щодо захисту споживачів, управління ризиками, операційної стійкості, кібербезпеки та ВК/ФТ однаковою мірою поширюються і на AI-рішення. Нові AI-орієнтовані політики не замінюють це регулювання, а доповнюють його, формуючи багаторівневі рамки врядування.

Документ детально показує, що більшість азійських юрисдикцій обирають еволюційний підхід, поєднуючи національні AI-стратегії,

фінансово-секторні рекомендації, інструменти саморегулювання та інноваційні пісочниці. Лише обмежена кількість країн планує запровадження спеціальних обов'язкових законів про AI, причому ці ініціативи мають переважно підтримувальний і ризик-орієнтований характер, а не репресивний. Важливу роль у формуванні політик відіграють міжнародні стандарти, насамперед Принципи OECD щодо штучного інтелекту, які розглядаються як універсальна рамка для балансування інновацій, фінансової стабільності, захисту прав споживачів і етичних вимог.

У підсумку OECD доходить висновку, що штучний інтелект стає невід'ємною частиною фінансової інфраструктури Азії, а головним викликом для державної політики є не питання дозволу чи заборони AI, а здатність регуляторів забезпечити його відповідальне, прозоре й безпечне використання без стримування інновацій. Для цього необхідні постійний моніторинг реального використання AI, усунення інформаційних прогалин, узгодженість різних рівнів регулювання та посилення міжнародної координації, з огляду на транскордонний характер як фінансових ринків, так і самих AI-технологій.

Національна стратегія кібербезпеки нового покоління: міжнародні стандарти, практична реалізація та довгострокова стійкість [13]



Документ є масштабним аналітично-практичним керівництвом, яке відображає сучасне міжнародне розуміння кібербезпеки як фундаментального елементу державної спроможності, економічної стійкості та суспільної довіри в умовах цифрової трансформації. Його зміст побудований на усвідомленні того, що цифрові технології та глобальна підключеність стали базовою інфраструктурою функціонування держав, фінансових систем, критичних послуг і повсякденного життя громадян, а отже будь-які системні збої або зловмисні кібервтручання мають прямі наслідки для національної безпеки, економіки та соціальної стабільності

Документ виходить з того, що кіберризики більше не є винятковими подіями або суто технічними інцидентами. Вони носять постійний, транснаціональний і системний характер, посилюються розвитком нових технологій, складних ланцюгів постачання, зростанням ролі приватного сектору та взаємозалежністю державних і недержавних цифрових екосистем. У цьому контексті національна стратегія кібербезпеки розглядається не як набір заходів реагування, а як інструмент довгострокового державного управління ризиками цифрового розвитку, покликаний забезпечити баланс між інноваціями, економічним зростанням і безпекою.

Третє видання керівних настанов принципово зміщує акценти з формального стратегічного планування на реалізацію, вимірюваність і сталість. Документ прямо констатує, що у світі накопичено значний масив національних стратегій кібербезпеки, однак їх практичний вплив часто обмежений через відсутність чітких механізмів впровадження, фінансування та відповідальності. Саме тому стратегія подається як процес безперервного циклу, в якому розроблення документа є лише одним з етапів, а не фінальною метою.

Важливим концептуальним елементом є розмежування між процесною та змістовною складовими стратегії. З одного боку, держава повинна мати чітко визначену модель управління: політичний мандат, уповноважений координуючий орган, міжвідомчі механізми, процедури

[13] https://ncsguide.org/wp-content/uploads/2025/12/NCS-Guide-2025.pdf

залучення приватного сектору та громадянського суспільства. З іншого боку, сама стратегія повинна охоплювати всі ключові елементи національної кібербезпеки — від управління ризиками й захисту критичної інфраструктури до розвитку кадрів, правового регулювання та міжнародної взаємодії. Ця логіка підкреслює, що кібербезпека не може бути фрагментованою політикою, оскільки вразливість в одному секторі неминуче створює ризики для всієї системи.

Окреме місце в документі відведено питанню фінансування, яке подається як ключова умова реальної дієздатності стратегії. Кібербезпека повинна бути інтегрована в національні бюджетні процеси, середньострокове планування та програми розвитку, а не фінансуватися за залишковим принципом або через разові донорські проєкти. Підкреслюється, що відсутність планування повних витрат життєвого циклу — включно з обслуговуванням систем, підготовкою персоналу та оновленням технологій — призводить до створення ілюзорної безпеки та нових вразливостей. У цьому контексті стратегія має виступати інструментом перекладу політичних пріоритетів у конкретні, профінансовані державні інвестиції.

Змістовно документ формує цілісну філософію національної кібербезпеки, яка базується на системі наскрізних принципів. Вони покликані забезпечити узгодженість стратегії з ширшими цілями держави — економічним розвитком, захистом прав людини, цифровою довірою та міжнародними зобов'язаннями. Особливого значення набуває принцип технологічного передбачення, який відображає необхідність переходу від реактивної моделі безпеки до проактивного управління майбутніми ризиками, пов'язаними зі штучним інтелектом, квантовими технологіями, цифровими фінансами та автоматизованими системами прийняття рішень.

Документ також чітко підкреслює міжсекторальний характер кібербезпеки. Захист критичної інфраструктури, фінансової системи, державних реєстрів і цифрових сервісів неможливий без активної участі приватного сектору, операторів послуг, технологічних компаній і наукової спільноти. У цьому сенсі стратегія має виступати платформою для інституціоналізованої співпраці, а не лише інструментом державного контролю. Водночас держава зберігає ключову роль у формуванні правил, стандартів, механізмів нагляду та міжнародної координації.

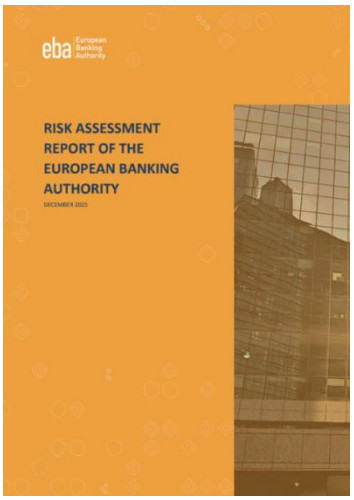
Узагальнюючи, керівні настанови формують чітке експертне бачення: національна стратегія кібербезпеки — це не документ про IT-безпеку, а про здатність держави керувати ризиками цифрової епохи. Її ефективність визначається не кількістю задекларованих заходів, а рівнем інституційної зрілості, фінансової забезпеченості, міжвідомчої координації та здатністю адаптуватися до динамічних технологічних і геополітичних змін. Саме в такому вигляді документ позиціонується як універсальний

Висновки:

- **Національна стратегія кібербезпеки повинна бути фінансово забезпеченим інструментом державної політики, а не концептуальним документом:** необхідні багаторічні бюджетні зобов'язання, закріплені нормативно, з урахуванням повних життєвих витрат і кадрових потреб.
- **Ефективність стратегії вимірюється не наявністю заходів, а досягненням конкретних результатів,** що вимагає впровадження SMART-показників, регулярного моніторингу та незалежної оцінки реалізації.
- **Управління кіберризиками має бути національним і системним,** із веденням постійно оновлюваного національного реєстру кіберризиків, який напряму впливає на пріоритети інвестування, регулювання та кризове реагування.
- **Кібербезпека повинна бути інтегрована в загальну економічну, фінансову та цифрову політику держави,** включно з критичною інфраструктурою, фінансовими системами та міжнародним співробітництвом, а не розглядатися як ізольований сектор.

орієнтир для держав з різним рівнем розвитку, який дозволяє трансформувати кібербезпеку з реактивної функції у стратегічний актив державної політики.

Банківський сектор ЄС у 2025 році: стійкість на тлі геополітичних і структурних ризиків [14]



Документ є масштабним аналітичним документом, який формує цілісне уявлення про стан банківського сектору Європейського Союзу та Європейського економічного простору в умовах системної трансформації ризиків. Звіт виходить далеко за межі класичної фінансово-пруденційної оцінки та фактично демонструє, як банківська система поступово адаптується до нової реальності, у якій фінансові, геополітичні, технологічні та операційні ризики стають тісно переплетеними і взаємопідсилюючими

У макроекономічному контексті ЕВА підкреслює, що банківський сектор функціонує в середовищі помірного, але крихкого економічного зростання. Хоча економіка ЄС у 2025 році продемонструвала стійкість завдяки сильному ринку праці, зростанню заробітних плат і поступовому зниженню інфляції, цей позитивний фон постійно нівелюється високим рівнем невизначеності. Геополітичні конфлікти, торговельні напруження, використання тарифів як інструменту геоекономічного тиску та внутрішня політична нестабільність у низці держав-членів формують середовище, у якому очікування бізнесу та домогосподарств залишаються стриманими. Особливо наголошується, що фіскальні дисбаланси, пов'язані з різким зростанням витрат на оборону, інфраструктуру та соціальні програми, призводять до збільшення державного боргу і, відповідно, до підвищення ризиків на ринках суверенного фінансування.

Ці макроекономічні та фіскальні процеси безпосередньо відображаються у структурі балансів банків. Звіт детально показує, що зростання активів у 2025 році відбувається не лише через класичне кредитування, а й через істотне нарощування вкладень у боргові цінні папери, насамперед суверенні. Таким чином, банки дедалі більше інтегруються у фінансування державного сектору, що підсилює так званий «суверенно-банківський зв'язок». Попри те, що з регуляторної точки зору такі активи використовуються як основа високоліквідних буферів, ЕВА наголошує: їх надмірна концентрація підвищує вразливість банків до коливань дохідності, розширення кредитних спредів та політичної нестабільності в окремих країнах.

Кредитна активність банків, за оцінкою ЕВА, демонструє асиметричний характер. Кредитування домогосподарств, особливо іпотечне, залишається головним драйвером зростання портфелів, що пояснюється відновленням ринку житлової нерухомості, зниженням ставок і відносно стабільним фінансовим становищем населення. Водночас корпоративне кредитування зростає значно повільніше і дедалі більше концентрується у вибраних секторах. Звіт чітко простежує, що банки спрямовують фінансування у сфери, які відповідають стратегічним пріоритетам Європейського Союзу, зокрема енергетику, оборонно-безпековий сектор, інфраструктуру та цифрові технології. Таким чином, банківська система фактично стає одним із ключових каналів реалізації промислової, енергетичної та безпекової політики ЄС.

Оцінюючи якість активів, ЕВА наголошує на парадоксальній, але показовій ситуації: за збереження історично низького рівня непрацюючих кредитів спостерігається структурно висока

[14] https://www.eba.europa.eu/sites/default/files/2025-12/8acb45c4-912b-4f0f-b887-37b8fc058779/Risk%20Assessment%20Report%20Autumn%202025.pdf

частка кредитів, класифікованих у Stage 2 відповідно до Міжнародного стандарту фінансової звітності 9 «Фінансові інструменти». Цей феномен трактується як прояв зміни поведінки банків, які дедалі частіше застосовують обережний, превентивний підхід до управління кредитним ризиком. Підвищення частки Stage 2 не супроводжується зростанням вартості ризику або різким погіршенням платоспроможності позичальників, що дозволяє EBA зробити висновок про наявність прихованої стійкості банківських портфелів, але водночас підкреслити потребу у пильному наглядовому моніторингу, особливо у сегментах комерційної нерухомості та малих і середніх підприємств.

Фондування і ліквідність у 2025 році залишаються однією з найсильніших сторін банківського сектору ЄС/ЄЕЗ. Роздрібні депозити продовжують відігравати центральну роль, забезпечуючи стабільність пасивів навіть в умовах ринкових коливань. Водночас EBA детально аналізує структурні зрушення у складі ліквідних активів, звертаючи увагу на зменшення ролі готівки та резервів у центральних банках і зростання частки суверенних паперів. Цей зсув підвищує ефективність використання ліквідності, але водночас робить банки більш вразливими до ринкової волатильності та суверенних ризиків. Окремим елементом ризикового профілю визначається валютна ліквідність, зокрема в доларах США, що є критично важливим для банків з істотними міжнародними або ринковими операціями.

Висновки:

- **Банкам і органам банківського нагляду необхідно системно інтегрувати геополітичні та геоекономічні сценарії до процесів внутрішньої оцінки достатності капіталу та внутрішньої оцінки достатності ліквідності,** включно з урахуванням непрямих ризиків, що виникають через корпоративних клієнтів і небанківських фінансових посередників, а не обмежуватися виключно прямими країновими ризиками.
- **Високий рівень кредитів, віднесених до другої стадії відповідно до Міжнародного стандарту фінансової звітності 9,** слід розглядати як інструмент раннього попередження про накопичення ризиків, що потребує посиленого наглядового аналізу в межах процесу наглядової перевірки та оцінки, але не як автоматичний індикатор погіршення якості активів за умови стабільного рівня вартості ризику та непрацюючих кредитів.
- **Зростання суверенних експозицій у складі високоліквідних активів** потребує більш активного управління концентраційними та ринковими ризиками, особливо в державах із підвищеним борговим навантаженням і політичною нестабільністю.
- **Операційна та цифрова стійкість поступово стає рівнозначною капіталу та ліквідності:** ефективне впровадження Регламенту про цифрову операційну стійкість, належне управління ризиками аутсорсингу та протидія шахрайству з використанням штучного інтелекту мають бути ключовим пріоритетом як для банків, так і для фінансових регуляторів.

Капітальна позиція банківського сектору описується як надзвичайно сильна. Рівні базового капіталу першого рівня та запас капіталу над мінімальними вимогами досягли історичних максимумів, що створює значний буфер для поглинання шоків. Навіть з урахуванням зростання ризикозважених активів, пов'язаного з імплементацією CRR3 та CRD6 і підвищенням ваги операційного ризику, банки мають достатній простір для поступової адаптації до нових регуляторних стандартів без різкого скорочення кредитування або підвищення ризиковості бізнес-моделей.

Прибутковість у 2025 році зберігається на високому рівні, однак її джерела змінюються. EBA підкреслює, що чистий процентний дохід поступово втрачає роль головного драйвера рентабельності через тиск на процентні маржі. Натомість дедалі більшого значення набувають комісійні доходи,

оптимізація витрат, автоматизація та цифровізація процесів. Це свідчить про стратегічний зсув у бізнес-моделях банків, які все більше орієнтуються на ефективність і стійкість, а не на екстенсивне зростання.

Значний обсяг звіту присвячено операційним ризикам і стійкості. Кіберзагрози, зловмисні атаки, залежність від третіх сторін, зокрема хмарних і платіжних провайдерів, а також стрімке зростання шахрайства, посиленого використанням інструментів штучного інтелекту, формують новий вимір системних ризиків. У цьому контексті Регламент про цифрову операційну стійкість розглядається як ключовий інструмент підвищення здатності банків протидіяти інцидентам, забезпечувати безперервність діяльності та координувати реагування на кризові події на рівні ЄС.

Фінальним концептуальним акцентом звіту є геополітичні та геоекономічні ризики як довгостроковий структурний фактор. EBA чітко демонструє, що ризики для банків дедалі частіше виникають не безпосередньо з фінансових дисбалансів, а через непрямі канали — корпоративні ланцюги створення вартості, небанківських фінансових посередників, транскордонні інвестиції та політичні рішення третіх країн. Зростання експозицій до небанківських фінансових посередників, особливо за межами ЄС, визначається як один із ключових викликів для нагляду, прозорості та фінансової стабільності.

У підсумку звіт формує глибоку й багатовимірну картину банківського сектору ЄС/ЄЕЗ, який на поточному етапі є капітально, ліквідно та операційно стійким, але водночас дедалі більше залежить від якості управління геополітичними, технологічними та структурними ризиками. Саме здатність інтегрувати ці ризики у стратегічне управління та наглядові рамки визначатиме реальну стійкість банківської системи у середньостроковій перспективі.

Scambling: нова віха фінансової злочинності на перетині гемблінгу, кіберзлочинів та відмивання коштів [15]

Зростаюча інтеграція цифрових технологій у повсякденне життя призвела до появи нових, високотехнологічних форм злочинності, які вміло експлуатують інфраструктуру глобального інтернету та психологічні особливості користувачів. Однією з таких форм, що викликає особливу тривогу у фінансових та правоохоронних колах Австралії та отримує потенційну можливість поширення у всьому світі, є явище, відоме під терміном «Scambling».

Цей неологізм, утворений від слів «scam» (шахрайство) та «gambling» (азартні ігри), описує не просто незаконні онлайн-казино, а складний симбіотичний механізм, який одночасно є інструментом шахрайства, платформою для викрадення персональних даних, каналом вербування фінансових посередників та ефективною системою для відмивання кримінальних коштів. Звіт AUSTRAC та Fintel Alliance розкриває внутрішню механіку цього явища, демонструючи, як воно трансформувалося з маргінальної загрози у системну проблему, що підриває фінансову безпеку та соціальний добробут.

Суть Scambling полягає у створенні та просуванні цифрових платформ, які за зовнішніми ознаками імітують легальні онлайн-казино, покер-руми чи ігрові автомати, але за своїм функціоналом та цілями є злочинними підприємствами. Вони виникають переважно в

[15] https://www.austrac.gov.au/sites/default/files/2025-12/Scambling%20-%20the%20nexus%20between%20scams%2C%20money%20mules%20and%20micro-laundering.pdf

офшорних юрисдикціях, що ускладнює юрисдикційний контроль, але цілеспрямовано та агресивно рекламуються серед австралійської аудиторії через основні соціальні мережі, залучаючи відомих блогерів та створюючи спільноти навколо «гарячих» посилань та ексклюзивних бонусів. Важливою рисою є їхня доступність через офіційні магазини додатків, що надає їм вигляду легітимності в очах непідготовленого користувача. Однак за привабливим інтерфейсом, системою винагород, лідербордами та соціальними елементами гри ховається фундаментальна незаконність: ці сайти прямо порушують австралійський Закон про інтерактивні азартні ігри 2001 року, який забороняє надання послуг онлайн-гемблінгу без відповідної ліцензії та спрямований на захист споживачів.

Справжня небезпека Scambling виходить далеко за межі звичайного шахрайства в азартних іграх, де гравець може програти гроші. Ці платформи реалізують двосторонній шкідливий механізм. По-перше, вони конструюють середовище, де шанси гравця на виграш мінімальні або відсутні, а будь-які виграші часто блокуються різними штучними припонами: технічними збоями, неможливістю виведення коштів за межі платформи, заміною грошових виплат на ігрові кредити або просто ігноруванням запитів. Користувач, залученый гейміфікованими елементами, часто сприймає втрати як частину гри і рідко повідомляє про це як про шахрайство. По-друге, і це є найкритичнішим аспектом, ці сайти виступають потужними інструментами збору конфіденційної інформації. Реєструючись і поповнюючи рахунок, користувачі передають злочинцям дані своїх банківських карток, доступ до онлайн-банкінгу, реквізити сервісів миттєвих платежів на кшталт PayID, а також великий масив персональних даних. Ця інформація стає товаром на чорному ринку або ж використовується для подальших цілеспрямованих атак, таких як фішинг та шахрайство.

Однак найінноваційнішою та найнебезпечнішою рисою Scambling є його органічне вплетення в глобальні мережі відмивання коштів. Злочинні угрупування, що стоять за цими платформами, використовують їх не лише для отримання первинних доходів, але й як інструмент для легітимізації та відмивання коштів, отриманих від інших видів злочинної діяльності, таких як кібершахрайство, торгівля людьми або наркоторгівля. Ключовим ланцюгом у цьому процесі є вербування так званих «грошових мулів» — звичайних громадян, чиї банківські рахунки використовуються для переказу та розмивання кримінальних коштів. Механізм вербування часто інтегрований прямо в ігровий процес. Гравцям можуть пропонувати «легкий заробіток»: невеликі грошові винагороди або великі ігрові кредити за надання доступу до їхнього рахунку або реквізитів PayID. Людина, яка може перебувати у скрутному фінансовому становищі або просто не усвідомлює наслідків, погоджується, вважаючи це частиною гри або безневинним підробітком. Її рахунок потім включається в складну, багаторівневу мережу, через яку проходять сотні низьковартісних транзакцій. Ця техніка, відома як мікро-відмивання, дозволяє розбити великі суми «брудних» грошей на непомітні для автоматичних систем фінансового моніторингу операції, що не викликають підозр. Таким чином, громадянин, який вважав, що грає в покер на телефоні, насправді стає ланкою в міжнародній схемі відмивання коштів, беручи на себе юридичні ризики та потенційно руйнуючи власну кредитну історію.

Соціальний вимір цієї загрози є особливо глибоким та тривожним. Дані, зібрані Fintel Alliance, свідчать про чітку цільову аудиторію злочинців. Найбільш вразливими виявляються представники груп з нижчим соціально-економічним статусом: мешканці віддалених та сільських регіонів, корінні народи Австралії (First Nations peoples), трудові мігранти, а також люди з обмеженим доступом до фінансової освіти. Для багатьох із цих спільнот смартфон часто є основним, а інколи й єдиним вікном у цифровий світ та джерелом розваг. Scambling-платформи, рекламовані в соціальних мережах, легко потрапляють у їхнє поле зору. Фактори, що роблять їх особливо вразливими, включають фінансову скруту, яка робить пропозицію «швидкого заробітку» привабливою; соціальну ізоляцію, що обмежує доступ до достовірної інформації та порад; мовні та культурні бар'єри, які ускладнюють розуміння правових нюансів;

та глибоку інтеграцію азартних ігор у культурний контекст деяких спільнот. Звіт наводить конкретні приклади, коли жителі віддалених громад, активно граючи в онлайн-автомати, ділилися деталями своїх рахунків, щоб отримати додаткові ігрові кредити, і таким чином потрапляли в мережі «грошових мулів», навіть не підозрюючи про це. Мігранти, які часто працюють у ізольованих сільськогосподарських регіонах, також виявилися ціллю через свою залежність від цифрових комунікацій та можливі труднощі з розумінням місцевих норм.

Наслідки цих дій катастрофічні як на індивідуальному, так і на суспільному рівні. Окрім прямых фінансових втрат, жертви втрачають контроль над своєю фінансовою ідентичністю, що може призвести до довготривалого збитку кредитного рейтингу, судових позовів з боку банків або правоохоронних органів, а також до поглиблення бідності та соціальної виключеності. Крім того, легальні програми з мінімізації шкоди від азартних ігор, які зобов'язані надавати ліцензовані оператори, на цих незаконних майданчиках відсутні, що залишає проблемних гравців без будь-якої підтримки. Мало того, особи, які вже стали жертвами Scambling, через викриття своїх даних потрапляють у спеціальні бази і стають цілями для повторних та більш цілеспрямованих шахрайств.

Відповідь австралійської влади на цю загрозу формується як багаторівнева та міжвідомча стратегія, координацію якої здійснює AUSTRAC через платформу Fintel Alliance, що об'єднує фінансові установи, правоохоронні органи та державні агенції, такі як ACMA. Стратегія включає в себе одночасне застосування репресивних, профілактичних та просвітницьких заходів. З одного боку, ACMA активно використовує свої повноваження для видачі наказів інтернет-провайдерам про блокування незаконних ігрових сайтів, створивши вже значний бар'єр для доступу. З іншого боку, розуміючи, що блокування не є панацеєю в епоху віртуальних приватних мереж та швидкої реєстрації нових доменів, велика увага приділяється саме профілактиці та зміцненню стійкості суспільства. Національна інформаційна кампанія «Have you been Scambled?» розроблена з урахуванням особливостей мовлення та каналів комунікації вразливих груп, зокрема в регіональних та корінних громадах. Для фінансових установ та правоохоронців розроблені детальні типології, показники підозрілої поведінки та навчальні кейси, які допомагають виявляти рахунки, що використовуються як «мули», та аномальні патерни мікро-транзакцій, характерні для відмивання коштів через гемблінгові платформи.

Висновки:

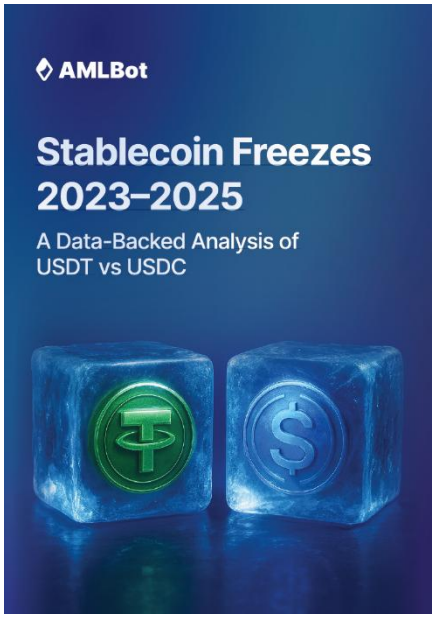
- **Scambling — це комплексна гібридна загроза,** яка поєднує в собі елементи онлайн-шахрайства, гемблінгу, викрадення персональних даних та відмивання коштів у єдину ефективну кримінальну модель.
- **Ключовою ланкою системи є вербування «грошових мулів» з соціально вразливих груп.** Злочинці використовують ігрові механіки, соціальні мережі та фінансові спокуси, щоб залучити людей.
- **Соціальний вплив є нерівномірним і руйнівним для окремих спільнот.** Основним об’єктом атак стають групи з нижчим соціально-економічним статусом, жителі віддалених регіонів, мігранти та інші вразливі категорії, для яких наслідки втрати контролю над фінансами можуть бути катастрофічними.
- **Ефективна протидія вимагає комплексного підходу,** що поєднує технологічні заходи, правове втручання, цільову просвітницьку роботу серед груп ризику та тісну координацію між фінансовими установами, правоохоронними органами та громадськими організаціями.

Таким чином, явище Scambling виступає яскравим прикладом того, як сучасна злочинність еволюціонує, інтегруючи різні механізми в єдину ефективну модель. Боротьба з нею вимагає не

лише технологічних рішень та силових методів, але й глибокого розуміння соціально-економічного контексту, інвестицій у фінансову грамотність найбільш вразливих верств населення та тісної співпраці між державним, приватним та громадським секторами на всіх рівнях. Досвід Австралії слугує прецедентом та попередженням для інших країн, де поширення смартфонів, доступ до соціальних мереж та онлайн-платежів створює аналогічне середовище для виникнення подібних гібридних загроз фінансовій безпеці та суспільній стабільності.

Звіти окремих інституцій та експертів

Механізми заморожування стейблкоїнів у глобальному вимірі: досвід USDT та USDC (2023–2025) [16]



Документ є комплексним аналітичним дослідженням практик заморожування стабільних криптоактивів у період 2023–2025 років і присвячений порівняльному аналізу двох домінуючих стейблкоїнів — USDT (емітент Tether) та USDC (емітент Circle). Його ключовою метою є не просто кількісне зіставлення обсягів заблокованих активів, а глибоке розкриття філософії комплаєнсу, правоохоронної взаємодії та операційної моделі, які стоять за кожним із цих активів і безпосередньо формують їхню роль у глобальній системі протидії відмиванню коштів, фінансуванню тероризму та іншим формам фінансової злочинності

Документ ґрунтується на масштабному ончейн-аналізі даних мереж Ethereum (ERC-20) та TRON (TRC-20) і демонструє, що різниця між USDT та USDC є не випадковою, а системною. Упродовж аналізованого періоду Tether заморозив активи на суму близько 3,29 млрд доларів США, охопивши понад 7 200 адрес, тоді як Circle заморозив приблизно 109 млн доларів США на близько 370 адресах. Таким чином, масштаб втручання USDT у процеси заморожування приблизно у 30 разів перевищує відповідні показники USDC, що одразу вказує на різні підходи до управління ризиками та взаємодії з державними органами.

У документі детально описано механізм заморожування USDT як елемент проактивної моделі комплаєнсу. Смартконтракти USDT містять вбудовані функції чорного списку, які дозволяють Tether блокувати перекази з конкретних адрес, а також здійснювати спалювання заморожених токенів із подальшим перевипуском «очищених» активів для відшкодування потерпілим або передачі правоохоронним органам. Така модель інтегрована у постійну співпрацю з понад 275 правоохоронними органами у 59 юрисдикціях і застосовується не лише на підставі судових рішень чи санкційних списків, а й у випадках, коли емітент вважає заморожування доцільним для негайного припинення руху викрадених або підозрілих коштів. Документ наводить приклади масштабних заморожувань, пов’язаних із шахрайськими мережами, торгівлею людьми, фінансуванням тероризму та транскордонними кримінальними кластерами, зокрема в Південно-Східній Азії.

Водночас автори підкреслюють, що така висока ступінь централізованого контролю породжує суттєві ризики. У документі детально розглядається проблема часової затримки між запитом на

[16] https://blog.amlbot.com/stablecoin-freezes-2023-2025-a-data-backed-analysis-of-usdt-vs-usdc-by-amlbot/

заморожування та його фактичним виконанням, зумовлена мультипідписною моделлю управління, що в окремих випадках дозволяло зловмисникам вивести кошти до завершення процедури. Окрему увагу приділено й правовим конфліктам, які виникають унаслідок оскарження підстав заморожування, що ілюструє напруження між оперативною ефективністю та дотриманням належної правової процедури.

На противагу цьому, модель Circle та USDC описується як суворо реактивна та юридично обмежена. Circle застосовує механізм «відмови у доступності», за яким адреси блокуються у смартконтракті, але лише за наявності чітких правових підстав — судових наказів, санкційних вимог або серйозних інцидентів безпеки. Заморожені активи при цьому не спалюються і не перевипускаються, а залишаються статичними до моменту офіційного розморожування. Такий підхід забезпечує високу передбачуваність і прозорість, включно з публічним розкриттям інформації про заморожені адреси, але водночас суттєво обмежує оперативність реагування у складних, динамічних кримінальних схемах.

Центральне місце в дослідженні займає ончейн-аналіз динаміки заморожувань. Дані демонструють, що USDT характеризується майже безперервним зростанням кількості заблокованих адрес із регулярними кластерами масових заморожувань, особливо після 2023 року. Для USDC, навпаки, типовими є рідкісні, але різкі сплески активності, які корелюють із конкретними судовими або регуляторними подіями. Така відмінність у «темпі» заморожувань безпосередньо відображає різні філософії втручання емітентів.

Особливий акцент зроблено на мережі TRON, яка виявляється ключовою інфраструктурою для USDT. Саме в TRC-20 зосереджено близько 1,75 млрд доларів США заморожених активів, що перевищує обсяги в Ethereum і свідчить про центральну роль TRON у P2P-переказах, OTC-операціях та високошвидкісних транскордонних розрахунках, зокрема в регіонах із підвищеними ризиками ВК/ФТ. Динаміка заморожувань у цій мережі показує різке зростання після 2023 року та концентрацію великих обсягів блокувань у межах окремих днів, що відповідає масштабним правоохоронним операціям.

У завершальній частині документ формує узагальнену картину двох принципово різних моделей. USDT постає як актив із повним операційним циклом — від заморожування до розслідування, спалювання та перевипуску коштів, фактично інтегрований у міжнародну

Висновки:

- **USDT є де-факто активним інструментом фінансових розслідувань,** а не лише платіжним засобом: його модель заморожування та перевипуску дозволяє не просто блокувати кошти, а й здійснювати реальне відшкодування потерпілим і підтримувати міжнародні розслідування у справах шахрайства, торгівлі людьми та фінансування тероризму.
- **USDC забезпечує вищу юридичну передбачуваність, але нижчу оперативну ефективність:** сувора прив’язаність до судових і регуляторних тригерів зменшує ризики зловживань, однак обмежує швидкість реагування у динамічних схемах ВК/ФТ.
- **Мережа TRON є критичною зоною ризику та контролю для USDT:** концентрація понад половини всіх заморожених обсягів саме в TRC-20 свідчить, що без глибокого моніторингу TRON неможлива ефективна протидія транскордонним незаконним фінансовим потокам.
- **Централізовані повноваження емітентів створюють нову дилему для регуляторів:** з одного боку — безпрецедентна прозорість і контроль, з іншого — ризики надмірної дискреції, правових спорів і ерозії принципів децентралізації, що потребує чіткіших міжнародних стандартів і процесуальних гарантій.

систему фінансових розслідувань. USDC, своєю чергою, виконує роль юридично стриманого інструменту, який мінімізує дискрецію емітента, але водночас обмежує можливості швидкого реагування. У ширшому контексті документ піднімає фундаментальне питання для регуляторів і фінансових розвідок: чи може криптоіндустрія поєднати ефективну протидію фінансовій злочинності з мінімізацією централізованого контролю, не підриваючи базові принципи децентралізації, на яких вона історично ґрунтується.

Як російська «тіньова флотилія» використовує прогалини в морському праві для обходу санкцій [17]

Центр досліджень енергії та чистого повітря опублікував ґрунтовне розслідування, яке розкриває складну та небезпечну мережу операцій російської «тіньової флотилії». Документ під назвою є не просто статистичним звітом, а детальним описом того, як сучасна система міжнародного морського права, заснована на принципі «прапора держави», була систематично використана для створення паралельної логістичної інфраструктури, що дозволяє росії продовжувати експорт нафти, уникаючи санкцій та міжнародного тиску.

Аналіз даних за перші три квартали 2025 року виявляє вражаючі масштаби явища: 113 суден, які входять до так званої «тіньової» флотилії, здійснили перевезення російської нафти під фальшивими прапорами на загальну суму 4,7 мільярда євро. Ця цифра становить 13 відсотків від усього обсягу нафти, перевезеної «тіньовими» суднами за цей період, що еквівалентно 11 мільйонам тонн сирої нафти. Однак, крім чистих обсягів, дослідження розкриває глибші структурні проблеми, що стосуються морської безпеки, екології та ефективності міжнародного права. Фактично, кожне судно, що працює під фальшивим прапором, автоматично втрачає страхове покриття, що перетворює його на плавучу екологічну загрозу, ризики якої у разі аварії ляжуть на плечі прибережних держав та їхніх громадян. Це створює парадоксальну ситуацію, коли санкції, спрямовані на обмеження фінансування російської військової машини, можуть непрямим чином сприяти створенню екологічних та фінансових ризиків для країн, які ці санкції й запровадили.

Окрему увагу в дослідженні приділено динаміці розвитку ситуації. Якщо в грудні 2024 року лише 15 суден використовували фальшиві прапори, то вже до вересня 2025 року їхня кількість зросла вшестеро, до 90 одиниць. Цей стрімкий зріст тісно пов'язаний із посиленням санкційного тиску з боку ЄС, США та Великої Британії, що змусило операторів шукати все більш радикальні способи ухилення. Більш того, 96 із 113 суден, які зафіксував CREA, вже перебували під санкціями, що чітко вказує на те, що використання фальшивих прапорів є не випадковим явищем, а цілеспрямованою стратегією збереження операційної здатності «тіньового» флоту. У третьому кварталі 2025 року 52 таких судна були активними, перевозячи російську нафту під прапорами держав, які часто навіть не підозрюють про використання своєї символіки.

Феномен «тіньового» флоту нерозривно пов'язаний з історично складною системою «зручних прапорів». Згідно з Конвенцією ООН з морського права, кожна держава має суверенне право визначати умови надання свого прапора судам. Ця норма, створена для забезпечення свободи судноплавства, згодом породила цілу індустрію відкритих юрисдикцій — держав, які пропонують швидку та дешеву реєстрацію, мінімальні технічні вимоги та податкові пільги, часто без жодного реального зв'язку між судном і самою країною прапора. CREA виявляє, що з 46

[17] https://energyandcleanair.org/wp/wp-content/uploads/2025/11/CREA_Flags-of-inconvenience_11.2025.pdf

юрисдикцій, які надавали прапори російським «тіньовим» суднам після повномасштабного вторгнення в Україну, 23 офіційно класифікуються Міжнародною транспортною федерацією як юрисдикції «зручних прапорів». Ці 23 юрисдикції відіграли ключову роль у транспортуванні російської нафти на суму 50 мільярдів євро, що становить майже п'яту частину всього обсягу, перевезеного «тіньовою» флотилією. Таким чином, історично складені слабкі місця глобальної морської системи були використані для створення масштабного механізму обходу сучасних санкцій.

Однак після низки санкційних рішень 2024-2025 років навіть традиційні «зручні прапори», такі як Панама та Ліберія, почали обмежувати співпрацю з «тіньовими» суднами. Панама, наприклад, змінила свою реєстраційну політику, запровадивши жорсткіші вимоги до стану суден, що призвело до масової міграції «тіньових» танкерів з-під її прапора. У відповідь на це на ринку з'явилися абсолютно нові гравці — юрисдикції, які раніше не мали жодного досвіду роботи з нафтовими перевезеннями. CREA ідентифікував шість таких юрисдикцій, які станом на вересень 2025 року мали в своєму флоті щонайменше 10 російських «тіньових» суден кожен, а разом вони обслуговували 162 танкери. Це свідчить про формування нового паралельного ринку морських послуг, готового працювати з високими ризиками заради фінансової вигоди.

Ще більш тривожним є масове використання відверто фальшивих прапорів. Міжнародна морська організація визначає фальшивий прапор як такий, що використовується через шахрайські вебсайти, припинені реєстрації або навмисне цифрове викривлення даних. Яскравим прикладом став танкер «Boracay», затриманий французьким флотом 1 жовтня 2025 року, який перебував під прапором Беніну. Розслідування показало, що прапор Беніну пропонувався через фальшивий вебсайт, не пов'язаний з урядом країни, при цьому офіційно під прапором Беніну зареєстроване лише одне нафтове судно. Історія з прапором Малаві виявилася ще драматичнішою: так званий «реєстр» цієї країни виявився повністю фіктивним. Незважаючи на офіційний лист міністерства транспорту Малаві до IMO з вимогою вжити заходів проти шахраїв, 24 судна продовжували використовувати прапор країни для транспортування російської нафти. Ці випадки демонструють не просто порушення правил, а існування цілих злочинних схем, що експлуатують саму систему міжнародного морського реєстру.

Водночас, дослідження CREA показує, що санкції як інструмент не є неефективними — вони просто змінюють ландшафт ринку, створюючи нові механізми адаптації. За перші три квартали 2025 року підсанкційні судна перевезли 44% російського експорту нафти, що свідчить про зростаючу залежність росії саме від цієї частини флоту. Ключовим інструментом виживання для цих суден стала практика «зміни прапорів»: 134 судна змінили прапор реєстрації протягом трьох місяців після потрапляння під санкції, а 85 суден зробили це двічі за шість місяців. Ця тактика дозволяє суднам постійно залишатися в «сірій зоні», унеможливлюючи їхнє ефективне відстеження та притягнення до відповідальності.

Важливим аспектом дослідження є аналіз географії перевезень. Близько 30% російської нафти, перевезеної санкціонованими судами, пройшло через Балтійські порти та данські протоки, потрапляючи під безпосередній контроль ЄС та Великої Британії. У третьому кварталі 2025 року судна під фальшивими прапорами перевезли через данські протоки нафту на суму понад 900 мільйонів євро, причому п'ять із цих суден були санкціоновані ще до початку 2025 року, але продовжували працювати без перешкод. Це вказує на системні прогалини в механізмах контролю навіть у стратегічно важливих морських зонах, де теоретично можна було б здійснювати найефективніший нагляд.

У контексті політичних рекомендацій CREA пропонує не поодинокі заходи, а комплексну перебудову системи морського регулювання. Серед ключових пропозицій — створення єдиної бази даних легітимних прапорів для портів ЄС, що дозволить у реальному часі верифікувати статус кожного судна; розширення вимог щодо обов'язкового пред'явлення сертифікатів

прапора для транзиту через європейські води; активна дипломатична робота з відкритими юрисдикціями для посилення їхньої відповідальності. Особливо важливою є пропозиція щодо реформи правил IMO, спрямованої на уніфікацію вимог до держав прапора, особливо коли вони передають свої функції приватним операторам третіх країн. Крім того, автори наполягають на безпосередніх діях: берегові служби ЄС та Великої Британії повинні активно затримувати судна, що пливуть під фальшивими прапорами, оскільки такі дії безпосередньо порушують статтю 94 Конвенції ООН з морського права, яка вимагає від держави прапора здійснювати ефективний контроль за судном.

У глобальному контексті звіт CREA можна розглядати як дзеркало, яке відображає ширшу проблему: сучасна система міжнародного права та торгівлі, побудована на принципах відкритості та довіри, виявилася вразливою до системного використання в цілях обходу норм. Російська «тіньова» флотилія — це не просто сукупність окремих суден, а складний організм, що адаптується до тиску, знаходячи прогалини в міжнародних регуляціях, експлуатуючи економічні нерівності між країнами та використовуючи технологічні можливості для цифрового шахрайства. Боротьба з цим явищем вимагає не лише технічних заходів, але й глибокого переосмислення принципів морської юрисдикції, посилення міжнародної співпраці та створення механізмів, здатних реагувати на виклики, які не передбачалися при створенні нинішньої системи морського права. Ігнорування цих проблем загрожує не тільки підривом ефективності санкцій, але і серйозними наслідками для безпеки світового океану, стабільності морської торгівлі та екологічного балансу прибережних регіонів.

Висновки:

- **Масове використання фальшивих прапорів:** У перших трьох кварталах 2025 року 113 суден російської «тіньової» флотилії перевезли близько 11 млн тонн російської нафти (на суму 4,7 млрд євро) під фальшивими прапорами.
- **Санкції не зупиняють «тіньовий» флот, а змушують його адаптуватися:** Після введення санкцій судна активно міняють прапори реєстрації. 44% російського експорту нафти досі перевозиться підсанкційними суднами.
- **Експлуатація слабкостей глобальної системи морського права:** росія системно використовує відкриті юрисдикції та шахрайські схеми для обходу санкцій.
- **Європейські води залишаються вразливими:** Значна частина нафти, перевезеної під фальшивими прапорами, проходить через стратегічні протоки ЄС (Данські протоки, Ла-Манш), що свідчить про недостатність контролю з боку європейських прибережних держав.

ВНУП

Мережі таємниць: як надавачі корпоративних послуг стають бар'єром або інструментом для фінансових злочинів [18]

Опубліковане британським податковим та митним управлінням (HMRC) керівництво щодо ризиків для надавачів корпоративних послуг (Trust or Company Service Providers, TCSP) є багатошаровим аналітичним дослідженням, яке розкриває логіку та механіки сучасних фінансових злочинів. Цей документ можна розглядати як детальну карту

[18] https://www.gov.uk/government/publications/anti-money-laundering-guidance-for-trust-or-company-service-providers/risks-common-to-trust-or-company-service-providers

вразливостей, які виникають на перетині корпоративного права, міжнародних фінансів та кримінальних намірів. Він чітко демонструє, як легальні на перший погляд інститути – створення компаній, призначення номінальних директорів, управління трастами – перетворюються на складні інструменти для приховування, трансформації та легітимізації злочинного капіталу. Головний лейтмотив документа полягає в тому, що ризик не є статичною категорією; це динамічне явище, що еволюціонує разом із зміною геополітичної ситуації, появою нових технологій та адаптацією злочинних угруповань до регуляторних заходів.

Надзвичайно показовим є те, що HMRC, виконуючи вимоги Регламенту про відмивання коштів 2017 року, не просто перераховує ризики, а пропонує логічну структуру для їхнього осмислення. Центральне місце в цій структурі займає географічний фактор, який розглядається не як просте формальне позначення країни, а як комплексний індикатор інституційної зрілості та рівня загрози.

Країни, визнані FATF такими, що мають стратегічні недоліки (high-risk third countries), становлять очевидну небезпеку, проте документ йде значно далі. Він звертає увагу на ширший спектр закордонних юрисдикцій, які можуть мати формально належне законодавство, але на практиці відрізняються високою корупцією, слабкою судовою системою, відсутністю ефективного обміну інформацією або культурою фінансової секретності. Особливо важливими вважаються юрисдикції, що межують з високоризиковими країнами, оскільки потоки нелегального капіталу нерідко проходять через кілька суміжних територій для ускладнення відстеження. Крім того, документ виділяє специфічні правові особливості, що роблять юрисдикцію привабливою для злочинців: дозвіл на випуск акцій на пред'явника, відсутність обов'язку оновлювати інформацію про бенефіціарних власників, слабкі вимоги до корпоративної реєстрації. Таким чином, географічний ризик для TCSP трансформується з питання «звідки клієнт?» у складну аналітичну задачу, що потребує оцінки політичного, правового та економічного контексту цілої країни.

Окремої уваги заслуговує концепція ланцюгів постачання послуг (supply chains). HMRC описує їх як канали, через які послуга доставляється кінцевому споживачеві за участю одного або кількох посередників. Феноменально, що саме ця, здавалося б, суто бізнес-модель стає основним механізмом створення штучної анонімності. Кожна ланка в такому ланцюжку – додатковий шар, що віддаляє постачальника послуги від кінцевого бенефіціарного власника, ускладнює перевірку джерел коштів та справжніх намірів. Ризик зростає експоненційно зі збільшенням довжини ланцюга, залученням закордонних посередників і, що найважливіше, за відсутності чіткої комерційної логіки такого опосередкування. Чому кінцевий власник не може звернутися напряму? Це ключове питання, яке, за словами HMRC, має стати центральним у внутрішніх процедурах оцінки ризиків. Документ наголошує, що посередники можуть свідомо просувати послуги з приховування власності або діяти в юрисдикціях з жорсткими законами про таємницю, що робить їх не просто передавачами запиту, а активними учасниками потенційної схеми з уникнення прозорості.

Детальний розбір специфічних послуг розкриває, як абстрактні ризики матеріалізуються у конкретних діях. У сфері формування компаній основним тригером ризику виступає відсутність очевидної економічної доцільності. Запит на створення нової юридичної особи, особливо якщо у замовника вже є низка бездіяльних фірм або він уникає пояснень щодо бізнес-моделі, має розглядатися як серйозний сигнал. Документ детально описує феномен shell companies – юридичних оболонок без реальної діяльності, персоналу чи активів. Хоча вони можуть використовуватися для законних цілей (наприклад, для майбутніх проектів), їхня вразливість для зловживань є надзвичайно високою. Особливо ризикованими вважаються «готові» (shelf) компанії з історією та відкритими банківськими рахунками, оскільки вони можуть минати посилену перевірку з боку фінансових установ, які схильні з меншою підозрою ставитися до фірм з кількарічною історією. Формування компаній, які стають частиною складних міжнародних структур, особливо з елементами високоризикових юрисдикцій, створює

навмисні перешкоди для відстеження власності та потоків коштів, перетворюючи корпоративну структуру не на інструмент бізнесу, а на бар'єр для нагляду.

Номінальні директорські та акціонерні послуги розкривають іншу грань проблеми – ризик пасивності та надмірного розподілу обов'язків. Коли номінальний директор не має реального розуміння бізнесу, не контролює його операційну та фінансову діяльність, особливо якщо рахунки знаходяться за кордоном, він перетворюється з формального керівника на маріонетку, чия роль зводиться до підписання документів за вказівкою реального власника. Це не лише полегшує злочинцям контроль, але й руйнує саму ідею корпоративного управління як системи контролю та балансів. Ще більш виразним сигналом є ситуація, коли одна особа виступає номінальним директором для десятків чи навіть сотень компаній. Фізична неможливість якісного виконання обов'язків у таких умовах є прямим свідченням того, що послуга куплена не для адміністративного зручності, а виключно для створення видимості легальності. Аналогічна логіка поширюється на номінальних акціонерів: тривале володіння акціями від імені клієнта без плану передачі або обслуговування цілої низки пов'язаних компаній вказує на системну спробу розмити та приховати картину бенефіціарного контролю.

Віртуальні офісні послуги, що включають надання юридичної адреси та пересилання пошти, в документі HMRC представлені як потужний інструмент для створення фіктивної присутності. Відсутність регулярного фізичного контакту з клієнтом створює ідеальні умови для використання підроблених документів та шахрайської ідентифікації. Однак найбільш проникливими є спостереження щодо шаблонів використання цих послуг. Регулярне пересилання великих обсягів пошти, особливо якщо воно не корелює з заявленою діяльністю клієнта, може бути ознакою масових шахрайських схем, де листи розсилаються тисячам потенційних жертв. Часта зміна осіб, які забирають пошту, або їх поява без попереднього узгодження може свідчити про ротацію кадрів у злочинній організації або про несанкціоновану субаренду адреси. Надання кількох віртуальних адрес пов'язаним бізнесам без очевидної потреби, наприклад, для різних підрозділів однієї фірми, розкриває спробу створити ілюзію масштабу та місцевої присутності, щоб викликати більшу довіру у жертв шахрайства або у контрагентів.

У сфері трастових послуг документ зосереджується на фігурі професійного трасті (professional trustee). Траст, як юридична конструкція, за своєю суттю призначений для відокремлення управління майном від права користування ним, що вже створює потенціал для уникнення прозорості. HMRC підкреслює, що професійний трасті не може бути пасивним виконавцем вказівок засновника (settlor). Він зобов'язаний активно розуміти мету створення трасту, джерела його активів, механізми розподілу вигод та мати реальний нагляд за фінансовими потоками. Ризик різко зростає, коли джерела коштів трасту неясні або мають ознаки корупційного походження, коли довіритель не має доступу для моніторингу закордонних рахунків трасту або коли засновник або бенефіціар постійно тиснуть на нього, намагаючись відхилитися від задекларованих цілей. У таких умовах траст легко перетворюється з інструменту сімейного або благодійного планування на ефективний апарат для відмивання коштів та ухилення від санкцій.

Окремою та критично важливою темою, яку піднімає документ, є явище професійних посередників (professional enablers). Це не зовнішні злочинці, а представники респектабельних професій – юристи, бухгалтери, фінансові радники, інші TCSP, – які, скориставшись довірою та складністю регуляторного поля, свідомо або через кричущу недбалість стають співучасниками злочинних схем. Вони можуть спеціально проектувати корпоративні структури, щоб обійти вимоги щодо ідентифікації, давати поради щодо вибору юрисдикцій зі слабким наглядом або просто ігнорувати свої обов'язки з проведення належної перевірки клієнтів (due diligence). HMRC прямо зазначає, що не всі професіонали дотримуються стандартів однаково, і саме ця неоднорідність створює додатковий операційний ризик для суміжних TCSP, які можуть надто

довіряти «колегам по цеху». Відтак, довіра має бути підкріплена перевіркою: чи перебуває цей партнер під наглядом відповідного органу? Чи виконує він свої регуляторні зобов'язання? Відмова від бізнес-відносин з непідконтрольними особами представлена в документі не як рекомендація, а як обов'язкова вимога.

Керівництво також постійно акцентує увагу на динамічному характері ризику, що вимагає не разової перевірки, а постійного моніторингу та переоцінки. Початкова ідентифікація клієнта – це лише перший крок. Зміна контролюючих сторін, роду діяльності компанії, невідповідність між заявленими обсягами операцій (особливо готівкових) та реальними, раптова активізація «сплячої» компанії – все це вимагає негайної реакції та перегляду рівня ризику. Документ надає TCSP роль не пасивного реєстратора, а активного наглядача, який повинен виявляти аномалії в поведінці та бізнес-активності клієнта протягом усього терміну співпраці.

Таким чином, аналітичний зміст документа HMRC далеко виходить за рамки простого списку небезпек. Він конструює цілісну систему мислення, в якій кожна послуга, кожна географічна прив'язка, кожна бізнес-модель розглядається через призму її потенційного використання для дестабілізації фінансової системи. Ключовим висновком є те, що ефективна боротьба з фінансовими злочинами на рівні TCSP вимагає не лише технічного дотримання процедур KYC, але й глибокого розуміння бізнесу клієнта, здорового скептицизму щодо надмірно складних або нелогічних схем, а також здатності постійно аналізувати зміни в поведінці та зовнішньому середовищі. Це керівництво можна розглядати як визнання того, що у сучасній фінансовій екосистемі TCSP стали частиною першої лінії оборони, і від їхньої пильності, професійної сумлінності та готовності відмовляти в послугах при найменших сумнівах залежить цілісність значно ширшої системи економічної безпеки.

Висновки:

- **Юрисдикції, що мають стратегічні недоліки в боротьбі з відмиванням коштів та фінансуванням тероризму, автоматично підвищують ризиковість операцій.** Навіть країни без формального статусу "високоризикових", але з високим рівнем корупції, слабким корпоративним регулюванням або культурою фінансової секретності, становлять значну загрозу.
- **Використання посередників та багаторівневих схем надання послуг створює штучну анонімність,** ускладнює ідентифікацію кінцевого бенефіціарного власника та перевірку джерел коштів.
- **Окремі види послуг несуть підвищені ризики:** номінальні директори без реального контролю, компанії-оболонки без економічної доцільності, віртуальні офіси — все це може свідчити про спроби створити видимість легальності для злочинних активів.
- **Ризик є динамічною категорією.** Зміни у власності, діяльності клієнта, обсягах операцій, особливо готівкових, вимагають негайного реагування та перегляду рівня ризику. TCSP повинні функціонувати як активні наглядачі, а не пасивні виконавці формальних процедур.

Інші новини

Децентралізована загроза: як цифрові технології перетворюють молодь на мішені для терористичних мереж [19]

З початку другого десятиліття XXI століття Латинська Америка, традиційно не асоційовалась з масштабною джихадистською активністю, проте поступово перетворилася на арену інтенсивної онлайн-радикалізації молоді під впливом ідеології Ісламської держави. Цей процес, що набув особливої сили після 2015 року, демонструє глибоку трансформацію механізмів вербування та ідеологічної доктринації, тісно пов'язану з еволюцією цифрових технологій.

Аналізуючи зміст дослідження Global Network on Extremism & Technology, можна простежити, як класичні моделі терористичної пропаганди, що спиралися на централізовані соціальні мережі, поступилися місцем складній, розгалуженій екосистемі децентралізованого інтернету, що робить протидію радикалізації значно складнішою. Особливу увагу привертає випадок Бразилії, найбільшої країни регіону, де соціально-економічні проблеми поєднуються з поширенням технологій, створюючи родючий ґрунт для росту екстремістських ідей серед молоді, що шукає ідентичності та сенсу в умовах маргіналізації та цифрової ізоляції.

Операція «Хештег» у 2015 році стала своєрідною відправною точкою для розуміння масштабів проблеми. Затримання групи молодих бразильців, які планували атаки під час Олімпійських ігор у Ріо-де-Жанейро, вперше чітко продемонструвало, що ідеологія ІД проникла в латиноамериканський простір не як абстрактна загроза, а як конкретна оперативна реальність. Ці особи, об'єднані низьким соціально-економічним статусом та обмеженим доступом до якісної освіти, сформували своєрідну мікромережу, де віртуальна комунікація через Facebook, WhatsApp та Telegram доповнювалася реальними особистими зв'язками, що виникли, зокрема, під час навчання в Єгипті та відвідування радикальних проповідей у Сан-Паулу.

Ця рання модель була відносно прозорою для моніторингу: централізовані платформи, хоч і ускладнювали масове блокування, все ж надавали технічні можливості для відстеження комунікацій та контенту. У відповідь на подібні інциденти великі технологічні компанії розгорнули масштабну кампанію з виявлення та видалення терористичного контенту, впроваджуючи складні алгоритми на основі штучного інтелекту для створення цифрових відбитків фото- та відеоматеріалів, а також обмежуючи функцію масового пересилання повідомлень. Ці заходи, безсумнівно, ускладнили життя екстремістським групам у традиційних соціальних мережах, однак вони спричинили не ліквідацію загрози, а її міграцію — явище, відоме як «ефект витіснення».

Саме тут на сцену виходить децентралізований інтернет (DWeb) — принципово інша парадигма організації інтернет-простору, заснована на відсутності центральних серверів та контролюючих органів. Платформи, побудовані на протоколах децентралізації, такі як ZeroNet, Matrix (з клієнтами на кшталт Element), RocketChat або мережі розподіленого зберігання даних на кшталт IPFS (InterPlanetary File System) та Skynet, перевернули уявлення про можливості модерації. У цих екосистемах дані зберігаються на пристроях самих користувачів, комунікація часто відбувається через end-to-end шифрування, а видалення контенту з одного вузла не призводить до його зникнення з мережі, оскільки він може бути миттєво відновлений з інших джерел. Для терористичних медіа це створило ідеальне середовище: вони отримали технологічний

[19] https://gnet-research.org/2025/11/14/from-techhaven-to-telegram-how-latin-american-youth-are-being-drawn-into-jihadist-networks/

санктуарій, де можуть вільно публікувати пропагандистські журнали, як-от «Дабік», «Румія» чи «Голос Хорасану», інструкції з виготовлення вибухових пристроїв, хімічної зброї та проводити вербувальні кампанії, практично не побоюючись втручання.

Ілюстрацією ефективності цього підходу слугує історія групи на платформі TechHaven, яку адміністрував 45-річний бразилець, затриманий у 2024 році. Ця група була орієнтована виключно на португаломовну аудиторію і являла собою витончений приклад культурної гібридизації та локалізації пропаганди. Адміністратор виконував роль не лише технічного модератора, але й культурного перекладача, який адаптував глобальну апокаліптичну риторику ІД до бразильських реалій. Він поєднував офіційні комюніке агенції Amaq, перекладені португальською, з витягами з міжнародних джихадистських журналів та місцевим культурним контекстом — посиланнями на бразильську музику, соціальні проблеми, навіть використовував місцеві посібники з виживання, переосмислені в парадигмі терористичної підготовки. Це дозволяло будувати емоційний зв'язок з аудиторією, яка могла не відчувати безпосередньої причетності до конфліктів на Близькому Сході, але легко ідентифікувала себе з образами соціальної несправедливості та кризи в власній країні.

Крім ідеологічного змісту, група виконувала чітку оперативну функцію: вона слугувала хабом, що перенаправляв зацікавлених користувачів у закриті Telegram-канали. Саме там відбувалася спеціалізована «підготовка кадрів»: публікувалися детальні, покрокові інструкції з виготовлення саморобних вибухових пристроїв, пояснювався принцип дії детонаторів, наводилися рецепти отруйних речовин, таких як фосфін, сірководень або ціанід. Особливу турботу викликав той факт, що паралельно проводився збір коштів через криптовалютні гаманці, що демонструє фінансову автономність та адаптивність цих мереж.

Процес радикалізації в умовах DWeb набуває унікальних рис, особливо коли йдеться про неповнолітніх. Відсутність центральної модерації, зашифровані простори, атмосфера таємничості та доступ до «заборонених знань» часто перетворюють знайомство з екстремістським контентом на форму цифрового екстриму або гри. Підлітки, особливо ті, що страждають від соціальної ізоляції, почуття непотрібності або нав'язливого бажання знайти своє місце у світі, можуть сприймати участь у таких групах як виклик системі, спосіб підвищити свій статус серед однолітків або навіть як інтелектуальне дослідження. Випадок 14-річного уругвайця, який, спілкуючись з адміністратором бразильської групи в TechHaven, дійшов до публічної погрози атакувати синагогу в Монтевідео, показує, як швидко віртуальна радикалізація може трансформуватися в реальну загрозу.

Глобальна статистика лише підтверджує цю тенденцію: за даними Global Terrorism Index 2025, частка неповнолітніх серед затриманих за тероризм у Європі становить 20%, а кількість атак терористів-одинаків, часто юних віком, значно зросла. Ці особи, як правило, не мають формальних зв'язків з терористичними організаціями, а їхня ідеологія формується в результаті хаотичного потоку інформації з маргінальних форумів, ігрових чатів, зашифрованих месенджерів і темної мережі, змішуючи ісламістські, неонацистські та інші радикальні наративи в нестійкий, але вкрай небезпечний коктейль.

Окремої уваги заслуговує явище міжплатформної міграції, яке стало ключовою стратегією виживання джихадистських мереж. Коли один канал на Telegram блокується, його учасники отримують посилання на новий канал або групу в іншому месенджері, наприклад, у Discord або Signal. Коли стає «гаряче» на централізованих платформах, активність переміщується на децентралізовані хостинги типу ZeroNet. Ця «гідра» з безліччю голів унеможливлює повне знищення мережі; завдання правоохоронних органів та компаній ускладнюється до неймовірності, оскільки вони змушені грати в нескінченну гру переслідування по всьому спектру цифрового простору. Більше того, використання блокчейн-технологій та криптовалют

для фінансування створює додатковий, надзвичайно складний для відстеження шар операційної діяльності.

Усвідомлення цих викликів вимагає комплексного переосмислення підходів до запобігання та протидії. З технологічної точки зору, необхідна розробка більш витончених інструментів моніторингу, здатних аналізувати трафік і виявляти шаблони поведінки, характерні для екстремістської діяльності, навіть у децентралізованих та зашифрованих середовищах. Штучний інтелект і машинне навчання можуть бути спрямовані на ідентифікацію не стільки конкретного контенту, скільки мережевих зв'язків, сигнатур фінансових транзакцій та цифрових слідів, що залишаються навіть при використанні технологій анонімізації.

Важливим кроком є також впровадження інструментів на рівні користувача: наприклад, коли користувач намагається перейти за посиланням з безпечного середовища (як, наприклад, Facebook) на незахищену або децентралізовану платформу, система має показувати чітке попередження, що пояснює потенційні ризики та вимагає свідомого підтвердження дії. Це може сповільнити миттєвий, часто зумовлений цікавістю перехід у ризикові зони інтернету, особливо для молоді.

Висновки:

- **Перехід до децентралізованого інтернету різко ускладнив боротьбу з екстремістським контентом.** Платформи на кшталт ZeroNet, Telegram, Matrix та IPFS, через відсутність централізованого контролю та шифрування, стали ідеальними осередками для вербування, пропаганди та оперативного планування терористичних актів.
- **Культурна гібридизація пропаганди є ключовим інструментом радикалізації.** Екстремісти адаптують глобальні ідеологічні наративи до місцевого контексту, використовуючи національні символи, музику, соціальні проблеми, що робить їхню риторику близькою та привабливою для місцевої молоді.
- **Молодь та неповнолітні особливо вразливі через соціально-економічні фактори, а також через психологічний фактор:** участь у закритих онлайн-групах часто сприймається як гра, виклик або спосіб віднайти ідентичність.
- **Ефективна протидія вимагає комплексного підходу, що поєднує:** технологічні інновації, міжнародну координацію, оновлення законодавства та вирішення соціально-економічних проблем, що лежать в основі радикалізації.

Однак жодні технічні інновації не будуть ефективними без глибокої міжнародної координації між державними силовими структурами, розвідувальними службами, регуляторами та приватним технологічним сектором. Необхідні спеціалізовані міжнародні робочі групи, які займатимуться аналізом відкритих протоколів, що лежать в основі DWeb, та розробкою правових і технічних механізмів, що дозволяють здійснювати обмежений нагляд, не руйнуючи при цьому фундаментальні принципи конфіденційності та децентралізації, які є основою цих технологій. Законодавство повинно встигати за технологічним прогресом, передбачаючи процедури примусового видалення терористичного контенту навіть з розподілених вузлів та механізми блокування цифрових активів, пов'язаних з фінансуванням тероризму.

Для загального розвитку

Chain-Hopping: нова реальність відмивання криптовалют [20]

Стаття від Elliptic проголошує chain-hopping провідною технікою відмивання криптовалют у 2025 році, що відображає глибоку трансформацію як самої крипто-екосистеми, так і методів, які використовують кіберзлочинці для приховування незаконних фінансових потоків. Сучасний криптоландшафт налічує сотні блокчейнів та тисячі цифрових активів, створюючи безпрецедентно складне середовище, в якому традиційні методи фінансового розслідування та комплаєнсу все частіше виявляються неефективними. Саме в цій складності злочинці знайшли родючий ґрунт для розвитку витончених схем обфускації коштів, з яких chain-hopping виділяється своєю системністю, масштабованістю та важливістю для розуміння сучасних тенденцій у сфері криптозлочинності.

Цей метод, по суті, є логічним наслідком еволюції децентралізованих фінансів (DeFi) та розвитку інфраструктури для взаємодії між різними блокчейнами. Злочинці більше не обмежуються переміщенням коштів в межах однієї мережі, на кшталт Bitcoin або Ethereum. Натомість вони активно експлуатують весь спектр доступних інструментів, щоб створити навмисно заплутаний шлях, що проходить через кілька незалежних блокчейнів, кожен з яких має свої особливості, стандарти анонімності та можливості відстеження. Це не просто технічний прийом, а стратегічний підхід, спрямований на експлуатацію децентралізації крипто-екосистеми — її найбільшої сили з точки зору інновацій, що перетворюється на найбільшу слабкість з точки зору безпеки та дотримання законодавства.

Ключовими технологічними складовими, що роблять chain-hopping можливим, є три типи сервісів, кожен з яких виконує свою специфічну роль у процесі відмивання. Децентралізовані біржі (DEX) діють як перший етап перетворення активів. Вони є протоколами DeFi, що дозволяють автоматично обмінювати один токен на інший в межах одного блокчейну за допомогою смарт-контрактів та пулів ліквідності. Повна відсутність централізованого посередника, а також, як правило, будь-яких процедур ідентифікації, робить їх ідеальним інструментом для швидкої конвертації вкрадених або «брудних» активів у більш ліквідні та менш помітні форми. Наприклад, злочинці часто міняють специфічні токени, отримані в результаті хакерської атаки на певний протокол, на універсальні стейблкоїни (USDT, USDC) або нативні активи блокчейнів (ETH, BNB). Ця операція не тільки збільшує ліквідність коштів, але й розмиває зв’язок між початковим злочином і конкретним активом, ускладнюючи його потенційне заморожування емітентом або правоохоронцями.

Другим критично важливим ланком є кросс-чейн мости. Ці механізми призначені саме для переміщення цінності між різними блокчейн-мережами, використовуючи модель «lock-and-mint». Коли користувач хоче перевести активи, скажімо, з Ethereum на Polygon, оригінальні активи блокується в спеціальному смарт-контракті в мережі Ethereum, а еквівалентна їм кількість у вигляді «wrapped»-токенів випускається в мережі Polygon з резервного пулу. Для злочинця кожен такий «перехід» через міст — це не просто зміна адреси, а кардинальна зміна середовища перебування коштів. Транзакція в мережі Polygon або Arbitrum перебуває в абсолютно іншому датасеті, з іншими аналітичними інструментами. Як показав приклад скандальної інвестиційної схеми CBEX, злочинці можуть здійснювати такі переходи понад сто разів між блокчейнами Tron та Ethereum, перетворюючи ручне відстеження на майже неможливу працю, де кожна нова транзакція збільшує необхідні витрати часу та ресурсів у геометричній прогресії.

[20] https://www.elliptic.co/blog/chain-hopping-defining-money-laundering-method-of-2025

Третім, особливо тривожним інструментом, є централізовані сервіси обміну монет (coin swap services). На відміну від DEX, вони часто є централізованими платформами, що працюють через веб-сайти або Telegram-канали. Їхня ключова риса — повна або практична відсутність процедур KYC (Know Your Customer). Дослідження Elliptic вказує на зростаючу популярність цих сервісів серед злочинців, які навіть почали віддавати їм перевагу перед класичними міксерами (tumblers). Як зазначає експерт Elliptic, це пов'язано з недавніми санкціями та конфіскаціями, спрямованими проти відомих міксерів. Сервіси обміну монет часто рекламують свої послуги в нелегальних онлайн-спільнотах, відкрито демонструючи готовність працювати з незаконними коштами. Вони пропонують обмін практично будь-яких активів на будь-яких блокчейнах, виступаючи таким чином універсальним і надзвичайно гнучким завершальним етапом ланцюга відмивання.

Важливо підкреслити, що chain-hopping як явище є технологічно нейтральним. Більшість обсягів, що проходять через DEX та мости, є абсолютно легальними — це мільярди доларів щоденних операцій інвесторів, трейдерів та користувачів DeFi. Згідно з даними, менше 1% від загального обсягу таких транзакцій має кримінальне походження. Проте саме цей невеликий відсоток демонструє надзвичайну ефективність технології для злочинних цілей. Злочинці використовують chain-hopping для приховування широкого спектру незаконної діяльності: від фінансування тероризму та роботи з підсанкційними юрисдикціями до організації шахрайських схем, азартних ігор, торгівлі в даркнеті та легалізації коштів від масштабних кібератак. Статистика Elliptic є виразним свідченням ускладнення цих схем: вже третина складних міжмережевих розслідувань включає понад три блокчейни, чверть — понад п'ять, а кожне п'яте розслідування стикається з шляхом, що пролягає через більше десяти різних мереж.

Реальна практика показує, що злочинці рідко обмежуються одним інструментом, натомість створюють багаторівневі каскади обфускації. Яскравий приклад — хакерська атака на Cetus Network, в результаті якої було викрадено приблизно 200 мільйонів доларів. Злодії не просто вивели кошти. Спочатку, використовуючи DEX, вони обміняли вкрадені USDT на USDC — два стейблкоїни, які, хоча й можуть бути заморожені їхніми емітентами, у цьому випадку використовувалися для розмивання сліду. Далі, за допомогою кросс-чейн моста, кошти були переведені в мережу Ethereum. На завершення, через інший DEX-агрегатор USDC був обміняний на Ethereum (ETH), ймовірно, з метою повністю позбутися від активів, що підлягають потенційному заморожуванню, і отримати абсолютно автономний актив. Така послідовність дій — це чітко продумана операційна стратегія, спрямована на нейтралізацію основних механізмів захисту та відстеження.

Очевидно, що протистояти такій складності вручну неможливо. Як констатує Метт Прайс, віце-президент з розслідувань та стратегічних консультацій в Elliptic, зростання кількості блокчейнів створює колосальний виклик як у плані обробки даних, так і у плані ресурсів. Злочинна поведінка стає все витонченішою, що вимагає аналогічної еволюції від інструментів розслідування. Відповіддю на цей виклик стає автоматизація.

Розроблена Elliptic технологія віртуальних подій передачі цінності (Virtual Value Transfer Events, VVTEs) є саме таким кроком еволюції. Вона повністю автоматизує процес відстеження транзакцій через кросс-чейн мости, встановлюючи прямі та перевіряючи зв'язки між вихідною транзакцією в одній мережі та цільовою транзакцією в іншій. Наразі система охоплює понад 300 комбінацій мостів та протоколів.

Операційний вплив VVTEs є трансформаційним для різних команд. Команди моніторингу транзакцій отримують миттєву видимість щодо джерела депозитів, що надійшли через міст. Спеціалісти з комплаєнсу та правоохоронці значно прискорюють розробку справ та збір доказів, прослідковуючи складні міжмережеві шляхи за лічені хвилини замість тижнів копіткої ручної

роботи. Фінансові установи, що проводять due diligence криптобізнесів, тепер можуть бачити повну картину кросс-чейн активності для точної оцінки ризиків.

Однак автоматизація відстеження через мости — це лише частина рішення. Традиційний підхід до скринінгу, який фокусується на одному активі (наприклад, тільки на ETH в гаманці Ethereum), створює небезпечні сліпі зони. Сучасний криптогаманець — це мультичейн-середовище. Він може одночасно містити токени стандарту ERC-20 на Ethereum, NFT на Polygon, власні токени в мережі BNB Smart Chain, та безліч інших активів. Скринінг лише нативного активу в такій ситуації є абсолютно недостатнім для формування повної картини ризиків. Тому наступним критичним елементом є впровадження цілісного (holistic) скринінгу, який у реальному часі аналізує всі активи та всі блокчейни, пов'язані з конкретною адресою або транзакцією.

Ці технологічні зміни формулюють нові, жорсткі операційні вимоги до команд з комплаєнсу в криптоіндустрії. Зростання обсягів кросс-чейн злочинності з 7 до 22 мільярдів доларів за два роки не залишає вибору. По-перше, необхідно розгорнути можливості цілісного скринінгу, що охоплюють всі активи та блокчейни. По-друге, обов'язковим стає впровадження автоматизованої інфраструктури для кросс-чейн відстеження, оскільки ручні методи не масштабуються. По-третє, процеси due diligence повинні розширюватися за рахунок інтеграції як ончейн, так і офчейн-розвідданих, оскільки аналіз лише транзакцій часто не розкриває справжніх бенефіціарів та зв'язків. По-четверте, правила оцінки ризиків повинні враховувати не лише прямі транзакції, а й опосередковану експозицію через ланцюг переказів, адже кошти, що знаходяться за кілька «стрибків» від санкційованої особи, все одно несуть суттєвий комплаєнс-ризик. І, по-п'яте, критично важливим є підтримання постійної обізнаності про нові типології злочинів, такі як інфраструктура шахрайства на основі штучного інтелекту та постійно техніки відмивання, які постійно еволюціонують.

Висновки:

- **Chain-hopping — метод відмивання криптовалют**, що базується на багаторазовому переміщенні коштів між різними блокчейнами через DEX, кросс-чейн мости та анонімні сервіси обміну, що ускладнює відстеження ручними методами до неможливості.
- **Зростання обсягів кросс-чейн злочинності з $7 млрд до $22 млрд за два роки** вимагає радикального оновлення комплаєнс-інструментів: автоматизації відстеження, цілісного скринінгу всіх активів мультичейн-гаманців та інтеграції офчейн-розвідки.
- **Злочинці все частіше відмовляються від класичних міксерів на користь централізованих сервісів обміну** монет без KYC, які відкрито працюють у нелегальних спільнотах, що свідчить про адаптацію їхніх схем до регуляторного тиску.
- **Ефективна боротьба з chain-hopping можлива лише за умови синхронної еволюції інструментів розслідування,** які повинні працювати в тому ж масштабі й складності, що й крипто-екосистема, з акцентом на автоматизацію, охоплення сотень блокчейнів і постійний моніторинг.

У підсумку, боротьба з відмиванням криптовалют перетворюється на безперервну гонку технологій та інтелекту. Злочинці інноваційно використовують децентралізовану архітектуру світу Web3, тоді як регулятори, правоохоронці та комплаєнс-спеціалісти змушені будувати аналогічно складні, автоматизовані та масштабовані системи аналізу. Як резюмує Метт Прайс, маючи потрібні інструменти, дані та можливість проводити розслідування в масштабі, можна перетворити обфускацію, створювану злочинцями, на перевагу для слідчих. Майбутнє фінансової безпеки в цифрову епоху залежатиме від здатності індустрії прийняти цю багатомережну реальність та протистояти її темній стороні з рівною мірою винахідливості.

Ваша думка важлива!

1. Наскільки ефективно українська система фінансового моніторингу здатна виявляти доходи від екологічних злочинів, якщо такі злочини часто мають транскордонний характер, а легалізація коштів здійснюється через складні корпоративні структури та іноземні фінансові центри?
2. Чи повинна Україна орієнтуватися на еволюційний, багаторівневий підхід до врядування штучного інтелекту у фінансовому секторі, чи доцільніше одразу закріпити окрему законодавчу рамку для AI з урахуванням євроінтеграційного курсу та стандартів ЄС?
3. Наскільки українська фінансова екосистема стійка до ризиків, подібних до Scambling? Чи можуть популярність онлайн-платежів (зокрема через додатки банків), широке використання соціальних мереж для реклами та наявність вразливих через війну і економічні труднощі груп населення створити ідеальне середовище для швидкого поширення аналогічних гібридних шахрайських схем в Україні?
4. Чи достатньо в Україні інституційних можливостей для ефективного нагляду за TCSP та професійними посередниками? Як українські регулятори можуть протистояти практикам створення складних корпоративних структур, враховуючи потенційний брак ресурсів та можливості для впливу?

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-2026-01

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

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