Методологічний бюлетень

Серійний номер: МінФін-AML-2025-36

Вересень 2025

“Любіть те, що робите — тоді робитимете це якнайкраще”

Кетрін Джонсон

Мета

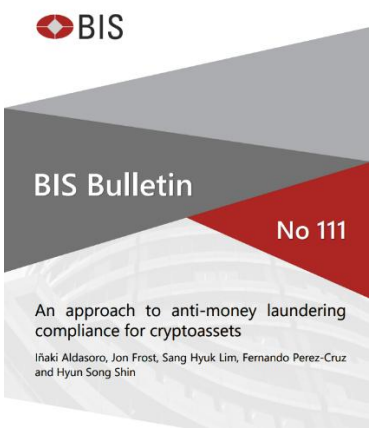
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Підхід до комплаєнсу з ПВК в сфері криптоактивів [1]



Документ BIS Bulletin No 111 присвячений пошуку нових підходів до забезпечення дотримання вимог ПВК/ФТ у сфері криптоактивів. Основна ідея полягає у використанні відкритих властивостей публічних блокчейнів для побудови більш ефективної системи контролю. Традиційна модель ПВК, яка спирається на посередників — банки та інші регульовані фінансові установи, — демонструє обмежену ефективність у випадку permissionless-блокчейнів, де відсутній якийсь один конкретний відповідальний суб’єкт. Дослідники відзначають, що нині стейблкоїни витіснили біткоїн як основний інструмент, який використовують злочинці у криптосфері, і станом на 2024 рік на них припадає близько 63% усіх сумнівних транзакцій.

[1] https://www.bis.org/publ/bisbull111.pdf

У роботі описано, як відкритий характер записів у блокчейнах може стати основою для нової системи оцінки ризиків. Замість покладання виключно на перевірки у точках входу/виходу з банківської системи, пропонується формування спеціального “AML compliance score”. Такий діагностичний показник визначав би ймовірність того, що конкретна одиниця криптоактиву чи баланс пов’язані з незаконною діяльністю. Високий бал означав би «чисті» кошти, низький — «забруднені», що дозволило б банкам, біржам чи емітентам стейблкоїнів блокувати або дозволяти операції залежно від порогових значень. Автори наголошують, що це може стимулювати культуру “обов’язку належної перевірки” серед учасників ринку.

Документ порівнює різні моделі блокчейнів. У випадку біткоїна застосовується модель UTXO, де кожна одиниця може бути відслідкована до моменту її створення. Для стейблкоїнів використовується account-based модель (Ethereum, Tron), яка не дає змоги розрізнити окремі токени, але все ж дозволяє простежити походження через історію гаманців. Крім того, централізований характер більшості стейблкоїнів дає емітентам можливість блокувати кошти чи відмовляти у конвертації на вимогу регуляторів.

Система AML-score може бути реалізована у різних варіантах — від жорстких до ліберальних. У «суворій» моделі допускаються лише транзакції через гаманці, які пройшли KYC та внесені до списку дозволених. У «ліберальній» — перевіряється лише факт проходження монети через «заборонені» адреси. Між цими крайнощами можливі проміжні варіанти, що враховують тривалість зберігання активів у «чистих» гаманцях, відсутність зв’язків із відомими схемами відмивання чи сумнівними протоколами, а також розмір операції залежно від рівня AML-score.

Документ наголошує на потребі чітко визначити, хто несе відповідальність за блокування незаконних потоків: користувачі, біржі, постачальники послуг з обміну чи окремі клірингові структури. Логічним виглядає покладення цього обов’язку на «оф-рампи» — точки виходу криптовалют у фіатну систему, зокрема банки та регульовані біржі. Такий підхід формуватиме стимули не приймати «забруднені» токени. Додатково відзначається можливість виникнення ринку спеціалізованих постачальників комплаєнс-послуг, які надаватимуть доступні інструменти перевірки активів навіть пересічним користувачам

З точки зору ширшої політики, автори підкреслюють, що принцип «same risk – same regulation» у цьому випадку не працює, оскільки ризики криптоактивів відрізняються від класичних фінансових інструментів. Використання історії транзакцій для формування цінності токена може призвести до ситуації, коли стейблкоїни з «підмоченою» репутацією торгуватимуться зі знижкою. Водночас упровадження системи AML-score здатне створити позитивний ефект саморегуляції серед користувачів, коли обов’язок належної перевірки стане загальною практикою. Міжнародна співпраця у цій сфері розглядається як ключовий елемент для подолання транскордонних викликів, які за своєю природою властиві криптоактивам

Висновки:

- Розробка AML-score на основі публічних даних блокчейну може стати інноваційним інструментом для блокування «забруднених» активів на етапі їхнього обміну на фіат.
- Стратегія контролю має варіюватися від жорстких KYC-орієнтованих моделей до ліберальних підходів, залежно від пріоритетів регулятора.
- Відповідальність за «чистоту» потоків доцільно зосередити на оф-рампах (біржі, банки, емітенти стейблкоїнів), що знизить ризик проникнення незаконних коштів у традиційну фінансову систему.
- Міжнародна координація та створення ринку комплаєнс-послуг є критично важливими для ефективного впровадження та забезпечення реальної практичної дії цього підходу.

CBDC, стейблкоїни та токенізація: глобальні результати опитування BIS 2024 і трансформація платіжної системи [2]

Документ є підсумковим дослідженням Банку міжнародних розрахунків, яке відображає глобальні тенденції у сфері цифрових валют центральних банків (CBDC), криптоактивів, стабільних монет та токенізації фінансових і реальних активів. Опитування охопило 93 центральні банки, юрисдикції яких представляють понад три чверті світового населення і майже весь обсяг світового ВВП, що робить висновки надзвичайно репрезентативними. Основний висновок полягає в тому, що центральні банки дедалі активніше працюють над питаннями впровадження CBDC, при цьому робота над оптовими CBDC є більш просунутою, ніж над роздрібними, а розвиток державних цифрових валют іде у тісному зв'язку з регуляторними ініціативами щодо стейблкоїнів, криптоактивів та процесами токенізації.

У 2024 році 91% опитаних центральних банків вели дослідження, експерименти або пілотні проєкти, пов'язані з CBDC. Розвинені країни значною мірою фокусуються на оптових цифрових валютах, тоді як у країнах, що розвиваються, більш активно розвивається напрям роздрібних CBDC з акцентом на фінансову інклюзію. Мотивація центральних банків різниться залежно від юрисдикцій, однак серед головних чинників виділяються необхідність збереження ролі грошей центрального банку в умовах падіння використання готівки, забезпечення єдності та довіри до національної грошової системи, підвищення ефективності та безпеки внутрішніх і транскордонних платежів. У країнах із розвиненою економікою CBDC розглядаються як спосіб підвищення ефективності розрахунків на фінансових ринках і підтримки операцій з токенізованими активами, тоді як у країнах, що розвиваються, їхня роль у підвищенні доступу до фінансових послуг має особливе значення. На практиці вже існують приклади функціонування роздрібних CBDC у Багамах, Ямайці та Нігерії, а також кілька десятків пілотних програм у різних регіонах світу.

Дизайн та архітектура майбутніх CBDC залишаються дискусійними. Для роздрібних валют центральні банки розглядають моделі двоетапного розповсюдження через банки і небанківських провайдерів, можливість використання без банківського рахунку, обмеження на обсяги зберігання і транзакції, відсутність нарахування відсотків та введення офлайн-функціоналу. Значна увага приділяється інтероперабельності з іншими платіжними системами та потенційними цифровими валютами інших держав, що має критичне значення для майбутніх крос-блокчейн-розрахунків. Для оптових валют пріоритетними є міжбанківські розрахунки, забезпечення взаємодії токенізованих активів, автоматизація виконання угод та інтеграція з іншими платіжними інфраструктурами. У цьому контексті особливе значення мають розподілені реєстри (DLT), які розглядаються більшістю центральних банків як основа для оптових CBDC, тоді як у сфері роздрібних валют до їх використання ставляться обережніше.

Зростання уваги до CBDC безпосередньо пов'язане з розвитком стейблкоїнів та криптоактивів. Попри те, що їх використання для платежів у більшості країн залишається обмеженим і носить переважно нішевий характер, у деяких країнах, що розвиваються, вони набули значення у сфері міжнародних переказів та транскордонних платежів. Саме це стало одним із ключових тригерів активізації роботи над CBDC, адже поширення приватних цифрових активів без належного регулювання може створювати ризики для стабільності грошової системи та фінансової безпеки. До кінця 2024 року понад дві третини юрисдикцій у світі вже мали або розробляли спеціальні регуляторні рамки для стейблкоїнів і криптоактивів, віддаючи перевагу саме

[2] https://www.bis.org/publ/bppdf/bispap159.pdf

спеціальному, а не загальному фінансовому регулюванню. Це свідчить про те, що глобальні регулятори прагнуть уникнути регуляторного арбітражу, забезпечити захист споживачів і зберегти монетарний суверенітет.

Важливою складовою звіту є аналіз процесів токенізації активів, які у 2024 році активно розвивалися в розвинених країнах і поступово поширювалися у країнах, що розвиваються. Найбільш популярним напрямом стала токенізація облігацій, як державних, так і корпоративних, що пояснюється високим потенціалом оптимізації цього сегмента через зниження ролі посередників та скорочення витрат на проведення операцій. Також у сфері токенізації розвиваються інвестиційні фонди, нерухомість та інші активи. Водночас реальний обсяг ринку токенізованих активів поки що залишається обмеженим. У низці юрисдикцій комерційні банки вже експериментують або навіть запровадили токенізовані депозити, що може стати важливим кроком у трансформації банківського сектору. На відміну від цього, випуск стейблкоїнів банками залишається обмеженим і використовується для специфічних завдань, тоді як їх інтеграція у фінансові ринки ще не має системного характеру.

Висновки:

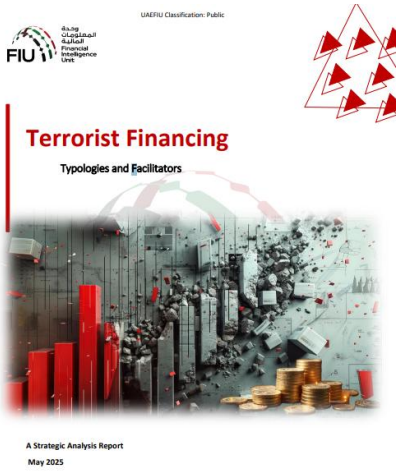
- **CBDC стають центральним елементом майбутньої грошової системи:** 91% центральних банків вже працюють над ними; оптові CBDC демонструють більший прогрес, ніж роздрібні CBDC .
- **Стабільність та суверенітет як драйвери:** основна мотивація – збереження ролі грошей центрального банку, підвищення безпеки платежів і зменшення залежності від приватних стейблкоїнів.
- **Регуляція криптоактивів посилюється:** понад дві третини країн світу вже мають або розробляють спеціальні рамки для стейблкоїнів і криптоактивів, щоб запобігти арбітражу та забезпечити фінансову стабільність .
- **Токенізація змінює фінансові ринки:** найчастіше токенізуються облігації; дедалі більше банків запускають токенізовані депозити, що вказує на майбутню інтеграцію цих інструментів у традиційні фінансові системи.

Загалом результати опитування демонструють, що платіжна екосистема перебуває у стані масштабної трансформації. Центральні банки намагаються зберегти контроль над грошовою системою в умовах зростаючої ролі приватних цифрових інструментів, а CBDC розглядаються як ключовий інструмент забезпечення стабільності, ефективності та довіри до національних валют. Паралельно відбувається формування нових правил для ринку криптоактивів і стейблкоїнів, а також поступова інтеграція токенізованих активів у фінансову систему. Хоча підходи різняться залежно від рівня розвитку економіки та політичних умов, усі країни стоять перед схожими викликами — потребою забезпечити баланс між інноваціями, фінансовою стабільністю та монетарним суверенітетом. У цьому контексті документ підкреслює ключову роль міжнародної координації та співпраці, без яких неможливо сформувати безпечну, стабільну і взаємопов'язану інфраструктуру майбутніх грошей і фінансових ринків.

Фінансування тероризму у глобальному вимірі: стратегічні тенденції та практичні індикатори [3]

Документ підготовлений UAEFIU у травні 2025 року є комплексним стратегічним аналізом сучасних тенденцій, типологій та посередників у сфері фінансування тероризму, заснованим на

[3] https://www.uaefiu.gov.ae/media/zinjjnj2/uaefiu-strategic-analysis-report-on-tf-26-june-public-version-final.pdf



аналізі даних, зібраних у період з 2021 по 2024 рік. Звіт детально пояснює, чому фінансова складова є критичною для функціонування терористичних організацій, адже саме через доступ до коштів вони здатні здійснювати планування, підготовку, логістику, вербування, навчання, пропаганду і проведення терактів. Виходячи з цього, протидія руху коштів є одним із найефективніших інструментів ослаблення терористичних мереж, а ефективність системи залежить від злагодженої роботи фінансових установ, визначених нефінансових установ і професій, провайдерів віртуальних активів та державних органів у виявленні та повідомленні підозрілих операцій.

Звіт окреслює міжнародні рамки та стандарти, зокрема рекомендації FATF, які передбачають криміналізацію фінансування тероризму, запровадження національних і секторальних оцінок ризиків та створення ефективних механізмів міжнародного співробітництва, а також положення Конвенції ООН 1999 року та резолюції РБ ООН 1373. У вступі наведено контекст поширення терористичних загроз, що дедалі частіше охоплюють нові географічні регіони, і підкреслено, що фінансова розвідка часто є єдиним інструментом, який дозволяє правоохоронним органам простежити зв'язки і виявити мережі.

Методологічно UAEFIU використало понад 397 повідомлень про підозрілі операції і діяльність, із яких лише 199 було визнано достатньо валідними та обґрунтованими для формування висновків, а також 104 справи, передані компетентним органам, дані міжнародних ПФР, відкриті джерела, відомості про осіб і групи, включених до санкційних списків. Аналітики сформували гіпотези щодо способів збору, руху, управління і маскування коштів, які були перевірені за допомогою внутрішніх і зовнішніх даних.

У результаті ідентифіковано широкий спектр типологій фінансування тероризму. До них належать використання фінансових установ та грошових сервісів для приховування бенефіціарів і руху коштів, застосування неліцензованих систем «Hawala», створення мереж компаній і номінальних власників для легалізації і багаторівневого переказу грошей, торгівля високовартісними товарами та використання торгівлі як каналу для «фінансування тероризму за допомогою торгівлі», інвестиції у нерухомість як спосіб збереження і відмивання ресурсів, краудфандинг та збір коштів через місцеві рахунки та іноземні неприбуткові організації, а також використання віртуальних активів, зокрема криптовалют, у фандрейзингу та транзакціях. Додатково виявлено схеми із залученням позик і кредитів, а також транзакції через високоризикові юрисдикції, що мають слабкі режими ПВК/ФТ.

Значну увагу приділено ролі посередників і фасилітаторів, серед яких ключовими виступають офіційно визначені або внесені до санкційних списків особи та організації, політичні екстремісти й корумповані посадовці з країн із високим рівнем терористичної загрози, члени сімей терористів, які можуть реєструвати компанії чи купувати нерухомість, так звані «грошові мули», що здійснюють дрібні перекази, номінальні особи, які прикривають справжніх бенефіціарів, а також юристи й бухгалтери, що надають структурам легальне прикриття.

Звіт виокремлює низку транзакційних і поведінкових ризикових індикаторів, які мають використовуватися фінансовими установами та наглядовими органами для своєчасного виявлення підозрілих операцій. До них належать зв'язки клієнтів із санкційними особами, статус PEP з конфліктних регіонів, використання підроблених документів, незвичні транзакційні патерни, регулярні перекази до/з юрисдикцій із високим рівнем терористичної активності, складні схеми переміщення вантажів і торгівлі, залучення невідомих або сумнівних

неприбуткових організацій, активне використання соціальних мереж і онлайн-платформ для збору коштів, інвестиції в предмети мистецтва й нерухомість.

Загалом звіт підкреслює, що фінансування тероризму дедалі частіше поєднує традиційні методи — банківські операції, торгівлю, Hawala — із сучасними інструментами, включно з криптовалютами, краудфандингом та цифровими платформами. Ця комбінація створює додаткові виклики для наглядових органів, вимагає підвищення якості фінансової розвідки, посилення контролю за корпоративними структурами і неприбутковим сектором, а також розвитку міжнародного співробітництва для ефективного виявлення і переривання фінансових потоків, що підтримують терористичну діяльність. Таким чином, UAEFIU надає своїм стейкхолдерам не лише аналітичний зріз ситуації, але й практичний інструментарій у вигляді типологій і ризикових індикаторів, які мають бути застосовані для підвищення ефективності виявлення, розслідування та запобігання фінансуванню тероризму.

Висновки:

- **Якість STR/SAR залишається критичною проблемою:** лише 50% поданих повідомлень були валідними, що вимагає навчання персоналу банків і ВНУП, розробки єдиних стандартів збору та верифікації даних.
- **Корпоративні структури та номінальні особи є найчастіше зловживаним каналом:** необхідно посилити перевірку КБВ, обмежити анонімність та запровадити дієві механізми контролю.
- **Криптовалюти та краудфандинг зростають як доповнення до традиційних каналів:** слід посилити регулювання VASP, впровадити аналітичні хаби для відстеження блокчейн-транзакцій і підвищити готовність установ до моніторингу онлайн-зборів.
- **Міжнародна співпраця є ключем до виявлення транскордонних схем:** необхідне активне використання каналів обміну ПФР-ПФР та участь у спільних типологічних дослідженнях для виявлення глобальних ланцюгів ФТ.

Вольфсберзька група 2025: нова ера моніторингу підозрілої активності з AI та машинним навчанням [4]

Документ є логічним продовженням попередньої заяви Вольфсберзької групи (2024), що окреслювала засади відходу від традиційного автоматизованого транзакційного моніторингу та формування більш ефективних програм MSA. Основний акцент зроблено на тому, що сучасні виклики фінансової злочинності вимагають від фінансових установ переходу до інноваційних підходів, які виходять за рамки класичних правилових сценаріїв і враховують поведінкові індикатори, ширший спектр даних та результати аналітики. Документ підкреслює, що класичні системи з високим рівнем хибнопозитивних сигналів є застарілими та не дають правоохоронним органам матеріалу належної якості, тоді як нове покоління систем повинно забезпечувати релевантність і точність, інтегрувати результати зворотного зв'язку від правоохоронців і надавати аналітикам дані, що мають безпосередню практичну цінність.

У центрі уваги – побудова рамкової моделі переходу, яка базується на трьох ключових стовпах: перехід і валідація, балансування між модельним ризиком і ризиком фінансових злочинів, а також забезпечення пояснюваності. Перший напрям передбачає відхід від «сітчастого» підходу,

[4] https://db.wolfsberg-group.org/assets/298bc488-6e47-465c-8d61-f776aa86594a/Wolfsberg_MSAP2_Transitioning%20to%20Innovation.pdf

коли моніторинг формує велику кількість сигналів низької якості, до більш цільових і точних моделей, що працюють з поведінковими індикаторами та різними наборами даних. Важливим є переосмислення очікуваних результатів програми MSA, впровадження нових метрик ефективності, таких як точність та повнота, аналіз якості SAR/STR та врахування здобутків аналітиків і внутрішніх підрозділів фінансової розвідки. Окремо відзначено, що класичні методи тестування, на кшталт паралельного запуску, є застарілими, натомість сучасні системи дозволяють проводити тестову перевірку концепції на історичних даних, балансуючи виявлення нових ризиків із якістю попередніх моделей. Також наголошується на потребі підвищення кваліфікації слідчих та використанні таких технологій, як великі мовні моделі, для пояснення складних сигналів і формування зрозумілих висновків.

Другий напрям стосується нової логіки балансування між модельним ризиком і ризиком фінансових злочинів. У документі критикується практика ототожнення фінансових злочинів із пруденційними ризиками, що призводить до надмірно жорсткого управління ризиками моделей і гальмує інновації. Пропонується розглядати моделі MSA в окремій площині, допускаючи їх застосування навіть у разі неповної оптимізації, якщо вони покращують виявлення злочинної діяльності порівняно з попередніми системами. Значну увагу приділено проблемі дублювання функцій контролю між аудитом, комплаєнсом та MRM, що спричиняє затримки у впровадженні нових моделей. Рекомендовано створювати більш узгоджену і пропорційну систему валідації, де основна модель проходить комплексну перевірку, а її подальші варіації для інших бізнес-ліній чи юрисдикцій оцінюються лише за дельтами, що значно прискорює процес.

Висновки:

- **Фінансовим установам слід відмовитися від «сітчастого» підходу та перейти до моделей, що забезпечують високу точність і релевантність сигналів,** із залученням поведінкових індикаторів, використанням зворотного зв'язку, SAR та сучасних показників ефективності (точність ідентифікації / повнота виявлення).
- **Управління модельним ризиком має бути диференційованим:** моделі для протидії фінансовим злочинам не повинні підпадати під ті ж жорсткі стандарти, що й пруденційні моделі. Це дозволить впроваджувати інновації швидше та ефективніше.
- **Необхідно забезпечити пояснюваність та прозорість нових моделей (Explainable AI):** від етапу розробки до практичного використання аналітиками, включаючи інструменти візуалізації для розслідувань.
- **Ключовою умовою успіху є управлінська та організаційна готовність:** керівництво має погодитися на зміни ризик-апетиту, контрольні функції повинні адаптувати нагляд, а підрозділи фінансової розвідки – навчити персонал працювати з новими технологіями та складними сигналами.

Третій напрям пов'язаний із забезпеченням пояснюваності. У документі підкреслюється, що довіра до нових систем можлива лише за умови, що фінансова установа здатна пояснити, які ризики покриває модель, як вона була розроблена та калібрована, і як користувачі повинні інтерпретувати її результати. Пропонується гібридний підхід, який поєднує правила, керовані та некеровані методи машинного навчання, дозволяючи одночасно охоплювати відомі ризики та виявляти нові типології. Важливими елементами є використання картування ризикових індикаторів, прив'язка алгоритмів до національних ризик-оцінок та пріоритетів, проведення аналізу вихідних даних, застосування візуалізацій для аналітиків та постійна перекалібровка моделей, які з часом втрачають ефективність.

У підсумку документ наголошує, що інновації у сфері моніторингу підозрілої активності є не факультативними, а обов'язковими для досягнення ефективних результатів. Успіх переходу

залежить від управлінської готовності приймати зміни ризик-апетиту, від адаптації внутрішніх контрольних функцій до нової реальності, від здатності пояснювати принципи роботи складних моделей та від підготовки персоналу. Вольфсберзька група підкреслює, що лише відповідальне впровадження інновацій з акцентом на якість, ефективність і прозорість дозволить фінансовим установам надати правоохоронним органам дійсно корисну інформацію та зміцнити систему протидії фінансовим злочинам.

Регулювання

Проект Положення про ПВК/ФТ Сполученого Королівства [5]

Документ є службовою запискою Міністерства фінансів Сполученого Королівства (HM Treasury) від вересня 2025 року, що супроводжує проєкт Законодавчого акта (SI) — "Правила 2025 року про відмивання коштів та фінансування тероризму (поправки та різноманітні положення)". Цей проєкт SI пропонує цілеспрямовані поправки до "Правил 2017 року про відмивання коштів, фінансування тероризму та переказ коштів (інформація про платника)" (MLRs). Метою цих поправок є усунення регуляторних прогалин, забезпечення пропорційності та реагування на ризики, що постійно змінюються, пов’язані з відмиванням коштів та фінансуванням тероризму. Проєкт документу є частиною урядової відповіді на зауваження, висловлені під час консультацій, та спрямований на створення більш ефективного та практичного режиму боротьби з фінансовими злочинами.

Службова записка описує низку ключових заходів у межах SI, кожен з яких має чітку політичну мету. Вона детально пояснює, як SI прагне зробити належну перевірку клієнта (CDD) більш пропорційною та ефективною. Це включає узгодження вимог до CDD для агентів з нерухомості та учасників ринку мистецтва з вимогами до дилерів, що займаються операціями з цінностями. Документ також запроваджує нові положення, які дозволяють проводити верифікацію особи клієнта після відкриття рахунку для клієнтів збанкрутілих банків, за умови дотримання певних запобіжних заходів. Крім того, SI уточнює, що посилена належна перевірка (EDD) вимагається лише для "надзвичайно складних або надзвичайно великих" транзакцій, що є нетиповим для певного сектора. Це допомагає фірмам зосередити свої ресурси на операціях, що становлять реальний підвищений ризик. SI також оновлює вимоги до EDD щодо "третіх країн з високим ризиком", зосереджуючись лише на країнах зі списку FATF.

Документ також стосується змін в об’єднаних клієнтських рахунках (PCA), виключаючи їх зі спрощеної перевірки. Нові положення вимагають від фінансових та кредитних установ вживати "розумні заходи", щоб зрозуміти призначення PCA, збирати достатню інформацію про бізнес клієнта та оцінювати пов'язані ризики. Власники PCA також повинні надавати інформацію про особу/осіб, чиї кошти утримуються на рахунку, на запит банку.

Іншою важливою сферою є зміцнення системної координації. SI додає Companies House та Уповноваженого з розгляду скарг фінансових регуляторів до переліку органів, які можуть обмінюватися інформацією з наглядовими органами з питань ПВК/ФТ. Це також розширює обсяг конфіденційної інформації, якою може обмінюватися Управління з фінансового регулювання та нагляду (FCA) щодо нагляду за криптовалютними фірмами.

[5] https://assets.publishing.service.gov.uk/media/68b5b70dcc8356c3c882a96c/Policy_note_-_MLRs_SI_technical_consultation.pdf

Крім того, SI надає ясність щодо сфери застосування та питань реєстрації. Це включає переведення всіх грошових порогів з євро у фунти стерлінгів (наприклад, €10 000 стає £10 000) та оновлення інших порогів для відповідності міжнародним стандартам. Він також усуває прогалину в правилах, включаючи продаж "готових фірм" постачальниками трастових і корпоративних послуг (TCSP) до сфери регульованої діяльності. Документ також деталізує поправки до порогів реєстрації та "зміни контролю" для криптовалютних фірм, узгоджуючи їх з Законом про фінансові послуги та ринки (FSMA).

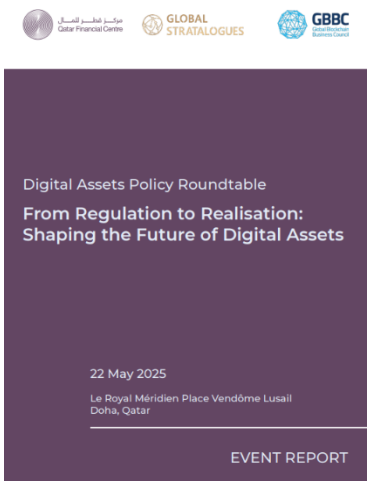
Додаткові зміни, викладені у записці, включають розширення типів трастів, які повинні реєструватися в Службі реєстрації трастів (Trust Registration Service), щоб підвищити прозорість кінцевих власників. Вона також уточнює винятки для суверенних фондів та прямо виключає договори перестрахування з визначення "страхове підприємство" для цілей ПВК. Нарешті, SI вимагає від постачальників послуг обміну та зберігання криптоактивів застосовувати посилену належну перевірку у кореспондентських відносинах, що відповідає рекомендаціям FATF.

Висновки:

- **Ризик-орієнтований підхід:** Оновлені правила зміщують акцент посиленої належної перевірки (EDD) з широких, потенційно розпливчастих категорій на більш цілеспрямований, ризик-орієнтований підхід. Це дозволяє фірмам спрямовувати ресурси на операції, що справді несуть високі ризики.
- **Узгодження регулювання криптоактивів:** SI вносить значні зміни для установ, що працюють з криптоактивами, узгоджуючи їхні вимоги до реєстрації та "зміни контролю" із Законом про фінансові послуги та ринки (FSMA). Це спрощує регуляторне середовище та забезпечує належний нагляд.
- **Покращення прозорості:** Нові правила спрямовані на підвищення прозорості. Тепер фінансові установи зобов'язані вживати заходів, щоб зрозуміти призначення об'єднаних клієнтських рахунків, а Companies House було додано до переліку організацій, які повинні співпрацювати та обмінюватися інформацією з наглядовими органами з питань ПВК/ФТ.

Звіти окремих інституцій та експертів

Від регуляції до реалізації: як Катар формує глобальні стандарти токенізації та цифрових активів [6]



Документ узагальнює результати першого круглого столу з цифрових активів, проведеного у м. Доха під егідою Qatar Financial Centre (QFC) разом із Global Stratalogues та Global Blockchain Business Council (GBBC). Головна ідея звіту полягає в тому, що цифрові фінанси перебувають на етапі переходу від спекуляцій до стратегічного впровадження, де ключову роль відіграє токенізація реальних активів. Організатори підкреслюють, що центр ваги має зміщуватися від хаосу крипторинку до створення зрозумілої інфраструктури, від абстрактних технологій — до практичних застосувань, від риторики виключення — до інклюзивних моделей доступу.

Qatar Financial Centre чітко задекларував свою позицію: криптовалюти залишаються під забороною, натомість стратегічний

[6] https://www.qfc.qa/-/media/project/qfc/qfcwebsite/documentfiles/research/qfc-dapr-report---22-may-2025.pdf

акцент робиться на токенізації активів, що мають реальну економічну цінність. Регуляторна модель будується на адаптації досвіду Ліхтенштейну, де діє перший у світі комплексний закон про токени (TVTG). Учасники відзначили, що саме ця юрисдикція створила унікальний підхід: принципово нейтральне, технологічно агностичне регулювання, яке забезпечує чіткі юридичні визначення, правову визначеність і умови для інновацій, включно з легальним визнанням DAO, створенням механізмів для токен-лендінгу, NFT-кастоді та інтеграцією з європейською MiCAR. Приклад Ліхтенштейну підкреслив, що регуляторна ясність і гнучкість важливіші за масштаб економіки чи розмір ринку.

Окрему увагу було приділено викликам у сфері боротьби з фінансовими злочинами. Експерти Global Coalition to Fight Financial Crime та OSCE наголосили, що сучасні блокчейн-аналітичні компанії працюють у роз'єднаному форматі, що унеможливлює ефективні міжнародні розслідування. Це створює «ефект PDF замість Excel», коли дані не сумісні та втрачається час на їх конвертацію замість реальної роботи. Було підкреслено необхідність створення технічних протоколів прямого обміну даними між органами влади різних країн і вироблення глобальних стандартів інтероперабельності. Водночас пролунала позиція, що віртуальні активи як технологічне явище не можна ігнорувати чи забороняти — завдання полягає в тому, щоб спрямовувати їх використання у законне та суспільно корисне русло.

GBBC представив свою роль як платформи, яка поєднує індустрію з регуляторами. Організація розробляє практичні освітні матеріали («Just the Facts» карти, довідники з реальних кейсів застосування блокчейну), які допомагають чиновникам і політикам розуміти складні концепції у спрощеному вигляді. Окремо було відзначено катарську регуляторну «пісочницю» як приклад кращої практики у світі завдяки її гнучкості, швидкості адаптації та орієнтації не на експерименти заради галочки, а на реальне впровадження.

Важливою частиною дискусій стала тема поєднання штучного інтелекту та блокчейну. Було показано, що ця конвергенція вже працює у реальному бізнесі: у фінансових продуктах UBS, у логістиці через платформу IBM-Maersk, у сфері медицини в ОАЕ, а також у процесах KYC у JPMorgan. Блокчейн забезпечує довіру та цілісність даних, тоді як AI додає інтелектуальну аналітику. Разом вони вирішують питання прозорості, достовірності та ефективності. Водночас було зазначено, що співвідношення часу на розробку та час на регуляторне узгодження є вкрай дисбалансованим: приблизно 10% йде на саму технологію і до 90% — на комплаєнс та узгодження між різними юрисдикціями.

Секційні панелі продемонстрували реалії ринку токенізації. Було визнано, що попри гучні заяви про масштаб у трильйони доларів, реальні впровадження стикаються з проблемами — від відсутності ліквідних вторинних ринків до невизначеності прав власності та трансакційних витрат. Найбільш перспективними секторами

Висновки:

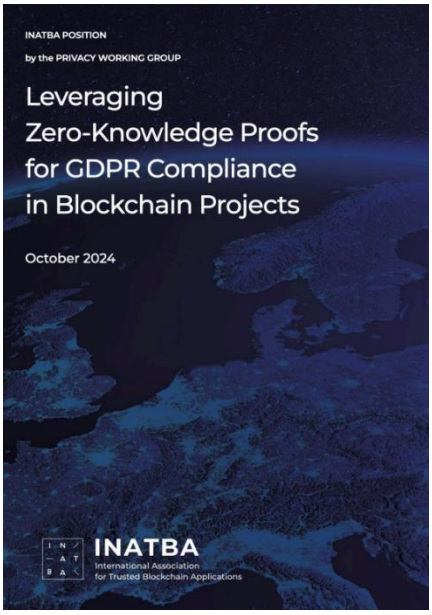
- **Регуляторна інтероперабельність є ключем до масштабування токенізації.** Необхідно укладати міждержавні угоди про взаємне визнання та створювати спільні стандарти.
- **Будівництво інфраструктури (зберігання, ліквідність, токен-стандарти) має передувати складним фінансовим продуктам.** Це знижує ризики та закладає основу для стійких ринків.
- **Токенізація може стати каталізатором фінансової інклюзії, відкриваючи МСП та населенню без доступу до банківських послуг нові можливості для фінансування та інвестицій.** Її потрібно вбудовувати в національні стратегії економічного розвитку.
- **Конвергенція AI та блокчейну потребує скоординованих міжнародних стандартів.** Лише спільне регулювання забезпечить прозорість даних, довіру і відповідність у фінансових системах.

визначено приватний кредит і трейд-фінанс, де токенізація вже показує користь для малих підприємств і торгівлі між країнами. Натомість у сфері нерухомості зберігаються серйозні бар'єри — складні процедури оцінки, залежність від посередників, високі транзакційні збори. Загальний висновок панелей — не варто прагнути миттєвої трансформації, а слід будувати ринок поступово, забезпечуючи інфраструктуру, ліквідність і регуляторну базу, перш ніж переходити до складних продуктів.

Наприкінці документ підсумовує чотири наскрізні теми: прагматичне регуляторне лідерство, де швидкість і ясність важливіші за масштаб; пріоритет інфраструктури перед технологічними експериментами; конвергенцію технологій як рушійну силу реальних змін; інклюзію як ключову цінність, що відкриває доступ до капіталу для малих та середніх підприємств (МСП) та небанківських регіонів. У стратегічних рекомендаціях підкреслюється необхідність досягати міжнародної регуляторної інтероперабельності, будувати інфраструктуру токенізації з акцентом на кастоді та ліквідності, інтегрувати інклюзивність у стратегії розвитку, координувати політики щодо AI та блокчейну і створювати спільні лабораторії для практичного відпрацювання кейсів.

Таким чином, документ є дорожньою картою для регуляторів, банків, інноваторів та міжнародних організацій, демонструючи, що майбутнє цифрових активів залежить від збалансованого поєднання регуляторної чіткості, технологічної інтеграції та прагматичного поступу. Він позиціонує Катар як потенційного регіонального хаба для токенізації та як активного учасника у формуванні глобальної архітектури цифрових фінансів.

GDPR і блокчейн: роль нульових доказів у побудові безпечних цифрових екосистем [7]



Документ є позиційним документом INATBA, який присвячений вивченню того, як технологія нульових доказів (ZKP) може допомогти подолати конфлікт між базовими характеристиками блокчейну – незмінністю та прозорістю – і суворими вимогами Загального регламенту про захист даних ЄС (GDPR). У вступі підкреслюється, що блокчейн, будучи децентралізованою та публічною інфраструктурою, має суттєві проблеми з виконанням таких принципів GDPR, як право на забуття та мінімізація даних, адже будь-які дані, що потрапили в блокчейн, неможливо видалити чи змінити. Крім того, в умовах децентралізації розмитим є і сам статус контролерів та процесорів даних, що ускладнює юридичну відповідальність за їх обробку. Проте, попри очевидний конфлікт, у документі зазначається, що блокчейн у поєднанні з технологіями підвищення конфіденційності може створювати нову модель довіри, знижувати ризик зловживань і забезпечувати цінності, близькі до GDPR – прозорість, контроль користувача і безпеку даних.

Далі розкривається, що ZKP надають технічний механізм доведення правдивості певного твердження без розкриття самих вихідних даних. Це означає, що особа може підтвердити, наприклад, свій вік або громадянство, не показуючи посвідчення особи чи дату народження. Завдяки цьому забезпечується реалізація принципу мінімізації даних: перевіряється лише той факт, який є необхідним, а сама персональна інформація залишається в офчейн-середовищі. Застосування ZKP також дає змогу вирішити проблему «права на забуття», оскільки, якщо дані видаляються поза блокчейном, то відповідний доказ на ланцюгу втрачає сенс. Особливої уваги

[7] https://inatba.org/wp-content/uploads/2024/11/Leveraging-ZKP-for-GDPR-Compliance-in-Blockchain-Projects.pdf

надано різниці між інтерактивними та неінтерактивними доказами: перші дозволяють суб'єкту самому вирішувати, чи брати участь у перевірці, що наближає їх до вимог GDPR, тоді як другі функціонують подібно до цифрових підписів і можуть бути або анульовані, або позначені як недійсні, але не видалені.

У документі виокремлено три ключові вигоди від використання ZKP для відповідності GDPR. По-перше, це посилення конфіденційності та захисту персональних даних, адже на блокчейні зберігаються лише криптографічні докази, а самі дані залишаються поза публічним доступом. По-друге, ZKP забезпечують дотримання принципу мінімізації, оскільки виключають збирання і збереження надлишкових відомостей, скорочуючи слід персональних даних у блокчейні. По-третє, технологія дозволяє наблизити блокчейн до реалізації права на забуття і виправлення, створюючи умови для контролю користувача над тим, чи можуть дані й надалі бути верифіковані.

Окрема частина присвячена практичним сферам застосування. Верифікація особи та KYC із використанням ZKP кардинально змінюють процес підтвердження ідентичності, мінімізуючи обсяг переданих даних та знижуючи ризики витоку, що особливо важливо в умовах цифрової економіки та Web3. Приклади таких рішень наведені на основі проєктів Privado ID, Togggle, zkMe та Dock, які розвивають концепцію самоврядної ідентичності (SSI), де користувач зберігає контроль над власними даними. Іншою перспективною сферою є електронне голосування, де ZKP дозволяють поєднати прозорість виборчого процесу із збереженням таємниці голосу. Серед прикладів — Vocdoni та Trevo, що застосовують zk-SNARKs для захисту анонімності та водночас забезпечують неможливість фальсифікацій. У фінансовій сфері Zcash та рішення EY Nightfall демонструють, як можна проводити транзакції, приховуючи дані про відправника, отримувача та суму, при цьому зберігаючи можливість селективного розкриття відомостей для аудиту чи контролю за дотриманням вимог протидії відмиванню коштів. Таким чином, ZKP створюють баланс між потребою у прозорості, регуляторними вимогами і захистом конфіденційності.

Висновки:

- **ZKP забезпечують механізм відповідності GDPR у блокчейні:** дозволяють підтверджувати факти без зберігання чи розкриття персональних даних, що вирішує конфлікт між прозорістю та правом на приватність.
- **Інтеграція ZKP у KYC та ідентифікацію знижує ризики витоків даних** та створює основу для SSI, де користувач сам контролює доступ до власної інформації.
- **Практичні кейси у фінансах (Zcash, EY Nightfall) та голосуванні (Vocdoni, Trevo) доводять ефективність ZKP** у поєднанні прозорості та приватності, що робить їх перспективними для масового застосування в регульованих секторах.
- **Для успішного впровадження потрібні стандарти, аудит і баланс між продуктивністю та безпекою,** оскільки різні схеми ZKP мають технічні обмеження та ризики, які слід враховувати при масштабному розгортанні.

У висновках наголошується, що хоча ZKP не є універсальним інструментом, вони становлять один із найважливіших напрямів розвитку технологій конфіденційності у блокчейні. Водночас їх впровадження супроводжується технічними викликами — оптимізацією розміру доказів, продуктивності та масштабованості, а також потребою у ретельному криптографічному аудиті для уникнення вразливостей. Проте в цілому автори підкреслюють, що ZKP є ключем до узгодження блокчейну з GDPR і водночас збереження його базових переваг: децентралізації, безпеки та довіри. Вони відкривають шлях для нових стандартів приватності у сферах цифрової ідентичності, голосування та фінансових послуг, і в майбутньому їхня роль лише зростатиме.

Цифрова оборона: Як країни протистоять розквіту онлайн-шахрайства [8]

Документ від Stimson Center є частиною ширшої ініціативи Countering Cyber Scam Operations Project, що реалізується за підтримки Global Affairs Canada. Цей матеріал, підготовлений авторами Allison Pytlak, Brian Eyler, Courtney Weatherby, Kathleen Scoggin та Shreya Lad детально досліджує проблему кібершахрайства, яке за останні два роки стало глобальною кризою, як було визнано Міжнародною організацією кримінальної поліції (INTERPOL) у 2023 році, коли вона класифікувала це явище як "серйозну та невідкладну загрозу громадській безпеці".

Кібершахрайство процвітає в особливих економічних зонах (SEZ) та уразливих регіонах Індо-Тихоокеанського регіону, зокрема в Південно-Східній Азії, де слабке управління, швидка цифровація, обмежена спроможність правоохоронних органів і недостатнє регулювання криптовалют створили ідеальні умови для діяльності транснаціональних злочинних груп. Автори наголошують, що пандемія COVID-19 стала переломним моментом, змусивши кримінальні організації, які раніше інвестували мільярди в азартні ігри та готельні комплекси, переорієнтуватися на кібершахрайство, використовуючи наявну інфраструктуру. Цей процес призвів до розширення шахрайських центрів, які залучають примусову працю та торгівлю людьми для забезпечення персоналу, а також розширюють свою діяльність на Африку, Латинську Америку та інші регіони, демонструючи глобальний масштаб проблеми.

Документ детально описує типові види онлайн-шахрайства, серед яких вирізняється "pig-butchering" — інвестиційні афери з елементами романтичних стосунків, де жертв "підгодовують" перед максимальним викачуванням коштів, а також шахрайство з підробкою особи (наприклад, правоохоронців, родичів чи урядовців) та фішинг із використанням шкідливого ПЗ. Розвиток генеративного штучного інтелекту (GenAI) значно посилив ці операції, що підтверджується зростанням на 600% контенту з deepfake у Південно-Східній Азії в 2024 році, за даними Офісу ООН з наркотиків і злочинності (UNODC).

Фінансові втрати від кібершахрайства сягають 1,03 трлн USD у 2024 році, з 75 млрд USD лише від "pig-butchering", підриваючи національну безпеку та економічну стабільність країн-жертв. Проблема ускладнюється низьким рівнем звітності через сором жертв, відсутність єдиної системи збору даних та різницю в підходах до відстеження шахрайства в різних країнах. Постраждалі включають як осіб, вимушених працювати в шахрайських центрах, так і громади, які зазнають фінансових втрат, з труднощами у вимірюванні загального впливу через різноманітність методів звітності та метрик, які варіюються від країни до країни.

У відповідь країни, такі як Австралія, Канада, Філіппіни, Сінгапур, Таїланд, Велика Британія та США, розробляють комплексні стратегії. Австралія, наприклад, створила Національний антишахрайський центр (NASC) при Австралійській комісії з конкуренції та захисту прав споживачів (ACCC), який координує зусилля з цифровими платформами, телекомунікаційними компаніями, банками та обмінниками криптовалют, заблокувавши понад 455,9 млн шахрайських дзвінків і 413,9 млн SMS у 2024 році, а також скасовуючи ліцензії підозрілих компаній. NASC також розробив Actionable Scam Intelligence Service для оперативного обміну інформацією та закриття понад 10 000 шахрайських сайтів, включаючи інвестиційні, криптовалютні, фішингові та комерційні ресурси. Канада фіксує втрати в 227 млн USD у 2024 році, використовуючи Канадський антишахрайський центр (CAFC) для збору даних про

[8] https://www.stimson.org/wp-content/uploads/2025/08/Countering-Digital-Deception-National-Responses-to-Online-Scams_PDF.pdf

шахрайство та крадіжки ідентифікаційної інформації. Документ підкреслює необхідність глобальної координації, включаючи створення централізованих платформ звітності, глобального центру обміну даними про шахрайство та залучення приватного сектору (банки, криптовалютні компанії, соціальні мережі). Міжнародне співробітництво, як-от операція Австралії та Філіппін проти шахрайських центрів у Манілі в жовтні 2024 року, де було заарештовано 250 підозрюваних, є прикладом ефективних дій. Автори пропонують проактивний підхід із простими національними системами звітності, глобальним центром обміну даними та заходами для залучення постачальників послуг, щоб зменшити вплив кібершахрайства на окремих людей, економіки та глобальну безпеку. Кожна країна демонструє унікальний підхід, але спільною рисою є акцент на профілактику, освіту громадськості та міжнародне партнерство, що відображено в профілях країн, підготовлених експертами Stimson Center та зовнішніми рецензентами з відповідних регіонів.

Документ також аналізує причини концентрації шахрайських центрів у Південно-Східній Азії, пов’язуючи це з руйнуванням азартного сектору під час пандемії та адаптацією китайських кримінальних мереж, які перепрофілювали інфраструктуру для кібершахрайства. Це призвело до створення великих комплексів із залученням жертв із понад 40 національностей, що підкреслює міжнародний характер злочину. Економічні втрати, такі як 6,5 млрд USD від шахрайства з криптовалютами у 2024 році за даними FBI, та емоційний тягар для жертв додають складності боротьбі з цим явищем.

Висновки:

- **Розробка централізованих платформ звітності:** Кожна з розглянутих країн (Австралія, Канада, Філіппіни, Сінгапур, Таїланд, Сполучене Королівство, США) повинна пришвидшити впровадження або оновлення централізованих платформ для звітності про кібершахрайство, таких як NASC в Австралії чи CAFC у Канаді, щоб підвищити ефективність реагування.
- **Посилення міжнародної співпраці:** Країнам рекомендовано активізувати операції, подібні до Operation Firestorm Австралії та Філіппін (2024), що включають спільні рейди та обмін даними, для розкриття та припинення діяльності транснаціональних шахрайських мереж.
- **Освітні кампанії та залучення приватного сектору:** Уряди повинні розширити кампанії з підвищення обізнаності, як-от "Fighting Scams" в Австралії, та зобов’язати телекомунікаційні компанії та банки до активного блокування шахрайських повідомлень і дзвінків, включаючи штрафні санкції за невиконання.

У відповідь країни впроваджують спеціалізовані агентства, такі як NASC в Австралії чи CAFC у Канаді, а також узгоджують дії з міжнародними партнерами через такі ініціативи, як ASEAN-Australia Counter Trafficking Program (ASEAN-ACT). Ці зусилля включають не лише правоохоронні заходи, а й освітні кампанії, як-от "Fighting Scams" в Австралії, та законодавчі рамки, такі як Cyber Resilience Framework (2023) і Scam Prevention Framework (SPF) у 2024 році, які регулюють діяльність телекомунікацій, банків та цифрових платформ.

Незважаючи на прогрес, автори зазначають, що проблема залишається складною через її транснаціональний характер, перетин із такими злочинами, як торгівля людьми та відмивання грошей, а також недостатню підготовку традиційних правоохоронних органів до боротьби з цифровими загрозами.

Фентанілові тіні: японський вузол китайської наркомережі [9]

Стаття Bellingcat описує складну міжнародну схему контрабанди прекурсорів фентанілу, в якій ключову роль відіграють китайські компанії та їхні представники, а Японія виявилася несподіваною базою для координації.

В центрі розслідування опинилася компанія Hubei Amarvel Biotech (AmarvelBio) з міста Ухань. Двоє її представників — виконавчий директор Цінчжоу "Брюс" Ван і менеджерка з маркетингу Її "Чірон" Чен — були заарештовані після операції DEA, екстрадовані з Фіджі до США і врешті засуджені в Нью-Йорку за змову щодо імпорту великих партій прекурсорів та відмивання грошей. Лише одна з вилучених партій сягала 200 кілограмів хімікатів, чого достатньо для виготовлення 25 мільйонів смертельних доз. Це стало першим випадком, коли американська юстиція притягнула до відповідальності керівників китайської компанії за торгівлю прекурсорами фентанілу.

Однак слідство виявило, що сліди діяльності AmarvelBio ведуть і до Японії. У судових документах з'явилося ім'я китайця Ся Фенчжи, описаного як "boss in Japan". Він очолював компанію Firsky Co. Ltd., зареєстровану у місті Нагоя, а також був пов'язаний із китайською компанією Fushikai Trading. За даними японської газети Nikkei, ці структури діяли під брендом "Firsky" і фактично були підконтрольні AmarvelBio. Докази, отримані з відкритих джерел і судових документів, підтвердили, що Firsky і AmarvelBio працювали як єдина мережа: вони мали спільні домени, використовували однакові контактні дані, фотографії, рекламу, сертифікати й навіть повторювані фабричні зображення у своїх матеріалах.

Компанії активно використовували інтернет-інструменти для обходу контролю. Виявлено десятки сайтів, які після блокування миттєво замінювалися новими. Чен особисто реєструвала домени для AmarvelBio, Firsky та афілійованих структур. Реклама поширювалась через даркнет-форуми на кшталт Breaking Bad, а також через платформу ChemicalBook, де Firsky і AmarvelBio часом навіть виступали під однією сторінкою. Для уникнення виявлення використовувалася складна система маскування: експортні партії оформлювались як корм для собак, горіхи чи моторна олія. Сертифікати якості також підроблялись або дублювались — AmarvelBio і Firsky демонстрували однакові документи, де відрізнялась лише назва компанії.

Розслідування підкреслює, що Японія стала привабливим майданчиком для таких операцій. Причинами стали географічна близькість до Китаю, культурні зв'язки, відносно проста процедура отримання довгострокового проживання через бізнес-

Висновки:

- У Японії варто запровадити обов'язкову перевірку кінцевих бенефіціарних власників і посилити вимоги до реєстрації бізнесу, щоб унеможливити створення фіктивних компаній для контрабанди.
- Потрібен міжнародний механізм моніторингу й блокування доменів, щоб мережі на кшталт AmarvelBio не могли безперешкодно запускати нові сайти після закриття старих.
- Митницям і поштовим службам слід впровадити системи аналізу ризиків для виявлення прихованих вантажів із прекурсорами, які маскують під корм, горіхи чи технічні товари.
- Санкційна та правова відповідальність має поширюватися на власників, менеджерів і технічних посередників, щоб паралізувати управління та логістику злочинних мереж.

[9] https://www.bellingcat.com/news/2025/08/07/a-chinese-fentanyl-smuggling-networks-footprints-in-japan/

канали, нижчі витрати на створення компанії та слабший регуляторний контроль порівняно з іншими глобальними центрами. Експерти вказують, що така ситуація створює "простір для експлуатації" з боку злочинних мереж, зокрема для відмивання грошей і логістики наркотрафіку. Nikkei повідомила, що Японія могла бути обрана ще й тому, що країна майже не асоціюється з торгівлею прекурсорами, отже відправлення звідси рідше піддаються перевірці.

Попри ліквідацію Firsky у Японії в 2024 році, мережа AmarvelBio продовжує діяти з Китаю, а оголошений у судових документах "керівник у Японії" Ся Фенчжи залишається в розшуку. Розслідування показує, що навіть під тиском міжнародних санкцій і після кримінального переслідування в США такі компанії легко відновлюють діяльність, створюючи нові сайти й фірми. Це свідчить про значні прогалини в міжнародній координації та контрольних механізмах і демонструє, наскільки гнучкою та стійкою є мережа контрабанди прекурсорів фентанілу.

Рекомендовані та навчальні матеріали

Чого ми не знаємо про корпоративну власність. Дослідження ланцюгів власності у 500 транснаціональних компаніях [10]

Документ Вери Побер досліджує, хто є кінцевими бенефіціарними власниками (КБВ) десяти найбільших акціонерів 500 найбільших транснаціональних корпорацій (ТНК) світу, і чому ця інформація так часто недоступна для громадськості. Дослідження виявляє, що лише для 5,8% із майже 5000 ланцюгів власності вдається ідентифікувати реальних власників, що вказує на значний брак прозорості. Ця непрозорість не обмежується лише податковими гаванями, а й поглиблюється прогалинами у світових системах розкриття інформації про КБВ, які не враховують посередницькі інвестиції.

						Use of intermediate structures (%)			
Ownership type	**N**	**%**	**Ownership interest[1]**	**FS score[2]**	**CTH score[3]**	**Secrecy jurisdictions[4]**	**Corporate tax havens[4]**	**Foundations or trusts**	**Funds**
Institutional investors	4,100	82.45	25.75	61.20	52.22	8 (0.20)	9 (0.22)	-	3,689 (89.98)
States	419	8.43	8.46	53.15	66.37	6 (1.43)	27 (6.44)	-	194 (46.30)
Individuals	225	4.52	4.35	60.82	60.51	86 (38.57)	63 (28.25)	34 (15.25)	1 (0.45)
Families	66	1.33	2.20	58.27	60.33	41 (62.12)	29 (43.94)	19 (28.79)	-
Widely held	58	1.17	1.47	59.18	61.85	36 (62.07)	22 (37.93)	-	-
Employees	40	0.80	0.30	57.95	62.48	-	-	-	-
Unknown	29	0.58	0.52	59.82	70.54	13 (41.94)	15 (48.39)	2 (6.45)	-
Foundations	28	0.56	0.45	53.89	59.19	7 (25.00)	8 (28.57)	-	-
Self-owned	8	0.16	0.31	55.38	60.50	5 (62.50)	6 (75.00)	-	-
Total	4,973	100.00	43.92	60.36	53.58	202 (4.06)	179 (3.60)	81 (1.63)	3,384 (68.05)

[1] Mean percentage of common shares outstanding per MNC as of September 2021. Note that voting interests can be higher.
[2] Mean financial secrecy score as of 2020, weighted according to the number of ownership chains per ownership type.
[3] Mean corporate tax haven score as of 2021, weighted according to the number of ownership chains per ownership type.
[4] Jurisdictions scoring higher than 60 are considered secrecy jurisdictions and corporate tax havens, respectively.

Sources: Bureau van Dijk 2021; S&P Global 2021; Tax Justice Network 2020e; Tax Justice Network 2021e

Основна проблема полягає в тому, що анонімна власність дозволяє бенефіціарним власникам та тим, хто управляє їхніми активами, уникати демократичної відповідальності, сприяючи

10 https://www.researchgate.net/publication/394998718_What_we_don't_know_about_corporate_ownership_A_study_of_ownership_chains_in_500_multinationalsWhat_we_don't_know_about_corporate_ownership_A_study_of_ownership_chains_in_500_multinationals

накопиченню багатства та влади нелегітимними засобами. Відсутність даних про КБВ також ускладнює точне вимірювання розподілу багатства, підриває здатність політиків розробляти справедливі податкові системи та негативно впливає на доступність державних послуг. Витоки документів, такі як Pandora Papers, підкреслюють масштаби використання фінансової таємниці для ухилення від податків та регулювання.

Дослідження визначає два ключові фактори, що сприяють цій непрозорості: податкові гавані та індустрія інвестиційних фондів. Податкові гавані характеризуються низькими або нульовими податками для нерезидентів, банківською таємницею, секретністю власності компаній, відмовою ділитися фінансовою інформацією з правоохоронними органами та гнучкими, дешевими умовами для реєстрації компаній, включаючи можливість створення компаній-оболонок без фізичної присутності. Серед перших податкових гаваней були Швейцарія, а також штати США Нью-Джерсі та Делавер. Сучасні податкові гавані, такі як залежні території Великої Британії та Карибські території, значно розмножилися в контексті глобалізації. Ці юрисдикції часто функціонують як офшорні фінансові центри, надаючи фінансові послуги нерезидентам у масштабах, що значно перевищують розмір їхньої внутрішньої економіки. Вони слугують "провідниками" (conduits), що передають вартість, або "сховищами" (sinks), де вартість осідає.

Інституційні інвестори – це фінансові посередники, що збирають та об'єднують гроші від фізичних та інших юридичних осіб для інвестиційних цілей, включаючи банки, страхові компанії, інвестиційні компанії, взаємні та пенсійні фонди. Їхній вплив зріс, зокрема, завдяки буму індексних фондів, що призвело до консолідації в індустрії інвестиційних фондів, де домінують такі гіганти, як BlackRock, Vanguard та State Street (так звана "Велика Трійка"). Ці три компанії володіють від 3% до 5% акцій тисяч публічних корпорацій по всьому світу. Дослідження виявило, що понад 80% із десяти найбільших акціонерів є інституційними інвесторами, і левова частка їхніх активів управляється "Великою Трійкою".

Аналіз стратегій реєстрації фондів "Великої Трійки" показує, що США є провідною країною, налічуючи 971 із 2728 фондів (35,6%), причому більшість з них зареєстровано в Делаварі (21,9%). Делавер також є домівкою для 72,2% усіх

Висновки:

- **Проблема:** Значна більшість КБВ великих транснаціональних корпорацій залишається невідомою, передусім через посередництво інституційних інвесторів, які переважно розміщують свої фонди в юрисдикціях, що пропонують податкові переваги та високий рівень фінансової таємності, таких як Делавер (США), Ірландія, Велика Британія та Люксембург.
- **Дія для політиків:** Для підвищення прозорості корпоративної власності необхідно терміново усунути критичні прогалини в існуючих рамках КБВ, що передбачає встановлення низьких порогових значень звітності, які базуються на вартості, а не на відсотках, скасування винятків для інвестиційних фондів та об'єднаних інвестиційних фондів, а також забезпечення публічно доступних та перевірених реєстрів КБВ.
- **Відповідальність ключових юрисдикцій:** США, особливо штат Делавер, разом з Ірландією, Великою Британією та Люксембургом, несуть непропорційно велику відповідальність за глобальну непрозорість власності. Цим юрисдикціям необхідно впровадити цілеспрямовані реформи щодо податкової прозорості, реєстрації КБВ та обміну інформацією (наприклад, приєднання до CRS), щоб ефективно боротися з анонімністю.
- **Роль фінансових посередників:** Слід зобов'язати фінансових посередників, таких як BlackRock, Vanguard та State Street, ідентифікувати та розкривати КБВ усіх керованих фондів, а також заборонити використання номінальних рахунків, що приховують справжню власність.

чистих активів, що управляються фондами "Великої Трійки". Інші важливі країни включають Ірландію, Велику Британію та Люксембург. Ці юрисдикції приваблюють інвестиційні фонди вигідними податковими та правовими режимами, такими як податкові пільги, податкова прозорість (коли дохід фонду перетікає безпосередньо до інвесторів), доступ до договорів про уникнення подвійного оподаткування та спеціалізовані юридичні форми. Делавер також відомий своєю швидкістю та низькою вартістю реєстрації компаній, відсутністю вимог до фізичної присутності та менш суворими правилами KYC/AML порівняно з іншими офшорними юрисдикціями.

Прогалини в існуючих рамках КБВ є значною перешкодою для прозорості. Багато юрисдикцій звільняють від вимог публічні компанії, а також правові утворення (як-от трасти), де власність і контроль розділені. Високі порогові значення для визначення КБВ (наприклад, 25% акцій або прав голосу для приватних компаній та 5% для публічних) дозволяють власникам залишатися анонімними, особливо у розрізнених структурах власності, або обходити вимоги шляхом дроблення власності. Використання номінальних рахунків, що об'єднують кошти багатьох кінцевих інвесторів, та посередництво фінансових установ також ускладнюють ідентифікацію КБВ. США, на відміну від Ірландії, Великої Британії та Люксембургу, не бере участі у Загальному стандарті звітності (CRS) ОЕСР щодо автоматичного обміну фінансовою інформацією, що посилює їх роль як юрисдикції з фінансовою таємницею. Навіть там, де існують централізовані реєстри КБВ (як у ЄС), високі пороги звітності часто звільняють інвестиційні фонди та біржові фонди від розкриття кінцевих власників.

У підсумку, переважна більшість невідомих власників великих корпорацій припадає на інституційних інвесторів, зосереджених у жменьці юрисдикцій, зокрема у США (особливо Делавері), Ірландії, Великій Британії та Люксембурзі. Ці юрисдикції пропонують як фінансову таємність, так і податкові переваги, що робить їх привабливими для реєстрації фондів. Документ підкреслює, що проблема непрозорості не може бути звинувачена лише на податкових гаванях; вона пов'язана з фундаментальними прогалинами у світових рамках КБВ, які не враховують посередницькі інвестиції та не забезпечують ефективної реалізації існуючих законів.

Практичне впровадження Регламенту DORA в Польщі [11]

Книга «Практичне впровадження DORA» — це практичний посібник і довідник, що глибоко аналізує ключові аспекти імплементації вимог Регламенту Європейського Парламенту та Ради (ЄС) 2022/2554 від 14 грудня 2022 року, що стосується операційної цифрової стійкості фінансового сектору (DORA). Видання також охоплює пов'язані з ним делеговані розробки Комісії – Регулятивні Технічні Стандарти (RTS). Книга є колективною працею під науковою редакцією Бартоша Бача , який також виступив одним з авторів , разом з іншими визнаними експертами, серед яких: Wojciech Dańczyszyn, Piotr Filipowski, Anna Jędrej-Giluń, Arkadiusz Kawulski, Magdalena Matysiak, Michał Mostowik, Adam Rasiński, Rafał Rudzki, Witold Srokosz, Paweł Szulik та Adam Woźniak. Видана у Варшаві у 2025 році видавництвом Wolters Kluwer, ця публікація призначена для директорів і менеджерів з питань комплаєнсу, а також фахівців з IT та безпеки в фінансовій та IT-індустріях.

Зміст книги структуровано відповідно до систематики Регламенту DORA, де кожен розділ присвячений окремій темі, що дозволяє читачеві поетапно зануритися у всі аспекти

[11] https://www.profinfo.pl/sklep/praktyczne-wdrozenie-rozporzadzenia-dora,696043.html

регулювання та вирішити практичні виклики. Зокрема, видання детально розглядає такі ключові питання:

- Рамки управління ризиком інформаційно-комунікаційних технологій (ІКТ): Цей розділ аналізує «рамки управління ризиком ІКТ» як головну концепцію DORA та її роль у загальній системі управління ризиками фінансових установ.
- Реєстр інформації: Описується, як реєстр інформації служить елементом управління ризиками, що походять від зовнішніх постачальників послуг ІКТ.
- Критичні або суттєві функції та послуги ІКТ: Книга містить вказівки щодо ідентифікації критичних або суттєвих функцій та класифікації послуг ІКТ, що є фундаментальним для застосування DORA.
- Відносини з третіми сторонами: Розглядаються вимоги щодо управління ризиками аутсорсингу ІКТ , зокрема, оцінка ризиків, що походять від зовнішніх постачальників послуг, та формування контрактних відносин, що відповідають вимогам регулювання.
- Тестування цифрової стійкості: Видання пояснює, як розробити та реалізувати комплексну програму тестування операційної цифрової стійкості.
- Інциденти та обмін інформацією: Описуються процеси ідентифікації, запобігання, виявлення та звітування про інциденти, а також механізми обміну інформацією про кіберзагрози між фінансовими суб'єктами.
- Взаємозв'язок з іншими стандартами: Аналізується кореляція між вимогами DORA та стандартами кіберстійкості, такими як ISO, NIST та BSI.

У вступі підкреслюється, що DORA є відповіддю на зростаючу залежність від технологій та ризики, пов'язані з цифровізацією послуг. Книга підкреслює, що DORA надає конкретні якісні вказівки для захисту, виявлення, стримування та відновлення після інцидентів, що є відходом від попереднього підходу, сфокусованого на кількісній оцінці ризику. Автори наголошують, що їхні думки та рекомендації ґрунтуються на досвіді, отриманому під час впровадження проєктів у найбільших фінансових установах Польщі, що робить публікацію особливо цінною з практичної точки зору.

Інші новини

Тіньова торгівля: розкриття незаконного трафіку галапагоських ігуан [12]

Стаття від Анни Альварадо, опублікована на платформі Mongabay, є детальним розслідуванням незаконного трафіку галапагоських ігуан, унікальних рептилій, ендемічних для Галапагоських островів під юрисдикцією Еквадору.

Ці чотири види — жовта наземна ігуана (Conolophus subcristatus), рожева наземна ігуана (C. marthae), ігуана Санта-Фе (C. pallidus) та морська ігуана (Amblyrhynchus cristatus) — еволюціонували протягом мільйонів років, адаптуючись до ізольованого архіпелагу, куди вони, ймовірно, потрапили, пливучи на природних плотах із водоростей. Їхній екзотичний вигляд — луската шкіра, що нагадує вулканічну породу, шипи на спині та довгі вигнуті кігті — робить їх привабливими для колекціонерів, а на чорному ринку кожна особина може коштувати десятки тисяч доларів. Усі види занесені до Червоного списку МСОП як такі, що перебувають під загрозою (рожева ігуана — критично endangered, інші — vulnerable), і підпадають під регуляцію

[12] https://news.mongabay.com/2025/08/study-uncovers-laundering-of-galapagos-iguanas-through-wildlife-export-permits/

Конвенції CITES, яка вимагає дозволів від країни походження для міжнародної торгівлі, хоча Еквадор таких дозволів на вивезення живих екземплярів не видає.

Дослідження, опубліковане в журналі Biological Conservation під керівництвом Марка Аулії з Інституту аналізу біорізноманіття в Німеччині, виявило, що щонайменше 60 галапагоських ігуан були вивезені по всьому світу під виглядом законної торгівлі завдяки фальсифікованим документам CITES, які позначають їх як вирощених у неволі. Цей процес "відмивання" включає незаконний вилов ігуан на островах, їхній експорт до країн-перехідників, таких як Малі, Уганда та Швейцарія, де вони отримують статус "captive-bred" для подальшого перепродажу в Азію, Європу, Африку та Північну Америку. Автори зазначають численні невідповідності в даних CITES, зокрема відсутність перевірки походження тварин і їхніх батьків імпортерами, а також брак координації з Еквадором. Наприклад, Уганда з 2017 по 2023 роки повідомила про експорт 64 ігуан, здебільшого позначених як вирощені в неволі, до країн Азії, тоді як імпортери задекларували отримання лише 47 особин, що вказує на можливі втрати або фальсифікацію.

Трафік ускладнюється через складність вилову ігуан, які активно захищаються, б'ючи хвостами та кусаючись. Охорона островів значна — 300 рейнджерів патрулюють 8000 км² національного парку, 143 000 км² Галапагоського морського резерву та 60 000 км² прилеглого резерву Hermandad, — але браконьєри, ймовірно, залучають місцевих, знайомих із теренами, зокрема на віддаленому вулкані Вольф, де мешкає рожева ігуана (близько 300 особин). Камери зафіксували незаконне проникнення, а арешти громадян Німеччини (2012) та Мексики (2015) за спроби контрабанди ювенільних ігуан підкреслюють проблему.

Країни-перехідники відіграють ключову роль у "відмиванні". Наприклад, у 2010 році в аеропорту Галапагосів виявили двох морських ігуан і мертву морську черепаху в потаємному відсіку пакунка, але контрабандист утік. Інший випадок — експорт двох жовтих і двох рожевих ігуан до Малі, а потім до Швейцарії, де документи містили невідповідності. У 2014 році Швейцарія видала дозволи на експорт чотирьох наземних і двох морських ігуан до Уганди для нібито розведення, хоча Малі ніколи не декларувала імпорт цих видів. Дослідження також пов'язує торгівлю з особами, такими як Томас Прайс (США-Фінляндія), засуджений у 2010 році в Новій Зеландії за контрабанду геконів, та Густаво Едуардо Толедо (Мексика), який керує центром CTC Conservation Center в Уганді, де тримають галапагоських ігуан. Соціальні мережі, зокрема Facebook, використовувалися для продажу юних ігуан.

Екологічна роль ігуан як розсіювачів насіння та інженерів екосистем, що контролюють рослинність, підкреслює шкідливість їхнього вилучення. Втрата навіть 10 рожевих ігуан може суттєво вплинути на популяцію. У 2010 році група CITES EU рекомендувала припинити імпорт галапагоських ігуан, а в 2020 році це рішення підтверджено. На зустрічі CITES у березні 2022 року Еквадор виступив за переведення ігуан до Додатку I, що заборонить експорт, окрім наукових цілей, і скасує чинні дозволи, хоча це ускладнюється через глобальний попит колекціонерів.

Нездатність запобігти шахрайству: практичні поради для фінансових установ [13]

Стаття на платформі UK Finance, є аналітичним матеріалом, підготовленим Етаном Салатіелем, старшим менеджером KPMG UK, та Чарлі Льюїс-Орром, асоційованим партнером KPMG LLP. Цей документ зосереджується на підготовці організацій до нового правопорушення у Великобританії — "нездатність запобігти шахрайству", яке набуло чинності 1 вересня 2025 року. Автори наголошують на важливості врахування досвіду, отриманого з попередніх корпоративних злочинів, зокрема хабарництва та ухилення від сплати податків, для

[13] https://www.ukfinance.org.uk/news-and-insight/blog/what-previous-corporate-offences-can-teach-us-about-failure-prevent-fraud

ефективного реагування на нові законодавчі вимоги. Матеріал підкреслює актуальність теми і пропонує практичні поради для фінансових установ різного масштабу та секторів.

Основна частина тексту розгортається навколо трьох ключових аспектів, які автори детально розробляють на основі свого 18-місячного досвіду роботи з фінансовими клієнтами. По-перше, вони наголошують, що запобігання шахрайству має бути загальною ініціативою, яка потребує залучення широкого спектру ресурсів і активів. Початковим кроком має бути глибоке розуміння рівня ризику, якому піддається організація, та оцінка пропорційності існуючих процедур. Оскільки внутрішнє шахрайство не є новим явищем, автори рекомендують використовувати дані з попередніх оцінок ризиків шахрайства (Fraud Risk Assessments, FRA) та самостійних оцінок ризиків і контролю (Risk & Control Self Assessments, RCSA), які проводяться щорічно багатьма підрозділами.

Однак цього недостатньо — необхідно розширити ці оцінки, додавши специфічні сценарії ризиків, пов’язані з "нездатністю запобігти", особливо в ситуаціях, де організація може виступати бенефіціаром, а не жертвою шахрайства. Такий підхід вимагає детального картування "асоційованих осіб" та залучення команд із протидії шахрайству, які мають пояснити різницю між традиційними та новими типами ризиків командам, які з ними не знайомі. Крім того, автори радять звернути увагу на наявні дані та контролі, які можуть перетинатися з іншими корпоративними злочинами, такими як хабарництво чи ухилення від сплати податків, а також із питаннями екологічної, соціальної та управлінської відповідальності (ESG), що розподілені по різних частинах бізнесу.

Другим ключовим аспектом є необхідність об’єднання різноманітних команд із ризиків і комплаєнсу для всебічної підготовки. Автори зазначають, що базові правопорушення, які охоплює нове законодавство, виходять далеко за межі Закону про шахрайство 2006 року (який включає дезінформацію, неспроможність розкрити інформацію та зловживання посадою) і включають участь у шахрайському бізнесі, отримання послуг нечесним шляхом, фальшиву бухгалтерію, шахрайські заяви директорів компаній та шахрайську торгівлю. Такий розширений спектр вимагає ширшого погляду на можливі ризики та наявні контролі. Для цього рекомендовано залучати не лише команди протидії шахрайству, але й представників фінансових, кадрових, IT, юридичних, маркетингових підрозділів, а також інших функцій, пов’язаних із економічними злочинами. Цей комплексний підхід забезпечує виявлення всіх потенційних сценаріїв і контрольних прогалин, що є критично важливим для побудови ефективної стратегії.

Третім важливим елементом є акцент на юрисдикційній експозиції, яка є спільною складністю для всіх трьох "нездатностей запобігти" — хабарництву, ухиленню від податків і тепер шахрайству. Автори нагадують, що законодавство застосовується до організацій за межами Великобританії, якщо працівник скоїв шахрайство за британськими законами або проти британських жертв, незалежно від того, де зареєстрована компанія чи де базується працівник. Це створює складність для транснаціональних корпорацій, і тому організації повинні включити до своїх підготовчих заходів детальний юридичний та юрисдикційний аналіз. Такий аналіз включає вивчення відносин між материнськими та дочірніми компаніями, а також структурного налаштування бізнесу, щоб переконатися, що всі можливі юрисдикційні аспекти враховані. Цей підхід допомагає уникнути несподіваних юридичних ризиків і забезпечує відповідність міжнародним вимогам.

Стаття завершується розділом про подальші кроки, де автори повідомляють про наміри Serious Fraud Office вперше перевірити захист "достатніх процедур" у справах про хабарництво, що

свідчить про посилення нагляду за виконанням законів. З огляду на швидкий підхід дедлайну, організації, які ще не завершили підготовку, повинні пришвидшити запровадження розумних процедур.

Загрози молоді: як працює violence-as-a-service та як його зупинити [14]

Стаття від Europol, являє собою детальний огляд явища "violence-as-a-service" — злочинної моделі, де насильство організується як підрядна послуга з чіткою ієрархією ролей та етапів, що простягається від віддалених організаторів до підлітків, залучених до безпосереднього виконання атак.

Інформація, підготовлена Оперативною робочою групою (OTF) GRIMM, розкриває складні механізми цієї мережі, акцентуючи увагу на тому, як молоді люди без кримінального минулого стають частиною ланцюга насильства, і пояснює, чому ця модель є особливо небезпечною для сучасного суспільства.

У статті описано чотири ключові ролі: організатор, який замовляє та фінансує злочин, зазвичай перебуваючи за межами країни, де планується напад, що дозволяє йому уникати прямого зв'язку з подією; рекрутер, який виступає посередником і шукає потенційних виконавців через зашифровані месенджери чи ігрові платформи, діючи цілодобово з використанням тиску чи переконання; посередник, який забезпечує логістику, інструменти, контакти та фінансові ресурси, створюючи умови для реалізації злочину; і виконавець — особа, що безпосередньо вчиняє злочин, часто неповнолітній, обраний через його непомітність для правоохоронних органів. Ця структура нагадує конвеєр, де кожен учасник виконує свою спеціалізовану функцію, а фрагментованість ланцюга дозволяє маскувати справжніх організаторів, водночас роблячи молодь особливо вразливою до маніпуляцій.

Europol, у співпраці з міжнародними партнерами, активно протидіє цій моделі через OTF GRIMM, ініціативу, започатковану в 2025 році, яка об'єднує зусилля правоохоронних органів десяти країн: Бельгії, Данії, Фінляндії, Франції, Німеччини, Ісландії, Нідерландів, Норвегії, Швеції та самої Europol. Ісландія стала останнім учасником, що посилило колективні зусилля, а в найближчі місяці очікується приєднання інших країн, що свідчить про розширення масштабів боротьби з цією загрозою. Завдяки обміну розвідувальною інформацією всередині групи вже вдалося заарештувати низку важливих цілей, а розслідування тривають по всій Європі, зосереджуючись не лише на виконавцях, але й на тих, хто замовляє, організовує та отримує прибуток від насильства. Цей комплексний підхід підкреслює важливість розриву ланцюга на всіх етапах, відстеження фінансових потоків та ідентифікації ключових фігур, що стоять за злочинами. Концепція "conveyor belt for violence" ілюструє, як організатори платять, рекрутери знаходять виконавців, посередники готують ґрунт, а виконавці беруть на себе ризик, створюючи систему, де складність відстеження поєднується з легкістю маніпуляції молоддю.

Стаття також звертає увагу на ширший контекст боротьби з організованою злочинністю через European Multidisciplinary Platform Against Criminal Threats (EMPACT), платформу, яка протягом чотирирічних циклів зосереджується на ключових загрозах, пов'язаних із серйозною міжнародною злочинністю, що впливає на Європейський Союз. EMPACT сприяє зміцненню розвідки, стратегічної та оперативної співпраці між національними органами, установами ЄС та міжнародними партнерами, забезпечуючи координацію зусиль для протидії таким явищам, як

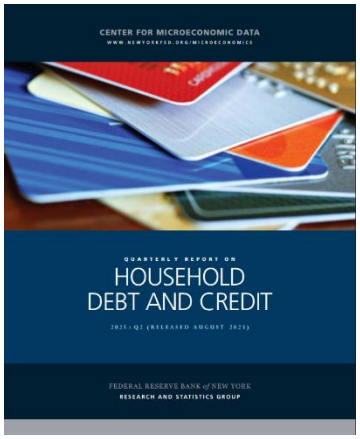
[14] https://www.europol.europa.eu/media-press/newsroom/news/instigator-to-perpetrator-how-violence%E2%80%91%E2%80%91%E2%80%91service-operates

"violence-as-a-service". Документ наголошує на важливості обміну інформацією та оперативної координації.

Ця публікація також включає заклик до дій, спрямований як на правоохоронні органи, так і на суспільство, наголошуючи на необхідності підвищення обізнаності серед молоді про ризики, пов'язані з використанням ігрових платформ та зашифрованих додатків, які стають інструментами рекрутингу. Europol і її партнери працюють над тим, щоб не лише зупинити тих, хто скоює насильство, але й розкрити всю мережу, що стоїть за цими злочинами, демонструючи перші успіхи у вигляді арештів та розширення міжнародної співпраці. Таким чином, стаття не лише інформує про сучасні виклики, але й пропонує шлях до їх подолання через спільні зусилля та інноваційні підходи до розслідування.

Для загального розвитку

Звіт про борги та кредити домогосподарств США [15]



Загальна сума боргу домогосподарств у II кварталі 2025 року зросла на 185 млрд дол. (+1% кв./кв.) і досягла 18,39 трлн дол., що на 4,24 трлн дол. більше, ніж наприкінці 2019 року. Структурно портфель і надалі переважно іпотечний: близько 70% всіх зобов'язань припадає на житлові кредити, що підкреслює системну роль іпотеки у борговому профілі домогосподарств США. У межах кварталу іпотечні залишки зросли на 131 млрд дол. до 12,94 трлн дол.; кредитні лінії під заставу житла (HELOC) додали 9 млрд дол. і досягли 411 млрд дол. (на 94 млрд дол. вище мінімуму I кв. 2022 року). Кредитні картки збільшилися на 27 млрд дол. до 1,21 трлн дол. (на 5,87% р/р), автопозики — на 13 млрд дол. до 1,66 трлн дол., студентські позики — на 7 млрд дол. до 1,64 трлн дол. Разом нежитлові зобов'язання (без іпотеки) зросли на 45 млрд дол. (+0,9% кв./кв.).

Потоки нових видач відображають стабілізацію попиту й вибіркове пом'якшення пропозиції. Нових іпотек (включно з рефінансуванням) було оформлено на 458 млрд дол., нових автопозик і лізингів — на 188 млрд дол. (проти 166 млрд дол. у I кв. 2025 р.). Ліміти за кредитними картками підвищилися ще на 78 млрд дол. (+1,5% кв./кв.), а ліміти HELOC — на 18 млрд дол. Якість нових боргових зобов'язань різноспрямована: медіанне значення оцінки кредитоспроможності за автопозиками знизилося на 6 пунктів, тоді як за іпотекою підвищилося на 5 пунктів, причому 10-й перцентиль зріс одразу на 13 пунктів (це свідчить про відбір позичальників із сильнішими профілями в іпотеці на тлі вищих ставок і жорсткіших стандартів).

Показники прострочення підвищені, але без ознак різкого погіршення. На кінець червня 4,4% всього боргу перебувало в певній стадії прострочення (на 0,1 в.п. вище кв./кв.). Переходи у ранню прострочку (30+ днів) загалом залишалися стабільними майже для всіх видів боргу; виняток — студентські позики, де спостерігалося чергове зростання частки боргу, що переходить із «поточних» у «прострочені», через відновлення відображення прострочень у кредитних звітах після майже п'ятирічної паузи у зв'язку з пандемією. Переходи у серйозну прострочку (90+ днів) були здебільшого стабільними для автопозик і кредитних карток, дещо зросли для іпотеки та HELOC і відчутно зросли для студентських позик. Близько 131 тис. споживачів отримали позначку про банкрутство у кредитних звітах, частка споживачів із колекторськими записами стабільна — 4,7%; позначки про звернення стягнення на заставну нерухомість (foreclosure) з'явилися приблизно у 53 тис. осіб і навіть знизилися відносно

[15] https://www.newyorkfed.org/medialibrary/interactives/householdcredit/data/pdf/HHDC_2025Q2

попереднього кварталу. У студентських позиках 10,2% агрегованого боргу перебуває у стані 90+ днів прострочення, однак це значною мірою наслідок повернення повного звітування, а не виключно погіршення платіжної дисципліни.

Порівняння з докризовими й кризовими періодами (до 2008 року та під час Великої рецесії) ґрунтується на національних часових рядах звіту за 1999–2025 роки. Візуально частка іпотечного боргу в серйозній простроченні нині суттєво нижча за пікові значення кінця 2000-х, тоді як у кредитних картках і автопозиках показники зрушилися вгору з «ковідних» мінімумів, але залишаються в межах історичних коридорів для цих продуктів. З урахуванням технічних ефектів у студентських позиках, сукупна картина більше схожа на нормалізацію після періоду аномально низьких прострочень 2021–2022 рр., ніж на формування хвилі системного кредитного стресу.+

Регіональний та віковий розрізи підтверджують нерівномірність чутливості до кредитного стресу: штати з більш волатильними житловими ринками мають вищі частки боргу 90+, а молодші когорти — швидші переходи у серйозне прострочення за окремими продуктами. Ця аналітика важлива для пріоритизації наглядових дій і програм раннього втручання саме там, де маржинальний ефект від пом'якшувальних заходів буде найбільшим.

На підставі даних звіту бачимо: (1) значне номінальне нарощення боргу з 2019 року за збереження домінування іпотеки; (2) поліпшення відбору в іпотеці та помірне ослаблення якості в автосегменті; (3) підвищені, але не синхронні й не критичні показники прострочення; (4) значний «статистичний шум» у студентських позиках через відновлення звітування. Сукупно це радше пізня фаза кредитного циклу з осередковими вразливостями (передусім у незабезпечених продуктах), аніж наближення до системної кризи на кшталт 2008 року.

Висновки:

- **Акцент ризику — у незабезпечених продуктах.** Підвищення переходів у 90+ днів за картками та автопозиками потребує таргетованого нагляду за відбором і стягненням, з особливою увагою до емітентів/регіонів із швидким зростанням лімітів і виданих кредитів.
- **Іпотека залишається стійкою, HELOC потребує пильності.** Рекомендовано стрес-тестування портфелів із забезпеченням житлом (враховуючи 13 послідовних кварталів зростання HELOC) та збереження підвищених стандартів відбору в іпотеці, які вже відображають поліпшення нижніх перцентилів.
- **Студентські позики: правильно інтерпретувати дані.** Різкий підйом 90+ днів пов'язаний із поверненням відображення прострочень, тож в аналітиці доцільно відокремлювати технічний компонент і працювати із послугами щодо програм реструктуризації/планів погашення.
- **Ризик-орієнтований нагляд за географією та віком.** Використовувати карти переходів у 30+/90+ і часток 90+ для пріоритезації дій у штатах і когортних групах із прискореним погіршенням, поєднуючи це з локальними програмами фінансової обачності та раннього втручання.

Ваша думка важлива!

1. Наскільки CBDC здатні реально замінити або витіснити приватні стейблкоїни, і які ризики це створює для фінансової стабільності?
2. Які з ідентифікованих у звітах типологій фінансування тероризму є найбільш актуальними для України, і як їх можна ефективно виявляти та блокувати?
3. Які можливості та виклики ви бачите для фінансових установ у переході до AI/ML-моделей моніторингу підозрілої активності, зокрема у сфері пояснюваності алгоритмів?
4. Як, на вашу думку, токенізація активів може вплинути на розвиток фінансової інклюзії та економічні можливості для малого та середнього бізнесу?
5. Які ефективні стратегії, на вашу думку, можуть бути застосовані для боротьби з новими формами кібершахрайства, особливо з огляду на використання AI та примусової праці?
6. Які заходи профілактики та освіти могли б бути впроваджені в Україні для захисту молоді від маніпуляцій через ігрові платформи та інші додатки, з огляду на високу цифровацію суспільства?
7. Наскільки реалістичним є впровадження в Україні системи AML-compliance score для криптовалют, і які технічні та правові бар'єри для цього існують?
8. Які механізми міжнародної співпраці між фінансовими розвідками є найбільш ефективними у протидії фінансуванню тероризму, і як Україна може посилити свою роль у цих мережах?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-36

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].