Методологічний бюлетень

Серійний номер: МінФін-AML-2025-14

Квітень 2025

“Ви не переможете, якщо не почнете”

Гелен Роуленд

Мета

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи 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.

Включає 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

Підозрілі транзакції під контролем: Керівництво з ефективного подання SARs[1]

Документ є комплексним методичним посібником, призначеним для суб’єктів фінансового моніторингу (СПФМ), які зобов’язані подавати Звіти про підозрілі транзакції (Suspicious Activity Reports, SARs). Його основна мета – підвищити якість і точність фінансової звітності, а також зміцнити ефективність виявлення та розслідування підозрілих фінансових операцій. Посібник пропонує розширені рекомендації щодо заповнення SARs, методологію ідентифікації фінансових схем, які можуть бути пов’язані з відмиванням коштів (AML) та фінансуванням тероризму (CFT), а також описує механізми взаємодії між фінансовими установами, державними регуляторами та правоохоронними органами.

Одним із ключових аспектів документа є детальне визначення критеріїв, за якими транзакції можуть вважатися підозрілими. У посібнику наведено низку ситуацій, які можуть викликати обґрунтовану підозру у СПФМ, зокрема:

[1] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/742-sars-reporter-booklet-march-2025/file

- Незвично великі або часті транзакції, що не відповідають фінансовому профілю клієнта.
- Перекази коштів до юрисдикцій із високим рівнем фінансового ризику або слабкими механізмами протидії ПВК/ФТ.
- Використання складних багаторівневих схем із залученням підставних компаній, що приховують кінцевих бенефіціарів.
- Дроблення великих сум на низку менших платежів для уникнення порогових значень фінансового моніторингу (smurfing).
- Використання підставних осіб, які здійснюють транзакції на користь третіх сторін без логічного обґрунтування.
- Операції, що включають криптовалютні активи без чіткої ідентифікації джерела коштів або кінцевого отримувача.

Документ детально описує етапи аналізу транзакцій, які допомагають СПФМ ухвалювати рішення про необхідність подання SARs. Важливою частиною цього процесу є застосування ризик-орієнтованого підходу, що дозволяє фінансовим установам приділяти більше уваги високоризиковим клієнтам та операціям. Посібник рекомендує використовувати технології автоматизованого моніторингу, які можуть відстежувати аномальні транзакції, аналізувати поведінкові патерни клієнтів та зіставляти їх із базами даних підозрілих осіб і компаній.

Окрему увагу приділено структурі та змісту Звіту про підозрілі транзакції. Документ наголошує, що якісний SAR повинен містити:

- Чітку ідентифікацію сторін, які беруть участь у транзакції, включаючи їхні персональні дані, адреси, ідентифікаційні номери та історію фінансової активності.
- Опис характеру транзакції, включаючи її обґрунтованість, суму, частоту та відхилення від типової поведінки клієнта.
- Детальний виклад причин, чому транзакція вважається підозрілою, із посиланням на конкретні індикатори ризику та попередні аналогічні випадки.
- Додаткові докази або документи, які можуть допомогти компетентним органам у подальшому розслідуванні.

Посібник підкреслює важливість використання аналітичного підходу під час подання SARs. Замість того, щоб просто перераховувати факти, фінансові установи повинні надавати контекст та аналіз операцій, що допоможе регуляторам зрозуміти ймовірний сценарій злочинної діяльності. Недостатньо просто вказати, що клієнт здійснив підозрілий переказ – необхідно описати, чому саме ця операція не відповідає типовій діяльності клієнта, які фактори вказують на можливе відмивання коштів або фінансування тероризму, а також які подальші дії рекомендується вжити.

Висновки:

- **Посилення контролю над ризиковими транзакціями** - Впровадження автоматизованих алгоритмів для аналізу аномальної поведінки клієнтів, зокрема при транзакціях з офшорними зонами та високоризиковими юрисдикціями.
- **Якість поданих SARs важливіша за їхню кількість** - Орієнтація на подання детально обґрунтованих звітів із достатньою доказовою базою замість надмірної генерації SARs із низькою аналітичною цінністю.
- **Покращення внутрішньої взаємодії та навчання персоналу** - Регулярне навчання та тренінги для аналітиків з фінансового моніторингу щодо виявлення складних схем відмивання коштів і фінансування тероризму.
- **Спрощення комунікації між СПФМ та регуляторами** - Використання цифрових платформ для ефективного обміну інформацією та забезпечення зворотного зв'язку щодо поданих SARs.

Окремий розділ документа присвячено взаємодії між СПФМ та державними фінансовими моніторинговими органами. Посібник наголошує, що ефективна боротьба з фінансовими злочинами можлива лиЗше за умови активної комунікації та обміну інформацією. Пропонується впровадження покращених цифрових платформ для подання SARs, що дозволяють оперативно оновлювати дані та отримувати зворотний зв'язок від регуляторів. Також розглянуто можливість застосування механізмів спільного розслідування, коли декілька фінансових установ можуть обмінюватися інформацією щодо клієнтів, які здійснюють транзакції з ознаками відмивання коштів.

Документ також розглядає юридичні наслідки неналежного виконання обов'язків у сфері фінансового моніторингу. Недотримання вимог щодо подання SARs може призвести до накладення штрафних санкцій на фінансові установи, обмеження їхньої діяльності або навіть кримінальної відповідальності посадових осіб. У посібнику наведено реальні приклади випадків, коли неналежна звітність ускладнювала розслідування злочинної діяльності або призводила до значних фінансових втрат для банків і державних органів.

Окремо наголошується на необхідності регулярного навчання співробітників СПФМ. Оскільки фінансові злочини постійно еволюціонують, працівники, відповідальні за фінансовий моніторинг, повинні постійно оновлювати свої знання та навички. Рекомендується проведення тренінгів, участь у міжнародних конференціях та використання передових програмних рішень для аналітики транзакцій.

Виконання наведених рекомендацій сприятиме підвищенню прозорості фінансової системи, зменшенню ризиків зловживань та ефективнішій боротьбі з фінансовими злочинами на міжнародному рівні.

Оцінка ризиків відмивання коштів і фінансування тероризму у сфері криптоактивів: регуляторна модель Південної Африки як приклад ризик-орієнтованого підходу[2]

Документ, оприлюднений 1 квітня 2025 року Південноафриканським центром фінансової розвідки (FIC), є ґрунтовним дослідженням сектора постачальників послуг у сфері криптоактивів (CASPs) у ПАР з точки зору ризиків ВК/ФТ. Його основна мета — надати аналіз уразливостей сектору, потенційних загроз та чинників, які сприяють використанню криптоактивів у злочинних цілях. Документ має регуляторний характер, побудований на методології «desktop research» та моніторингу, а також містить елементи типологічного аналізу.

Звіт починається із загального опису природи відмивання коштів та фінансування тероризму, а також акцентує увагу на позиції CASPs як високоризикового сегменту, визначеного міжнародними стандартами FATF. У ПАР поняття «надавч послуг у сфері криптоактивів» було офіційно закріплене у грудні 2022 року шляхом внесення змін до Закону про фінансову розвідку (FIC Act), що дало старт формальній регуляції сектора. Регулювання також підтримується положеннями Закону про фінансові послуги (FAIS Act), відповідно до якого криптоактиви визнані фінансовими продуктами, а CASPs зобов'язані отримувати ліцензії на

[2] https://www.fic.gov.za/wp-content/uploads/2025/04/2025.3-PUB-Sector-risk-assessment-%E2%80%93-Crypto-asset-service-providers-1.pdf

надання послуг. У зв'язку з цим, FIC та FSCA (регулятор ринку фінансових послуг) здійснюють спільний нагляд за дотриманням вимог ПВК/ФТ/ФР у діяльності цих провайдерів.

У документі детально охарактеризовано ринок криптоактивів у ПАР: станом на лютий 2025 року зареєстровано 256 CASPs, а частка користувачів криптовалют сягнула понад 9,4% населення (близько 5,8 млн осіб). Характерно, що основними користувачами є представники середнього та нижчого класу з річним доходом до 450 тис. ZAR, а більшість провайдерів орієнтовані на роздрібний сегмент. Обсяг щомісячної торгівлі у 2022 році сягав понад 520 млн ZAR. Однак ринок характеризується високим рівнем тінізації: виявлено низку суб'єктів, що мають інтернет-присутність, але не зареєстровані в реєстрі компаній чи не мають ліцензії FIC/FSCA.

Серед ключових загроз — міжнародні та локальні вектори зловживання. У міжнародному контексті звіт вказує на використання CASPs у схемах з відмивання коштів через міксери, тумблери, DeFi-платформи та P2P біржі. Chainalysis ілюструє, що центральні біржі залишаються основною точкою входу/виходу коштів, отриманих злочинним шляхом, і часто є «точками концентрації» таких коштів. У регіоні Субсахарської Африки понад 50% усіх криптотранзакцій здійснюються саме через централізовані біржі, що створює високу концентрацію ризиків. У документі наведено також аналіз структури «криптовідмивання» (вхід–конверсія–маскування–відмивання–вивід), із детальним розбором кожного етапу.

В окремому розділі висвітлено практику подання звітності CASPs до FIC. Протягом 2023/24 фінансового років подано лише 43 звіти про готівкові транзакції (CTR) і 7248 звітів про підозрілі транзакції (STR). Звіти про терористичні активи (TPR) взагалі не подавалися, що свідчить або про недостатню ідентифікацію ризиків, або про слабкість механізмів моніторингу з боку CASPs.

Висновки:

- CASPs повинні запровадити розширені засоби верифікації клієнтів та джерел походження коштів, особливо щодо клієнтів з підсанкційних країн, користувачів приватних монет і анонімних платформ (P2P, DeFi).
- Використання криптоаналітичних інструментів (наприклад, Chainalysis, Elliptic) для моніторингу транзакцій — критично важливе для ідентифікації peel chains, міксінгу та зв'язків з гаманцями, пов'язаними з терористичними групами або кіберзлочинністю.
- FIC та FSCA мають посилити нагляд за незареєстрованими CASPs, що мають цифрову присутність у ПАР, але не виконують вимоги законодавства (реєстрація, звітність, процедури ПВК/ФТ).
- Впровадження Travel Rule (16 Рекомендація FATF) стане ключовим кроком у забезпеченні транзакційної прозорості. Від CASPs очікується технічна та організаційна готовність до реалізації вимог до 30 квітня 2025 року.

У розділі ризиків, що базуються на дослідженнях, здійснено глибоку деталізацію шести основних категорій: ризики продуктів/послуг, клієнтів, транзакцій, каналів доставки, географічні ризики та ризики ФТ/ФР. Наприклад, вказано, що використання анонімних монет, децентралізованих платформ, IP-адрес із санкційних юрисдикцій або реєстрація сайтів через анонімні хостинги — усе це є червоними прапорцями. Також наголошено, що CASPs мають проводити ретельний аналіз джерел коштів клієнтів, перевіряти наявність пов'язаних осіб у списках TFS (санкції ООН та США), впроваджувати моніторингові інструменти (наприклад, блокчейн-аналітику), відслідковувати peel-chain транзакції, використання банкомати Bitcoin, географічні зв'язки з «вразливими» країнами та транзакції з гаманцями, пов'язаними з даркнетом чи терористичними організаціями.

Терористичне фінансування та фінансування розповсюдження зброї масового знищення (ФР) виділені в окремі категорії. FIC наголошує, що криптовалюти все частіше використовуються для краудфандингу під виглядом гуманітарної допомоги. В ПАР уже триває перший судовий процес, пов'язаний із ФТ через Bitcoin. Вказано також на активне використання криптоактивів КНДР для обходу санкцій, через зломи гаманців клієнтів CASPs.

На завершення, документ класифікує інтегрований ризик відмивання коштів для CASPs як «високий», а залишковий ризик — як «середньо-високий», завдяки регуляторним зусиллям, таким як припис Директиви 9 щодо впровадження Travel Rule (набирає чинності з 30 квітня 2025 року). Однак ризик фінансування тероризму залишається «високим». У звіті наголошено, що сектор перебуває у стадії активного формування, і регуляторні та наглядові механізми потребують подальшого вдосконалення. Очікується, що протягом наступних двох років буде проведено оновлену оцінку ризиків.

Документ також містить реальні кейси, які ілюструють схеми шахрайства, використання гаманців третіх осіб (грошові мули), зловживання некастодіальними гаманцями та схеми з розкрадання інвестицій під виглядом страхових внесків. Згадується активне зростання неформальної криптоекономіки в ПАР, зокрема на базі Lightning Network, де транзакції залишаються поза периметром звітності.

Загалом, документ є зразком стратегічного підходу до оцінки сектору CASPs у контексті ПВК/ФТ. Він формує цілісне розуміння природи та масштабів загроз, і може бути використаний як шаблон для аналогічних оцінок у інших юрисдикціях.

Ризик проникнення мафії в муніципалітети Італії[3]

У цьому дослідженні ПФР Італії аналізує ризик мафіозного впливу на органи місцевого самоврядування шляхом застосування статистики та методів машинного навчання до фінансових даних муніципалітетів за 2016–2021 роки. Мета роботи — виявити відмінності у бюджетній поведінці між муніципалітетами, які були розпущені через мафіозне проникнення, і контрольними муніципалітетами, що не зазнали подібного втручання. Дослідження зосереджується на тому, як таке проникнення впливає на структуру витрат, ефективність збору доходів, автономію у прийнятті рішень і загальну фінансову поведінку місцевих адміністрацій.

Автори будують модель машинного навчання, яка з точністю 98,2% (AUC) дозволяє класифікувати муніципалітети за рівнем ризику проникнення. Ця модель використовує широкий набір бюджетних та соціально-економічних змінних, включаючи як витратні, так і дохідні показники, а також індикатори з офіційного Плану очікуваних бюджетних результатів.

Результати аналізу свідчать, що муніципалітети, які зазнали мафіозного впливу, мають низку спільних характеристик: вищі поточні витрати, менше фінансування соціальних послуг і освіти, більша частка видатків спрямована на житлове будівництво, утилізацію відходів та управління територією. Водночас ці адміністрації демонструють нижчу ефективність у зборі податків, особливо зборів за відходи, що може бути ознакою свідомої недорозподіленості або корупційних домовленостей із бізнесом.

[3] https://uif.bancaditalia.it/pubblicazioni/quaderni/2025/quaderno-27-2025/QAR-27.pdf

Модель також підтвердила валідність своїх висновків шляхом перевірки кореляції між ризиком інфільтрації та: (1) наявністю підприємств, пов'язаних із організованою злочинністю, і (2) рівнем непрозорості у сфері публічних закупівель. Для цього використовувалися як конфіденційні джерела ПФР, так і дані Антикорупційного агентства Італії (ANAC). Ці перевірки підтвердили, що вищий індекс ризику тісно пов'язаний з обома чинниками.

На регіональному рівні найвищі ризики зосереджені у Південній Італії (Калабрія, Сицилія, Кампанія, Апулія), тоді як муніципалітети на Півночі майже не мають ознак мафіозного проникнення. Це вказує на глибоку територіальну концентрацію явища. Модель є стабільною при зміні вибірки контрольних муніципалітетів та при зміні вагових коефіцієнтів, що свідчить про її надійність для майбутнього прогнозування.

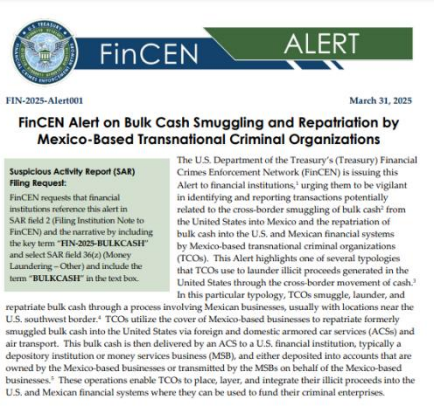
Висновки:

- **Муніципалітети, інфільтровані мафією, мають характерну бюджетну поведінку** — зменшення витрат на освіту, соціальні послуги та транспорт, збільшення фінансування будівництва й управління відходами, а також вищу жорсткість витрат і неефективний податковий збір.
- **Модель машинного навчання показала високу точність (AUC 98,2%) у прогнозуванні ризику інфільтрації**, що дозволяє її використовувати для моніторингу муніципалітетів із високим ризиком, навіть якщо вони ще не були офіційно розпущені.
- **Ризик інфільтрації має статистично значущий зв'язок із присутністю підприємств, пов'язаних із організованою злочинністю, та непрозорістю в публічних закупівлях**, що дозволяє ці чинники використовувати як індикатори в аналітичних системах ПВК.
- **Запропонована методологія може бути використана для національного картографування муніципалітетів із підвищеним ризиком**, підтримуючи рішення щодо нагляду, перевірок та розробки профілактичних політик.

Дослідження робить суттєвий внесок у методологію виявлення мафіозного впливу на органи місцевого самоврядування, пропонуючи обґрунтовану кількісну модель для виявлення ризиків, яка може застосовуватись як інструмент для прийняття рішень на державному рівні, включаючи планування заходів ПВК/ФТ та наглядову діяльність.

Попередження FinCEN про контрабанду та репатріацію готівки мексиканськими транснаціональними злочинними організаціями[4]

Цей документ є спеціальним аналітичним попередженням FinCEN, спрямованим на привернення уваги фінансових установ до однієї з ключових типологій відмивання коштів, що здійснюється мексиканськими транснаціональними злочинними угрупованнями. Механізм полягає у контрабандному перевезенні готівки з США до Мексики та її подальшій легалізації і репатріації через формально законні бізнес-операції, що маскують злочинне походження грошових коштів. У документі описано, як готівкові кошти, отримані в США внаслідок наркоторгівлі, торгівлі людьми та іншої кримінальної діяльності, спочатку незаконно перевозяться через південний кордон, а потім за допомогою перевезень інкасаторськими автомобілями або повітряним транспортом знову ввозяться до США під



FinCEN ALERT

FIN-2025-Alert001 March 31, 2025

FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**FIN-2025-BULKCASH**" and select SAR field 36(z) (Money Laundering – Other) and include the term "**BULKCASH**" in the text box.

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to financial institutions,[1] urging them to be vigilant in identifying and reporting transactions potentially related to the cross-border smuggling of bulk cash[2] from the United States into Mexico and the repatriation of bulk cash into the U.S. and Mexican financial systems by Mexico-based transnational criminal organizations (TCOs). This Alert highlights one of several typologies that TCOs use to launder illicit proceeds generated in the United States through the cross-border movement of cash.[3] In this particular typology, TCOs smuggle, launder, and repatriate bulk cash through a process involving Mexican businesses, usually with locations near the U.S. southwest border.[4] TCOs utilize the cover of Mexico-based businesses to repatriate formerly smuggled bulk cash into the United States via foreign and domestic armored car services (ACSs) and air transport. This bulk cash is then delivered by an ACS to a U.S. financial institution, typically a depository institution or money services business (MSB), and either deposited into accounts that are owned by the Mexico-based businesses or transmitted by the MSBs on behalf of the Mexico-based businesses.[5] These operations enable TCOs to place, layer, and integrate their illicit proceeds into the U.S. and Mexican financial systems where they can be used to fund their criminal enterprises.

[4] https://www.fincen.gov/sites/default/files/shared/BCS-Alert-FINAL-508C.pdf

виглядом легального виторгу мексиканських компаній. Ці кошти депонуються у фінансові установи США або передаються через установи з грошових переказів (MSB), часто з використанням спільних логістичних зв'язків між мексиканськими та американськими постачальниками інкасаторських послуг (ACS).

У процесі легалізації готівки використовується широка географія: окрім стандартного переміщення через південний кордон, описано також сценарії із транзитом через Канаду. Після фізичного переміщення готівки вона або зараховується на рахунки у США шляхом безпосереднього внеску, або зараховується як електронна кредитна операція. Надалі кошти переводяться до Мексики через банківські перекази або використовуються в схемах відмивання коштів на основі торгівлі (наприклад, купівля товарів у США з подальшим продажем у Мексиці).

Важливим аспектом документа є систематизація індикаторів підозрілої діяльності для депозитних установ та інкасаторських перевізників. До них належать великі депозити, отримані через ACS на користь компаній із мексиканською юрисдикцією, швидке переведення коштів до Мексики, а також операції, що не відповідають профілю бізнесу. Також FinCEN підкреслює, що операції деяких ACS можуть підпадати під кваліфікацію діяльності MSB, і згадує прецедент — штраф проти Brink's Global Services за системне порушення вимог BSA (Bank Secrecy Act), включаючи перевезення готівки для високоризикових клієнтів.

Висновки:

- **Операції з інкасаторськими перевезеннями готівки для мексиканських компаній поблизу південного кордону США повинні вважатися високоризиковими**, особливо якщо пов'язані з незвичними маршрутами, швидким перерахуванням коштів до Мексики чи без чіткого джерела походження коштів.
- **Регулятори мають звернути увагу на ліцензування та реєстрацію броньованих перевізників як MSB**, якщо їхня діяльність фактично охоплює надання послуг переказу коштів — що є об'єктом регулювання відповідно до BSA й може призвести до санкцій, як у випадку Brink's.

Це попередження підтримує більш широку політику США, яка, зокрема, передбачає можливість класифікації картелів як терористичних організацій згідно з Указом Президента США №14157. Таким чином, фінансова розвідка та моніторинг стають важливим елементом державної безпеки в умовах транскордонної злочинності.

Санкції

Звіт про схеми обходу санкцій[5]

Звіт підготовлений у межах проєкту KLEPTOTRACE, який реалізується консорціумом Transcrime спільно з кількома університетськими партнерами та за підтримки Європейської Комісії. Документ є ґрунтовним аналітичним дослідженням щодо схем обходу санкцій, спрямованих на протидію високорівневій транснаціональній корупції та відстеження активів. У фокусі — системний аналіз 97 справ про порушення санкцій, зібраних з відкритих джерел, з метою ідентифікації тактик обходу та розробки рекомендацій для посилення ефективності санкційної політики ЄС.

[5] https://www.transcrime.it/wp-content/uploads/2025/03/KLEPTOTRACE-report_sanctions-circumvention.pdf

Основні висновки звіту стосуються трьох категорій порушень: (1) секторні порушення, пов'язані з недотриманням обмежень у певних секторах економіки; (2) порушення цільових санкцій, що передбачають спроби обійти заборони, накладені на конкретних осіб чи компанії (зокрема через номінальних власників або shell-компанії); (3) помилки в комплаєнсі, коли санкції порушуються через недбалість чи недостатні внутрішні процедури, а не зумисно.

Особливу увагу приділено географії схем обходу. У випадках порушення цільових санкцій активну роль відіграють юрисдикції поза межами ЄС — Швейцарія, Туреччина, Джерсі, Монако, Острів Мен, а також Британські Віргінські острови, Панама і Кіпр. Для секторних санкцій значущими є країни Азіатсько-Тихоокеанського регіону (Гонконг, Китай, Киргизстан, Казахстан) і Близький Схід (ОАЕ). Показово, що у 81% справ участь брали корпоративні структури, а у 12% — фінансові інституції. У середньому у кожній справі було залучено близько трьох осіб-посередників.

Визначено основні механізми транзакцій: банківські перекази (найпоширеніші), офшорні рахунки, грошові перекази, криптовалюти (рідко, але зростає значення), а також немонетарні інструменти — операції з елітною нерухомістю чи подарунками. Зазначено, що санкційні схеми запускаються майже одразу після запровадження нових обмежень, тому ефективність санкцій залежить від швидкої реакції правоохоронних органів.

Звіт також окреслює проблеми в застосуванні санкцій на рівні ЄС, серед яких: (1) розпорошеність нагляду між 160 національними органами, (2) недостатня гармонізація у криміналізації порушень санкцій, (3) складність у досягненні одностайності в Раді ЄС. Позитивною зміною є ухвалення Директиви (2024), яка встановлює єдині стандарти кримінальної відповідальності за порушення санкцій та включає їх до переліку предикатних злочинів за законодавством про ПВК/ФТ. Іншим важливим кроком є наказ Європейського банківського органу (ЕВА) про запровадження обов'язкових стандартів внутрішнього контролю в банках (з 30 грудня 2025 року), що має закріпити превентивну складову в боротьбі з обходом санкцій.

Окрема частина звіту присвячена міжнародній координації: через роботу FIU-груп (зокрема Russia-related Illicit Finance and Sanctions FIU Working Group), ініціативи REPO, Egmont Group та E-5 з питань контролю експорту. Акцентовано на важливості доступу до інформації про бенефіціарну власність, співпраці з офшорними центрами, а також підтримці ролі журналістів-розслідувачів та громадянського суспільства.

Звіт демонструє, що обхід санкцій — це не виняткове явище, а системна загроза, яка потребує узгоджених і багаторівневих відповідей з боку урядів, приватного сектору, регуляторів, судової системи та громадськості. Успіх залежить від того, наскільки швидко та скоординовано ЄС і його партнери

Висновки:

- **Запровадити практичні рекомендації для бізнесу щодо виявлення схем обходу санкцій** (типові транзакції, ризикові юрисдикції, структури власності) — з урахуванням прикладів зі 97 проаналізованих кейсів.
- **Забезпечити обов'язкову гармонізацію кримінальної відповідальності в усіх державах-членах ЄС** відповідно до Директиви 2024 року, включаючи санкції як предикатні злочини до ПВК/ФТ.
- **Підвищити прозорість у корпоративній структурі** шляхом розширення доступу до інформації про бенефіціарів, зобов'язавши юрисдикції-посередники (Кіпр, ОАЕ, Джерсі тощо) до звітності.
- **Фінансовим установам — переглянути політики внутрішнього контролю відповідно до нових стандартів ЕВА,** зокрема забезпечити навчання персоналу щодо санкційного ризику та процедур ескалації.

зможуть адаптувати правові рамки, наглядові механізми й цифрові інструменти до реалій транснаціональної злочинності.

США ввели санкції проти 13 установ, залучених до схеми відмивання коштів картелю Сіналоа[6]

Уряд США продовжує активні дії проти міжнародної організованої злочинності, зокрема — проти одного з найнебезпечніших наркокартелів світу — Сіналоа. Міністерство фінансів США, а саме Управління з контролю за іноземними активами (OFAC), наклало санкції на шістьох осіб та кілька компаній, звинувачених у причетності до операцій з відмивання грошей, які допомагали картелю приховувати доходи від незаконного обігу наркотиків.

Ці санкції спрямовані на підрив фінансової інфраструктури, яка підтримує злочинну діяльність картелю, включаючи торгівлю наркотиками, корупцію, відмивання коштів та інші незаконні дії. Зокрема, йдеться про операції з героїном і фентанілом — надзвичайно небезпечними речовинами, що стали причиною тисяч смертей від передозувань у США.

Картель Сіналоа відомий масштабною схемою відмивання доходів: через мережу компаній, фінансових посередників та підставних фірм кошти, здобуті незаконним шляхом, легалізуються і використовуються для фінансування подальшої злочинної діяльності.

Процес включає:

- використання обмінних пунктів і фіктивного бізнесу;
- транскордонні перекази через кордон США–Мексика;
- використання комерційних компаній для маскування джерела походження коштів.

Санкції OFAC роблять незаконною будь-яку взаємодію американських компаній чи фізичних осіб із зазначеними суб’єктами, а також заморожують їхні активи.

Серед осіб, які потрапили під санкції:

1. Енріке Данн Еспаррагоса Росас — ключова фігура у схемах відмивання коштів у Мексиці, використовував обмінні пункти для переказу мільйонів доларів до Мексики, пов’язаний із синами Хоакіна "Ель Чапо" Гусмана.
2. Алан Вірамонтес Сестега — співпрацював із картелем через бізнеси та координував великі грошові перекази; має зв’язки з Іваном Арчівальдо Гусманом Салазаром.
3. Сальвадор Діас Родрігес і Ісраель Даніель Паєз Варгас — обидва підтримували фінансову інфраструктуру картелю, зокрема у зборі боргів та контролі території. Паєз також був пов’язаний з мережею Альберто Давіда Бенгуат Хіменеза.
4. Бенгуат Хіменез — відповідав за відмивання понад 50 мільйонів доларів, використовуючи підставні компанії разом з партнером Крістіаном Ноє Амадором Валенсуелою.

Санкції США мають як символічне, так і практичне значення:

- Вони порушують функціонування злочинної фінансової системи, ускладнюючи використання глобальної банківської інфраструктури.
- Забороняють американським компаніям будь-які угоди з фігурантами.

[6] https://regtechtimes.com/us-sanctions-13-entities-involved-in-sinaloa/

- Сигналізують про рішучість США у боротьбі з наркокартелями на міжнародному рівні.

США вже не вперше вводять санкції проти картелю та його учасників. Боротьба з фінансуванням наркоторгівлі — частина ширшої стратегії протидії глобальним організованим злочинним мережам. Без доступу до фінансів ці угрупування втрачають можливість вести війну за території, підкупати чиновників та інвестувати в нові канали постачання наркотиків.

Звіти окремих інституцій та експертів

Синтетична загроза: Як наркотичні ринки Латинської Америки трансформують глобальну злочинність[7]

Публікація InSight Crime від 12 березня 2025 року за авторством Вікторії Діттмар, спирається на найновіші звіти Міжнародної ради з контролю за наркотиками (INCB) від 4 березня 2025 року і являє собою глибокий аналіз трансформації наркотичних ринків у Латинській Америці та Карибському басейні під впливом синтетичних наркотиків. Цей документ не просто констатує факти, а розкриває багатогранну картину, як швидка еволюція виробництва, глобалізація кримінальних мереж і адаптація до тиску з боку правоохоронців створюють безпрецедентні виклики для міжнародної спільноти. Авторка занурює читача в реальність, де синтетичні речовини — метамфетамін, фентаніл, MDMA, нові психоактивні сполуки (NPS) і навіть "дизайнерські" прекурсори — стають інструментами, що дозволяють злочинцям випереджати зусилля влади, використовуючи прогалини в законодавстві та хімічні інновації.

Перша велика тема статті — це географічне розширення ринків синтетичних наркотиків у регіоні, яке виходить далеко за межі традиційного лідера, Мексики. Завдяки близькості до Сполучених Штатів, одного з найбільших споживачів наркотиків у світі, Мексика десятиліттями була осередком виробництва синтетичних речовин, таких як метамфетамін і фентаніл. Проте звіти INCB фіксують, що ця діяльність тепер охоплює ширший регіон. У Центральній Америці та Карибському басейні за останні два роки спостерігається значне зростання: у 2023 році Коста-Рика конфіскувала рекордні 580 000 доз метамфетаміну, що свідчить про масштабність проблеми, а в Тринідаді і Тобаго правоохоронці виявили та ліквідували лабораторію з виробництва цієї речовини. Сальвадор, у свою чергу, повідомляє про стабільне зростання поставок метамфетаміну з Гватемали протягом останніх чотирьох років, що вказує на формування нових транзитних маршрутів. Але метамфетамін — це лише частина картини. У регіоні також з’являються нові психоактивні речовини, які додають складності: синтетична марихуана фіксується в Бразилії, синтетичні стимулятори, такі як фенідати, — в Аргентині, а синтетичні опіоїди поширюються в Аргентині, Чилі, Колумбії та Уругваї. Окремо виділяється "тусі" — популярний у Південній Америці коктейль із екстазі та кетаміну, який почали вилучати в Сальвадорі, Гватемалі та Коста-Риці, а також фентаніл, змішаний із іншими речовинами, що набирає обертів у Коста-Риці. Ця різноманітність ускладнюється появою "дизайнерських" прекурсорів — спеціально створених хімічних сполук, які не підпадають під міжнародні заборони, що робить боротьбу з ними ще більш проблематичною. Сесар Арсе, член INCB, під час презентації звітів наголосив, що така швидкість і гнучкість злочинних інновацій залишають владу в позиції наздоганяючих, а не тих, хто контролює ситуацію.

[7] https://insightcrime.org/news/3-key-findings-synthetic-drugs-latin-america-caribbean-from-the-incb/

Друга ключова тема — це глобалізація синтетичних наркотичних ринків і дедалі тісніші зв'язки між кримінальними мережами різних континентів. Мексиканські виробники метамфетаміну вже з 2010-х років співпрацюють із наркоторговцями в Нідерландах, обмінюючись не лише хімічними знаннями, а й технологіями виробництва. Ця співпраця, за даними INCB, може перерости в ширший обмін прекурсорами та готовою продукцією, що посилить потоки синтетичних наркотиків між Америкою та Європою. Але зв'язки Мексики не обмежуються Європою: у 2024 році в Індії було ліквідовано мережу виробництва метамфетаміну, пов'язану з мексиканською організацією, а в Південній Африці виявлено промислові лабораторії, які за своєю будовою та обладнанням нагадують мексиканські аналоги. Ці приклади свідчать про те, що знання та методи виробництва синтетичних наркотиків стають глобальним надбанням кримінального світу. Більше того, скорочення виробництва героїну в Афганістані, яке призвело до дефіциту цього наркотику в Європі, відкриває двері для мексиканських мереж, які можуть заповнити прогалину синтетичними опіоїдами, такими як фентаніл і нітазени. Такий розвиток подій, як зазначають звіти, може призвести до переплетення ланцюгів постачання в Європі та Північній Америці, ускладнюючи відстеження потоків наркотиків і посилюючи обмін технологіями та стратегіями між злочинними групами різних регіонів.

Третя важлива тема публікації — це адаптація ринків синтетичних опіоїдів до посиленого тиску з боку правоохоронців, особливо в контексті фентанілу, який став символом кризи передозувань у Північній Америці, забравши сотні тисяч життів. У відповідь на жорсткий контроль незаконного обігу фентанілу кримінальні мережі почали шукати альтернативні джерела, зокрема відводячи медичний фентаніл із аптек і медичних установ. Конкретні випадки ілюструють цю тенденцію: 3 березня 2025 року в Перу влада конфіскувала 6000 одиниць медичного фентанілу, який планувався до відправки в США, а в 2024 році в Домініканській Республіці було ліквідовано інтернет-схему продажу підроблених ліків із фентанілом, що діяла на глобальному рівні. Крім того, злочинці почали використовувати ветеринарні препарати, такі як ксилазин, для розширення обсягів фентанілових поставок, а також вводити в обіг більш потужні синтетичні опіоїди, такі як карфентаніл і похідні нітазену. Ці стратегії відображають гнучкість і винахідливість кримінальних мереж, які не лише реагують на тиск правоохоронців, а й знаходять способи підтримувати свої операції навіть у складних умовах, таких як перебої в постачанні чи внутрішні конфлікти в кримінальному світі.

Висновки:

- **Посилення регіонального моніторингу та обміну даними:** Країнам Латинської Америки та Карибського басейну необхідно стандартизувати звітність про споживання наркотиків і розширити співпрацю для відстеження нових психоактивних речовин, з огляду на їх швидке поширення.
- **Міжнародна координація проти глобальних мереж:** Влада має зосередитися на перехопленні обміну знаннями та прекурсорами між Мексикою, Європою, Азією та Африкою, зокрема через спільні операції, щоб запобігти поширенню синтетичних опіоїдів у Європі.
- **Контроль медичних і ветеринарних препаратів:** Необхідно посилити нагляд за аптеками та медичними установами для запобігання виведенню фентанілу і ветеринарних засобів, таких як ксилазин, у незаконний обіг.
- **Розробка стратегій проти адаптивності мереж:** Правоохоронним органам слід передбачати використання більш потужних опіоїдів (карфентаніл, нітазени) і розробляти спеціалізовані методи виявлення та нейтралізації таких речовин у відповідь на гнучкість злочинних груп.

Публікація завершується думкою Сесара Арсе, який під час презентації звітів заявив, що синтетичні наркотики надають злочинцям "практично необмежені можливості" для перебудови ринків. Ця фраза підсумовує головний меседж документа: попри міжнародні зусилля з контролю за наркотиками, швидкість, із якою злочинні мережі адаптуються та впроваджують інновації, залишає владу в позиції, коли вона змушена реагувати, а не передбачати. Автор підкреслює, що ця динаміка вимагає не лише посилення існуючих заходів, а й розробки принципово нових підходів до боротьби з синтетичними наркотиками, які стають дедалі складнішими та глобалізованими.

Геокримінальність у сучасному світі: Як геополітичні напруження підсилюють державно-кримінальну співпрацю [8]

Дослідження, опубліковане в The Journal of Illicit Economies and Development спільно з Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC) та Лондонською школою економіки, є глибинним дослідженням феномену геокримінальності — складного явища, яке виникає на перетині геополітичних напружень, державно-кримінальної співпраці та її впливу на глобальну безпеку. Автори наголошують, що сучасні геополітичні умови, зокрема зростання конкуренції між державами, глобалізація ринків, технологічний прогрес і послаблення міжнародних норм, сприяють появі нового типу загроз, коли держави дедалі частіше використовують кримінальні мережі як інструмент для досягнення своїх зовнішньополітичних цілей. Це явище, яке автори називають геокримінальністю, ускладнює традиційні підходи до боротьби з організованою злочинністю, оскільки межа між діями держав і кримінальних груп стає дедалі більш розмитою, що створює серйозні виклики для міжнародної спільноти в плані ідентифікації, відповідальності та протидії.

Для ілюстрації цього феномену автори наводять кілька конкретних прикладів, які демонструють, як держави використовують кримінальні елементи для реалізації своїх інтересів. Один із таких випадків стосується вбивства Зелімхана Хангошвілі, колишнього чеченського повстанця, яке сталося влітку 2019 року в берлінському парку Tiergarten. Хангошвілі був застрелений громадянином Росії, якого німецькі слідчі згодом пов’язали з Федеральною службою безпеки (ФСБ). Цей інцидент став прикладом того, як держава може використовувати кримінальних виконавців для здійснення політичних убивств за кордоном, уникаючи прямої відповідальності. Інший приклад переносить нас до Пекіна в березні 2021 року, де чоловік середнього віку отримав нагороду за патріотизм і внесок у бізнес від організації, тісно пов’язаної з Комуністичною партією Китаю, а також із Народно-визвольною армією. Пізніше з’ясувалося, що нагороджений — Ван Кук-кой, один із найвідоміших злочинців, якого розшукують за звинуваченнями у відмиванні коштів і торгівлі людьми. Цей випадок ілюструє, як держави можуть не лише толерувати, а й офіційно легітимізувати діяльність злочинців, якщо їхні дії відповідають державним інтересам, наприклад, у сфері економічного впливу чи політичної стабільності. Ще один приклад стосується подій у Швеції в травні 2024 року, коли шведські служби безпеки виявили, що іранський уряд використовував кримінальні мережі на території країни для здійснення насильницьких актів проти інших держав, груп і окремих осіб, які вважалися ворогами Ірану. Доповненням до цього стала кібератака в лютому 2025 року на італійські державні веб-сайти, здійснена проросійськими хакерами, що підкреслює, як сучасні

[8] https://globalinitiative.net/analysis/the-rise-of-geocriminality/

технології дозволяють державам і кримінальним групам діяти синхронно, ускладнюючи визначення того, хто саме стоїть за такими діями — державні структури чи незалежні злочинні організації.

Щоб надати ширший контекст, автори звертаються до історичних прикладів, які показують, що державно-кримінальна співпраця не є новим явищем, але сучасні умови значно посилили її масштаби та вплив. Вони згадують співпрацю Британії з мафією під час Другої світової війни, яка відбувалася за згодою королеви Єлизавети I, коли британський уряд використовував кримінальні мережі для боротьби з ворогами, зокрема для захисту морських шляхів від німецьких підводних човнів. Аналогічно, США в той же період співпрацювали з мафією, зокрема через операцію "Підземний світ", щоб забезпечити безпеку портів і запобігти саботажу з боку профспілок, які могли бути під впливом ворожих сил. Ці історичні паралелі підкреслюють, що держави завжди знаходили способи використовувати кримінальні структури для досягнення стратегічних цілей, але сучасна глобалізація, розвиток міжнародних ринків, технологій і комунікацій зробили цю співпрацю більш складною, масштабною та важкою для виявлення. Наприклад, сучасні кібератаки, такі як згадана атака на італійські державні веб-сайти, показують, як технології дозволяють державам і кримінальним групам діяти анонімно, використовуючи цифровий простір для досягнення своїх цілей без прямого ризику.

Дослідження GI-TOC розширює географічний фокус аналізу, вказуючи на те, що геокримінальність є глобальним явищем, яке проявляється по-різному в різних регіонах. Особливу увагу приділено Азії, де держави, такі як Росія, Іран і Північна Корея, демонструють чітку симетрію між діями державних структур і кримінальних мереж. Наприклад, у Росії кримінальні мережі часто використовуються для обходу міжнародних санкцій, у той час як в Ірані вони залучаються до операцій проти політичних опонентів за кордоном. У Північній Кореї кримінальні мережі відіграють ключову роль у фінансуванні режиму через незаконну торгівлю, зокрема наркотиками та зброєю. Ці приклади показують, що геокримінальність не обмежується окремими країнами чи регіонами, а є частиною ширшого глобального феномену, який потребує комплексного підходу для його розуміння та протидії.

Автори детально зупиняються на викликах, які виникають у зв’язку з геокримінальністю. Одним із головних є складність ідентифікації того, чи є певна дія результатом діяльності держави, чи кримінальних груп, що значно ускладнює притягнення винних до відповідальності. Наприклад, у випадку з убивством Хангошвілі в Берліні, хоча виконавець був пов’язаний із ФСБ, Росія офіційно заперечувала свою причетність, що створило дипломатичну напругу, але не призвело до чіткої відповідальності. Інший виклик пов’язаний із впливом міжнародних санкцій, які, як показує приклад Росії після анексії Криму, часто мають зворотний ефект. Санкції, накладені на Росію, посилили її залежність від кримінальних мереж для обходу економічних обмежень, що зробило ці мережі більш привабливими для держави як інструмент зовнішньої політики. У документі зазначається, що в таких умовах кримінальні групи стають не лише виконавцями, а й партнерами держав, отримуючи захист і легітимізацію в обмін на свої послуги. Крім того, автори звертають увагу на те, що міжнародна спільнота часто стикається з внутрішніми обмеженнями, такими як бюрократія, корупція та брак координації між країнами, що заважає ефективно протидіяти геокримінальності. Це, у свою чергу, посилює залежність держав від кримінальних груп для досягнення зовнішньополітичних цілей, створюючи замкнене коло.

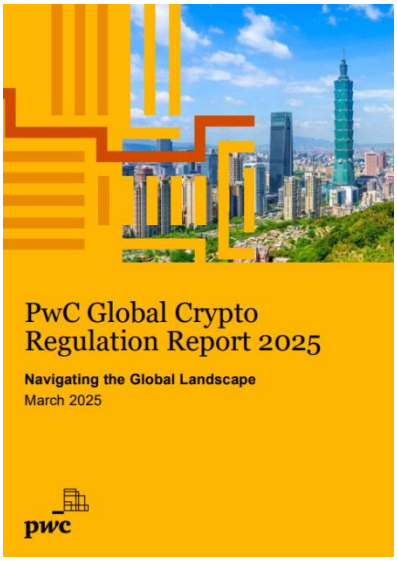
Документ завершується низкою запитань, які автори пропонують для подальших досліджень, щоб краще зрозуміти природу геокримінальності та розробити ефективні стратегії протидії. Вони запитують, чи є геокримінальність у демократичних країнах такою ж значущою, як в авторитарних, і як сучасні геополітичні пріоритети впливають на її масштаби. Також вони цікавляться, які нові форми державно-кримінальної співпраці можуть виникнути в майбутньому, враховуючи швидкий розвиток технологій і глобалізацію. Автори наголошують, що для ефективної боротьби з геокримінальністю необхідне глибше розуміння взаємозв’язків

між геополітикою, державними структурами та кримінальними мережами, а також закликають до посилення міжнародної співпраці. Вони критикують нинішні підходи до санкцій, які часто лише погіршують ситуацію, штовхаючи держави до співпраці з кримінальними групами, і пропонують переглянути ці інструменти, щоб зробити їх більш гнучкими та ефективними. У підсумку документ підкреслює, що геокримінальність є серйозною загрозою для глобальної безпеки, яка потребує комплексного підходу, включаючи не лише силові методи, а й дипломатичні, економічні та технологічні рішення, щоб розірвати зв'язки між державами та кримінальними мережами.

Висновки:

- **Посилення міжнародного моніторингу та співпраці:** Необхідно створити глобальні механізми для відстеження державно-кримінальних зв'язків, особливо в країнах із високим рівнем геополітичної напруги (наприклад, Росія, Іран), щоб зменшити використання кримінальних мереж для зовнішньополітичних цілей.
- **Вплив санкцій:** Санкції, як у випадку з Росією після анексії Криму, часто штовхають держави до співпраці з кримінальними групами для їх обходу. Міжнародній спільноті слід розробити більш гнучкі інструменти, які не посилюють геокримінальність.
- **Підвищення прозорості в авторитарних режимах:** У країнах, де держава легітимізує злочинців, необхідно посилити тиск через міжнародні організації, щоб викривати такі зв'язки та зменшувати їхню привабливість.
- **Розвиток кібербезпеки для боротьби з геокримінальністю:** З огляду на кібератаки, подібні до тих, що здійснили проросійські хакери в Італії у 2025 році, держави повинні інвестувати в кіберзахист і створювати міжнародні протоколи для швидкого реагування на такі інциденти.

Глобальне регулювання криптоактивів 2025: як США, ЄС та міжнародні стандарти формують нову фінансову архітектуру[9]



Звіт PwC є одним із найкомплексніших і найактуальніших аналітичних оглядів, присвячених глобальному регулюванню криптоактивів станом на початок 2025 року. Документ системно висвітлює динаміку становлення нормативно-правового поля у цій сфері, підкреслюючи як загальносвітові тренди, так і особливості ключових юрисдикцій: США, Європейського Союзу, Великої Британії, країн Азії, Близького Сходу та інших. Звіт має прикладну цінність як для регуляторів, так і для суб'єктів ринку, які прагнуть забезпечити відповідність новим вимогам і використати можливості, що виникають унаслідок появи більшої регуляторної визначеності.

На тлі стрімкого розвитку криптоіндустрії та зростання рівня її інтеграції у традиційний фінансовий сектор, 2025 рік демонструє кардинальний злам у підходах до регулювання цифрових активів. PwC фіксує, що ключові юрисдикції переходять від фрагментованих або репресивних моделей (зокрема, «регулювання через примус» у США) до системних і прозорих рамок. Особливу увагу у звіті приділено ситуації в США, де впроваджується структурована реформа, що включає законодавчу визначеність щодо стейблкоїнів (включно з ухваленням законопроєкту GENIUS), допуск до ринку інституційних інвесторів через запуск ETF на основі стейкінгу,

[9] https://legal.pwc.de/content/services/global-crypto-regulation-report/pwc-global-crypto-regulation-report-2025.pdf

формування єдиної регуляторної архітектури через нову Digital Asset Working Group, а також повне відмовлення від ідеї випуску CBDC. Усі ці зміни сигналізують про перехід до інноваційно-орієнтованого регулювання з пріоритетом прозорості, конкуренції та фінансової інклюзії.

У Європейському Союзі домінуючим нормативним актом став Регламент про ринки криптоактивів — MiCAR, який з грудня 2024 року повністю набув чинності. Він є першою у світі кодифікованою спробою побудови уніфікованого правового поля для обігу криптоактивів у межах внутрішнього ринку ЄС. MiCAR встановлює чіткі категорії токенів (ART, EMT, utility tokens), вводить обов'язкове ліцензування постачальників послуг з криптоактивами (CASPs), накладає суворі вимоги до структури whitepaper, захисту клієнтських коштів, корпоративного управління та боротьби з ринковими зловживаннями. Особлива увага приділяється так званим «значущим токенам» (significant tokens), які підлягають посиленому нагляду з боку Європейського банківського органу (EBA). Крім того, звіт підкреслює важливість нових регламентів AMLR, DORA і WTR II, які створюють фундамент для кіберстійкості, боротьби з фінансовими злочинами та посилення транзакційної прозорості в межах ЄС.

У звіті також проаналізовано позиції органів міжнародного регуляторного нагляду, включно з FATF, FSB, BCBS та IOSCO. FATF зафіксувала серйозне відставання більшості країн у впровадженні 15 Рекомендації, зокрема Travel Rule: понад 75% юрисдикцій залишаються лише частково сумісними або взагалі не відповідають стандартам, а 30% країн не впровадили жодної форми передачі ідентифікаційної інформації у криптотранзакціях. FSB наполягає на підході «однакова діяльність — однаковий ризик — одне регулювання» та звертає увагу на необхідність сегрегації клієнтських коштів, усунення конфліктів інтересів та координації між юрисдикціями. BCBS деталізував нову пруденційну модель для банків, яка розділяє криптоактиви на дві групи: із надійним забезпеченням (Group 1) — із пільговим ставленням у капіталі, та інші активи (Group 2), до яких застосовуються жорсткі вимоги з обмеженням до 2% Tier 1. IOSCO випустила 18 рекомендацій щодо ринкової поведінки CASPs, а також окремі рекомендації щодо DeFi — з особливим акцентом на ризики для роздрібних інвесторів, технологічну стійкість, прозорість та міжнародну співпрацю.

У регіональному вимірі звіт демонструє, що низка країн Азії (Гонконг, Сінгапур) вже перейшли до формування повноцінних ліцензійних режимів, що охоплюють не

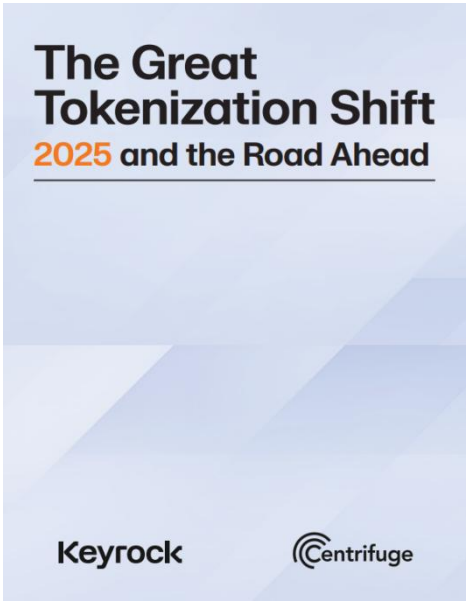
Висновки:

- **Суб'єктам ринку слід невідкладно ініціювати підготовку до авторизації згідно з MiCAR до завершення перехідного періоду (1 липня 2026 року), з урахуванням специфіки в кожній країні-члені ЄС.** Це означає адаптацію бізнес-процесів, підготовку whitepaper, впровадження заходів CDD, внутрішнього контролю та кастодіальної політики.
- **Фінансові установи, що мають справу з криптоконтрагентами (VASPs), повинні провести ревізію своїх партнерських зв'язків із позиції відповідності 15 Рекомендації FATF, зокрема перевірити виконання Travel Rule.** У разі невиконання — зростає ризик вторинного впливу (reputational & regulatory contagion).
- **Банкам рекомендовано адаптувати внутрішні пруденційні процедури згідно зі стандартами BCBS щодо експозицій до криптоактивів — особливо для групи 2 активів, що обмежуються до 2% Tier 1.** В іншому разі — можливе суттєве збільшення капітальних вимог через застосування1250% коефіцієнта ризику до відповідних активів.
- **Емітентам стейблкоїнів та інвесторам слід уважно відстежувати національні пріоритети регуляторів:** у США, Великій Британії та ЄС формується чіткий тренд на інтеграцію стейблкоїнів у платіжні системи, але лише для прозорих і повністю забезпечених токенів.

лише обмін криптоактивами, а й деривативи, кастодіальні послуги, кредитування. Аналогічну тенденцію демонструють ОАЕ, Саудівська Аравія, ПАР. Велика Британія перебуває на фінальній стадії розробки нормативної бази для криптоактивів з імплементацією у 2026 році. Водночас у багатьох юрисдикціях ринок залишається нерегульованим або напіврегульованим — це створює загрози регуляторного арбітражу та експлуатації слабких місць фінансової системи.

Загалом, звіт формулює основний висновок: 2025 рік — це точка переходу від спорадичного до системного підходу в регулюванні цифрових активів. Суб'єкти ринку, включаючи фінансові установи, технологічні компанії та інвесторів, мають адаптувати свою діяльність до нових вимог, які все більше орієнтовані на відповідальність, прозорість, ризик-орієнтованість і зменшення системних загроз. У перспективі PwC очікує на глобальну конвергенцію нормативних підходів, де моделі США, ЄС і FSB/FATF визначатимуть «правила гри» в цифровій фінансовій архітектурі нового покоління.

Великий зсув токенізації: як блокчейн трансформує глобальні фінансові ринки у 2025 році[10]



Звіт, підготовлений Keyrock і Centrifuge, є комплексним аналізом трансформації глобальних фінансових ринків шляхом інтеграції реальних активів у блокчейн-інфраструктуру. У центрі дослідження — не лише технологічна еволюція, а й фундаментальна перебудова механізмів доступу, ліквідності, регуляторної взаємодії та управління капіталом. Автори стверджують, що токенізація — це не спроба дублювати традиційну фінансову систему в ончейні, а радше створення принципово нової — більш відкритої, ефективної та доступної системи. Такий підхід відкриває двері до глобальної фінансової участі без посередників і зменшує бар'єри для інтеграції активів з високим вхідним порогом — наприклад, державних облігацій, приватного кредиту, товарів і акцій — у нову цифрову екосистему.

Особлива увага в дослідженні приділена токенізованим державним облігаціям США — наразі це найбільший і найдинамічніший сегмент ринку токенізованих активів. Автори описують, як нестача прибутковості в традиційних стейблкойнах спонукала криптоінвесторів до переходу на облігації з реальним дохідним потоком, обгорнуті у формі ERC-20 токенів. Такі продукти як USDY (Ondo), BENJI (Franklin OnChain), USYC (Hashnote) та інші дозволяють не лише отримувати дохід у розмірі 4–5% річних, а й використовувати ці активи як ліквідну заставу в DeFi-протоколах. Однак ринок стикається з технічними викликами, зокрема проблемами ціноутворення (модель наростаючої вартості vs. ребейсинг), обмеженнями оракулів, низькою глибиною ринку. Щоб вирішити ці питання, Centrifuge створив ETF-подібну модель «Anemoy Liquidity Network», яка гарантує 24/7 ліквідність через ринки з маркетмейкерами. Паралельно платформи як Chainlink вирішують проблему достовірних цінових фідів, дозволяючи токенізованим казначейським зобов'язанням стати повноцінною інституційною заставою в DeFi.

Другим фокусом звіту є токенізовані акції. У цьому напрямку ключовим бар'єром залишається регуляція. У США та ЄС токенізовані цінні папери підпадають під дію відповідно SEC/FINRA та MiFID II/Prospectus Regulation, що значно ускладнює їхній обіг. Однак нові моделі на кшталт Backed Finance (Швейцарія/Ліхтенштейн) пропонують повністю комплаєнтні акції ETF (як-от

[10] https://documents.keyrock.com/hubfs/The-Great-Tokenization-Shift.pdf

bCSPX) у режимі відкритого доступу, доступні без KYC. Водночас Ondo Finance будує власний блокчейн Ondo Chain — з нативною підтримкою корпоративних дій, proof-of-reserve, функціоналом для валідаторів із інституційного середовища. Ці моделі створюють передумови для появи цілодобового глобального фондового ринку з відкритим доступом. Прогноз на 2025 рік — потенційне зростання токенізованих акцій до $1 млрд загального обсягу вартості активів (TVL) у разі нормативного сприяння.

Сегмент токенізованих товарів представлений насамперед золотом. PAXG (від Paxos) і XAUT (Tether) — лідери ринку, але обсяги DeFi-використання залишаються мізерними. На фоні сплеску активності в інших секторах, токенізоване золото демонструє слабку динаміку, зменшуючи пропозицію (TVL знизився на 28% у 2024 р.). Основні причини — складність фізичного викупу, висока маржа на біржах, низький інтерес серед крипто-користувачів. На зміну їм приходять синтетичні моделі — такі як Ostium Labs — які дозволяють відкривати довгі/короткі позиції на товари з плечем до 200x. Це підходить для спекулянтів і трейдерів, хоча не є рішенням для інституцій, які шукають прозору фізичну прив'язку. Загальна оцінка — сегмент має обмежений потенціал зростання, доки не з'являться нові класи токенізованих товарів із інтеграцією в DeFi та кращими умовами викупу.

Найбільш інституційно перспективним сектором є токенізований приватний кредит. Тут мова йде про заміну традиційних джерел фінансування (банків, PE-фондів) децентралізованими позиками. Платформи як Centrifuge, Maple, Tradable та Figure пропонують гібридні моделі, де позики агрегуються в пули, токенізуються, і надходження розподіляються пропорційно. Використовуються спеціальні правові структури (SPV, Reg D, A+), інтегровані KYC/AML та whitelist-системи, які дозволяють інституціям брати участь. Centrifuge, зокрема, є рушієм галузі, стандартизувавши RWA через новий стандарт ERC-7540, що дозволяє інтегрувати приватний кредит у DeFi із затриманими або асинхронними розрахунками. На фоні попиту на високу прибутковість та низьку кореляцію з крипторинком, токенізований приватний кредит пропонує стратегічну альтернативу класичним борговим інструментам.

Загалом, звіт демонструє, що токенізація вже перейшла стадію експериментів і вступає у фазу масового впровадження. Платформи починають використовувати стратегії ETF-індустрії (ліквідність, ціноутворення, комплаєнс), DeFi-протоколи інтегрують реальні активи як заставу, а

Висновки:

- **Термінова дія для DeFi-протоколів:** Впровадження інтеграції з токенізованими Treasuries (USYC, USDY) може забезпечити нове джерело високоякісної застави з прогнозованим доходом у ~4%. Це критично для протоколів кредитування, як-от Aave, Morpho, Sky.
- **Регуляторам слід адаптувати законодавство:** Надання юридичної визначеності щодо токенізованих акцій через адаптацію існуючих норм (наприклад, SEC або MiFID II) дозволить інституціям розпочати масштабну токенізацію з реальним обігом на вторинному ринку.
- **Необхідність стандартизації цін і оракулів:** США та ЄС повинні активізувати санкційний тиск на дочірні компанії Rostec (Germanium JSC, Urals Optical and Mechanical Plant) та пов'язані фірми (Germanium and Applications, Cryotrade Engineering), щоб ускладнити доступ до критичних матеріалів.
- **Фінансовим розвідкам — моніторинг ризиків «reintermediation»:** Нові структури (SPV, позафондові зобов'язання) в DeFi вимагають адаптації аналітичних інструментів ПВК/ФТ. Зокрема, токенізовані фонди, які діють через ліцензованих агентів у низькорегульованих юрисдикціях (BVI, Cayman), можуть бути використані для прихованого переміщення капіталу.

провідні фінансові гравці (BlackRock, Circle, Securitize) будують власну інфраструктуру під нову модель обігу капіталу. Токенізовані активи стають не просто інновацією — вони поступово перетворюються на ключовий елемент глобальної фінансової архітектури майбутнього.

Tokeny T-REX: Повний цикл токенізації активів — інфраструктура нового покоління для цифрових цінних паперів[11]

Документ від компанії Tokeny є комплексним технічним та бізнес-орієнтованим описом процесу токенізації цінних паперів з використанням стандартизованої блокчейн-інфраструктури на базі смартконтрактів ERC3643. У центрі рішення — платформа T-REX, яка створена для забезпечення повного життєвого циклу токенізованих активів: від онбордингу інвестора до емісії, обслуговування і вторинної торгівлі. Платформа вирішує ключові проблеми традиційних ринків капіталу: фрагментованість, паперову бюрократію, складність відповідності нормативним вимогам та обмежену ліквідність.

Синопсис процесу починається з опису місії компанії Tokeny — спростити ринки капіталу за допомогою токенізації, усуваючи необхідність для користувачів взаємодіяти з технічними аспектами блокчейну. В основі платформи лежить модульний, юрисдикційно-нейтральний підхід із підтримкою будь-якого EVM-сумісного блокчейну, що дозволяє емітентам масштабувати рішення незалежно від правового середовища. Інфраструктура побудована таким чином, щоб забезпечити сумісність із різними типами активів — від облігацій до пайових цінних паперів і навіть товарів.

Онбординг інвестора є першим етапом. Він включає в себе автоматизовану перевірку особи з використанням ШІ-рішень для KYC, збір і валідацію необхідних документів, кваліфікацію інвестора емітентом або авторизованим агентом, а також підписання електронних документів через інтегровані e-signing модулі. Платформа підтримує приймання як фіатних платежів (через банківський переказ з реєстрацією референсів), так і криптовалют (токенізована готівка), що підтверджуються автоматично при надходженні на гаманець емітента.

Наступним кроком є емісія токенів, яка здійснюється через зручний інтерфейс без необхідності програмування. Емітенти або їхні агенти створюють смартконтракти, де задаються параметри випуску: обмеження на обіг, правила допуску (eligibility claims), whitelist цифрових ідентичностей (ONCHAINID), а також зберігання даних про інвесторів. Токени потім розподіляються між інвесторами з можливістю масових операцій. У процесі генерації токенів кожному інвестору автоматично створюється ідентифікатор інвестора в блокчейні, якщо він ще не існував, а баланс у гаманці оновлюється в реальному часі. Це дозволяє здійснювати прозоре та миттєве оновлення каптейблу (реєстру власників), що має критичне значення для комплаєнсу та звітності.

Обслуговування токенів виходить за межі простого зберігання. Емітенти можуть ініціювати корпоративні дії, експортувати звіти для аудитів, виконувати критичні дії з токенами (mint (створення), спалювання, заморожування, блокування, відновлення), а також примусово передавати токени в особливих випадках, наприклад, за рішенням регулятора чи для виправлення помилок. Важливим елементом є функція «Conditional Transfers» — додатковий рівень контролю над кожною транзакцією, навіть якщо вона відповідає всім умовам за

[11] https://tokeny.com/wp-content/uploads/2023/08/The-Complete-Tokenization-Process-Tokeny.pdf

замовчуванням. Комунікація з інвесторами централізована — через вбудовану систему повідомлень.

Особлива увага приділяється можливостям вторинної дистрибуції, що є одним із найбільш інноваційних елементів платформи. Емітенти можуть позначити токени як «торговельні» та відкривати доступ до кількох каналів ліквідності: від ліцензійно-вільних дошок оголошень (Billboard) до централізованих бірж (із перевіркою депозитних гаманців), децентралізованих протоколів (DeFi), DEX-платформ із наданням ліквідності, та маркетплейсів, які ведуть потенційного інвестора назад до процесу кваліфікації на T-REX. Усі операції — незалежно від платформи — відображаються в одному реєстрі каптейблу в реальному часі.

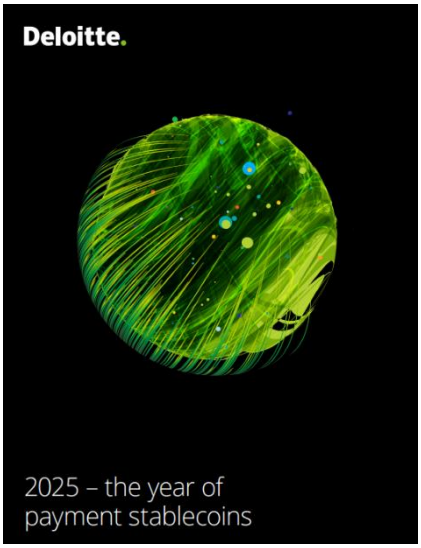
Tokeny підкреслює, що їхній підхід дозволяє реалізувати повну цифровізацію інвестиційного досвіду. Інвестори можуть самостійно інвестувати, управляти, отримувати доходи, відновлювати доступ до активів — усе без залучення третіх сторін. Емітенти при цьому зберігають контроль над правами доступу до токенів та реєстрацією нових учасників. Платформа також забезпечує прозорість, масштабованість і додаткові джерела доходів — як для емітентів (комісії, розширення пулу інвесторів через фрагментацію часток), так і для агентів, які можуть надавати послуги новим класам клієнтів.

У підсумку, документ Tokeny є практичним посібником для компаній, що планують здійснити токенізацію своїх активів і шукають зріле, нормативно-сумісне, масштабоване рішення. Він не лише описує процес, а й демонструє трансформаційний потенціал токенізації для всього фінансового ринку: від підвищення прозорості до покращення ліквідності та зниження вартості операцій.

Висновки:

- **Інтеграція автоматизованої інфраструктури токенізації дозволяє скоротити витрати на комплаєнс та збільшити обсяг інвесторів.** Автоматизація KYC/AML, управління реєстром, розподілу токенів і контролю трансфертів забезпечує ефективне масштабування операцій без збільшення ручної праці. Це особливо важливо для венчурних фондів, фондів нерухомості та приватного капіталу.
- **Модель «compliance-by-design» в ERC3643 забезпечує відповідність нормативним вимогам у транзакціях навіть поза платформою.** Завдяки вбудованим правилам доступу та верифікованому ідентифікаційному запису інвестора, токени можна безпечно переміщати між біржами, P2P або на DeFi, не порушуючи вимог KYC/AML або інших обмежень.
- **Токенізація відкриває можливості для нових джерел доходів як для емітентів, так і для агентів.** Модель «відкритої інфраструктури» дозволяє емітентам отримувати прибутки з: комісій за трансфери; надання ліквідності в DeFi; транзакційного обслуговування; маркетплейсів для вторинного обігу; а агенти можуть масштабувати свою присутність без лінійного зростання витрат.
- **Реєстр власників (каптейбл) оновлюється в реальному часі, що критично важливо для прозорості та аудиту.** Це забезпечує безперервний моніторинг інвестиційної активності, контроль за походженням коштів і можливість оперативного реагування на запити регулятора, аудиторів або внутрішнього контролю.

Платіжні стейблкоїни у 2025: трансформація фінансової інфраструктури та виклики регулювання[12]



Документ Deloitte є аналітичним прогнозом і стратегічним орієнтиром для фінансових установ, небанківських компаній та інших суб'єктів, які планують інтегрувати або вже працюють із платіжними стейблкоїнами (payment stablecoins, PSCs). Цей аналітичний звіт спирається на попередні публікації Deloitte (2021, 2023) і відображає суттєві зрушення у регуляторному, технологічному та ринковому середовищі, які спонукають до того, щоб 2025 рік став ключовим у масовому переході до використання стейблкоїнів як повноцінного платіжного засобу.

У центрі уваги звіту — констатація нової політичної та регуляторної волі в США щодо впровадження законодавчої бази для PSC. На момент підготовки документа в Конгресі вже було подано три ключові законопроєкти: GENIUS Act, STABLE Act та проєкт закону, запропонований представницею Максін Вотерс. Усі три ініціативи мають спільні принципи: обов'язкове забезпечення PSC високоякісними ліквідними резервними активами у співвідношенні 1:1, запровадження регулярного аудиту й звітності, обмеження кола емітентів (дозвіл лише для небанківських структур та дочірніх компаній банків), а також уніфікований підхід до ПВК/ФТ та комплаєнс-практик.

Значний акцент зроблено на зміні тональності у ставленні адміністрації США до цифрових активів. Після приходу до влади адміністрації Дональда Трампа у 2025 році було підписано виконавчий указ «Посилення лідерства США у сфері цифрових фінансових технологій», у якому прямо задекларовано підтримку зростання та глобального впровадження доларозабезпечених PSC. Цей політичний сигнал вже починає трансформуватися в дії з боку регуляторних органів, зокрема OCC (Office of the Comptroller of the Currency), який визнав правомірність участі банків у діяльності з цифровими активами, включаючи кастодіальні послуги та транзакції зі стейблкоїнами.

На практичному рівні Deloitte розглядає структуру ринку PSC як багатовимірну екосистему, яка включає: емітентів, резервні банки, банки транзакцій, технологічних провайдерів, кастодіанів, платіжні платформи, аналітиків та консультантів. Звіт ідентифікує кілька ключових бізнес-моделей, які можуть реалізуватися у PSC-сфері, та закликає учасників ринку вже зараз визначати своє стратегічне позиціонування у новому ланцюзі створення вартості.

Водночас Deloitte вказує на те, що ринок PSC несе серйозні ризики, як для емітентів, так і для сервісних учасників. До таких ризиків належать: кіберзагрози, вразливості у смарт-контрактах, ризик депегінгу (втрата прив'язки PSC до фіатної валюти), дефекти в управлінні резервами, операційні збої, комплаєнс-ризики, а також складність регуляторного дотримання у динамічному середовищі. Особливу увагу звернуто на необхідність побудови структурованої системи управління ризиками та контролю, яка охоплює як ризики традиційного фінансового сектору, так і специфіку криптопродуктів і технологій.

Документ окремо деталізує регуляторні очікування, які будуть застосовуватись як до PSC-емітентів, так і до неемітентів (наприклад, кастодіанів, платіжних сервісів, технологічних платформ). Ці очікування охоплюють сфери: стратегічного планування, управління звітності, управління резервами, інформаційної безпеки, відповідності податковим та бухгалтерським

[12] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-advisory-deloitte-2025-the-year-of-payment-stablecoins.pdf

стандартам, третейської взаємодії та корпоративного управління. Deloitte надає багаторівневу матрицю очікувань для обох категорій учасників — з розмежуванням за ступенем впливу («високий», «середній», «низький вплив») — що дозволяє компаніям здійснити самооцінку готовності до участі в PSC-екосистемі.

Звіт підкреслює, що успішне функціонування PSC залежатиме не лише від формального дотримання нормативів, а й від практичної готовності до оперативного управління ризиками у режимі реального часу. Йдеться про забезпечення надійного резервного покриття (тільки за рахунок визначених законом активів, таких як короткострокові казначейські облігації США), здатність здійснювати миттєве викуплення PSC у фіат, реалізацію прозорої звітності, в тому числі — щомісячного аудиту резервів сертифікованим аудитором. Для забезпечення довіри користувачів, емітенти повинні публікувати звіти про стан резервів, включаючи розподіл активів, обсяг токенів в обігу та показники ліквідності.

Окреме місце займає аналіз взаємодії між PSC і традиційною банківською інфраструктурою. Deloitte прогнозує, що з розгортанням PSC як засобу розрахунків, банки зіштовхнуться з ризиком часткової втрати клієнтського обслуговування та функції посередника — особливо в B2B і B2C платежах. У цьому контексті запропоновано декілька моделей співіснування: інтеграція PSC у банківські платформи, створення гібридних продуктів (наприклад, токенізовані депозити), а також роль банків як агентів емісії, кастодіанів чи резервних інституцій. Пропонується також сценарний підхід до оцінки стратегічного ризику — для розробки адаптивних бізнес-моделей.

Детально описується значення PSC у трансформації платіжної інфраструктури. Завдяки миттєвості, дешевизні транзакцій та трансграничній доступності, PSC здатні стати цифровим розширенням долара США. Їх застосування дедалі частіше виходить за межі крипторинку — вони використовуються в транскордонних переказах, B2B платежах, роздрібних розрахунках. Однак Deloitte вказує, що масове впровадження PSC можливе лише за умов інституційного прийняття: з боку банків, торгових платформ, процесингових центрів, мерчантів і кінцевих споживачів.

Крім того, документ містить глибоку деталізацію щодо того, які внутрішні можливості повинні бути створені або вдосконалені у PSC-емітента чи сервісного провайдера. Йдеться про: створення оновленої архітектури управління (governance), впровадження ефективної політики управління ліквідністю, резервами та фінансовим плануванням (treasury management), розробку та реалізацію політик щодо управління резервами, включаючи стрес-тестування, контингентне планування, моніторинг блокчейн-інфраструктури, управління ключами,

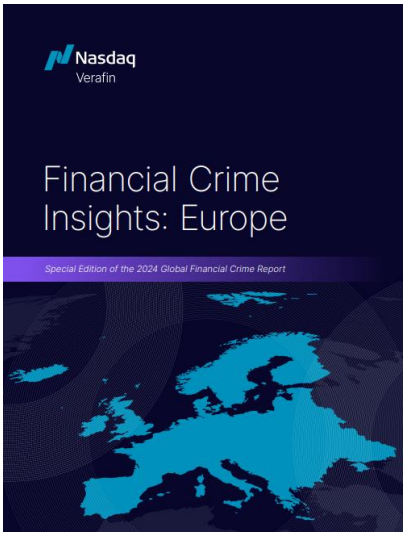
Висновки:

- **Компанії повинні готуватись до PSC як нового стандарту цифрових платежів.** Необхідно вже зараз інтегрувати PSC у стратегічне планування, IT-інфраструктуру та ризик-менеджмент, оскільки впровадження PSC очікується у 2025 році як масштабне явище, підтримане державним курсом.
- **Емітенти PSC повинні забезпечити повну резервну підтримку, прозору звітність і відповідність вимогам ПВК/ФТ.** Це включає щомісячні аудити, публікацію звітів про резерви, наявність процедур KYC/EDD, сценарне тестування ризиків депегінгу та кібербезпеки.
- **Участь у PSC-екосистемі потребує адаптації управління, комплаєнсу та treasury-функцій.** Зокрема, банки, фінансові компанії, платіжні процесори повинні мати чіткі SLA з контрагентами, оновлені політики щодо IT, звітності та відповідальності.
- **Система реагування на нові ризики має бути динамічною і модульною.** Підходи до моніторингу транзакцій, управління смарт-контрактами, контролю за резервами мають бути адаптивними до мінливого регуляторного середовища (Федеральні + штатні рівні).

запровадження інформаційної безпеки та кіберзахисту відповідно до стандартів FFIEC. Також приділяється увага вимогам до бухгалтерського обліку PSC — зокрема, класифікації PSC як фінансового зобов'язання або нематеріального активу в залежності від юрисдикції та бізнес-моделі.

Завершується звіт рекомендацією компаніям (як фінансовим установам, так і технологічним учасникам) формувати стратегію взаємодії з PSC вже зараз, враховуючи не тільки регуляторний ландшафт, а й конкурентні позиції, структуру витрат, потреби клієнтів та довгострокові інституційні ризики. Deloitte переконано наголошує: той, хто першим адаптує бізнес до нового режиму PSC і побудує відповідну інфраструктуру — отримає стратегічну перевагу на ринку цифрових фінансів нового покоління.

Статистика фінансових злочинів[13]



Документ глибоко аналізує масштаби та особливості фінансових злочинів у Європі, включаючи ЄС, Велику Британію та країни Північної Європи. У 2023 році через фінансову систему Європи пройшло приблизно 750,2 млрд дол. США нелегальних коштів, що становить 2,3% ВВП регіону. Серед основних джерел цих потоків — торгівля наркотиками (178 млрд), торгівля людьми (82,2 млрд) та фінансування тероризму (2,7 млрд). Понад чверть цих коштів — 194,9 млрд дол. — становили транскордонні операції, а 58,2 млрд дол. були переміщені за участі "грошових мулів", що додає складності до виявлення схем відмивання коштів.

Рівень втрат від шахрайства також вражаючий — 103,6 млрд дол. США, зокрема $61,5 млрд у ЄС, $33,2 млрд у Великій Британії, $3,4 млрд у Північній Європі. Найбільші втрати спричиняють шахрайство з банківськими картками, соціальні інженерні схеми (APP fraud), шахрайства з роботою, коханням, виграшами та державними виплатами. Особливо загрозливими є гібридні шахрайські схеми, що поєднують кілька типів обману, та шахрайства проти літніх людей, які становлять до 38% загальних втрат у деяких країнах.

Фінансові установи змушені діяти в умовах зростаючої складності регуляторного середовища, швидких змін у технологіях та агресивної еволюції кримінальних схем. Лише 22% установ відзначили наявність достатніх ресурсів (персоналу або технологій) для боротьби з фінансовими злочинами. Разом із цим 74% банків планують інвестувати в штучний інтелект та машинне навчання для покращення моніторингу, виявлення аномалій, виведення ризикових клієнтів та схем.

Великі надії покладаються на інформаційний обмін як у приватно-приватному (установа-установа), так і в державно-приватному партнерстві. У звіті окремо розглянуто ініціативи ЄС (AMLR, стаття 75) та Великої Британії (ECCTA), які забезпечують правову основу для партнерства та обміну інформацією з метою протидії відмиванню коштів, фінансуванню тероризму та шахрайству. Проте практичне впровадження цих механізмів гальмується через регуляторну невизначеність, побоювання щодо конкуренції, ризики конфіденційності та нестачу ресурсів.

[13] https://verafin.com/financial-crime-insights-europe/

Серед пріоритетів виділяється також модернізація регулювання: у документі наголошується на необхідності типологічних орієнтирів від регуляторів, що допоможе установам краще розставити пріоритети та фокусувати ресурси. Крім того, рекомендовано інтеграцію функцій боротьби з шахрайством і ПВК (FRAML-підхід), яка залишається недостатньо поширеною в європейських банках.

Цей звіт підкреслює, що міжнародна співпраця, спільне використання даних, розумна регуляторна політика, а також інноваційні технології є ключем до підвищення ефективності в боротьбі з відмиванням коштів, фінансуванням тероризму та фінансовим шахрайством у регіоні, що все більше стає глобальним еталоном у цій сфері.

Висновки:

- **Необхідне активне впровадження інформаційного обміну** між установами в межах ЄС та Великої Британії відповідно до AMLR (ст. 75) та ECCTA для ефективної боротьби з транскордонним шахрайством, ВК та ФТ.
- **Установам слід терміново інвестувати в AI і машинне навчання** для вдосконалення виявлення грошових мулів, APP-шахрайств та схем ФТ; більшість установ вже планують ці інвестиції в найближчі 1–2 роки.
- **Ризик-орієнтований підхід і FRAML-інтеграція** мають стати стандартом — зараз лише 37% банків його застосовують, і ще менше мають інтегровані функції AML і Fraud.
- **Захист вразливих клієнтів, особливо літніх людей**, потребує спеціалізованих програм моніторингу, внутрішнього навчання та цільового контролю — на сьогодні лише 68% установ мають відповідні стратегії, тоді як втрати серед літніх клієнтів становлять до 38% від усіх втрат у деяких країнах.

Аналітичний бюлетень FIH Insights[14]

Березневий випуск FIH Insights 2025 присвячено аналізу реформ у сфері ПВК/ФТ, з особливим акцентом на розвиток механізмів обміну інформацією між приватними суб'єктами (P2P), реформу положень про заборону розголошення («tipping-off») в Австралії, а також аналіз нових правових рамок в ЄС. Видання містить експертні матеріали провідних практиків, науковців і представників регуляторів, які підкреслюють, що ефективність заходів проти фінансових злочинів залежить не лише від законодавства, а й від культурних, організаційних і технологічних чинників.

Одним із центральних акцентів є досвід Південної Африки, де на симпозіумі з фінансових злочинів було наголошено на необхідності посилення P2P-обміну інформацією між банками й іншими підзвітними суб'єктами. Така форма обміну визнається «наступним фронтиром» в еволюції фінансової розвідки. Учасники симпозіуму підтримали тезу про те, що кримінальні мережі вже давно працюють без урахування кордонів та юрисдикцій, тоді як інституції, покликані протидіяти цим злочинам, досі діють у ізольованих «секторальних» умовах. У матеріалі аналізуються приклади партнерств, таких як британський JMLIT, австралійський Fintel Alliance, канадські та новозеландські ініціативи, а також підкреслюється, що саме приватний сектор, за належного нормативного захисту, може виступати каталізатором ідентифікації транскордонних схем.

[14] https://www.mq.edu.au/__data/assets/pdf_file/0007/1339018/FIH-Insights-March-2025.pdf

Іншим суттєвим тематичним блоком є огляд реформи австралійського законодавства щодо tipping-off — нового визначення, яке з 31 березня 2025 року дозволяє підзвітним суб'єктам ділитися інформацією про підозрілі транзакції за умови, що таке розкриття не створює загрози для розслідувань. Важливою зміною стало зміщення фокусу з формального порушення до сутнісного — потенційної шкоди. Це дозволяє фінансовим установам надійніше управляти ризиками шляхом міжінституційного обміну без страху порушення закону. Проте експерти підкреслюють, що цей механізм потребує зрозумілих інструкцій і належного контролю — від внутрішньої сегментації доступу до даних до належного інформування третіх сторін.

Особливу увагу приділено тому, що, попри нові повноваження AUSTRAC (зокрема, секції 49B, 49C та 172A про примусове надання інформації, добровільну співпрацю), ефективність ПВК все ще обмежується недостатнім рівнем обміну даними між суб'єктами, які мають відповідну інформацію. Зокрема, Michael Brand у системному аналізі стверджує, що самі по собі закони не дають змоги побачити фінансову картину цілком: злочинні типології розпорошені між різними установами, тоді як обробка інформації здійснюється у вузьких межах окремих рахунків. Автор пропонує концепцію PET-базованого рішення (FinTracer), яке дозволяє здійснювати повноцінний аналіз даних без порушення конфіденційності.

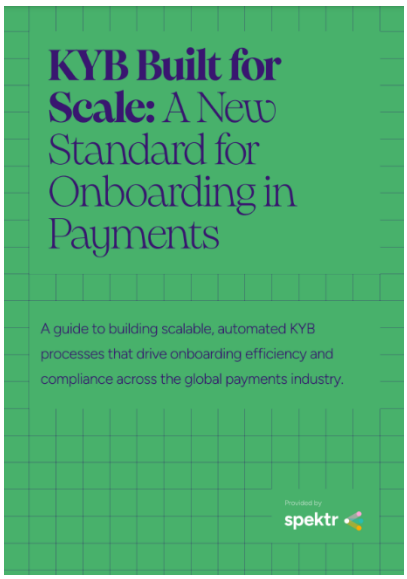
У європейському контексті Maxime Lassalle аналізує ухвалений у 2024 році пакет законодавства ЄС з ПВК/ФТ, який нарешті створює нормативну основу для P2P-обміну в межах ЄС. Ключові новації — Регламент 2024/1624 та Директива 2024/1640 — передбачають як можливість створення партнерств між підзвітними суб'єктами, так і надання фінансовим розвідкам повноважень на моніторинг транзакцій та видачу попереджувальних повідомлень. Водночас Lassalle застерігає, що імплементація буде залежати від кожної держави-члена, зважаючи на значну свободу розсуду.

Висновки:

- **Реформа tipping-off у Австралії створює нові можливості для обміну між підзвітними суб'єктами**, дозволяючи передавати інформацію за умови відсутності шкоди для розслідування, але вимагає впровадження надійних внутрішніх контролів і чітких інструкцій.
- **Розвиток P2P-обміну — ключовий напрям реформ**, який потребує законодавчого врегулювання, визначення обсягів дозволеної інформації, управління платформами та залучення установ.
- **ЄС офіційно визнав можливість P2P-обміну між підзвітними установами**, але ефективність залежатиме від національного рівня імплементації, зокрема, ролі ПФР у наданні попереджень і нагляді за дотриманням конфіденційності.
- **Проблеми у сфері обміну інформацією не є виключно юридичними — вони глибоко вкорінені в управлінських та культурних бар'єрах**, і їх подолання потребує централізованого лідерства, інституціоналізованої координації та довгострокових змін в організаційній поведінці.

Насамкінець, Diana Bocіga у своєму дослідженні підкреслює, що організаційна культура, недовіра, нестача ресурсів та фрагментованість між структурами — головні перешкоди ефективного обміну інформацією. Вона закликає не зупинятися на правових змінах, а впроваджувати системні інституційні рішення: централізовану координацію, інвестиції в аналітичні потужності, формалізацію неформальних механізмів довіри та стандартизацію інтерпретацій нормативних норм.

Новий стандарт перевірки клієнтів при здійсненні платежів[15]



Цей документ є керівництвом із побудови масштабованих, автоматизованих процесів перевірки бізнес-клієнтів (KYB — Know Your Business) у платіжному секторі. Він пропонує новий стандарт для ефективного онбордингу корпоративних клієнтів, зосереджуючись на викликах, пов'язаних із перевіркою складних, транснаціональних та ризикових суб'єктів господарювання. Проблематика документа охоплює труднощі з доступністю даних, складністю юридичних структур, багатоступеневими процесами прийняття рішень у великих організаціях та необхідністю дотримання міжнародних стандартів комплаєнсу.

Платформа spektr позиціонується як гіперконфігуровна система для автоматизації KYB-процесів. Вона дозволяє будувати багаторівневі верифікаційні стратегії, що адаптуються до юрисдикції, профілю ризику клієнта та етапу онбордингу. Замість того аби покладатися на одного постачальника даних, spektr дозволяє одночасно використовувати державні реєстри, комерційні джерела, преміальні аналітичні сервіси та власні канали перевірки. Це дає змогу збирати й доповнювати інформацію про структуру власності, кінцевих бенефіціарних власників (КБВ), управлінський склад і зміни у реєстраційних документах. Пост-онбордингові процеси включають автоматичне збагачення даних, що зменшує кількість ручних перевірок і підвищує повноту ризик-профілю.

З метою підвищення конверсії користувачів і скорочення часу до прийняття клієнта, система передбачає поділ процесу на окремі етапи: спочатку збирається інформація про юридичну особу, а потім про пов'язаних осіб (КБВ, директорів). Це дозволяє паралелізувати перевірки, покращити якість даних і зменшити кількість помилок. Для збору інформації використовуються інструменти на кшталт динамічного пошуку, перевірки домену компанії, інтерактивного редагування організаційної структури та інші smart-інтерфейси, які адаптуються до дій користувача.

Вбудована система управління кейсами дозволяє комплаєнс-фахівцям працювати в

Висновки:

- **Автоматизоване KYB-рішення Spektr зменшує навантаження на комплаєнс-команди** завдяки використанню багаторівневих перевірок, автоматичному збагаченню даних після онбордингу та інтегрованим AI-механізмам — що дозволяє швидше виявляти підозрілі бізнес-структури та мінімізувати людський фактор.
- **Модульна архітектура платформи дозволяє створювати юрисдикційно-специфічні процеси онбордингу**, що дає змогу ефективніше працювати з суб'єктами із різним рівнем ризику, уникати надмірних витрат і підвищувати конверсію клієнтів.
- **Окремі процеси для перевірки КБВ і директорів дають змогу підвищити точність перевірки та створити чіткий слід аудиту**, що критично важливо для відповідності вимогам FATF, AMLD та ISO-стандартів — з одночасним зменшенням часу онбордингу.
- **Сертифікація ISO 42001 і ISO 27001 підтверджує придатність системи для використання в регульованих секторах**, де автоматизовані рішення повинні не тільки бути ефективними, але й забезпечувати прозорість, контрольованість і відповідність міжнародним нормам у сфері ПВК/ФТ.

[15] https://www.spektr.com/api/guides?name=FINALKYBREPORT_f30b7902b6.pdf

єдиному середовищі з доступом до структури володіння, ризикових індикаторів, AI-рекомендацій і вбудованих тригерів для запиту документів, перевірки джерел походження коштів або ідентифікації PEP/санкцій. Завдяки сертифікаціям ISO/IEC 42001:2023 та ISO 27001:2022, система відповідає високим стандартам безпеки й управління ризиками, а використання AI-рішень у перевірці санкцій та медіа-аналітиці — дозволяє масштабувати перевірки без втрати якості.

Документ робить висновок, що лише платформи, які поєднують модульність, автоматизацію, аналітику та відповідність міжнародним стандартам, здатні забезпечити справжню ефективність у масштабному онбордингу бізнес-клієнтів. Це особливо актуально в контексті ПВК/ФТ, де ефективне й точне виявлення підозрілих бізнес-структур є ключем до вчасного реагування.

ВНУП

Арт-ринок Великобританії під тиском: великі штрафи розпалюють дискусію щодо відповідності AML-регуляціям [16]

У центрі уваги — ситуація, коли майже 50 британських арт-бізнесів, класифікованих як учасники ринку мистецтва (Art Market Participants, AMPs), отримали штрафи за порушення AML-регуляцій, спрямованих на запобігання відмиванню коштів через торгівлю мистецтвом. Ця проблема висвітлює напруженість між регуляторними органами та арт-ринком, а також піднімає питання справедливості й адаптованості чинних правил до реалій галузі.

Серед організацій, які потрапили під санкції, згадуються відомі галереї, такі як Opera і Carl Kostyál, а також благодійна ініціатива, очолювана White Cube, що є одним із ключових гравців на ринку сучасного мистецтва у Великобританії. Штрафи, накладені в період із 1 січня по 30 вересня 2024 року, варіюються від середнього значення понад £3000 до максимальної суми в £13000. Основною причиною цих санкцій стало недотримання дедлайну для реєстрації в HMRC, встановленого на червень 2021 року, коли учасники арт-ринку мали офіційно зареєструватися для відповідності AML-законодавству. Цей дедлайн був частиною ширшої стратегії уряду Великобританії щодо посилення контролю над фінансовими операціями в секторах, які вважаються вразливими до злочинної діяльності, зокрема відмивання грошей.

Особливу увагу в статті приділено реакції арт-спільноти на ці штрафи. Деякі компанії, усвідомлюючи свою затримку з реєстрацією, добровільно повідомили про це HMRC, сподіваючись на поблажливість. Однак замість цього вони зіткнулися з фінансовими санкціями, що викликало значне невдоволення. Один із учасників арт-ринку, який побажав залишитися анонімним, у коментарі для The Art Newspaper поділився, що штраф у £10000 "налякав багатьох дилерів, яких ми знаємо", залишивши відчуття, ніби їх покарали "за чесність". Інші джерела, також анонімно, розповіли, що вирішили не оскаржувати штрафи через бюрократичні

[16] https://www.artnews.com/art-news/news/uk-art-businesses-fined-money-laundering-compliance-aml-1234736548/

перепони, зокрема складність із пошуком відповідальної особи в HMRC для подання апеляції, а також через прагнення якомога швидше "рухатися далі й забути цей досвід". Ця ситуація підкреслює розрив між очікуваннями арт-бізнесу і жорстким підходом регулятора, а також вказує на демотивацію серед дрібних гравців ринку.

Експерти галузі висловили серйозну критику щодо методів, які застосовує HMRC. Рахі Талвар, консультант із комплаєнсу в мистецтві, зазначила, що штрафи за пізню реєстрацію розраховуються за фіксованою формулою, але ця формула є недосконалою й непропорційною. Вона вказала, що до розрахунку включаються прибутки від транзакцій, які не перевищують поріг у €10000 (приблизно £8500 залежно від курсу), а також від послуг, не пов’язаних із торгівлею мистецтвом, таких як консультації чи логістична підтримка. Це, на її думку, несправедливо, адже такі операції часто не становлять реального ризику для відмивання грошей. Сюзан Мамфорд, засновниця платформи ArtAML, яка спеціалізується на допомозі арт-бізнесам із дотриманням AML-вимог, додала, що особливо вразливими є мікробізнеси — невеликі галереї чи незалежні дилери, чиї угоди рідко перевищують цей поріг. Вона порадила таким підприємствам співпрацювати з HMRC для розробки гнучких графіків платежів, щоб уникнути фінансового краху, і зазначила, що добровільна реєстрація може зменшити штраф удвічі, а сплата протягом 30 днів від моменту накладення санкцій — ще на 25%. Ці практичні рекомендації стали своєрідним дороговказом для тих, хто намагається впоратися з наслідками санкцій.

Представник HMRC, відповідаючи на критику, відстоював позицію агентства, наголошуючи, що їхня мета — не просто карати, а "підтримувати бізнеси в захисті від злочинців, які можуть використовувати їхні послуги для відмивання грошей". Він підкреслив, що дії проти порушників є необхідною частиною забезпечення виконання юридичних зобов’язань, передбачених AML-законодавством. Однак цей аргумент не розвіяв сумнівів у галузі, де багато хто вважає підхід регулятора надмірно суворим і недостатньо адаптованим до специфіки арт-ринку, де значна частина угод є невеликими за обсягом і не пов’язана з фінансовими злочинами.

Сфера дії британських AML-регуляцій виявилася надзвичайно широкою, охоплюючи не лише традиційних учасників ринку, таких як галереї та дилери, а й посередників — арт-консультантів і фірми з дизайну інтер’єрів, які також потрапили до списку порушників. Це викликало додаткову хвилю критики, адже основна кампанія HMRC із підвищення обізнаності була зосереджена на галереях і дилерах, тоді як посередники, схоже, не отримали достатньої уваги чи підтримки для підготовки до вимог. Такий підхід поставив під сумнів ефективність роботи агентства з усіма групами, які підпадають під регуляції. У відповідь на це торгові асоціації, що представляють інтереси арт-ринку, почали активно закликати до реформ. Вони пропонують підвищити поріг транзакцій із €10000 до більш реалістичного рівня, який би краще відображав обсяги угод у галузі, а також переглянути класифікацію арт-ринку як "високоризикового". На їхню думку, ця класифікація не враховує різноманітності діяльності в секторі й створює надмірний тиск на дрібних гравців, які не становлять значної загрози в контексті відмивання грошей.

Загалом матеріал висвітлює складну взаємодію між регуляторними вимогами та реаліями арт-ринку, підкреслюючи потребу в балансі між боротьбою з фінансовими злочинами та підтримкою життєздатності галузі, особливо для її менших представників.

Інші новини

Масштабне шахрайство в Грузії: Розслідування та суспільний резонансу [17]

Публікація від організації OCCRP, опублікована 2 квітня 2025 року у рамках проєкту "Scam Empire", розкриває шокуючі подробиці розслідування діяльності шахрайського кол-центру в Тбілісі, що став осередком масштабного обману іноземних жертв. Спільна робота журналістів iFact та OCCRP виявила, що з травня 2022 року близько 85 молодих працівників цього центру ошукали понад 6100 людей на суму більш ніж **35,3 мільйона доларів**, переконуючи їх інвестувати в неіснуючі проєкти. Однак не лише фінансовий масштаб злочину вразив грузинське суспільство, а й безпрецедентна жорстокість і цинізм шахраїв, які висміювали своїх жертв і відкрито хвалилися своєю безкарністю.

Розслідування ґрунтується на аудіозаписах, які стали ключовими доказами. У них зафіксовано, як працівники кол-центру, наприклад Маріам Чарчіан, що діяла під псевдонімом Мері Робертс, знущалися з жертв. В одному з епізодів канадець, зрозумівши, що втратив усі заощадження, погрожував звернутися до поліції, на що Чарчіан вибухнула сміхом, заявивши, що його життя зруйноване, а правоохоронці різних країн ніколи не знайдуть її справжньої особи. Ця холоднокровність викликала в грузинів цілу гаму емоцій: від початкового шоку до сорому й гніву. Наприклад, 26-річна Цісі Моїстрапеїшвілі зазначила, що чутки про подібні операції ходили давно, але реальні голоси шахраїв і їхня поведінка стали справжнім ударом.

Суспільна реакція виявила глибший розкол у сприйнятті проблеми. Дехто, як 30-річний Лука Чохарадзе, вказував на економічні причини: середня зарплата в Грузії становить лише 750 доларів на місяць, тоді як топові шахраї заробляли до 20 000 доларів, що робило злочинну діяльність привабливою для молоді. Інші, як Марина Тавберіздзе, що живе за кордоном, обурювалися не лише самими шахраями, а й їхніми сім'ями, які, ймовірно, ігнорували джерела раптового багатства. Деякі грузини навіть пов'язували себе з винуватцями: одна користувачка TikTok згадала, що Маріам Чарчіан була її однокласницею, що додало особистого виміру до загального приголомшення.

Матеріальні прояви успіху шахраїв лише посилили обурення. Один із них прибув на власне весілля на гелікоптері, виклавши фото в соцмережі, інші демонстрували розкішні відпустки й екстравагантний спосіб життя. Але найстрашнішим стало те, що працівники кол-центру доходили до крайньої жорстокості, закликаючи жертв покінчити з собою. 33-річна Кетеван Лабадзе назвала це потенційним убивством, підкресливши, що злочин вийшов за межі простого шахрайства.

Після публікації розслідування грузинська влада відреагувала швидко, заморозивши активи ключових фігур і розпочавши офіційне розслідування, хоча багато громадян вимагали негайних арештів і судів. Цісі Моїстрапеїшвілі висловила недовіру до правоохоронців, запитуючи, чому журналісти виявили схему раніше за Службу державної безпеки чи МВС, які активно стежать за протестувальниками, але пропустили масштабний злочин. Скандал розгорнувся на тлі ширшої кризи в Грузії: політичної нестабільності через протести проти фальсифікації виборів і затримки вступу до ЄС, а також масової еміграції молоді — у 2023 році 70% із 163 480 емігрантів були

[17] https://www.occrp.org/en/project/scam-empire/from-rumors-to-ugly-reality-georgians-stunned-by-scam-call-centers-cruelty

молодшими за 30 років. Цей контекст підкреслює системні проблеми, які штовхають молодь до таких дій, і водночас ускладнює пошук рішень. Стаття завершується відкритим питанням про те, чи варті були ці гроші ганьби й моральної деградації, залишаючи читачів із відчуттям тривоги за майбутнє грузинського суспільства.

Зупинення Kidflix, великої платформи сексуальної експлуатації дітей[18]

У результаті масштабної міжнародної операції під назвою "Operation Stream" правоохоронні органи ліквідували одну з найбільших у світі платформ для розповсюдження матеріалів сексуального насильства над дітьми — "Kidflix". Ця платформа, створена у 2021 році, налічувала близько 1,8 мільйона користувачів по всьому світу та містила понад 91 000 унікальних відео з матеріалами сексуального насильства над дітьми.

"Kidflix" відрізнялася від інших подібних платформ тим, що дозволяла не лише завантажувати, але й переглядати відео у режимі стрімінгу. Користувачі здійснювали платежі за допомогою криптовалют, які конвертувалися в токени для доступу до контенту. Крім того, учасники могли заробляти токени, завантажуючи нові матеріали, перевіряючи назви та описи відео, а також присвоюючи їм категорії.

Операція "Operation Stream" розпочалася у 2022 році та охопила 35 країн. У березні 2025 року правоохоронці Німеччини та Нідерландів вилучили центральний сервер платформи, що містив близько 72 000 відео. У ході операції було ідентифіковано майже 1 400 підозрюваних, з яких 79 були заарештовані за розповсюдження та зберігання матеріалів сексуального насильства над дітьми; деякі з них також підозрюються у безпосередньому вчиненні насильства над дітьми.

Під час обшуків було вилучено понад 3 000 електронних пристроїв, а 39 дітей були взяті під захист. Європол назвав цю операцію найбільшою в історії агентства у боротьбі з експлуатацією дітей. Вона підкреслює зростаючу загрозу сексуальної експлуатації дітей у цифрову епоху та необхідність міжнародної співпраці для протидії таким злочинам.

Ліквідація платформи "Kidflix" є значним кроком у боротьбі з онлайн-експлуатацією дітей. Цей успіх став можливим завдяки скоординованим зусиллям міжнародних правоохоронних органів та підкреслює важливість продовження глобальної співпраці для захисту найуразливіших членів суспільства.

Для загального розвитку

Кейс: Як 20 мільярдів доларів було переведено з Росії до решти світу[19]

У період з 2010 по 2014 рік діяла масштабна схема відмивання грошей, відома як "Російська пральня" (Russian Laundromat), через яку з росії було виведено від 20 до 80 мільярдів доларів США. Ця схема охоплювала складну мережу офшорних компаній, підроблених позик та корумпованих суддів, залучаючи банки в Молдові та Латвії для переказу коштів у різні країни світу.

[18] https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users
[19] https://www.amlcube.com/post/the-russian-laundromat-how-20-billion-were-transferred-from-russia-to-the-rest-of-the-world

Механізм схеми

Ключовим елементом "Російської пральні" було створення фіктивних компаній у Великій Британії, Кіпрі та Новій Зеландії. Ці компанії укладали між собою фіктивні кредитні угоди. Потім одна з компаній "не виконувала" свої зобов'язання, що призводило до судових рішень у Молдові, які зобов'язували боржника сплатити значні суми. Гарантами за цими позиками виступали російські компанії, які, відповідно до судових рішень, переводили кошти на молдовські рахунки. Після цього гроші переводилися на рахунки в латвійських банках, звідки розподілялися по всьому світу.

Масштаби та наслідки

За даними розслідувань, у схемі брали участь близько 500 осіб, включаючи російських олігархів, банкірів та осіб, пов'язаних із ФСБ. Більше половини відмитих коштів пройшли через британські банки, такі як HSBC, Royal Bank of Scotland та Coutts. Крім того, значні суми були переведені через банки в інших країнах, включаючи США.

Роль В'ячеслава Платона

Молдовський бізнесмен та колишній депутат В'ячеслав Платон вважається одним з головних організаторів цієї схеми. У 2017 році він був засуджений до 18 років ув'язнення за звинуваченнями у відмиванні грошей. Однак у 2021 році його виправдали та звільнили.

Розслідування та викриття

Схема була розкрита в 2014 році журналістським розслідуванням, проведеним Organized Crime and Corruption Reporting Project (OCCRP). Вони отримали доступ до банківських документів, які детально описували приблизно 70 000 транзакцій, пов'язаних із цією схемою. Розслідування показало, як складна мережа компаній та банків використовувалася для відмивання грошей та виведення їх з росії.

Висновки

"Російська пральня" продемонструвала, як корумповані особи можуть використовувати міжнародну фінансову систему для відмивання величезних сум грошей. Цей випадок підкреслив необхідність посилення міжнародного співробітництва та контролю для запобігання подібним схемам у майбутньому.

Роль OSINT у боротьбі з відмиванням коштів

Сьогодні ми говоримо про OSINT (Open Source Intelligence - Розслідування на основі відкритих джерел) і дедалі важливішу роль, яку відіграють відкриті джерела в процесах протидії відмиванню коштів, які здійснюють підзвітні установи.

Щоб виконати ефективну оцінку ризиків клієнтів, важливо покладатися на надійну, актуальну та легкодоступну інформацію. OSINT відповідає цій потребі, бездоганно інтегруючись у процеси належної перевірки клієнта, профілювання ризиків і процедури постійного моніторингу.

Інформацію з відкритих джерел, таку як державні веб-сайти, публічні реєстри, новинні статті, соціальні мережі та вільно доступні бази даних, можна використовувати для:

- Визначення потенційної причетності до судових процесів або фінансових скандалів
- оцінки суспільної репутації окремих осіб чи компаній
- реконструкції структури власності та відповідних економічних відносин
- виявлення впливу конкретних географічних або галузевих ризиків

Особливо актуальним у контексті ПВК є використання OSINT для збору та аналізу чотирьох ключових категорій інформації:

1. Бенефіціарна власність, щоб визначити, хто в кінцевому підсумку контролює юридичні особи та запобігти приховуванню справжніх бенефіціарів;
2. Негативні згадки у ЗМІ, тобто загальнодоступні негативні новини, які можуть свідчити про загрозу репутації або зв'язки з незаконною діяльністю;
3. Політично значущі особи (PEP), які потребують посиленої належної перевірки через підвищену схильність до корупційних ризиків;
4. Санкційні списки, як національні, так і міжнародні, які ідентифікують фізичних та юридичних осіб, на яких поширюються обмеження, пов'язані з загрозами безпеці, тероризмом або іншою протиправною поведінкою.

Інтеграція цих джерел у процеси з належної перевірки зміцнює профілактичні можливості системи, забезпечуючи більш комплексний і динамічний аналіз ризиків. Вкрай важливо, щоб ця діяльність здійснювалася з дотриманням правил захисту даних і базувалася на принципах пропорційності та відстеження.

Ваша думка важлива!

1. Як ви визначаєте баланс між кількістю та якістю SAR у вашій установі? Чи є у вас внутрішні критерії, які допомагають аналітикам ухвалювати рішення про їх подання?
2. Які виклики ви бачите при поданні SAR щодо клієнтів, що оперують криптовалютами або використовують DeFi? Чи вважаєте ви, що Travel Rule в її поточному вигляді буде ефективним в українському контексті?
3. Які з індикаторів ризику, пов'язаних із CASPs, ви вважаєте найбільш складними для виявлення? Які практики вам вже довелося адаптувати у відповідь на розвиток ринку криптоактивів?
4. Чи спостерігали ви у своїй практиці операції, які можуть свідчити про непрямий обхід санкцій? Як у вашій установі організовано внутрішній порядок реагування або передачі таких випадків для подальшого аналізу?
5. Чи вважаєте ви, що чинні інструменти ПВК/ФТ достатньо ефективно ідентифікують випадки державно-кримінальної кооперації (геокримінальності)? Які аналітичні підходи або індикатори могли б посилити таку ідентифікацію?
6. Які OSINT-джерела ви використовуєте у своїх перевірках в контексті ПВК/ФТ/ФР і в яких процессах ви вважаєте їх найбільш цінними?

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-2025-14

Бюлетень є волонтерською 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].