ДЕРЖАВНА СЛУЖБА ФІНАНСОВОГО МОНІТОРИНГУ УКРАЇНИ
THE STATE FINANCIAL MONITORING SERVICE OF UKRAINE
Україна

Серійний номер: ДСФМУ-ДК-2024-039
Грудень 2024

Методологічний Бюлетень

Мета

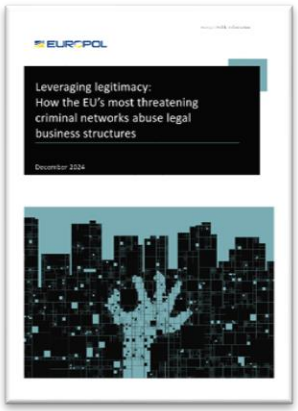
Методологічний Бюлетень видається Держфінмоніторингом на регулярній основі починаючи з квітня 2024 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено 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

Тіньова економіка ЄС: як злочинні мережі використовують легальні бізнес-структури для зміцнення своєї влади [1]



Документ глибоко аналізує способи, якими організовані злочинні мережі в ЄС використовують легальні бізнес-структури (ЛБС) для здійснення, маскування та розширення своєї злочинної діяльності. Основний акцент робиться на масштабі загрози, типах діяльності, які підтримуються ЛБС, і секторах економіки, найбільш вразливих до інфільтрації. У документі надається структурований аналіз того, як легальні бізнес-структури слугують інструментами для підтримки кримінальних схем, відмивання грошей, ухилення від сплати податків і здійснення транснаціональної злочинної діяльності.

Однією з ключових знахідок є те, що 86% найнебезпечніших злочинних мереж в ЄС використовують ЛБС. Це робить такі

[1] https://media.licdn.com/dms/document/media/v2/D4E1FAQHkapPP41Cyng/feedshare-document-pdf-analyzed/B4EZPdybNIGwAc-/0/1734592814265?e=1736380800&v=beta&t=7RWqC4mIzVA8JHn4oKQCZvqHdEWNvdeFjU3jVodOOaY

структури центральним елементом злочинного середовища, дозволяючи уникати уваги правоохоронців, маскувати походження нелегальних доходів і зміцнювати свій вплив у легальній економіці. ЛБС часто служать прикриттям для транспортування заборонених товарів, проведення шахрайських фінансових операцій або реалізації схем відмивання грошей. Зловживання може включати як використання існуючих компаній без відома їх керівників, так і створення нових компаній, які повністю контролюються злочинними угрупованнями.

Документ підкреслює, що зловживання ЛБС є явищем із широкою географією. Найчастіше експлуатуються компанії, розташовані в межах ЄС або в сусідніх країнах, що спрощує логістику та дозволяє ефективніше здійснювати незаконні операції. У багатьох випадках компанії створюються для конкретних злочинних схем і після виконання свого призначення ліквідуються, що ускладнює їхній моніторинг та розслідування.

Вразливі сектори включають логістику, будівництво, готельний бізнес, фінансовий сектор та ринки нерухомості. Логістичні компанії використовуються для перевезення наркотиків, контрабанди та транспортування нелегальних товарів. Будівельний сектор часто служить платформою для інвестування та легалізації нелегальних доходів, а готельний бізнес використовується як прикриття для таких видів діяльності, як рекет або наркоторгівля.

Дослідження також наголошує, що ЛБС відіграють важливу роль на всіх стадіях злочинного процесу, включаючи планування, транспортування незаконних товарів і відмивання коштів. ЛБС можуть бути використані для створення фіктивних контрактів, виписки підроблених рахунків та створення банківських рахунків для приховування слідів фінансових операцій.

Висновки:

- **Більшість злочинних мереж використовують ЛБС** для легалізації доходів через придбання нерухомості, створення фіктивних компаній або реєстрацію підставних осіб.
- **Логістика, готельний бізнес та будівництво** найбільше піддаються впливу через високу оборотність готівки. Для зменшення ризиків необхідно посилити перевірку компаній в цих секторах та вдосконалити систему аудиту.
- **Злочинні мережі маскують свої схеми**, змішуючи легальну та нелегальну діяльність, використовуючи фіктивні документи та підставних осіб.
- **Для протидії зловживанням ЛБС потрібен спільний підхід** правоохоронних органів, регуляторів та приватного сектору. Рекомендується створення спеціальних робочих груп для оперативного виявлення та ліквідації таких схем.

Документ наголошує на необхідності міжнародної координації для боротьби з цією проблемою. Він пропонує залучення правоохоронців, регуляторів, приватного сектора та громадянського суспільства для створення ефективної системи протидії. Такі заходи включають вдосконалення системи перевірки бенефіціарів, посилення фінансового моніторингу та розвиток механізмів для виявлення схем, пов’язаних із ЛБС.

Таким чином, цей документ є ключовим аналітичним ресурсом для розуміння того, як злочинні мережі використовують економічну інфраструктуру для досягнення своїх цілей. Він також визначає пріоритети для розробки політик, спрямованих на захист економічної цілісності та забезпечення верховенства права в ЄС.

Стандарти доброчесності у політичному фінансуванні: Дорожня карта для прозорості [2]

Документ є масштабним стратегічним керівництвом, яке визначає стандарти та принципи для забезпечення чесності, прозорості й відповідальності у фінансуванні політичних процесів. Його мета – створення політичних фінансових систем, які мінімізують корупційні ризики, забезпечують рівний доступ до участі в політичному житті та зміцнюють довіру суспільства до політичних інституцій.

Основою документа є переконання, що прозорість є ключовим елементом у запобіганні корупції та гарантуванні підзвітності політичних суб'єктів. Інформація про джерела фінансування, витрати та донорів має бути доступною виборцям у зручному та відкритому форматі. Це дозволить суспільству робити усвідомлений вибір і контролювати процеси фінансування. Однак реальна прозорість потребує не лише публікації даних, а й перевірки їх якості незалежними органами, наділеними відповідними повноваженнями.

Важливою складовою є впровадження принципу "чистих" грошей у політиці. Документ акцентує увагу на необхідності запобігання проникненню нелегальних коштів у політичні кампанії, що досягається через заборону анонімних пожертв, регулювання криптовалютних транзакцій і введення практик "знай свого донора" (KYC). Залучення коштів має здійснюватися виключно з легальних джерел, що відповідають інтересам суспільства, а не вузьких груп впливу. Крім того, сторонні організації, які прагнуть впливати на результати виборів, повинні підлягати звітності та контролю.

Документ також приділяє значну увагу створенню рівних умов для політичних суб'єктів. Це включає обмеження розміру пожертв і витрат на кампанії, а також забезпечення доступу до державного фінансування для партій та кандидатів. Особливий акцент зроблено на підтримці недостатньо представлених груп, таких як жінки, молодь, етнічні меншини, через цільове фінансування і субсидії. Водночас ефективність таких заходів залежить від прозорості критеріїв розподілу фінансування та належного моніторингу їх використання.

Гендерна рівність є ще одним критично важливим аспектом документа. Для забезпечення рівного доступу жінок до політичної участі пропонуються заходи, які передбачають обов'язкове виділення частини державного фінансування на підтримку жіночих кандидатур і публікацію гендерно розподіленої інформації про фінансові ресурси. Це допоможе долати бар'єри, зумовлені дискримінацією та недостатнім доступом до фінансування.

Окремий розділ присвячено забезпеченню нейтральності держави у виборчих процесах. Документ чітко окреслює заборону використання державних ресурсів для виборчих кампаній, зокрема фінансових, матеріальних і людських. Для забезпечення дотримання цього принципу пропонується наділити наглядові органи необхідними повноваженнями для моніторингу, розслідування та накладення санкцій за порушення.

[2] https://images.transparencycdn.org/images/Integrity-Standards_English.pdf

Останнім ключовим аспектом є відповідальність та підзвітність. Документ наголошує на важливості створення незалежних органів нагляду, які володіють фінансовою автономією та мають можливості для ефективного контролю за політичними фінансами. Пропонується також посилити міжвідомчу співпрацю між виборчими комісіями, антикорупційними агентствами, фінансовими розвідками та правоохоронними органами. Для забезпечення ефективності цієї системи необхідно встановити суворі санкції за порушення правил фінансування та сприяти залученню громадянського суспільства до моніторингу.

Висновки:

- **Політичні суб'єкти мають зобов'язання забезпечувати повну прозорість** своїх фінансових операцій через електронні системи звітності. Необхідно запровадити публікацію звітів у режимі реального часу, що значно зменшить ризик корупції.
- **Обов'язковим є посилення фінансового моніторингу**, особливо виявлення анонімних пожертв і регулювання криптовалютних транзакцій, для уникнення проникнення нелегальних коштів у політику.
- **Встановлення лімітів** на розміри пожертв і витрат, а також забезпечення доступу до державного фінансування сприятиме справедливому розподілу політичних можливостей.
- **Ефективний контроль** за дотриманням стандартів можливий лише за умови створення незалежних органів нагляду з адекватним фінансуванням і необхідними інструментами.

Таким чином, документ є детальною дорожньою картою для реформування систем політичного фінансування. Його реалізація може суттєво підвищити рівень довіри до політичних процесів, зменшити вплив корупційних практик та забезпечити справедливу конкуренцію в політичному середовищі.

Застосування машинного навчання для виявлення аномалій: інноваційний підхід до фінансового моніторингу [3]

Документ досліджує можливості використання методів машинного навчання для виявлення аномалій у діяльності пунктів обміну валют (MSB — Money Services Business) у Малайзії. Центральний банк Малайзії збирає транзакційні дані від ліцензованих MSB з 2017 року, що дозволяє проводити моніторинг галузі поза межами фізичних перевірок. Однак через великий обсяг даних та значну кількість операторів, регулятори стикаються з труднощами у своєчасному виявленні ризикових моделей поведінки на рівні окремих точок обслуговування. Це дослідження пропонує підхід машинного навчання, який поєднує різні методи, для автоматизації процесу виявлення аномалій на основі транзакційних і геолокаційних даних.

Методологія включає використання алгоритму Isolation Forest (IF) для початкового виявлення аномальних спостережень у наборі даних, який складається з інформації про транзакції, клієнтів та місцезнаходження пунктів обміну. Дані агрегуються на рівні окремих точок

[3] https://www.bis.org/ifc/publ/ifcwork23.pdf

обслуговування та доповнюються часовим виміром, що дозволяє враховувати сезонні коливання та забезпечує регулярний моніторинг. IF модель генерує спеціальні позначки для подальшого навчання моделей, таких як Light Gradient Boosting Machine (LightGBM) та Random Forest, які показали найвищу точність у класифікації аномалій. LightGBM досягла найвищих показників точності (93,1%) та F1-оцінки (74,3%).

Особлива увага приділяється поясненню роботи моделей через використання Shapley Additive Explanations (SHAP), що дозволяє визначити, які саме характеристики найсуттєвіше впливають на ідентифікацію аномалій. Найважливішими характеристиками були визнані показники, пов'язані з демографічними даними клієнтів, транзакційними моделями та геолокацією. Наприклад, точки обміну валют, які переважно обслуговують клієнтів із високоризикових юрисдикцій або мають значний обсяг транзакцій у нестандартний час доби, частіше визначалися як аномальні.

Практична реалізація результатів включає створення геопросторової панелі Power BI, яка дозволяє наглядовим органам візуалізувати розташування пунктів обміну, класифікованих як аномальні або нормальні. Панель також забезпечує детальну інформацію про кожен об'єкт, включаючи основні характеристики, що вплинули на прогноз. Це значно спрощує процес планування та реалізації наглядових заходів, дозволяючи регуляторам зосереджуватися на високоризикових точках обслуговування.

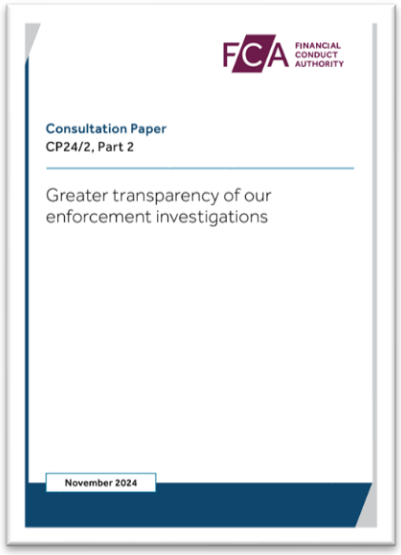
У дослідженні також пропонуються шляхи вдосконалення моделі, зокрема шляхом інтеграції додаткових джерел даних, таких як інформація від правоохоронних органів або підрозділів фінансової розвідки. Зворотний зв'язок від наглядових органів щодо точності прогнозів також визнано ключовим фактором для зменшення хибно-позитивних результатів.

Цей підхід демонструє значний потенціал для підвищення ефективності моніторингу діяльності MSB, знижуючи навантаження на ресурси та покращуючи здатність регуляторів вчасно реагувати на нові ризики у сфері ПВК/ФТ. Документ підкреслює важливість інноваційних наглядових технологій (suptech) у зміцненні системи фінансового моніторингу.

Висновки:

- **Ефективність машинного навчання:** Слабко навчена модель на основі Isolation Forest та LightGBM показала найвищу точність (93,1%) для виявлення аномалій, що дозволяє суттєво скоротити час і ресурси на ручний аналіз.
- **Геолокаційні та транзакційні дані як ключові:** Дані про розташування та тип клієнтів є найбільш інформативними для визначення ризикованих пунктів обслуговування, що акцентує увагу на важливості якісного збору та аналізу цих даних.
- **Покращення через інтеграцію даних:** Включення інформації від правоохоронних органів та зворотного зв'язку від наглядових органів може знизити рівень хибнопозитивних результатів і підвищити точність прогнозування.

Прозорість у дії: як FCA змінює підхід до розслідувань для захисту споживачів та фінансової стабільності [4]



Документ представлений Financial Conduct Authority (FCA) і спрямований на вдосконалення підходів до прозорості в рамках регуляторної діяльності. Основна ідея полягає у створенні механізму, що дозволить публічно повідомляти про розпочаті розслідування в обмежених випадках, коли це є в суспільних інтересах. Пропозиції FCA відображають необхідність врахування суспільної користі від раннього інформування споживачів, потенційного впливу на компанії, а також захисту репутації фінансових ринків Великобританії.

FCA обґрунтовує свої пропозиції потребою у кращому захисті споживачів, адже своєчасне повідомлення про розслідування може допомогти зменшити шкоду та підвищити довіру до регулятора. Зокрема, споживачі зможуть приймати зважені рішення, уникати недобросовісних посередників або вчасно отримувати інформацію про можливу компенсацію. Пропозиції також передбачають, що ширша прозорість допоможе стимулювати компанії до вдосконалення своїх внутрішніх процесів, підвищуючи стандарти дотримання законодавчих вимог. Крім того, більша відкритість розслідувань сприятиме заохоченню свідків та інформаторів до співпраці з FCA.

У документі наголошується, що підхід до прозорості не змінюватиме практики нагляду, а буде застосовуватися лише до розслідувань у рамках процедур правозастосування. FCA окреслює чіткі критерії, коли публічне оголошення відповідає суспільним інтересам. До них належать фактори, такі як можливість попередження шкоди споживачам, підтримка довіри до фінансового ринку, освітній ефект для інших учасників ринку та забезпечення публічної відповідальності FCA перед суспільством. Водночас пропозиції враховують потенційні ризики для компаній, включаючи вплив на їх репутацію, ринкову вартість та фінансову стабільність. Передбачено, що FCA надаватиме компаніям 10 робочих днів для підготовки своїх зауважень до публікації оголошення, що дає змогу врахувати всі аргументи та потенційні ризики.

У документі також розглядаються реальні кейси з минулого, які демонструють можливості нового підходу. Наприклад, у випадку з British Steel Pension Scheme раннє оголошення про розслідування могло б попередити додаткові збитки споживачів, тоді як у випадку з CB Payments Limited (Coinbase Group) прозорість могла б сприяти підвищенню довіри до регулятора в контексті боротьби з відмиванням коштів у секторі криптовалют. Аналіз кейсів підкреслює важливість збалансованого підходу, де враховуються як потенційні вигоди для суспільства, так і можливі ризики для компаній.

Документ також пропонує створення інструменту для анонімного інформування, коли оголошення назви компанії може завдати значної шкоди. Наприклад, для розслідувань у сфері кібербезпеки або відмивання коштів публікація загальних висновків без зазначення конкретних компаній може мати значний освітній ефект і сприяти запобіганню правопорушенням.

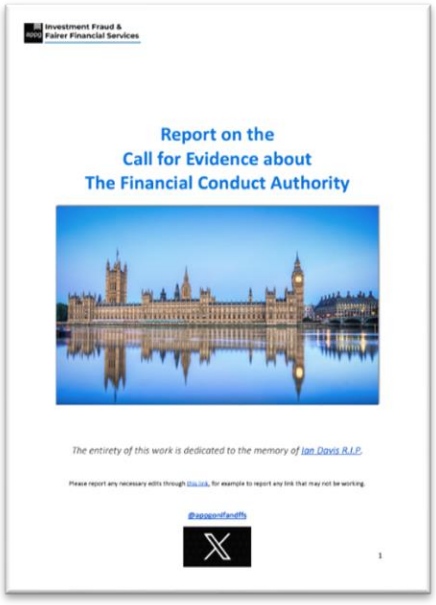
[4] https://www.fca.org.uk/publication/consultation/cp24-2-part-2.pdf

Висновки:

- **Раннє інформування** про розслідування допоможе захисту споживачів та покращенню довіри до ринку.
- **Зміни у підході до прозорості** вимагають інтегрованого процесу, що враховує вплив на компанії.
- **Запропоновані критерії прозорості** зміцнюють принципи належного регулювання.
- **Прозорість сприятиме покращенню процесів** у галузі через приклади найкращих практик.

У підсумку FCA визнає, що запропоновані зміни є еволюцією, а не революцією в їхній політиці, і пропонує продовжувати обговорення з усіма зацікавленими сторонами до остаточного ухвалення рішень у 2025 році. Ця ініціатива демонструє прагнення FCA до прозорості, справедливості та забезпечення довіри до фінансової системи Великобританії.

Оцінка ефективності FCA: ключові виклики та перспективи реформування регулятора фінансових послуг Великобританії [5]



Документ, представлений Багатопартійною парламентською Групою з протидії інвестиційному шахрайству та справедливості фінансових послуг (All-Party Parliamentary Group (APPG) on Investment Fraud and Fairer Financial Services), є масштабним звітом, спрямованим на аналіз діяльності Financial Conduct Authority (FCA), ключового регулятора фінансового сектору Великобританії. Основною метою дослідження було виявлення проблемних аспектів роботи FCA через збір свідчень від осіб, які стикалися з діяльністю цього органу, і формулювання рекомендацій щодо підвищення його ефективності.

FCA, як головний регулятор, відіграє важливу роль у забезпеченні фінансової стабільності, захисті споживачів і підтримці довіри до фінансових послуг. Проте численні скандали останніх років, зокрема, пов'язані з інвестиційним шахрайством, банківськими порушеннями та неетичними практиками у фінансовому секторі, підкреслюють його недоліки. Ці проблеми спонукали APPG до ініціювання відкритого збору свідчень, який тривав два з половиною роки і став найбільшим у своєму роді дослідженням у Великобританії.

Документ базується на свідченнях 174 респондентів, серед яких були жертви фінансового шахрайства, малий та середній бізнес, який постраждав від неправомірних дій банків, а також колишні співробітники FCA та інші зацікавлені сторони. Вони поділилися своїм досвідом взаємодії з FCA, підкреслюючи низку системних недоліків, таких як відсутність прозорості, повільна реакція, недостатня захищеність споживачів і неспроможність регулятора ефективно використовувати свої повноваження.

Особлива увага в документі приділена організаційній культурі FCA, яка, за словами респондентів, має серйозні вади. Регулятору закидають закритість, низький рівень

[5] https://www.appgifffs.org/wp-content/uploads/2024/11/FINAL-Call-for-Evidence-Report-PUBLIC-1.pdf

підзвітності, недостатню підтримку свідків, які надають інформацію про порушення, та відсутність активних дій щодо попередження шахрайства. Численні респонденти також вказували на проблеми з «регуляторним захопленням», коли інтереси великих фінансових установ домінують над захистом споживачів.

Звіт містить детальний аналіз свідчень і підсумовує ключові теми, включаючи проблеми прозорості FCA, його імунітет від цивільної відповідальності, конфлікти інтересів і недостатню ефективність використання наявних повноважень. Результати дослідження підкріплені конкретними прикладами із досвіду респондентів, які вказують на серйозні системні недоліки регулятора.

Значна частина звіту присвячена рекомендаціям, розробленим панеллю експертів. Рекомендації включають створення нової місії FCA, орієнтованої на споживачів, посилення прозорості та підзвітності, зміни в системі управління й фінансування регулятора, а також забезпечення належного захисту свідків. У разі невдачі запропонованих реформ автори документа не виключають можливості проведення радикальних змін у регуляторному ландшафті, включаючи створення нових органів і перегляд розподілу повноважень.

Висновки:

- **Необхідність реформ:** FCA не виконує своїх функцій на належному рівні. Необхідно запровадити зміни в організаційній культурі, системі управління та правовій базі.
- **Посилення захисту споживачів:** FCA повинна забезпечити більш оперативну реакцію на шахрайства, підвищити свою ефективність у захисті прав споживачів та відновленні їх фінансових втрат.
- **Робота зі свідками:** Розробити механізми захисту для свідків і забезпечити належну обробку наданої ними інформації.
- **Періодичні перевірки:** Ввести незалежний моніторинг виконання реформ FCA, що дозволить оцінювати прогрес і вплив змін на споживачів.

Цей звіт підкреслює гостру потребу у швидких і рішучих діях для відновлення довіри до регулятора і фінансової системи загалом. Автори наголошують, що зміни повинні відбуватися прозоро й з урахуванням інтересів усіх зацікавлених сторін. У висновках зазначено, що лише реальні кроки до реформ зможуть попередити подальші кризи і скандали, які загрожують не лише репутації FCA, але й стабільності фінансового сектору Великобританії.

Гармонізація регулювання криптоактивів у ЄС: Керівні настанови ESMA щодо класифікації фінансових інструментів [6]

Документ від Європейського управління з цінних паперів та ринків (ESMA) спрямований на створення гармонізованого підходу до регулювання криптоактивів у межах Європейського Союзу. З огляду на прийняття Регламенту щодо ринків криптоактивів (MiCA) та його інтеграцію з чинною нормативною базою, такий підхід є ключовим для усунення регуляторних прогалин і забезпечення стабільності ринків.

[6] https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf

Основний зміст документа полягає у визначенні умов і критеріїв для класифікації криптоактивів як фінансових інструментів відповідно до визначень Директиви про ринки фінансових інструментів (The Markets in Financial Instruments Directive (MiFID II)) . Це має критичне значення, адже від того, чи підпадає криптоактив під регулювання MiFID II, залежить його правовий статус і застосовувана нормативна база. Документ ґрунтується на принципах технологічної нейтральності та «сутність понад форму», що означає, що класифікація активів базується на їхніх економічних і юридичних характеристиках, а не на технології, яка лежить в їх основі. Такий підхід дозволяє однаково регулювати активи з подібними ризиками, незалежно від їхньої цифрової природи.

У документі розглядається складність і неоднорідність підходів до класифікації фінансових інструментів у різних країнах-членах ЄС, що може призводити до регуляторного арбітражу і фрагментації ринку. Щоб уникнути цього, ESMA пропонує чіткі умови та критерії, які повинні забезпечити узгодженість застосування MiFID II в різних юрисдикціях. Важливо, що пропоновані керівні настанови не охоплюють усіх типів фінансових інструментів, а лише ті, які одночасно підпадають під визначення криптоактивів за MiCA і фінансових інструментів за MiFID II.

Документ також детально описує специфічні аспекти класифікації окремих категорій криптоактивів, таких як NFT, гібридні токени, стейкінгові активи, а також інструменти колективного інвестування. Для кожної категорії наведено основні критерії та підходи до оцінки їхніх економічних характеристик, прав власності та функцій, які вони виконують. Особливу увагу приділено гібридним токенам, які поєднують риси різних фінансових і нефінансових активів. У таких випадках пропонується ієрархічний підхід, де фінансові характеристики мають переважне значення.

Висновки:

- **Єдність регуляторного підходу:** Для уникнення фрагментації ринку необхідно впровадити гармонізовані підходи до класифікації криптоактивів як фінансових інструментів, засновані на єдиних критеріях і принципах.
- **Технологічна нейтральність:** Забезпечення регуляторного підходу, який базується на характеристиках активів, а не на їх технологічній основі, для створення справедливих умов конкуренції.
- **Акцент на захисті інвесторів:** Запропоновані критерії класифікації підвищують захист інвесторів завдяки застосуванню регулятивної бази MiFID II, особливо у випадках гібридних і складних токенів.
- **Динамічність і гнучкість:** Регуляторні органи та учасники ринку повинні регулярно переоцінювати класифікацію криптоактивів у світлі змін їх економічних функцій.

Документ містить оцінку витрат і вигод від впровадження керівних настанов. Серед основних переваг виділено підвищення захисту інвесторів, зниження ризиків неправильної класифікації активів і створення прозорого ринкового середовища. Зазначено, що регуляторні органи та учасники фінансових ринків можуть зазнати мінімальних витрат, пов’язаних із впровадженням нових процедур класифікації. Водночас гармонізація підходів сприятиме зниженню адміністративних витрат для учасників ринку, які працюють у кількох юрисдикціях.

Завершуючи, ESMA наголошує, що запропоновані керівні настанови спрямовані на посилення регуляторної узгодженості, зменшення правової невизначеності та сприяння інноваціям у межах безпечного і прозорого ринкового середовища. Їх імплементація запланована після завершення періоду перекладу та адаптації для національних нормативних систем країн-членів ЄС.

Регулювання

Реформа системи ПВК/ФТ у ЄС: нові правила для провайдерів криптоактивів і розширення функцій [7]

Консультаційний документ присвячений змінам до Регуляторних Технічних Стандартів (RTS), викладених у Делегованому Регламенті ЄС 2018/1108. Основна мета цих змін – адаптація існуючої нормативної бази до сучасних викликів, пов'язаних із розширенням регуляторного охоплення на провайдерів послуг криптоактивів (CASP). Це рішення стало наслідком внесення поправок до Директиви (EU) 2015/849, яка зобов'язує держави-члени ЄС встановлювати однакові стандарти у сфері протидії відмиванню коштів (ПВК) і фінансуванню тероризму (ФТ) для всіх типів фінансових установ, включно з CASP.

Документ детально розглядає питання призначення центральних контактних пунктів (ЦКП) для EMI, PSP та CASP, які діють на території держав-членів ЄС через установи, що не мають статусу філій. ЦКП слугують ключовою ланкою для забезпечення відповідності місцевим вимогам у сфері ПВК/ФТ і представляють інтереси установ перед регуляторами. Основні функції ЦКП включають впровадження та моніторинг політик ПВК/ФТ, навчання персоналу, надання звітності регуляторним органам та забезпечення відповідності місцевим законам.

Документ пояснює, що CASP можуть працювати у хост-країнах ЄС через електронні платформи, що створює виклики для нагляду у сфері ПВК/ФТ через їхню децентралізовану природу. Для вирішення цього питання пропонується розширити критерії призначення ЦКП на CASP. Серед них визначено ключові показники, зокрема розмір і обсяг діяльності, а також рівень ризику, який асоціюється з їхньою операційною моделлю. Наприклад, якщо сукупний обсяг транзакцій перевищує 3 млн євро за фінансовий рік, призначення ЦКП стає обов'язковим.

EBA також пропонує залишити незмінними положення для PSP та EMI, оскільки чинна нормативна база є ефективною, а внесення нових вимог могло б спричинити додаткові витрати для зацікавлених сторін. Разом із тим, додавання CASP до існуючих регуляторних стандартів мінімізує додаткові витрати для регуляторів та учасників ринку.

Документ також передбачає публічні консультації до лютого 2024 року, щоб забезпечити врахування зауважень зацікавлених сторін. Останній варіант тексту буде підготовлений до середини 2025 року, а впровадження нових положень очікується у 2026 році.

У контексті впровадження змін акцент зроблено на гармонізації підходів між CASP, PSP та EMI, що сприятиме посиленню системи ПВК/ФТ в ЄС. Водночас документ визнає, що специфіка роботи CASP потребує адаптації певних положень, наприклад, щодо визначення «установи», яка може бути суто віртуальною. Таким чином, запропоновані зміни покликані забезпечити прозорість, знизити ризики фінансових злочинів і сприяти стабільності фінансової системи ЄС.

[7] https://www.eba.europa.eu/sites/default/files/2024-12/3e76c3f2-b611-40f7-87a0-7baf3978fa0c/CP%20on%20amending%20RTSon%20%20CCP.pdf

Санкції

США наклали нові санкції на «Північний потік-2» [8]

Сполученими Штатами Америки було запроваджено санкції щодо суб'єктів, пов'язаних із проєктом газопроводу «Північний потік-2». Цей крок є продовженням зусиль США, спрямованих на обмеження російського впливу на енергетичний сектор Європи та на перешкоджання використанню енергетичних ресурсів як інструменту геополітичного тиску. Санкції було накладено на низку компаній, фізичних осіб і суден, що брали участь у реалізації проєкту, який мав на меті збільшення поставок російського газу до Німеччини через Балтійське море.

Під санкції потрапили суб'єкти, вже раніше згадані в контексті «Закону про захист енергетичної безпеки Європи» (PEESA), а також нові суб'єкти, які набули активів або забезпечували підтримку реалізації проєкту. Зокрема, це включає такі організації, як «Самара» і «Мортранссервіс», а також судна «Академік Черський», «Фіона» та інші. Додатково зазначається, що активи цих суб'єктів, які перебувають у юрисдикції США або під контролем американських осіб, будуть заблоковані, а будь-які фінансові чи комерційні операції з ними заборонені без спеціального дозволу Управління з контролю за іноземними активами (OFAC).

Важливим аспектом санкцій є їхній символічний і стратегічний характер. Документи наголошують, що США прагнуть запобігти відновленню проєкту, який вже зазнав серйозних втрат після вибухів на газопроводах «Північний потік-1» і «Північний потік-2» у 2022 році. Ці події були кваліфіковані західними країнами як ймовірна диверсія, тоді як Росія відкидає свою причетність до пошкоджень.

Санкції також підкреслюють зусилля США щодо сприяння енергетичній диверсифікації в Європі. У відповідь на російське використання газу як політичного інструменту, країни Європейського Союзу значно зменшили залежність від російського газу, збільшивши імпорт зрідженого природного газу (СПГ) із США та інших постачальників, інвестуючи у відновлювані джерела енергії та розширюючи інфраструктуру для регазифікації.

Акцентується увага на прагненні США забезпечити, щоб усі суб'єкти, які залучені до порушень міжнародного права або підтримують агресію Росії, стикалися з економічними наслідками. Крім того, вони демонструють спільну стратегію західних країн, яка спрямована на посилення тиску на Росію з метою її ізоляції та ослаблення фінансових можливостей для продовження військових дій в Україні. Згадане обґрунтовується довгостроковою метою санкцій – не лише покаранням, але й стимулюванням до змін у поведінці підсанкційних суб'єктів.

Таким чином, запровадження санкцій щодо «Північного потоку-2» є важливим інструментом зовнішньої політики США, який не лише підкреслює їхню підтримку енергетичної безпеки Європи, але й посилає чіткий сигнал щодо неприпустимості використання енергетики як зброї у геополітичному протистоянні.

[8] https://www.state.gov/re-imposing-sanctions-on-certain-entities-involved-in-nord-stream-2/

Звіти окремих інституцій та експертів

Кримінальне управління в серці Амазонки: Трикутник злочинності на кордоні Бразилії, Колумбії та Перу[9]

Звіт присвячений аналізу ключових подій і тенденцій 2024 року, які визначили розвиток токенізації як важливого напряму в блокчейн-індустрії. Автор фокусується на токенізації реальних фінансових активів (RWAs) і описує її зростання, зокрема у контексті інституційного впровадження, появи нових фінансових продуктів, розвитку регуляторного середовища та домінування Ethereum як основної блокчейн-платформи.

2024 рік характеризується стрімким збільшенням вартості токенізованих активів, що свідчить про зростання зацікавленості серед інституційних інвесторів. Загальна вартість токенізованих RWAs сягнула $13,59 млрд, демонструючи експоненційне зростання у порівнянні з попередніми періодами. Прогнози великих фінансових установ, таких як Standard Chartered, Citi та McKinsey, підтверджують амбітність цього сектору, оцінюючи його потенціал у трильйони доларів до кінця десятиліття. Такі перспективи підкреслюють необхідність подальшої стандартизації та вдосконалення регуляторних вимог.

Ethereum продовжує бути основною платформою для токенізації завдяки своїй надійності, широкій екосистемі та глобальному визнанню. Зокрема, токенізовані активи на базі Ethereum (за виключенням стейблкоїнів) досягли ринкової капіталізації $3,25 млрд, що становить значну частину загального ринку. Це демонструє стійкість платформи, навіть попри конкуренцію з боку інших блокчейн-рішень.

Нові фінансові продукти, зокрема стейблкоїни із відсотковою дохідністю, такі як USDY, стали значним проривом. Ці інструменти пропонують привабливу дохідність (наприклад, 4.65% APY), що відкриває нові можливості для інституцій та приватних інвесторів. Незважаючи на домінування традиційних стейблкоїнів, таких як USDT, продукти з дохідністю швидко завойовують популярність завдяки своїй привабливості для Web3.0 організацій.

Регуляторне середовище також відіграє ключову роль у розвитку галузі. Офшорні юрисдикції, такі як Кайманові острови та Британські Віргінські острови, стали центрами для випуску токенізованих активів завдяки прогресивним регуляторним ініціативам, включаючи впровадження VASP Act. Ці регіони залучають значну частину цифрових активів, хоча глобальна невизначеність у регуляторній сфері все ще залишається головним викликом. Водночас уряди Сінгапуру та Гонконгу вже почали активно працювати над впровадженням нормативних рішень для токенізації, що свідчить про поступове формування глобального консенсусу.

[9] https://media.licdn.com/dms/document/media/v2/D4D1FAQEj_0uzkljmvA/feedshare-document-pdf-analyzed/B4DZPeZMXIHUAc-/0/1734602988344?e=1736380800&v=beta&t=Hf9F-VotmsDlJmlbVt230pbvzcUo5e8FIISu4cC6NGc

Загалом, звіт наголошує, що 2024 рік став переломним моментом у визнанні токенізації як революційного інструменту для фінансового сектору. Хоча галузь перебуває на початковому етапі свого розвитку, її потенціал оцінюється як надзвичайно високий, і найближчі роки можуть стати вирішальними для її інтеграції у глобальну економіку.

Висновки:

- **Токенізація як тренд:** Інституційні прогнози оцінюють ринок токенізованих активів у $30 трлн до 2034 року. Рекомендація: зосередитись на стандартизації регуляторних вимог для прискорення глобального впровадження.
- **Перевага Ethereum:** Ethereum продовжує лідирувати серед платформ завдяки своїй надійності та широкій екосистемі.
- **Зростання дохідних стейблкоїнів:** Поява APY-продуктів відкриває нові можливості для інституцій та приватних інвесторів. Рекомендація: стимулювати розвиток альтернативних фінансових інструментів у цій ніші.
- **Регуляторні виклики:** Хоча юрисдикції на кшталт Каймановых островів демонструють успіх, регуляторна невизначеність залишається головним ризиком, тому необхідно посилювати глобальну співпрацю між регуляторами.

Розшарування у відмиванні коштів: Аналіз ризиків та інструменти протидії [10]

Документ детально описує процес відмивання коштів із фокусом на другій стадії – розшарування, яка є однією з найбільш складних та критичних у схемах відмивання. Розшарування спрямоване на маскування джерела незаконно отриманих коштів через створення складних фінансових структур і багаторівневих транзакцій. Ця стадія передбачає переміщення активів між рахунками, компаніями та юрисдикціями, що ускладнює їхнє відстеження та ідентифікацію.

Спочатку пояснюється трирівнева структура процесу відмивання коштів: розміщення (placement), розшарування (layering) та інтеграція (integration). На етапі розміщення незаконні кошти вводяться у фінансову систему, використовуючи банки, бізнес або цінні активи. Далі розшарування створює штучні бар'єри між джерелом коштів та їхнім кінцевим використанням, використовуючи складні операції, зокрема трансфери між офшорними рахунками, фіктивними компаніями та трастами, а також маніпуляції з фінансовими інструментами. Завершальна стадія – інтеграція – дозволяє використовувати кошти у легальній економіці через придбання активів, таких як нерухомість, цінні папери або предмети розкоші.

Документ також аналізує техніки, що найчастіше використовуються для розшарування. Серед них – використання компаній-оболонок в офшорних зонах, відмивання коштів у сфері торгівлі через фіктивні інвойси, створення трастів для приховування власників коштів, часті міжнародні перекази без комерційного обґрунтування та інвестиції у високоліквідні активи.

[10] https://amluae.com/wp-content/uploads/2023/11/The-Complete-eBook-on-Layering-in-Money-Laundering.pdf

Особливу увагу приділено технікам подрібнення сум (smurfing) та маніпуляцій із транзакціями, щоб уникнути підозр у межах порогових значень для звітності.

Значна частина документа присвячена важливості впровадження ефективної системи у сфері протидії відмиванню коштів (ПВК). Наголошується на необхідності використання технологій, зокрема систем штучного інтелекту (ШІ), для виявлення підозрілих транзакцій, аналізу великих обсягів даних та конфігурації правил моніторингу транзакцій. Крім того, підкреслюється важливість належної перевірки клієнтів (KYC/EDD), моніторингу транзакцій у режимі реального часу та документування індикаторів ризику.

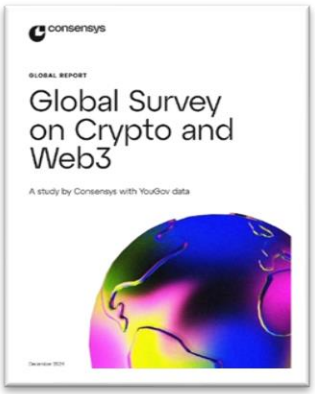
Описані «червоні прапорці», що допомагають виявити розшарування, включають часті перекази між країнами, невідповідність транзакцій фінансовому профілю клієнта, використання компаній-оболонок, інвестування у предмети розкоші, маніпуляції із валютами та фіктивні торгові угоди. Також згадані труднощі боротьби з розшаруванням, зокрема складність відстеження транзакцій через різні юрисдикції та швидкість електронних переказів.

Висновки:

- **Необхідність посилення технологічності моніторингу:** Використання систем ШІ значно підвищує ефективність ідентифікації підозрілих транзакцій, дозволяючи автоматично аналізувати великі обсяги даних та ідентифікувати закономірності.
- **Посилена перевірка клієнтів (EDD):** Включає перевірку джерела коштів, аналіз пов'язаних осіб, скринінг на зв'язки з політично значущими особами (PEP) та підозрілі транзакції.
- **Чітка документація червоних прапорців:** Організації повинні фіксувати індикатори ризику та регулярно передавати ці дані своїм співробітникам, аби швидше реагувати на потенційні загрози.
- **Міжнародна кооперація:** Важливою є участь країн у міжнародних ініціативах, для обміну інформацією щодо підозрілих транзакцій і усунення прогалин у регуляторній базі.

Документ завершується рекомендаціями щодо вдосконалення практик у сфері ПВК. Вони включають впровадження ефективних систем моніторингу, навчання персоналу, посилення регуляторного нагляду та співпраці з міжнародними організаціями, такими як FATF. Наголошується, що тільки комплексний підхід дозволяє ефективно боротися з відмиванням коштів, захищати фінансову систему та зменшувати ризики фінансування тероризму чи інших злочинів.

Глобальні крипто-тренди і Web3 у 2024 році: виклики та можливості [11]



Звіт представляє результати другого щорічного дослідження, проведеного компаніями Consensys та YouGov, щодо глобального сприйняття, обізнаності та участі суспільства у криптовалютах, блокчейні та екосистемах Web3. Дослідження, що охопило 18 652 респонденти із 18 країн світу, дозволяє простежити зміни у ставленні до цих технологій порівняно з 2023 роком. Основний акцент зроблено на дослідженні розширення участі, зростанні

[11] https://consensys.io/insight-report/web3-and-crypto-global-survey

обізнаності, основних бар'єрах для входу на ринок і потенційних можливостях, які відкриває Web3.

Документ вказує на зростання глобальної обізнаності щодо криптовалют: 93% опитаних чули про них, і 51% стверджують, що розуміють їхню суть. Африканські країни, такі як Нігерія та Південна Африка, а також Індія демонструють найвищий рівень участі у Web3, тоді як Європа та Північна Америка залишаються більш скептичними. Криптовалюти асоціюються з такими концепціями, як «майбутнє грошей», «альтернатива традиційній фінансовій системі» та «майбутнє цифрової власності». Однак бар'єри, такі як волатильність ринку, все ще стримують багатьох від участі, хоча їхня значимість знизилася порівняно з минулим роком.

Окрема увага приділена децентралізації, яку 82% респондентів вважають необхідною через надмірний вплив великих технологічних компаній. Багато хто впевнений, що децентралізація може позитивно вплинути на фінансову систему, соціальні мережі та штучний інтелект. Більшість респондентів також занепокоєні конфіденційністю даних: 83% називають її важливою, а 71% бажають отримувати вигоду від монетизації своїх персональних даних. Використання блокчейну розглядається як потенційне рішення для боротьби з ризиками, створеними ШІ, такими як генерація фейкових новин, що турбує понад 76% респондентів.

Активна участь у Web3 за останній рік зросла у всіх основних напрямках. Зокрема, використання Web3-гаманців збільшилося на 6%, як і участь у таких активностях, як збір NFT, гра у блокчейн-ігри та стейкінг. Найбільше зростання спостерігається у Нігерії, Індії, Південній Африці та на Філіппінах. Незважаючи на зростання обізнаності, концепції Web3 і NFT все ще недостатньо зрозумілі багатьом. Тим не менш, планування інвестицій у NFT протягом наступного року є значним у країнах Африки та Азії, зокрема у Нігерії (93%) та Південній Африці (87%).

Окремо досліджено сприйняття криптовалют з екологічної точки зору. У країнах Африки, Азії та Латинської Америки криптовалюти частіше вважають екологічно дружніми, на відміну від Європи, Японії та Канади, де рівень скептицизму вищий. Ethereum після переходу на алгоритм підтвердження частки володіння (Proof of Stake) став енергоефективнішим, але загальна обізнаність про це залишається обмеженою.

Висновки:

- **Прийняття криптовалют:** Глобальна обізнаність про криптовалюти досягла 93%, а інтерес до інвестування зростає, особливо в Африці (87%) та Азії (51%).
- **Проблеми конфіденційності:** 83% респондентів заявили, що конфіденційність даних є важливою, а 71% хочуть отримувати вигоду від монетизації їхніх даних.
- **Роль блокчейну у боротьбі зі ризиками, що пов'язані з ШІ**: Понад 54% вважають, що блокчейн може допомогти боротися з фейковим контентом, згенерованим ШІ.
- **Децентралізація як майбутнє:** 37% респондентів вважають, що децентралізація може покращити міжнародну банківську систему та соціальні мережі, сприяючи більшій прозорості та довірі.

Звіт також торкається питань, пов'язаних із фінансовою системою. Лише 47% респондентів вважають її задовільною, тоді як 18% вважають, що вона потребує повної перебудови. Це відображає загальний запит на інновації та альтернативи, які пропонують блокчейн і криптовалюти. Підсумовуючи, документ окреслює зростаючий інтерес до нових технологій, проте підкреслює необхідність посилення обізнаності та усунення бар'єрів для їхнього прийняття.

Рекомендовані матеріали

ШІ змінює правила гри: наскільки безпечна ваша банківська біометрія? [12]

Подкаст від BBC висвітлює актуальну та критичну проблему у сфері безпеки фінансових установ — уразливість систем голосової автентифікації до шахрайських дій, що використовують технології штучного інтелекту (ШІ) для клонування голосів. Журналістка BBC Шарі Валь у рамках програми "Scam Safe Week" провела експеримент, щоб перевірити ефективність голосових систем захисту банківських рахунків проти згенерованого штучним інтелектом голосу.

У своєму розслідуванні Шарі клонувала свій голос, використовуючи запис радіоінтерв'ю, і за допомогою цього клонованого голосу здійснила спробу входу в свої банківські рахунки в установах Santander і Halifax. Технологія генерації голосу забезпечила високу якість копії, яка була практично ідентичною до оригіналу. Експеримент довів, що навіть за допомогою простого динаміка домашнього пристрою клонований голос міг пройти автентифікацію в обох банках. Після проголошення фрази "My voice is my password" системи успішно підтвердили ідентичність і надали доступ до рахунків.

Варто зазначити, що для здійснення таких дій злочинцям також необхідно мати доступ до зареєстрованого номера телефону власника рахунку. Однак це не є нездоланною перешкодою, враховуючи можливість фізичної крадіжки телефона чи інших форм шахрайства.

Попри успіх експерименту, банки запевняють, що голосова автентифікація забезпечує вищий рівень захисту, ніж традиційні методи, такі як паролі чи PIN-коди. Santander підкреслив, що голосова автентифікація є лише частиною багаторівневого підходу до безпеки, а Halifax назвав її додатковою опцією для клієнтів.

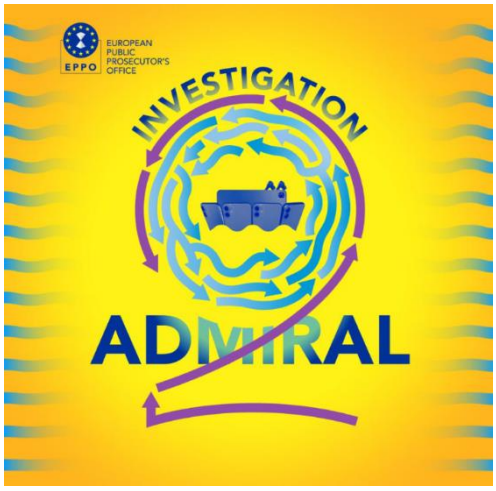
Розслідування також висвітлює коментарі експертів, таких як Сай Хак, члена Національної кібер-консультативної ради Великої Британії. Він висловив глибоку стурбованість розвитком генеративних ШІ-технологій, які створюють нові ризики для фінансових установ і приватних осіб. Експерт наголосив на необхідності переосмислення підходів до безпеки, щоб протидіяти загрозам, що виникають через використання ШІ в шахрайських цілях.

Цей випадок привертає увагу до ширшої проблеми адаптації систем фінансової безпеки до викликів сучасних технологій. Швидкий розвиток генеративних алгоритмів на основі ШІ ставить під загрозу традиційні методи ідентифікації, особливо ті, що базуються на біометрії. Документ наголошує на необхідності впровадження багаторівневих систем автентифікації, інвестицій у нові технології для виявлення підробок та проведення освітніх кампаній серед користувачів, щоб підвищити їхню обізнаність щодо потенційних ризиків.

[12] https://www.bbc.com/news/articles/c1lg3ded6j9o

Інші новини

Операція «Admiral 2.0»: Як ЄС викрив найбільшу схему шахрайства з ПДВ в історії [13]



Розслідування Admiral 2.0, проведене Європейською прокуратурою (EPPO), стало найбільшим в історії ЄС випадком шахрайства з ПДВ, збитки від якого оцінюються у €2.9 мільярда. Ця масштабна схема обману, що охопила 16 країн-членів ЄС, ґрунтувалася на зловживанні правилами транскордонних операцій, звільнених від ПДВ, та використанні "карусельного" шахрайства. Основним механізмом шахрайства стало створення понад 400 фіктивних компаній у 15 країнах, які діяли як постачальники електронних товарів, продавши їх через онлайн-майданчики на загальну суму €1.48 мільярда. Хоча кінцеві споживачі сплачували ПДВ, компанії не передавали ці кошти до податкових органів, а натомість – кошти зникали. Інші учасники схеми, що діяли у її ланцюгу, подавали заявки на відшкодування ПДВ, тим самим завдавши прямої шкоди на суму €297 мільйонів.

Крім фінансових втрат, розслідування виявило, що ця схема мала глибокі зв'язки з іншими кримінальними видами діяльності, включаючи відмивання коштів, отриманих від торгівлі наркотиками, кіберзлочинів та інвестиційного шахрайства. Існують підозри щодо участі російських організованих злочинних угруповань, які надавали фінансову підтримку операції в обмін на регулярні виплати. Цей полі-кримінальний характер схеми свідчить про її інтегрованість у міжнародну злочинну мережу.

Операція, проведена 28 листопада 2024 року, залучила 624 правоохоронців з різних країн. У рамках транснаціональної акції було виконано 350 обшуків і затримано 32 особи, зокрема у Латвії, Литві та Естонії. У результаті цих дій заморожено 62 банківських рахунки з активами на €5.5 мільйонів, а також вилучено товари, зокрема електроніку на суму понад €47.5 мільйонів, готівку (€126 965) та розкішні автомобілі. Задіяні документи й цифрові докази тепер стануть ключовими у подальшому розслідуванні.

EPPO вдалося досягти такого результату завдяки унікальній моделі децентралізованого розслідування та використанню централізованої аналітичної платформи, що дозволила виявити зв'язки між компаніями та підозрюваними. Серед партнерів, які брали участь у розслідуванні, були Europol, Eurojust та підрозділи фінансової розвідки з усіх залучених країн. Ця справа стала яскравим прикладом ефективного міжнародного співробітництва у боротьбі з транскордонними злочинами проти фінансових інтересів ЄС.

[13] https://www.eppo.europa.eu/en/media/news/investigation-admiral-20-europes-biggest-vat-fraud-links-to-organised-crime

Синтетичні дані як прорив у боротьбі з відмиванням коштів: новий проєкт для інновацій у фінансовому секторі [14]

Публікація описує новаторський проєкт, реалізований Інститутом Алана Тюрінга, Plenitude Consulting, Napier AI та Financial Conduct Authority (FCA), метою якого є подолання основних бар'єрів для інновацій у сфері виявлення відмивання коштів. Однією з головних перешкод на шляху до розробки ефективних рішень у цій галузі є обмежений доступ до реалістичних фінансових даних, необхідних для тестування та впровадження нових підходів. У відповідь на цю проблему проєкт пропонує створення синтетичних наборів даних, які максимально точно відтворюють властивості реальних фінансових транзакцій, включаючи типові схеми відмивання коштів.

Цей синтетичний набір даних буде сформований на основі анонімізованих транзакцій, зібраних від роздрібних банків Великобританії, та доповнений даними, що відображають поширені методи фінансових зловживань. Очікується, що ці дані стануть доступними через FCA Digital Sandbox – платформу для тестування в ізольованому середовищі. Учасники, серед яких фінансові установи, розробники програмного забезпечення та дослідницькі команди, отримають можливість використовувати ці дані для розробки, тестування та демонстрації ефективності нових підходів і алгоритмів виявлення відмивання коштів.

Проєкт спрямований не лише на перевірку ефективності нових методів, але й на оцінку надійності самих синтетичних даних. Завдяки можливості моделювання різних сценаріїв у контрольованих умовах, фінансові організації зможуть забезпечити адаптивність та стійкість своїх моделей до змін у поведінці злочинців. У свою чергу, це допоможе створити динамічний ринок, де будуть впроваджені більш конкурентоспроможні та інноваційні рішення для боротьби з фінансовими злочинами.

Проєкт також має стратегічне значення для виконання довгострокових планів FCA та уряду Великобританії у сфері боротьби з фінансовою злочинністю. Його реалізація сприятиме зменшенню шкоди від відмивання коштів, підвищенню рівня захисту клієнтів банків та зміцненню довіри до фінансової системи. Учасники цього процесу зможуть оцінити потенціал нових технологій, водночас сприяючи формуванню кращого розуміння того, як ефективно використовувати синтетичні дані у боротьбі з відмиванням коштів.

Ця ініціатива відкриває нові перспективи для фінансового сектору, забезпечуючи доступ до передових методів тестування та впровадження технологій, що у майбутньому можуть бути масштабовані на інші юрисдикції. Результати проєкту не тільки вдосконалять процеси виявлення підозрілих транзакцій, але й сприятимуть створенню глобальної практики, яка зробить боротьбу з відмиванням коштів більш ефективною та технологічно розвиненою.

[14] https://www.turing.ac.uk/news/new-data-science-project-uses-synthetic-data-address-main-barriers-innovation-field-money

Для загального розвитку

Travel Rule у криптовалютних транзакціях [15]

Публікація від OKX детально пояснює запровадження та виконання міжнародного регулювання Travel Rule, яке застосовується до криптовалютних транзакцій у Європейській економічній зоні (EEA), починаючи з 30 грудня 2024 року. Метою Travel Rule є протидія фінансовим злочинам, зокрема відмиванню коштів та фінансуванню тероризму, шляхом запровадження обов'язкової ідентифікації сторін криптовалютних переказів.

Згідно з вимогами, кожен користувач платформи OKX, який здійснює перекази криптовалюти (депозити чи зняття коштів), має надавати додаткову інформацію про отримувача або відправника. Зокрема, при здійсненні транзакції необхідно вказувати, чи здійснюється вона на приватний гаманець або на акаунт біржі. Для переказів на приватні гаманці користувач має надати повне ім'я одержувача, а також може бути запитана додаткова інформація, залежно від суми або контексту транзакції. Для переказів, що перевищують €1000, обов'язковою є верифікація власності на приватний гаманець. Це може бути здійснено шляхом криптографічного підпису або так званого Satoshi тесту, який включає відправлення певної кількості криптовалюти на перевірку.

Для переказів між біржами також передбачено надання інформації про отримувача, включаючи його ім'я, зареєстроване на відповідній платформі. У разі отримання депозиту з іншої біржі користувач повинен переконатися, що надана інформація відповідає його даним у системі OKX, оскільки будь-які розбіжності в іменах можуть викликати помилки в процесі верифікації.

Документ також окреслює дії, які необхідно вжити у разі проблем із транзакціями, наприклад, якщо інформація про відправника чи отримувача не відповідає вимогам Travel Rule. У таких випадках рекомендується звертатися до служби підтримки OKX для уточнення деталей або для вирішення технічних питань. Якщо транзакція походить із біржі, яка не підтримує Travel Rule, необхідно зв'язатися з цією біржею, щоб передати потрібну інформацію через спеціально створений контактний канал OKX.

Особливу увагу приділено інтеграції бірж із рішеннями Travel Rule. Якщо біржа не має відповідного підключення, її необхідно зв'язати з OKX для впровадження технологічного рішення, яке забезпечить дотримання вимог регулятора. Цей процес є критично важливим для забезпечення безперервності транзакцій між користувачами різних платформ.

Документ підкреслює важливість точного дотримання вимог, оскільки невиконання може призвести до блокування або відхилення транзакцій. Також зазначається, що зміни не впливають на торгівлю криптовалютами безпосередньо на платформі, а лише стосуються процесів введення та виведення коштів. Travel Rule є обов'язковим регулюванням, якого необхідно дотримуватися для всіх операцій у межах Європейського Союзу, і OKX, як платформа, повністю підтримує його впровадження.

[15] https://www.okx.com/ua/help/travel-rule-faq-eea

Комплексний підхід до протидії фінансуванню тероризму [16]

European Banking Authority (EBA) опублікувала інформаційний бюлетень присвячений комплексному аналізу протидії фінансуванню тероризму (ПФТ), який описує ключові аспекти, що забезпечують ефективність заходів у цій сфері. У бюлетені пояснюється сутність фінансування тероризму, яка полягає у наданні фінансових чи інших ресурсів, що можуть бути використані для здійснення терористичних актів як на національному, так і на міжнародному рівнях. Особливу увагу приділено тому, що джерела таких коштів можуть бути як нелегальними, включаючи доходи від відмивання грошей, торгівлі людьми чи викрадення за викуп, так і легальними – наприклад, добровільні пожертви чи доходи від законних комерційних підприємств.

Документ акцентує увагу на важливій відмінності між виявленням фінансування тероризму та застосуванням цільових фінансових санкцій. Виявлення включає ідентифікацію осіб або груп, які фінансово пов’язані з терористичними організаціями, але не внесені до санкційних списків. У той же час цільові фінансові санкції спрямовані на заморожування активів осіб чи організацій, що визначені санкційними резолюціями ООН, ЄС чи іншими міжнародними структурами. Обидва підходи є критично важливими, адже виключно зосередженість на санкціях може призводити до пропуску ризиків, пов’язаних із одиночними терористами або малими терористичними осередками.

Особливе місце в документі займає роль European Banking Authority (EBA), яка надає фінансовим установам та їхнім наглядовим органам рекомендації щодо оцінки ризиків ПФТ та впровадження відповідних заходів контролю. Зокрема, у 2023 році EBA оновила свої рекомендації, щоб уникнути надмірного дерискінгу неприбуткових організацій, сприяючи їхньому доступу до фінансових послуг. Також EBA розробила детальні керівництва для забезпечення надійності систем управління ризиками та співпраці з органами фінансового моніторингу й правоохоронними структурами.

Документ наголошує на необхідності постійного оновлення оцінок ризиків ПФТ на основі надійних і актуальних джерел, таких як звіти FATF, Europol та ПФР країн. Оцінка ризиків дозволяє ідентифікувати нові схеми фінансування тероризму та приймати превентивні заходи. У цьому контексті також підкреслюється важливість міжнародної кооперації, зокрема через AML/CFT колегії, для ефективного обміну інформацією та спільного реагування на ризики.

Загальний підхід до ПФТ базується на розумінні, що жоден окремий суб’єкт чи держава не можуть ефективно вирішити проблему самостійно. Тому співпраця між організаціями, державами та секторами є ключовим елементом стратегії.

Таким чином, документ розкриває багатогранність проблематики ПФТ, висвітлюючи як стратегічні, так і практичні аспекти, що дозволяють ефективно протидіяти фінансуванню тероризму на різних рівнях.

[16] https://media.licdn.com/dms/document/media/v2/D4E1FAQFygoeZSNYOnA/feedshare-document-pdf-analyzed/B4EZPEV6RiH0Ac-/0/1734165900520?e=1736380800&v=beta&t=PF0H5nLVtMzgganwOnUt-DxT0_GDR38tSY1-STzfvjA

Модні штрафи: Як закон США про боротьбу з шахрайством змінює правила гри для індустрії моди [17]

Публікація висвітлює застосування американського закону про боротьбу з шахрайством, відомого як False Claims Act (FCA), у контексті індустрії моди. Автор пояснює, як цей закон, що традиційно використовується для виявлення шахрайства у відносинах з урядом США, може бути інструментом для боротьби з недобросовісними практиками в бізнесі, зокрема ухиленням від сплати митних зборів.

False Claims Act дозволяє приватним особам, які діють як викривачі, подавати позови проти компаній, що обманюють уряд, наприклад, занижують вартість імпортованих товарів. Викривач, може ініціювати розслідування і, за наявності доказів, залучити державу до справи. Якщо справа завершується стягненням коштів, викривач отримує частку від суми, що є потужним стимулом для розкриття шахрайських схем. Цей механізм дозволяє боротися зі складними шахрайськими діями, які уряд не завжди може виявити самостійно.

Основний акцент статті зроблено на митному шахрайстві у модній індустрії. Серед найбільш поширених схем автор описує транзитне перевезення, коли товари транспортуються через треті країни з метою фальсифікації їх країни походження для ухилення від митних зборів та квот. Інший метод – подвійне інвойсування, коли компанії надають занижені рахунки-фактури для митних органів, одночасно оплачуючи додаткові суми своїм постачальникам через окремі документи, приховані від митної служби.

На прикладах резонансних кейсів проілюстровано, як такі схеми розкривалися завдяки викривачам. Наприклад, у 1997 році справу проти бренду The Limited ініціювала Американська асоціація текстильних виробників, яка звинуватила компанію у транзитному перевезенні одягу з Китаю через Гонконг, що дозволяло уникнути митних зборів. Хоча цей позов не завершився успіхом, він став сигналом для посилення уваги до індустрії моди. У 2014 році справу проти компаній Dana Kay та Siouni & Zar було успішно розглянуто, що призвело до виплати уряду США $10 млн. У більш сучасному кейсі 2022 року компанія Luchiano Visconti та її менеджер були оштрафовані на $3,64 млн за заниження вартості імпорту, причому менеджер став особисто відповідальним за шахрайство.

Особливу увагу в статті приділено ролі викривачів, які можуть бути співробітниками компаній, конкурентами, постачальниками або асоціаціями. Наведені приклади показують, як викривачі допомагають уряду виявляти приховані схеми, забезпечуючи повернення значних сум до бюджету. Викривачі захищені законодавством, а їхні дії часто ведуть до покращення прозорості бізнесу. Автор підсумовує, що компанії зі сфери моди повинні бути пильними та уникати будь-яких схем ухилення від сплати мит, адже ризики значно перевищують вигоди.

Стаття завершується закликом до представників індустрії дотримуватися законодавства та нагадує, що боротьба з митними шахрайствами є одним із ключових трендів у сучасній практиці.

[17] https://fashionunited.com/news/business/fashion-police-types-of-fraud-the-us-false-claims-act-can-target-in-the-fashion-industry/2024112763112

Контактуйте щодо цього документу з Держфінмоніторингом:

- **Email:** bulletin@fiu.gov.ua
- **Поштова адреса:** Державна служба фінансового моніторингу України, Україна, 04050 м. Київ, вул. Білоруська, 24
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № ДСФМУ-ДК-2024-039

Бюллетень є волонтерською розробкою методологічної команди Державної служби фінансового моніторингу України відповідно до пункту 18 частини 2 статті 25 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 Держфінмоніторингу].