Методологічний бюлетень

Серійний номер: МінФін-AML-2025-15

Квітень 2025

“Ви не переможете, якщо не почнете”

Гелен Роуленд

Мета

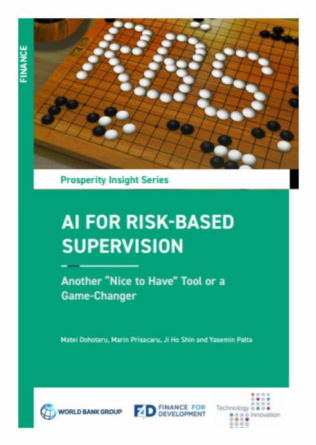
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). 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

Штучний інтелект для нагляду: ще один "приємний" інструмент чи зміна правил гри [1]



Документ, опублікований в рамках серії "Prosperity Insight Series" Світового банку, є ґрунтовним дослідженням ролі штучного інтелекту (ШІ) у трансформації нагляду за фінансовим сектором. Авторами виступають Matei Dohotaru, Marin Prisacaru, Ji Ho Shin та Yasemin Palta, які представляють підрозділ фінансової стабільності та доброчесності Світового банку разом із лабораторією технологій та інновацій ITS. Цей документ аналізує, як ШІ може стати революційним інструментом для впровадження нагляду на основі ризиків (Risk-Based Supervision, RBS), що протягом останніх двох десятиліть вважається "золотим стандартом" у фінансовому нагляді, але стикається з труднощами реалізації, особливо в країнах із середнім і низьким рівнем доходу. Основна мета дослідження — не лише окреслити потенціал ШІ, але й детально розглянути його переваги, виклики, ризики, стратегії

[1] https://openknowledge.worldbank.org/entities/publication/4f8b828d-3eb0-4f16-a816-b5143c414e70

впровадження та майбутні перспективи, пропонуючи практичні рекомендації для наглядових органів.

Документ розпочинається з виконавчого резюме, яке підкреслює трансформаційний потенціал ШІ для фінансового сектору — однієї з найбільш регульованих галузей у світі. Автори зазначають, що хоча розвинені країни досягли значного прогресу у впровадженні RBS, країни з обмеженими ресурсами продовжують мати складнощі з його ефективною реалізацією. ШІ розглядається як інструмент, здатний змінити цю ситуацію завдяки автоматизації рутинних завдань, обробці великих обсягів даних і створенню проактивного підходу до нагляду. При цьому наголошується, що ШІ не замінить людину в ключових рішеннях, а сприятиме симбіозу між технологією та людським досвідом, що може підвищити стабільність фінансової системи, захистити споживачів і зменшити зловживання.

Далі документ занурюється в аналіз основних викликів, з якими стикаються наглядові органи при впровадженні RBS. Ці виклики охоплюють обмеженість людських ресурсів, що ускладнює оцінку всіх ризиків навіть у розвинених країнах, а також проблеми з якістю та деталізацією даних, які часто страждають через відсутність стандартів звітності, надмірність, розрізненість і слабке управління. Аналітика в багатьох органах залишається недостатньою, здебільшого орієнтованою на ретроспективу, а не на прогноз.

Звіт підкреслює, що ШІ може стати ключовим інструментом для автоматизації процесів, підвищення ефективності та створення проактивного підходу до нагляду, особливо в країнах із обмеженими ресурсами. Основні виклики включають брак людських ресурсів, низьку якість даних і застарілі процеси, тоді як ШІ пропонує рішення через обробку великих даних, прогнозну аналітику та автоматизацію. У звіті також розглядаються приклади використання ШІ, ризики (упередженість, непрозорість), виклики впровадження (дані, інфраструктура, навички) та стратегії адаптації, такі як поетапне впровадження та хмарні рішення. Прогнозується, що ШІ сприятиме нагляду в реальному часі, інтеграції даних і повній автоматизації простих процесів. Автори доходять висновку, що ШІ не замінить людину, але створить симбіоз для підвищення ефективності нагляду.

Застарілі процеси, які не враховують потенціал сучасних технологій, і брак експертизи в аналітиці даних та ШІ додатково ускладнюють ситуацію, особливо в умовах конкуренції з приватним сектором за кваліфікованих фахівців. Цей аналіз ґрунтується на оцінках відповідності Базельським принципам, проведених у рамках програм оцінки фінансового сектору (FSAP) Світовим банком та МВФ.

Наступний розділ присвячений тому, як ШІ може посилити можливості наглядових органів. Завдяки технологіям, таким як машинне навчання, обробка природної мови (NLP) і оптичне розпізнавання символів (OCR), ШІ здатен обробляти величезні обсяги структурованих і неструктурованих даних, автоматизувати рутинні завдання, як-от перевірку документів чи складання звітів, і надавати прогнозну аналітику для виявлення ризиків і аномалій, наприклад, підозрілих транзакцій у контексті AML/CFT (протидія відмиванню грошей і фінансуванню тероризму). Великі мовні моделі (LLM), такі як GPT-4, дозволяють швидко узагальнювати документи й надавати інсайти, тоді як здатність ШІ до безперервного навчання забезпечує адаптацію до нових даних і умов. Ці можливості дозволяють наглядачам зосередитися на високоризикових операціях, підвищуючи ефективність і проактивність.

Документ також наводить приклади використання ШІ у діяльності наглядових органів, зокрема аналіз великих даних для оцінки кредитних ризиків, моніторинг транзакцій у реальному часі (наприклад, центральним банком Нідерландів) і створення систем раннього попередження. Проте впровадження ШІ супроводжується ризиками, такими як упередженість моделей, непрозорість ("чорна скринька"), атаки на дані (data poisoning) і проблеми з конфіденційністю, що вимагає міцних рамок управління, як-от EU AI Act чи NIST AI Risk Management Framework.

Виклики впровадження ШІ включають доступність і якість даних, які мають бути релевантними, достатніми й достовірними, що часто ускладнено через старі системи чи обмеження доступу. Брак спеціалістів із ШІ, потреба в потужній інфраструктурі (яку можна компенсувати хмарними рішеннями) і відповідність регуляторним вимогам, таким як прозорість і захист даних, також є суттєвими перешкодами. Побудова довіри до ШІ вимагає пояснюваності моделей і поступового впровадження.

Стратегії адаптації ШІ передбачають управління очікуваннями керівництва, подолання культурного опору через навчання, поетапне впровадження від пілотних проєктів до масштабування, гібридний підхід до джерел ШІ (внутрішні та зовнішні ресурси) і використання хмарних платформ для демократизації доступу. У майбутньому автори прогнозують нагляд у реальному часі, коли ШІ миттєво аналізуватиме дані, інтеграцію структурованих і неструктурованих даних для кращого розуміння ризиків, покращення прогнозного моделювання (наприклад, стрес-тестування), повну автоматизацію простих процесів (наприклад, затвердження перепризначень) і навіть інтеграцію з дарквебом для виявлення вразливостей. ШІ також зможе надавати консультації в реальному часі стейкхолдерам, хоча повна заміна людини в нагляді не передбачається через складність галузі.

Висновки:

- **Покращення даних як пріоритет:** Наглядовим органам необхідно терміново вдосконалити управління даними, впроваджуючи стандарти звітності та переходячи до дата-центричного підходу, щоб забезпечити ШІ якісними даними для аналізу ризиків.
- **Інвестиції в хмарні рішення:** Використання хмарних платформ (AWS, Azure) для навчання та запуску ШІ-моделей дозволить країнам із обмеженими ресурсами швидко впроваджувати передові технології.
- **Розвиток навичок і поетапне впровадження:** Інвестувати в навчання персоналу з ШІ та почати з пілотних проєктів у високоризикових сферах (наприклад, AML/CFT), щоб продемонструвати цінність і побудувати довіру.
- **Регуляторна відповідність і пояснюваність:** Розробити рамки управління ШІ (на основі EU AI Act) і використовувати пояснювані моделі (XAI) для забезпечення прозорості та відповідності нормам.

Документ завершується додатком із технічною архітектурою для інтеграції ШІ, включаючи хмарні платформи, сховища функцій (Feature Store) і API для доступу до моделей. Загалом, звіт підкреслює, що ШІ є не просто допоміжним інструментом, а потенційним "змінником гри", який може революціонізувати фінансовий нагляд, якщо подолати наявні виклики й ефективно інтегрувати його в існуючі процеси.

Оцінка загроз для юридичних послуг: Виклики дотримання фінансових санкцій у Великій Британії [2]

Документ, підготовлений Управлінням з імплементації фінансових санкцій (OFSI) при Казначействі Її Величності (HM Treasury), є детальним аналізом загроз для дотримання фінансових санкцій Великої Британії з боку постачальників юридичних послуг. Цей звіт зосереджується на подіях, що розгорнулися після незаконного вторгнення Росії в Україну в лютому 2022 року, коли Велика Британія разом із міжнародними партнерами запровадила безпрецедентні санкції проти російських осіб та організацій. Метою звіту є допомога британським зацікавленим сторонам у розумінні та протидії ризикам недотримання санкцій, а

[2] https://assets.publishing.service.gov.uk/media/67ee635698b3bac1ec299c3e/OFSI_Legal_Services_Threat_Assessment.pdf

також демонстрація проактивного підходу OFSI до розслідування порушень. Він є частиною серії секторальних оцінок, спрямованих на підвищення обізнаності та зміцнення санкційного режиму в умовах еволюціонуючого ландшафту фінансових обмежень.

Звіт підкреслює значні зміни в санкційному середовищі після лютого 2022 року, коли понад 75% позначень у рамках санкцій Великої Британії стосувалися Росії. У цей період юридичний сектор став другим за кількістю звітів про підозрювані порушення, подавши 16% від загальної кількості (після фінансового сектору з 65%). Основну увагу приділено діяльності постачальників юридичних послуг, таких як адвокатські фірми, а також постачальники трастових і корпоративних послуг (TCSPs), які відіграють ключову роль у забезпеченні дотримання санкцій як для своїх клієнтів, так і в межах власної діяльності. Звіт базується на даних, зібраних OFSI з січня 2022 по березень 2024 року, і включає аналіз звітів про порушення, які не обов'язково відображають поточні розслідування чи примусові дії, але слугують основою для рекомендацій щодо ризиків.

Одним із центральних висновків є висока ймовірність того, що TCSPs не повідомили про всі підозрювані порушення, адже лише 2% звітів від юридичного сектору надійшло від них, тоді як 98% подали адвокатські фірми. Це викликає занепокоєння, враховуючи введення в грудні 2022 року трастових санкцій, які забороняють надання таких послуг особам, пов'язаним із Росією (PCWR), без відповідної ліцензії чи винятку. OFSI закликає TCSPs до ретроспективних перевірок для виявлення незадекларованих порушень. Інший важливий аспект — майже певність того, що більшість випадків недотримання пов'язані з порушенням умов ліцензій OFSI, наприклад, перевищенням лімітів платежів від позначених осіб (DPs), операціями після закінчення терміну дії ліцензій чи недостатньою звітністю. Звіт також вказує, що складні корпоративні структури, включаючи трасти, пов'язані з російськими DPs та їхніми родичами, майже напевно використовуються для приховування права власності на активи, які підлягають заморожуванню, а також на ймовірність того, що DPs передають ці активи непозначеним особам, що в деяких випадках є порушенням санкцій.

Аналіз загроз включає огляд звітів про порушення, де російські санкції домінують, але згадуються й інші

Висновки:

- **Провести ретроспективні перевірки у TCSPs:** Постачальники трастових та корпоративних послуг повинні негайно провести ретроспективні перевірки для виявлення та повідомлення OFSI про незадекларовані порушення санкцій з лютого 2022 року, враховуючи їх низький рівень самозвітності (2%).
- **Посилити контроль за дотриманням умов ліцензій:** Юридичним фірмам слід ретельно перевіряти платежі від позначених осіб (DPs), уникаючи перевищення лімітів чи операцій після закінчення терміну дії ліцензій, та повідомляти OFSI про порушення протягом 14 днів.
- **Розширити due diligence для складних структур:** Фірми повинні посилити перевірки KYC щодо трастів та корпоративних структур, особливо з російськими зв'язками, щоб виявити приховане право власності DPs та запобігти передачі активів непозначеним особам.
- **Звернути увагу на посередницькі юрисдикції:** Юридичні постачальники мають підвищити пильність до транзакцій через юрисдикції типу БВО, Кіпру чи ОАЕ, де часто фіксуються порушення, та співпрацювати з місцевими органами для забезпечення санкційного режиму.

санкційні режими, такі як Лівія, Білорусь, М'янма та Глобальні санкції з прав людини. OFSI наголошує на необхідності пильності щодо всіх санкційних режимів. У звіті деталізовано типові порушення умов ліцензій, такі як несвоєчасна звітність чи переказ заморожених активів у неналежні рахунки, і надано перелік "червоних прапорців", які сигналізують про потенційні порушення. До них належать нечітка структура трастів, зв'язки з російськими DPs через родичів чи партнерів, а також операції через посередницькі юрисдикції, такі як Британські Віргінські Острови, Кіпр чи Швейцарія, які фігурують у 23% звітів про порушення. Ці юрисдикції часто слугують для структурування фінансових інтересів російських DPs, ускладнюючи відстеження активів.

Особливу увагу приділено діяльності російських DPs та їхніх пособників (enablers), які намагаються обійти заморожування активів через складні структури та передачу їх непозначеним особам. Звіт розрізняє професійних пособників, які діють свідомо чи недбало, та непрофесійних, таких як родичі чи довірені особи DPs, які використовують менш витончені методи. Наведено вигаданий кейс-стаді, що ілюструє передачу портфеля нерухомості від російського DPs через траст на Британських Віргінських Островах до маловідомої британської компанії з подальшим перерозподілом прав власності, що викликає підозри в обході санкцій. OFSI закликає юридичні фірми ретельно перевіряти такі операції та повідомляти про них.

Додатково звіт торкається інших загроз, таких як діяльність позначених російських бізнесів із історичними інтересами у Великій Британії, які намагаються позбутися активів, та ризиків відмивання грошей через криптоактиви, як виявлено в розслідуванні Національного агентства з боротьби зі злочинністю (NCA) у грудні 2024 року. OFSI підкреслює свою співпрацю з NCA та іншими органами, а також анонсує подальші секторальні звіти в 2025 році.

Звіт EBA про споживчі тенденції 2024/25 [3]

Звіт Європейського банківського органу (EBA) є ґрунтовним оглядом динаміки роздрібного банківського ринку в Європейському Союзі та виявлених проблем, які впливають на споживачів фінансових послуг. Він охоплює дані за 2022–2023 роки й акцентує увагу на ключових викликах для споживачів, зокрема у сфері іпотеки, споживчого кредитування, платіжних послуг, електронних грошей, платіжних рахунків і депозитів. Уперше EBA також порушує теми небанківського кредитування та криптоактивів, підготовлюючи ґрунт для їх подальшого аналізу.

У першому розділі представлено заходи, які були вжиті EBA та національними компетентними органами (NCAs) у відповідь на теми минулого звіту: шахрайство в платіжних операціях і надмірна заборгованість. EBA у 2024 році оприлюднила висновок щодо нових форм шахрайства в роздрібних платежах, таких як APP (authorized push payment) шахрайство, й ініціювала щорічну публікацію даних про платіжне шахрайство спільно з ЄЦБ. У відповідь на виклики заборгованості були розроблені інформаційні кампанії, огляди ефективності кредитного нагляду, а також здійснено глибокий аналіз практик оцінки кредитоспроможності небанківських кредиторів, які часто надають кредити без належної перевірки платоспроможності позичальників.

[3] https://www.eba.europa.eu/sites/default/files/2025-03/514b651f-091b-42d3-b738-1fae79264044/Consumer%20Trends%20Report%202024-2025.pdf

Другий розділ демонструє динаміку розвитку роздрібних фінансових продуктів. Іпотека залишається основним джерелом боргового навантаження на споживачів, складаючи 79% загального обсягу кредитування домогосподарств. Зростання відсоткових ставок і рівень заборгованості стали причиною зростання арештів, потреби у реструктуризації боргів та загального погіршення умов іпотечного обслуговування. Для споживчих кредитів спостерігається підвищений попит на BNPL-продукти й короткострокові позики, особливо серед молоді. Разом із тим, звіт підкреслює серйозні проблеми з неналежною оцінкою платоспроможності позичальників, відсутністю прозорої передконтрактної інформації та агресивною цифровою рекламою.

Платіжні послуги демонструють зростаючу цифровізацію — карткові платежі залишаються домінуючими, але водночас збільшується кількість скарг на несанкціоновані транзакції, непрозорість комісій та зниження доступності послуг для вразливих категорій споживачів. В електронних грошах, хоча вони залишаються локалізованим явищем, найбільш поширеними проблемами є непрозорі тарифи та умови. Щодо платіжних рахунків, занепокоєння викликає обмеження доступу до базових рахунків, особливо серед мігрантів, безхатченків та осіб із поганою кредитною історією. Щодо депозитів, помітне зниження обсягів нічних вкладів на тлі зростання ставок та популярності строкових депозитів.

У третьому розділі EBA виділяє три головні теми, що впливають на добробут споживачів: шахрайство в платіжних операціях, зростаюча заборгованість та "невиправдане уникнення ризику" (unwarranted de-risking), тобто закриття або відмова у відкритті банківських рахунків через профілі ризику без прозорих обґрунтувань. Це явище особливо зачіпає вразливі групи, а саме: мігрантів, транскордонних працівників, безхатченків і людей з низьким рівнем фінансової обізнаності.

Усі ці фактори лягають в основу подальшої роботи EBA у 2025–2026 роках — зокрема у сфері регуляторного впливу, розробки керівних документів і посилення споживчого захисту на рівні ЄС. EBA наголошує на необхідності адаптації регуляторного середовища до умов зростаючої цифровізації, складних економічних реалій і посилення ролі небанківських гравців на фінансовому ринку.

Висновки:

- **Платіжне шахрайство залишається провідною проблемою для споживачів у ЄС**, зокрема через соціальну інженерію (APP fraud); EBA пропонує зміцнити захист шляхом оновлення нормативних вимог у PSD3/PSR та впровадження нових безпекових стандартів.
- **Зростання BNPL (Buy Now, Pay Later) і небанківського кредитування супроводжується критичними порушеннями у практиках оцінки кредитоспроможності**, що сприяє надмірній заборгованості; EBA вимагає гармонізації стандартів оцінки кредитоспроможності на рівні всього ЄС.
- **Дискримінація та обмеження доступу до платіжних рахунків для вразливих груп набувають системного характеру**, вимагаючи від регуляторів термінових дій із забезпечення справедливого доступу до фінансових послуг.
- **Наявні нормативні підходи недостатньо адаптовані до цифрової епохи**, що вимагає не лише оновлення законодавства (зокрема через CCD2, PSD3 та MiCAR), а й розширення наглядових ресурсів у національних органів для ефективного моніторингу ринку.

Регулювання

НКЦПФР представила Матрицю оподаткування віртуальних активів для потенційних учасників крипторинку України [4]

Голова Національної комісії з цінних паперів та фондового ринку (НКЦПФР) України Руслан Магомедов повідомив про відкритий доступ до матриці оподаткування віртуальних активів для потенційних учасників крипторинку. У березні 2025 року документ вперше представили під час засідання робочої групи при профільному Комітеті Верховної Ради України.

Матриця оподаткування віртуальних активів в Україні, розроблена за ініціативи та безпосередньої участі Національної комісії з цінних паперів та фондового ринку (НКЦПФР), є стратегічним документом, що має на меті створення прозорої, ефективної та справедливої системи оподаткування операцій із віртуальними активами в умовах стрімкої цифрової трансформації економіки України. У контексті глобальних тенденцій до зростання популярності децентралізованих фінансових технологій, цей документ пропонує комплексний підхід до регулювання ринку віртуальних активів, враховуючи як їх економічну природу, так і правові особливості. Він ґрунтується на аналізі міжнародного досвіду провідних юрисдикцій, таких як Німеччина, Швейцарія, Естонія, Сінгапур, адаптованого до українських реалій, і спрямований на забезпечення прозорості операцій, запобігання фінансовим зловживанням, мінімізацію ризиків відмивання коштів, а також створення умов для легального використання цифрових активів і залучення інвестицій у цей сектор.

Документ охоплює три ключові напрями: таксономію віртуальних активів, оподаткування доходів фізичних осіб та регулювання податку на додану вартість (ПДВ). У першій частині представлена таксономія, яка слугує фундаментом для правового та податкового регулювання, забезпечуючи чітке визначення класифікаційних груп віртуальних активів. Вона поділяє активи на токени електронних грошей (EMT), що прив'язані до однієї офіційної валюти для підтримки стабільної вартості, токени з прив'язкою до активів (ART), які стабілізують свою вартість через прив'язку до різних об'єктів цивільних прав, таких як валюти чи метали, і можуть посвідчувати права вимоги, а також інші токени, до яких належать сервісні токени, децентралізовані валюти (наприклад, Bitcoin) та NFT. Такий підхід дозволяє ідентифікувати економічну сутність активів і формувати відповідні податкові режими, зберігаючи технологічну нейтральність.

Друга частина документа присвячена оподаткуванню доходів фізичних осіб і детально аналізує складнощі, пов'язані з децентралізованим характером транзакцій, анонімністю, відсутністю податкових агентів, проблемами документального підтвердження витрат, високою волатильністю ринку та низьким рівнем податкової обізнаності користувачів. Як об'єкт оподаткування розглядаються два варіанти: чистий дохід (дохід мінус витрати), що враховує реальний приріст вартості, але ускладнює адміністрування через потребу в доказах витрат, і виручка, що спрощує розрахунки, особливо при обміні на фіатні валюти, але може бути обтяжливою для волатильних токенів. Момент виникнення доходу пропонується визначати або за загальним правилом (отримання чи відчуження активів), що є стандартом у ЄС, або при обміні на валютні цінності чи нецифрові активи, як це практикують країни, що не оподатковують crypto-to-crypto транзакції (Австрія, Франція, Сінгапур). Ставки податку

[4] https://www.nssmc.gov.ua/wp-content/uploads/2025/04/matrytsia-opodatkuvannia-va-1.pdf

включають стандартну (18% ПДФО + 1,5% військовий збір) та пільгову (5% або 9%), причому для EMT і ART, прив'язаних до валют чи металів, розглядається можливість звільнення від оподаткування задля нейтральності. Врахування витрат ускладнене чинними положеннями Податкового кодексу України, тому пропонується спеціальна категоризація (EMT+ART окремо від інших токенів) і використання методу FIFO для розрахунку. Курсові різниці та збитки потребують уточнення: збитки можуть переноситися на майбутні періоди, але з можливими обмеженнями. Окремі операції, такі як майнінг і стейкінг, можуть кваліфікуватися як підприємницька діяльність, тоді як airdrops і хардфорки оподатковуються або в момент отримання, або при відчуженні. Звільнення від оподаткування передбачає фінансові ліміти (наприклад, до 600 євро, як у Німеччині), пільги за період володіння (1–3 роки) та операції на кшталт дарування чи переказу між гаманцями. Для токенів, набутих до легалізації ВА в Україні, пропонується тимчасовий податок з обороту з мінімальною ставкою через складність підтвердження витрат. Щодо обов'язків податкових агентів, повне утримання податку CASP визнано складним через брак даних про витрати, тому акцент робиться на самостійному декларуванні, що полегшить інтеграцію з міжнародними стандартами CARF і DAC8.

Третя частина фокусується на застосуванні ПДВ до операцій із віртуальними активами, спираючись на практику ЄС і рішення Суду ЄС у справі C-264/14, яке звільнило обмін криптовалют від ПДВ як фінансову послугу. Майнінг, стейкінг, airdrops і обмін токенів не підлягають ПДВ, тоді як постачання товарів чи послуг за ВА оподатковується на загальних підставах. Зберігання активів із винагородою може підпадати під ПДВ, якщо є прямий зв'язок між оплатою та послугою. NFT трактуються як послуги, а не товари, і оподатковуються ПДВ, якщо пов'язані з економічною цінністю чи доступом; в іншому випадку їхній статус лишається невизначеним. Досвід країн ЄС (Німеччина, Франція, Італія, Польща) підтверджує тенденцію до звільнення обміну ВА від ПДВ, але оподаткування комерційних операцій зберігається.

Загалом документ підкреслює необхідність спрощених моделей декларування, цифрової інфраструктури для полегшення виконання податкових зобов'язань, гармонізації з міжнародними стандартами (MiCA, CARF, DAC8) і створення умов для інтеграції українського ринку віртуальних активів у глобальний фінансовий простір. Він пропонує практичний інструмент для платників податків, регуляторів і законодавців, детально структуруючи оподаткування різних сценаріїв використання ВА.

Заява SEC щодо стейблкоїнів [5]

У своїй заяві від 4 квітня 2025 року Управління корпоративних фінансів Комісії з цінних паперів і бірж США (SEC) оприлюднило позицію, що має потенціал докорінно змінити правову визначеність для ключового сегмента ринку цифрових активів — стейблкоїнів. Цей документ став довгоочікуваною реакцією на багаторічні заклики ринку, що вимагав чіткості у тому, чи є певні види стейблкоїнів цінними паперами за законодавством США, а отже — підлягають суворому регуляторному режиму SEC.

У центрі уваги заяви — поняття "Covered Stablecoins". Це стейблкоїни, які відповідають конкретним характеристикам, що дозволяють SEC зробити висновок: їх випуск і обіг не

[5] https://www.sec.gov/newsroom/speeches-statements/statement-stablecoins-040425

підпадають під регулювання як “пропозиція цінних паперів” відповідно до чинного законодавства. І хоча заява не є юридично обов’язковою, вона надає регуляторну ясність, яку можна вважати “компасом” для емітентів, інвесторів, провайдерів платформ, а також традиційних фінансових установ, які розглядають інтеграцію зі стейблкоїнами.

Визначення "Covered Stablecoins" побудовано навколо чітких функціональних, економічних і технічних характеристик. Згідно із заявою SEC, Covered Stablecoin має:

- бути прив’язаним до долара США в режимі 1:1 (fixed peg to USD);
- бути повністю забезпеченим відповідними резервними активами, такими як готівкові долари, депозити в банках США, державні казначейські облігації з коротким строком погашення (T-bills);
- використовуватися виключно як засіб платежу, передавання вартості або збереження вартості (store of value), а не як інвестиційний актив, тобто не передбачати для користувачів очікування прибутку від зберігання такого токена;
- мати передбачену політику викупу (redemption policy), яка дозволяє утримувачу обміняти токен на долар США або еквівалент резерву без затримки та зі зрозумілими умовами;
- бути запропонованим через процес, який не включає рекламу потенційної вигоди або прибутковості від володіння токеном.

Ключовий висновок SEC полягає у тому, що сам факт створення, обігу або викупу таких Covered Stablecoins не створює “інвестиційного контракту”, який є базовим тестом у судовій практиці (зокрема, за тестом Гові – Howey test) для визначення статусу цінного паперу. У такий спосіб SEC чітко сигналізує, що за відсутності інших інвестиційних характеристик, стабільні токени, які відповідають критеріям Covered Stablecoins, не є цінними паперами, а отже — не підлягають обов’язковій реєстрації чи звітності відповідно до федерального законодавства про цінні папери.

Однак важливим є те, що це позиція лише одного підрозділу SEC, а не колегіального рішення самої Комісії або суду. Це означає, що вона не створює обов’язкової сили для регуляторного чи судового застосування, але може бути використана як посилання у правових позиціях або попередній консультації з SEC. Ба більше — заява прямо попереджає, що інші цифрові активи, навіть якщо вони мають стабільну вартість, можуть бути визнані цінними паперами, якщо не відповідають усім озвученим критеріям.

Ця заява має кілька значущих наслідків для учасників ринку:

По-перше, емітенти тепер мають більш чітку модель легального запуску токенів, прив’язаних до долара, без ризику порушення законів про цінні папери, якщо вони суворо дотримуються вимог до резервів, функціонального призначення та прозорості щодо викупу.

Висновки:

- **SEC підтверджує, що стейблкоїни, які відповідають критеріям Covered Stablecoins, не є цінними паперами:** Це відкриває простір для законного обігу таких активів без вимоги реєстрації, за умови повного забезпечення, фіксованої прив’язки до USD, та відсутності інвестиційної мотивації.
- **Емітенти мають забезпечити наявність надійної системи викупу та прозорих резервів:** Відповідність статусу Covered вимагає не просто декларації, а стабільної політики викупу і наявності ліквідних активів для підтримки довіри до стейблкоїна.
- **Рішення не є загальним для всіх стейблкоїнів і не має сили юридичного прецеденту:** Компаніям слід постійно переглядати структуру свого продукту та шукати індивідуальні консультації з SEC, зважаючи на ризик втрати відповідності.

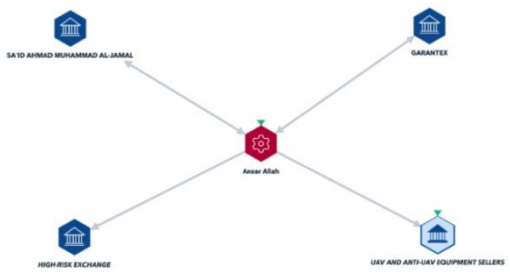
По-друге, для вже існуючих гравців на ринку, включаючи операторів великих стейблкоїнів, таких як USDC або PayPal USD, це може стати аргументом для формалізації статусу своїх активів як “позарегуляторних” (non-securities), принаймні на рівні федерального закону про цінні папери.

По-третє, провайдери гаманців, платіжних рішень та фінансові установи, які інтегрують такі стейблкоїни, отримують більшу впевненість у регуляторному статусі цих активів — що потенційно відкриває двері для ширшого банківського та роздрібного прийняття.

Не менш важливо, що заява SEC також підкреслює динамічність правового статусу цифрових активів: стейблкоїн, який сьогодні відповідає критеріям, може втратити статус Covered, якщо, наприклад, зміниться резервна політика, додадуться інвестиційні функції, або якщо з'явиться стимул для спекулятивного тримання. Таким чином, постійне дотримання стандартів прозорості, ліквідності, нейтральності щодо прибутковості — є критично важливим.

Санкції

Казначейство США запроваджує санкції проти фінансових мереж хуситів [6]



2 квітня 2025 року Міністерство фінансів США, через Управління з контролю за іноземними активами (OFAC), запровадило санкції проти фінансової інфраструктури єменського руху «Ансар Аллах» (хусити), який вважається спеціально визначеною глобальною терористичною організацією. Ці заходи включають блокування восьми криптовалютних адрес, що належать хуситам та пов'язаним з ними особам. Це частина ширшої стратегії США з перешкоджання фінансовій підтримці хуситів та їх зв'язків з Корпусом вартових ісламської революції – Силами Аль-Кудс (IRGC-QF) та іншими суб'єктами.

Згідно з аналізом TRM Labs, ці криптовалютні адреси були використані для переказу мільйонів доларів до інших високоризикових та підсанкційних суб'єктів, включаючи Саїда аль-Джамаля, іранського фінансового посередника, пов'язаного з хуситами та IRGC-QF, а також до адрес, пов'язаних з виробниками та продавцями безпілотних літальних апаратів та обладнання, пов'язаного з Китаєм та Росією.

Ці санкції є частиною ширшої кампанії США проти хуситів, яка включає військові удари та економічні заходи у відповідь на їхні атаки на торгові судна в Червоному морі. Хусити, які контролюють значну частину території Ємену, використовують різноманітні джерела фінансування, включаючи податки, митні збори, контрабанду та цифрові валюти, щоб обійти міжнародні санкції та фінансувати свою діяльність.

Ці дії підкреслюють важливість моніторингу цифрових активів у боротьбі з фінансуванням тероризму та необхідність міжнародної співпраці для запобігання використанню криптовалют у незаконних цілях.

[6] https://www.trmlabs.com/resources/blog/us-treasury-sanctions-houthi-financial-networks-including-eight-crypto-addresses?utm_campaign=Brand-Global_Weekly-Roundup_Newsletter&utm_medium=social&utm_source=linkedin&utm_campaignname=Brand-Global&utm_activity=Weekly-Roundup&utm_activitytype=Newsletter

Звіти окремих інституцій та експертів

Як російські «тіньові» кораблі загрожують Лівії та Європі[7]

Публікація Міжнародного консорціуму журналістів-розслідувачів (ICIJ), розкриває складну схему використання Росією так званого "тіньового флоту" — сотень старих комерційних суден із прихованим володінням — для обходу західних санкцій та постачання військового обладнання до Лівії. У центрі розслідування — випадок із судном Barbaros, зареєстрованим під камерунським прапором, яке перевозило російське обладнання до східної Лівії, підконтрольної воєначальнику Халіфі Хафтару. Ця історія є частиною ширшої стратегії Кремля, спрямованої на зміцнення впливу в Середземноморському регіоні та країнах Африки, що викликає занепокоєння європейських і американських офіційних осіб.

Події розгортаються навесні 2024 року, коли Barbaros перетнув Босфорську протоку в Стамбулі. Судно, яке розпочало свій шлях із Росії, привернуло увагу Йорюка Ішика, експерта з морської діяльності, який сфотографував його вантаж — вантажівки російського виробництва, часто використовувані у військових цілях і виготовлені компанією, що перебуває під санкціями. Ішик опублікував ці знімки на платформі X, назвавши Barbaros "судном, що викликає інтерес". Цей інцидент спричинив активність європейської морської місії Operation Irini, яка відстежує порушення міжнародного ембарго на постачання зброї до Лівії. Витік документів, отриманих ICIJ, показав, що Barbaros використовував низку хитрощів для уникнення виявлення: маніпуляції з автоматичною ідентифікаційною системою (AIS), що передає дані про місцеперебування судна, а також неодноразові зміни назви (тричі) та прапора (щонайменше 10 разів із 2013 року). Інтерпол склав звіт, у якому припустив, що судно могло перевозити вогнепальну зброю до Лівії, і рекомендував ретельний моніторинг.

1 травня 2024 року Operation Irini здійснила обшук Barbaros і виявила 115 російських вантажівок. Хоча ці транспортні засоби не були спеціально модифіковані для військового використання і формально не порушували ембарго, місія зазначила, що їхнє перевезення до порту Тобрук, контрольованого Хафтаром, свідчить про триваючу мілітаризацію регіону. Хафтар, ключовий союзник Росії в Лівії протягом майже десяти років, отримує від Москви зброю, фінансову підтримку та військовий персонал. ООН у 2023 році звинуватила його сили у скоєнні злочинів проти людяності, а Amnesty International повідомила про звірства, вчинені силовими органами під командуванням його сина. Водночас Хафтар, який має подвійне громадянство США та Лівії й десятиліттями проживав у Вірджинії, уникнув серйозних міжнародних наслідків: цивільні позови проти нього в США були відхилені, а в серпні 2024 року американські високопосадовці навіть провели з ним зустріч у Лівії.

"Тіньовий флот" відіграє ключову роль у російській стратегії, допомагаючи не лише обходити санкції на продаж нафти, а й розширювати вплив у Африці. Судна регулярно вимикають AIS поблизу сирійського порту Тартус, де Росія утримує базу, або фальсифікують дані про своє місцеперебування. Один із задокументованих випадків показав, як судно, що перевозило зброю з Сирії до Лівії, помилково передало своє розташування на суші біля аеропорту Бейрута замість морського порту. З початку 2024 року російська присутність у Лівії значно зросла: кількість авіарейсів до країни подвоїлася порівняно з 2023 роком, а найманців Wagner Group

[7] https://www.icij.org/news/2025/03/russias-ghost-ships-haunt-libya/

замінили підрозділи Africa Corps, підконтрольні російським збройним силам. Падіння режиму Башара Асада в Сирії у грудні 2024 року посилило цей процес — Росія почала переміщувати озброєння та підрозділи з Сирії до Лівії, уклавши угоду з Хафтаром про модернізацію авіаційної інфраструктури. За даними української військової розвідки, до Лівії перекинуто близько 3000 російських солдатів.

Ця ситуація викликає тривогу в Європі, де Лівію розглядають як "м'яке підчерев'я" континенту через її близькість до кордонів НАТО (400 миль) та роль у міграційних потоках. Росія використовує Лівію як плацдарм для логістичних маршрутів до Сахелю, отримуючи доступ до ресурсів, таких як уран у Нігері чи золото в Центральноафриканській Республіці. Європейські офіційні особи закликають до активнішого залучення до східної Лівії, щоб протидіяти Росії, однак Захід уникає жорсткої політики щодо Хафтара, побоюючись залишити вакуум, який заповнить Москва. Аналітик Анас Ель Гоматі з Інституту Садека називає це "стратегічною недбалістю Заходу", підкреслюючи, що російська військова присутність у Лівії загрожує не лише стабільності країни, а й безпеці Європи через контроль над міграцією та військовими операціями в Середземномор'ї. Хоча Росія не єдина країна, що порушує ембарго (Туреччина також використовувала подібні "тіньові судна"), її дії вирізняються масштабом і геополітичною вагою, що робить Лівію важливим елементом протистояння із Заходом.

Фінансові злочини 2025: Геополітика, ШІ та кіберзагрози — виклики та стратегії протидії [8]

Документ від Kroll являє собою ґрунтовне дослідження, яке детально аналізує сучасні тенденції, виклики та стратегії боротьби з фінансовими злочинами на порозі 2025 року. Звіт базується на результатах онлайн-опитування, проведеного у вересні-жовтні 2024 року, яке охопило понад 600 керівників вищої ланки — від генеральних директорів до головних юрисконсультів, директорів із комплаєнсу та ризик-менеджерів — із ключових фінансових і регульованих секторів, таких як фінансові послуги, бухгалтерія, страхування, нерухомість і юриспруденція. Географічно дослідження охоплює широкий спектр регіонів: США, Великобританію, Західну Європу (Франція, Німеччина, Ірландія, Італія, Іспанія, Швейцарія), Скандинавію (Норвегія, Швеція), Азію-Тихоокеанський регіон (Австралія, Індія, Японія), Гонконг, Сінгапур, Близький Схід і Африку (ОАЕ, ПАР), а також офшорні фінансові центри, такі як Британські Віргінські Острови, Кайманові Острови та Джерсі. Відповіді були анонімними, а дані аналізувалися в сукупності, що забезпечило об'єктивність і репрезентативність висновків. Звіт структурований за тематичними розділами, кожен із яких заглиблюється в конкретні аспекти фінансових злочинів, пропонуючи як аналітичний огляд, так і практичні рекомендації для організацій, які прагнуть протистояти зростаючим загрозам.

У вступному виконавчому резюме, підготовленому Девідом Льюїсом і Томасом Боком, підкреслюється, що 2025 рік стане переломним через поєднання факторів: геополітичної нестабільності, стрімкого розвитку штучного інтелекту (ШІ) та посилення регуляторного тиску. Згідно з опитуванням, 71% респондентів прогнозують зростання ризиків фінансових злочинів у порівнянні з 67% у 2023 році, що відображає зростаючу тривогу серед бізнес-лідерів. Водночас лише 23% оцінюють свої програми комплаєнсу як "дуже ефективні", що вказує на значний розрив між сприйняттям загроз і реальною готовністю до них. Ключовими драйверами зростання ризиків названо кібератаки (68%), використання ШІ злочинцями (61%),

[8] https://www.kroll.com/en/insights/publications/financial-crime-report-2025

а також зростання предикатних злочинів (38%), політичну нестабільність (30%), фінансові труднощі для окремих осіб (34%) і геополітичні ризики (30%). Криптовалюти також викликають занепокоєння: 59% вважають їх помірною або значною загрозою, при цьому 29% організацій уже приймають, визнають або здійснюють транзакції в криптовалютах, а ще 32% розглядають таку можливість, що свідчить про їхню трансформацію з нішевого інструменту в загальноприйнятий фінансовий актив. Позитивним моментом є те, що 57% респондентів бачать у ШІ потенціал для посилення програм боротьби зі злочинами, а 79% очікують, що їхні функції комплаєнсу візьмуть на себе більше відповідальності, причому 80% зазначають, що їхнє керівництво активно підтримує культуру доброчесності. Очікується також зростання співпраці між регуляторами та фінансовими установами (62%), а також посилення вимог до корпоративної прозорості та правозастосування, що додає складності для організацій у регульованих секторах.

Методологічна основа звіту детально описує процес збору даних, підкреслюючи, що опитування проводилося серед професіоналів із фінансових і регуляторних галузей, із рівним розподілом між фінансовими послугами (50%) та іншими секторами, такими як бухгалтерія, страхування, нерухомість і юриспруденція. Географічна різноманітність і анонімність відповідей дозволили отримати широкий спектр думок, а аналіз у сукупності усунув потенційні упередження.

У розділі ключових висновків звіт підсумовує основні тренди, які формують ландшафт фінансових злочинів. 71% респондентів очікують зростання ризиків, але лише 23% вважають свої програми комплаєнсу "дуже ефективними", що може бути пов’язано з недостатніми інвестиціями в технології (лише 30% сильно згодні з їхньою достатністю) та слабким управлінням (29% впевнені в надійності інфраструктури). Кібербезпека та ШІ є провідними каталізаторами ризиків, але лише 20% тих, хто використовує ШІ, відзначають його "дуже позитивний" вплив на комплаєнс, що становить падіння з 37% у 2023 році, ймовірно, через проблеми з даними та обмежені навички персоналу. Криптовалюти викликають занепокоєння у 59%, але лише 31% програм готові до пов’язаних ризиків, а 23% планують це в майбутньому. Геополітичні виклики також є проблемою: лише третина програм вважаються "дуже підготовленими", а менше 40% впевнені в санкційному скринінгу, що вказує на вразливість перед санкційними порушеннями.

Розділ, присвячений геополітичним напруженням, підготовлений Говардом Купером, Деном Райсом та Олівером Стерном, заглиблюється в те, як глобальні конфлікти, зокрема в Україні та на Близькому Сході, а також економічні тертя, наприклад, тарифи США, стимулюють фінансові злочини. Лише третина респондентів вважають свої програми готовими до геополітичних викликів, при цьому кіберзлочини (59%) та санкції (45%) є головними загрозами. Наприклад, кібератаки, підтримувані Іраном чи Росією, стають більш доступними завдяки ШІ, що ускладнює захист. Санкційні проблеми включають складність оновлення регуляцій (49%, зростання з 33% у 2023) і захист даних (44%, зростання з 38%). Криптовалюти також викликають занепокоєння у 77%, оскільки вони полегшують незаконні транзакції в умовах санкцій. Звіт підкреслює, що лише 38% впевнені в оцінці геополітичних загроз, із особливими тривогами в Азії-Тихоокеанському регіоні через напруження між США, Китаєм і Тайванем. Рекомендації включають доступ до різноманітних джерел розвідки, диверсифікацію ланцюгів поставок і зміцнення кіберстійкості, а також наголошують на потребі глобальної співпраці, яка ускладнена фрагментацією міжнародних норм і націоналістичними тенденціями.

Розділ про нову еру фінансових кіберзлочинів, авторства Тірнана Коннолі та Джона деКрейна, попереджає про експоненціальне зростання кіберзагроз: за оцінками МВФ, до 2027 року вони можуть коштувати світу $23 трлн, а організаційні збитки зросли до $2,5 млрд із 2017 року. Кібератаки (68%) та використання ШІ злочинцями (61%) очолюють список ризиків, особливо для юридичних, страхових секторів та сектору нерухомості. Проблеми ланцюгів поставок, як-

от "секретні витоки" (ненавмисне розкриття паролів чи ключів), посилюються залежністю від сторонніх інструментів і швидкими циклами розробки програмного забезпечення. Лише 37% впевнені в оцінці загроз ланцюгів поставок, а 56% тих, хто не впевнений, називають кібербезпеку головною проблемою. Регуляторні зміни, такі як DORA та NIS2 в ЄС, додають складності, вимагаючи від організацій посиленого управління ризиками сторонніх постачальників. Рекомендації зосереджені на управлінні обліковими даними, контролі доступу до мережі, належній перевірці SaaS-додатків і підвищенні кіберстійкості через регулярні оцінки та обмін даними.

Розділ про виклики ШІ, написаний Деном Райсом, Марком Тернером і Річардом Тейлором, детально аналізує подвійну природу ШІ: 57% бачать у ньому переваги для комплаєнсу, але 49% — значний ризик через його використання злочинцями, наприклад, для створення діпфейків чи фішингових атак. 25% організацій уже інтегрували ШІ у свої програми, 30% перебувають на ранніх етапах, але позитивне сприйняття впало до 20% із 37% у 2023 році через проблеми з якістю даних, недостатню підготовку персоналу та високий рівень хибних позитивів у таких процесах, як KYC. Регуляторні вимоги, зокрема AI Act в ЄС чи різноманітні закони США про алгоритмічну дискримінацію, ускладнюють адаптацію: лише 55% готові до них, а в юриспруденції та нерухомості цей показник ще нижчий (30% і 40% відповідно). Звіт підкреслює, що ШІ використовується для виявлення підозрілих моделей (63%), аналізу мереж (54%), виявлення ризиків (44%) та автоматизації завдань (41%), але його ефективність залежить від якісних даних і чіткого управління. Рекомендації включають регулярне навчання, тестування ШІ-систем, створення гнучких політик і "повернення до основ" у боротьбі з шахрайством, як-от людська перевірка, щоб протистояти складним атакам.

Висновки:

- **Посилення кіберстійкості та санкційного скринінгу:** Оскільки 68% респондентів називають кібератаки головною загрозою, а лише 39% впевнені у санкційному скринінгу, організації повинні інвестувати у кібербезпеку (47% уже планують це) та оновлювати санкційні процеси для відповідності регуляціям.
- **Стратегічне впровадження ШІ:** (57% респондентів бачать користь ШІ у боротьбі зі злочинами, але лише 20% відзначають позитивний вплив) зважаючи на це, компанії повинні впроваджувати ШІ з фокусом на якісні дані, регулярне тестування та навчання персоналу, щоб уникнути помилок.
- **Підготовка нефінансових секторів:** Сектори нерухомості та юриспруденції відстають у готовності (лише 26% і 33% планують інвестиції в ШІ), тому ці галузі повинні прискорити освіту персоналу та адаптувати програми комплаєнсу до нових вимог FATF, уникаючи шаблонних рішень.
- **Перегляд самовпевненості:** Лише 23% програм "дуже ефективні" (проти 31% у 2023), тому компанії повинні провести аудит своїх програм, інтегрувати технології з чітким управлінням та посилити навчання, щоб відповідати реальним загрозам, а не покладатися на хибну впевненість.

У розділі про те, що фінансові злочини не є виключно проблемою фінансового сектору, Ханна Россітер і Тарун Бхатія аналізують, як розширення регуляцій, зокрема зусилля FATF, впливає на нефінансові галузі. Фінансові послуги випереджають інші сектори завдяки строгим вимогам, таким як Bank Secrecy Act і KYC, із 36% організацій, де ШІ є частиною програм комплаєнсу. Натомість сектори нерухомості (58% впевнені в управлінні) і юриспруденції (63% — у технологіях) значно відстають, що робить їх уразливими до нових правил. Страхування демонструє високу готовність (88% вважають технології достатніми), але стикається з ризиками на стороні активів, тоді як бухгалтерія (97% готові до due diligence) бореться зі складнощами аудиту fintech-клієнтів і вимогами звітності про шахрайство в

таких країнах, як Індія та Японія.

Регулятори посилюють тиск: наприклад, в Гонконзі страхова компанія отримала штраф у $2,9 млн за недоліки в AML, а в Великобританії агенти з нерухомості оштрафовані на £1,6 млн. Рекомендації пропонують освіту персоналу, цільове навчання з AML/KYC, аутсорсинг для швидкого нарощування експертизи та уникнення шаблонних рішень, які не відповідають специфічним потребам організацій.

Останній розділ, підготовлений Амандою Вуд, Марком Тернером і Лорою Волстер, під назвою "Впевненість чи самовдоволення?" застерігає про розрив між високою впевненістю організацій і їхньою реальною ефективністю. 71% вважають свої технології достатніми, 90% мають певну впевненість у виявленні геополітичних загроз, але лише 23% програм оцінені як "дуже ефективні" — падіння з 31% у 2023 році. Приклади великих штрафів у 2024 році, таких як $3 млрд для північноамериканського банку за системні недоліки в AML чи £29 млн для британського онлайн-банку за слабкий санкційний скринінг, підкреслюють проблему. Регіональні відмінності також помітні: 39% у Близькому Сході та Африці оцінюють свої програми як "дуже ефективні" проти 20% у Великобританії, що може відображати меншу зрілість регуляцій у деяких регіонах. Проблеми включають недостатнє розуміння вразливостей, слабку інтеграцію технологій (особливо при додаванні ШІ до застарілих систем) і низьку якість даних, що знижує ефективність комплаєнсу. Рекомендації зосереджені на міцному управлінні, регулярному навчанні, адаптації до специфічних ризиків і створенні культури підзвітності, де звіти про підозрілі дії сприймаються серйозно на всіх рівнях.

Загалом звіт малює складну картину, де фінансові злочини еволюціонують під впливом технологій, геополітики та регуляторних змін. ШІ та кібербезпека є як можливостями, так і загрозами, тоді як розширення вимог до нефінансових секторів вимагає швидкої адаптації. Організації закликаються переглянути свої програми комплаєнсу, інвестувати в технології та навчання, співпрацювати з регуляторами і перейти від потенційної самовпевненості до справжньої готовності, щоб ефективно протистояти викликам 2025 року в дедалі складнішому глобальному ландшафті.

Аналітика боротьби з фінансовими злочинами [9]

Цей звіт є комплексним оглядом нових викликів, ризиків та кращих практик у сфері протидії фінансовим злочинам, зібраним на основі практичного досвіду провідних фахівців та компаній, що надають технологічні рішення для ПВК/ФТ/ФР. У центрі уваги — ключові виклики 2025 року: зростання складності нормативного регулювання, еволюція методів шахрайства та відмивання коштів, зростання ролі штучного інтелекту, а також потреба у тісній інтеграції комплаєнсу з бізнес-цілями.

У першому блоці увага зосереджена на проблемі хибнопозитивних спрацювань у моніторингу транзакцій, які забирають значні ресурси та сповільнюють реакцію на реальні загрози. Замість намагань зменшити їхню кількість, автори пропонують зробити їх операційно незначущими через автоматизацію, гнучке управління правилами моніторингу, чітке вимірювання витрат і інтеграцію з бізнес-процесами. Йдеться також про критичну необхідність розуміти реальні можливості ШІ-рішень, запроваджуючи лише ті, що дозволяють контроль і адаптацію.

[9] https://www.amlcube.com/_files/ugd/8d37e4_a5808c9fc0fe4dfdb5d0ad05332faed0.pdf

Другий тематичний блок стосується управління нормативними змінами. Відзначено, що динамічне правове середовище (особливо у ЄС, ОАЕ, Австралії та Канаді) ускладнює підтримку політик у відповідності до вимог. Важливими є не лише своєчасне оновлення процедур, але й цифровізація політик, запровадження безперервного навчання працівників із використанням ШІ-платформ та забезпечення людського контролю у застосуванні автоматизованих рішень. Особливої уваги потребує проблема браку кваліфікованих кадрів, що поєднують знання права, ризик-менеджменту і бізнесу.

Третій блок аналізує зростання загроз, пов'язаних із шахрайством при верифікації клієнтів. Звіт демонструє, що використання deepfake-відео, віртуальних камер і синтетичних ідентичностей суттєво підриває надійність класичних процедур перевірки. Пропонується поєднувати різні типи біометричної перевірки (active та passive liveness), ШІ-аналіз документів, багатоканальне джерело даних та додаткові перевірки у випадках високого ризику. Компанії мають тісно співпрацювати з вендорами для адаптації до нових патернів шахрайства.

У четвертому блоці детально розглядається виклик миттєвих платежів, які вимагають трансформації інфраструктури комплаєнсу. Основні проблеми — несумісність застарілих систем з реаліями реального часу, фрагментованість інструментів моніторингу та недостатня координація між командами з ПВК та боротьби з шахрайством. Автори наполягають на впровадженні концепції FRAML (поєднання Fraud + AML), що дозволяє виявляти схеми відмивання через шахрайські входи в систему, підвищити точність моніторингу та зменшити кількість хибних спрацювань. Особливо важливою стає прозорість та пояснюваність моделей ШІ, що використовуються у моніторингу.

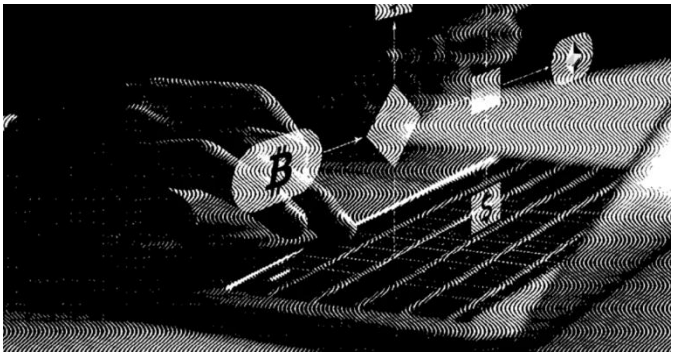
Останній блок присвячений скринінгу клієнтів і контрагентів. Документ наголошує на проблемі фрагментованих скринінгових систем, які ускладнюють оцінку ризиків, підвищують ймовірність пропуску загроз та призводять до регуляторних претензій. Пропонується централізувати процес скринінгу, забезпечити єдині підходи до оцінки ризиків, стандартизувати джерела даних і запровадити безперервний моніторинг. Застосування ШІ у скринінгу має базуватися на якісних даних та відповідати регуляторним вимогам.

Загалом звіт є глибоким практичним посібником, який спрямований на трансформацію фінансового комплаєнсу з реактивної функції у стратегічний елемент управління ризиками через інноваційні підходи, інтегровані технології та безперервну адаптацію до змін.

Висновки:

- **Перехід від скорочення хибнопозитивних спрацювань до їх операційної нейтралізації:** установи мають інвестувати у системи "пригнічення", що дозволяють ігнорувати неактуальні хибні сигнали, забезпечуючи швидку обробку дійсно ризикованих транзакцій.
- **Впровадження FRAML-підходу**: слід створити єдину платформу моніторингу з можливістю реального часу, де аналітики з ПВК і шахрайства працюють узгоджено над спільними ризиками.
- **Оновлення верифікаційних систем для протидії ID-шахрайству:** слід поєднувати активну та пасивну перевірку присутності, ШІ-документ-аналіз, додаткові ідентифікаційні фактори та періодично оновлювати системи верифікації відповідно до нових загроз.
- **Цифровізація політик і навчання:** замість періодичних тренінгів варто впроваджувати адаптивні ШІ-моделі безперервного навчання працівників з урахуванням їхньої ролі та змін у законодавстві; цифрові політики повинні бути динамічними, з автоматизованим управлінням змінами.

Як безпечно вести банківські операції з криптовалютою: системи належної перевірки та управління ризиками для фінансових установ [10]



У статті компанія Elliptic висвітлює один із найактуальніших і найскладніших викликів для фінансового сектору — ефективне та безпечне обслуговування криптовалютних бізнесів у рамках відповідності до вимог ПВК/ФТ/ФР. Історично банки та інші традиційні фінансові установи демонстрували обережність або й відмову працювати з представниками криптоіндустрії через ризики, пов'язані з відмиванням коштів, шахрайством та технологічною складністю моніторингу цифрових активів. Проте зростання крипторинку та поява зрілих, ліцензованих гравців, які впроваджують комплаєнс-стандарти, робить питання налагодження взаємодії більш актуальним, ніж будь-коли.

Elliptic аргументовано демонструє, що для того, щоб обслуговувати криптовалютні компанії надійно та безпечно, фінансовим установам слід не уникати ризику, а управляти ним на основі адаптованих процедур належної перевірки та структурованого ризик-менеджменту. Автори радять банкам не відмовляти криптокомпаніям у доступі до рахунків лише через їхню діяльність, а натомість оцінювати конкретні ризики, пов'язані з кожним клієнтом, з урахуванням його типу (біржа, кастодіан, постачальник DeFi-послуг тощо), географії, характеру активів та історії регуляторної взаємодії.

Висновки:

- **Криптобізнеси можуть бути безпечними клієнтами, якщо банки адаптують CDD до специфіки цифрових активів.** Оцінка гаманців, типів активів, сегрегації коштів та історії комплаєнсу є критичною для правильної класифікації ризику.
- **Поступова стратегія співпраці — найкращий шлях для банків.** Варто починати з менш ризикових клієнтів і переходити до складніших випадків через пілотні проєкти.
- **Інвестиції у комплаєнс та партнерство з аналітичними провайдерами — ключ до стабільної взаємодії з крипторинком.** Це дозволяє реагувати не реактивно, а на основі системного підходу до ідентифікації, моніторингу та реагування на ризики.
- **Банки, які зможуть побудувати ефективну модель роботи з криптоклієнтами, отримають ринкову перевагу.** У контексті глобалізації фінансових технологій, взаємодія з віртуальними активами стає не опцією, а неминучістю.

Ключову частину статті становить опис чотирьох додаткових міркувань, які банки повинні включити до процедури CDD щодо криптовалютних клієнтів:

1. Перевірка криптовалютних гаманців: установи мають з'ясовувати, якими гаманцями користуються їхні клієнти — кастодіальними чи ні, чи здатні вони ідентифікувати бенефіціара кожного гаманця, і як клієнт розмежовує власні кошти від коштів користувачів.
2. Типи активів: важливо розуміти, з якими токенами працює клієнт. Наприклад, наявність стейблкоїнів, монет з функціями анонімності (privacy coins) чи нішевих цифрових активів, які використовуються в схемах шахрайства, має суттєве значення для оцінки ризиків.
3. Сегрегація коштів: чи належним чином криптобізнес відокремлює свої

[10] https://www.elliptic.co/blog/how-to-safely-bank-a-crypto-business

власні активи від клієнтських. Цей елемент не лише має значення в контексті ПВК, але і впливає на захист прав клієнтів у разі банкрутства.

4. Прозорість та історія комплаєнсу: установи повинні перевіряти, чи проходив криптобізнес аудит, чи є в нього задокументовані комплаєнс-процедури, чи брав він участь у публічних розслідуваннях або мав претензії з боку регуляторів.

На додаток до цих елементів, Elliptic пропонує фінансовим установам побудувати стратегію управління ризиками у форматі поступового розширення взаємодії з криптосектором. На першому етапі — це може бути співпраця з компаніями, які лише опосередковано пов'язані з цифровими активами (наприклад, провайдери платіжних послуг). Далі — з повністю ліцензованими біржами чи постачальниками кастодіальних послуг, які мають відкриту публічну політику, звітність і досвід взаємодії з регуляторами. На фінальному етапі — співпраця з новими ринками або складними продуктами (наприклад, DeFi-платформами або DAO), але лише після впровадження пілотних проєктів.

Elliptic також радить банкам розглядати впровадження пілотних програм співпраці з криптовалютними компаніями. Це дозволяє протестувати політики, процедури та технологічні рішення в умовах контрольованого ризику. Такий підхід допомагає банку навчити свої команди, адаптувати внутрішні процеси та поступово вибудувати компетенцію в обслуговуванні цифрових активів.

Загалом, стаття є практичним дороговказом для будь-якої фінансової установи, яка бажає (або вже змушена) мати справу з криптоклієнтами. Вона переконує, що уникнення — це не стратегія, а втрачена можливість. Натомість потрібні глибоке розуміння специфіки криптовалютного середовища, перевірені інструменти моніторингу та обміну даними (зокрема, аналітика блокчейнів), а також гнучка, але структурована політика управління ризиками.

ВНУП

Загроза торгівлі антикваріатом: Чому США потребують команди прокурорів із культурних злочинів [11]

Ексклюзивне інтерв'ю з Ріком Сент-Хіларом, адвокатом і експертом у галузі права культурної спадщини, присвячене перевиданню його політичного брифінгу 2016 року, в якому він запропонував конкретне рішення для боротьби з безкарністю торговців антикваріатом — створення спеціалізованої команди прокурорів у Міністерстві юстиції США (DOJ). Інтерв'ю складається з трьох ключових питань, які детально розкривають сучасний стан проблеми незаконної торгівлі культурними цінностями, прогрес у законодавстві та правозастосуванні США за останні десять років, а також актуальність і практичність рекомендацій Сент-Хілара в умовах сьогодення. Текст базується на аналізі реальних прикладів, статистики та змін у правовому полі, пропонуючи читачеві глибоке занурення в цю складну тему.

Минуло майже десять років з моменту, коли Сент-Хілар спільно з Antiquities Coalition вперше звернув увагу на проблему безкарності торговців антикваріатом. Автор зазначає, що, хоча правоохоронні органи США досягли певних успіхів у перехопленні вкрадених і розграбованих

[11] https://acthinktank.scholasticahq.com/post/3055-holding-antiquities-traffickers-accountable-an-exclusive-interview-with-think-tank-author-rick-st-hilaire

артефактів на кордоні, кримінальне переслідування, засудження та ув'язнення злочинців залишаються рідкістю. У 2016 році він запропонував створити спеціалізовану команду прокурорів у DOJ, яка б мала необхідні знання та досвід для розслідування таких справ, винесення вироків і демонтажу кримінальних мереж. Перевидання брифінгу в 2025 році стало приводом для цього інтерв'ю, в якому Сент-Хілар оцінює, наскільки його ідеї залишаються актуальними, враховуючи зміни в американському правовому та правоохоронному ландшафті.

Перше питання стосується еволюції проблеми безкарності за останнє десятиліття. Сент-Хілар визнає, що США, як найбільший арт-ринок світу з часткою 42% у $65-мільярдній індустрії 2024 року, несуть особливу відповідальність за боротьбу з культурним рекетом. Він відзначає певний прогрес, зокрема створення унікального Підрозділу боротьби з торгівлею антикваріатом (ATU) у Мангеттені під керівництвом помічника окружного прокурора Метью Богданоса. Цей підрозділ використав закони штату Нью-Йорк про отримання вкраденого майна, щоб забезпечити винесення 16 вироків за торгівлю культурними цінностями — підхід, який Сент-Хілар підтримував ще з 2005 року. Водночас на федеральному рівні ситуація залишається менш обнадійливою. Як приклад наводиться справа U.S. v. Eldarir, де контрабандист Ашрам Омар Ельдарір був спійманий із 500 єгипетськими артефактами, визнав провину за чотири федеральні злочини, але його покарання ще не визначено. Сент-Хілар ставить питання: чи буде вирок достатньо суворим, щоб стримати інших злочинців, і чи почнуть федеральні прокурори активніше боротися з цією проблемою? Він висловлює скептицизм, базуючись на історичних прецедентах.

Далі автор переходить до критики нинішньої федеральної стратегії боротьби з культурними злочинами. Сент-Хілар згадує справу Фредеріка Шульца, відомого арт-дилера, засудженого у 2000-х до трьох років в'язниці, як втрачену можливість для створення стійкої системи переслідування. Замість того, щоб розвинути цей успіх, федеральні органи зосередилися на вилученні артефактів і поверненні їх країнам походження — підхід, який він називає "лінивою політикою seize & send". Така стратегія, на його думку, не замінює ретельних розслідувань, обвинувальних актів і судових процесів, необхідних для боротьби зі злочинністю. Він стверджує, що відсутність послідовного переслідування надсилає торговцям чіткий сигнал: незаконна торгівля антикваріатом залишається прибутковою діяльністю з низьким ризиком і м'якими наслідками навіть у разі затримання. Для ефективної боротьби потрібні рішучість, компетентність, готовність іти на ризик і наполегливість — якості, яких, на його думку, федеральним прокурорам поки що бракує.

Друге питання фокусується на змінах у законодавстві США з 2016 року та їх впливі на потребу в команді прокурорів із культурних злочинів. Сент-Хілар вітає кілька ключових нововведень. По-перше, включення дилерів антикваріатом до Закону про банківську таємницю (BSA) стало значним кроком уперед, адже тепер вони зобов'язані повідомляти про підозрілі фінансові операції, що допомагає виявляти відмивання грошей. По-друге, розширення двосторонніх угод за Законом про імплементацію культурної власності (CPIA) ввело імпортні обмеження на артефакти з країн, що страждають від розграбування, зменшуючи потік незаконних предметів до США. По-третє, успіхи спеціалізованих підрозділів, таких як ATU у Мангеттені, демонструють, що цілеспрямоване переслідування може бути ефективним. Проте ці зміни, хоч і створюють міцну основу, не призводять до систематичних вироків без спеціалізованої команди в DOJ. Така команда могла б перетворювати фінансову розвідувальну інформацію на кримінальні справи, посилювати стримуючий ефект імпортних обмежень через судові переслідування та забезпечувати єдиний національний підхід до боротьби з цими злочинами. Сент-Хілар підкреслює, що вилучення артефактів без покарання злочинців недостатньо — потрібні реальні судові наслідки, включно з тюремними строками та штрафами.

Третє питання заглиблюється в конкретну пропозицію Сент-Хілара: призначення щонайменше чотирьох прокурорів, які б спеціалізувалися на транснаціональній торгівлі антикваріатом. Він

визнає, що це не єдиний можливий шлях, але вважає його значним кроком уперед, якщо є воля до переслідування. Автор розрізняє два типи прокурорів: тих, хто долає труднощі заради справедливості, і тих, хто зосереджується на перешкодах і уникає дій. У контексті культурних злочинів він закликає до стратегічного підходу, який би максимізував вплив за обмежених ресурсів. Як приклад він наводить просте, але ефективне звинувачення — брехню в митних деклараціях. Уявіть, каже він, ситуацію, коли контрабандист декларує етруську вазу вартістю $25,000 як "керамічний виріб" за $2,000 із Великобританії. Показавши присяжним документи та реальний предмет, прокурор може легко довести федеральний злочин із очевидною брехнею. Такий підхід робить вироки швидкими, переконливими та зрозумілими, підвищуючи ризик для злочинців. Сент-Хілар стверджує, що створення команди спеціалізованих прокурорів у DOJ залишається актуальним і практичним рішенням, яке могло б скористатися останніми законодавчими змінами для реального впливу.

Таким чином, створення спеціалізованої команди прокурорів у Міністерстві юстиції США є критично важливим кроком для подолання безкарності торговців антикваріатом. Така команда повинна зосередитися на транснаціональних культурних злочинах, координуючи зусилля між такими агентствами, як ФБР, Homeland Security Investigations (HSI) та Financial Crimes Enforcement Network (FinCEN). Її завдання — не лише реагувати на випадки контрабанди, а й переводити фінансові розвіддані, отримані завдяки Закону про банківську таємницю, у конкретні обвинувальні акти та судові вироки, забезпечуючи системний підхід до боротьби з цими злочинами на національному рівні.

Федеральна політика потребує радикального зрушення від нинішньої практики вилучення артефактів і їх повернення країнам походження до активного кримінального переслідування. Замість того, щоб зупинятися на поверненні культурних цінностей, DOJ має інвестувати в ретельні розслідування, які виявлятимуть і руйнуватимуть кримінальні мережі. Це означає зміну фокусу з пасивного "seize & send" на стратегію, яка передбачає тюремні строки фінансові штрафи та демонтаж інфраструктури злочинців, щоб зробити торгівлю антикваріатом менш привабливою через реальні наслідки.

Висновки:

- **Необхідно створити спеціальну команду прокурорів:** Призначити щонайменше чотирьох спеціалізованих прокурорів для боротьби з торгівлею антикваріатом, щоб забезпечити системне переслідування та координацію між ФБР, HSI та FinCEN.
- **Необхідно відійти від політики "seize & send":** Замість вилучення та повернення артефактів зосередитися на розслідуваннях і судових вироках, щоб зруйнувати кримінальні мережі.
- **Потрібно використовувати прості звинувачення:** Застосування чітких звинувачень, таких як, наприклад, брехня в митних деклараціях, для швидких і переконливих вироків, підвищує ризик для злочинців.
- **Необхідне посилення виконання законів:** Повною мірою реалізація BSA та CPIA, перетворює фінансову прозорість і імпортні обмеження на інструменти для кримінального переслідування.

Прокурорам слід обирати прості, але ефективні звинувачення, такі як фальсифікація митних декларацій, щоб забезпечити швидкі та переконливі вироки. Наприклад, доведення обману в документах — коли контрабандист декларує археологічний артефакт як дешевий сувенір — може стати потужним інструментом у суді. Такий підхід мінімізує складність справ, робить докази зрозумілими для присяжних і підвищує ймовірність засудження, одночасно збільшуючи ризик для злочинців і змінюючи їхнє сприйняття торгівлі як "безпечного" бізнесу.

Необхідно максимально реалізувати потенціал нещодавніх законодавчих змін, таких як включення дилерів антикваріатом до Закону про банківську таємницю та розширення

імпортних обмежень за Законом про імплементацію культурної власності. Ці інструменти повинні працювати не лише для виявлення підозрілих транзакцій чи вилучення артефактів, а й для створення міцної бази для кримінальних справ. DOJ має гарантувати, що фінансова прозорість і контроль імпорту стають основою для переслідувань, а не зупиняються на адміністративних заходах, забезпечуючи реальні покарання для порушників.

Рекомендовані матеріали та заходи

Розбіжності між ЄС та США у застосуванні санкцій [12]

В умовах нової геополітичної реальності, коли санкції стали не лише інструментом стримування, але й важелем геоекономічного впливу, другий епізод подкасту This Month in EU Sanctions виступає як змістовний дороговказ для розуміння сучасної санкційної політики ЄС. Випуск, присвячений подіям березня 2025 року, порушує важливі питання про ефективність санкцій, їхню еволюцію, взаємодію між юрисдикціями та ризики, які санкційний режим ЄС створює для третіх сторін — передусім, для фінансових установ за межами ЄС.

У центрі дискусії — зростаюча різниця у підходах між Європейським Союзом та Сполученими Штатами щодо санкцій проти росії. Попри загальну солідарність у відповідь на військову агресію рф, ЄС, як підкреслюють ведучий Ян Дунин-Вашовіч та запрошені експерти Джефф Нільсен і Гонсало Саїс, поступово формує власну нормативну автономію та підхід, зокрема через інструменти вторинного та допоміжного санкційного впливу. Йдеться про так звані “ancillary listings” — явище, коли ЄС включає до списку санкцій не лише основних порушників, а й третіх осіб, що прямо або опосередковано сприяють санкційно обмеженим суб’єктам.

Окрема увага приділяється питанню включення неєвропейських фінансових установ до санкційного списку. Після такого включення жодна особа чи організація, яка підпадає під дію права ЄС, не має права здійснювати фінансові чи комерційні операції з цією установою. Це, фактично, ізолює банк від європейського фінансового ринку й завдає серйозних збитків, перетворюючи санкції на економічну зброю довготривалої дії. Такий режим є попередженням для глобального банківського сектору: навіть не будучи фізично присутнім в ЄС, банк може опинитись під його санкційним впливом, якщо він співпрацює з особами, що підтримують російську війну.

Підкаст також висвітлює складні політичні дилеми, які стояли перед лідерами ЄС у березні 2025 року: з одного боку, загроза трансатлантичної торговельної війни через політику тарифів США, з іншого — необхідність нарощування витрат на оборону й одночасного збереження єдності у санкційній коаліції. Європейський Союз намагається утримати цей баланс, впроваджуючи нові санкційні заходи проти росії, зокрема в межах вже 17-го пакету, а також розширюючи регуляторне охоплення на інші юрисдикції, зокрема Білорусь і Демократичну Республіку Конго.

Інституційна модернізація теж не залишилась поза увагою. ЄС у березні запустив спеціальну “санкційну гарячу лінію” — Help Desk — для малих та середніх підприємств, які часто стикаються з труднощами у розумінні й дотриманні складних вимог санкційного режиму. Це

[12] https://www.youtube.com/watch?v=lN-DusahpS4&ab_channel=ThisMonthinEUSanctions

рішення є визнанням того, що ефективність санкцій залежить не лише від нормативної строгості, а й від практичної здатності бізнесу до відповідності цим нормам.

Обговорення з Нільсеном і Саїсом зосереджується також на вторинних санкціях: їхній природі, межах правового регулювання в рамках ЄС і ризиках, які вони створюють. Експерти наголошують на необхідності чіткого концептуального підходу до розуміння санкційного впливу на третіх осіб — компанії, банки, постачальників, що не є прямо пов'язаними з росією, але можуть через ланцюжки постачання чи посередництво фактично сприяти обходу обмежень. У центрі уваги — необхідність правової ясності та послідовності: санкційна рамка ЄС, зокрема Регламент Ради № 269/2014, поступово розширює критерії включення до санкційних списків, охоплюючи все більше структур за межами рф.

Підкаст завершується важливою тезою: у разі послаблення санкційної політики США, ЄС може опинитися в ситуації, коли саме він залишиться головним носієм санкційного тиску на росію. Це вимагає від Брюсселя стратегічного переосмислення санкційного інструментарію, з урахуванням не лише поточної геополітики, а й довгострокової відповідальності за міжнародну безпеку.

European Anti-Financial Crime Summit 2025 [13]

Європейський саміт з протидії фінансовим злочинам 2025 (European Anti-Financial Crime Summit 2025) стане однією з ключових подій року у сфері ПВК/ФТ, фінансового комплаєнсу та кіберзахисту. Захід відбудеться 7 травня 2025 року в самому серці Дубліна, Ірландія, у престижному конференц-центрі RDS Convention Centre. Цей саміт традиційно збирає провідних експертів галузі, високопосадовців регуляторних органів, представників правоохоронних структур, банків, фінтех-компаній, криптоплатформ, а також фахівців із боротьби з шахрайством та торгівлею людьми.

Програма EAFCS2025 включає як пленарні сесії з ключовими виступами, так і дискусійні панелі з глибоким аналізом найгостріших викликів. Основна тематика саміту зосереджена на стрімких змінах регуляторного середовища у ЄС та Великій Британії, а також на наслідках політики "нормативного згортання" у США, що створює нові виклики для комплаєнс-підрозділів у Європі. Очікується, що учасники отримають не лише стратегічні орієнтири, а й практичні інструменти для посилення ефективності комплаєнс-функцій у своїх установах.

Серед основних тем, які будуть висвітлюватися на саміті: запуск AMLA та створення Єдиного регуляторного зводу правил (Single Rule Book), виклики впровадження ШІ та інновацій у боротьбі з фінансовими злочинами, побудова ефективних публічно-приватних партнерств для обміну інформацією, специфіка ризиків у криптосекторі, комплексне управління ризиками шахрайства в банках, а також протидія торгівлі людьми та сучасному рабству.

Серед підтверджених спікерів — Бруна Шего, голова новоствореного органу ЄС - AMLA, яка виголосить вступну доповідь. Участь у панелях візьмуть також Андреа Боу, директор FCA; Катерін Де Болль, виконавчий директор ЄВРОПОЛ; Маркус Плеєр, заступник генерального директора німецького міністерства фінансів та колишній Президент FATF; модератори панелей — знані експерти, серед яких Стівен Рей, Патрісіа Данн та Авалон Інгрем.

[13] https://www.amlintelligence.com/asp-products/european-anti-financial-crime-summit-2025/

Захід відкриється о 7:00 ранку реєстрацією учасників, а з 7:30 розпочнеться сніданок "Women in FinCrime" — окремий нетворкінг-формат для жінок, що працюють у сфері протидії фінансовим злочинам. Основна сесія саміту офіційно відкриється о 09:00, а завершиться о 17:00 фуршетом у атмосферній бібліотеці RDS. Для учасників передбачено знижки на проживання у партнерських готелях, а реєстраційна вартість становить €547.

Участь у саміті буде особливо цінною для керівників та фахівців комплаєнс-департаментів, аналітиків ПВК/ФТ, розробників технологічних рішень, юристів, державних службовців, працівників ПФР і банківських установ. Це також унікальна можливість для професійного розвитку цілих команд, адже формат саміту поєднує стратегічне мислення з практичною експертизою.

Для реєстрації або отримання листа-підтвердження для внутрішнього затвердження участі (approval request), організатори просять звертатися на електронну адресу: afcsummit@amlintelligence.com.

Інші новини

Цифрова допомога чи обман: правда про DFC [14]

Публікація є ґрунтовним розслідуванням діяльності американської компанії Digital Forensics Corporation (DFC), що базується в Огайо та пропонує послуги з боротьби з фінансовим сексторшеном — видом кіберзлочинів, який стрімко набирає обертів у Північній Америці, переважно вражаючи дітей і молодих людей. Розслідування спирається на широкий спектр джерел: бізнес-документи, судові позови, внутрішні матеріали компанії, понад 100 скарг до державних регуляторів і Better Business Bureau (BBB), а також інтерв'ю з майже трьома десятками клієнтів і шістьма співробітниками — трьома колишніми та трьома чинними. Основна теза статті полягає в тому, що DFC, попри свою репутацію одного з лідерів у сфері комерційної допомоги жертвам сексторшену, стикається зі звинуваченнями у завищених обіцянках, високих цінах, маніпулятивних тактиках продажів і сумнівній ефективності своїх методів, хоча сама компанія категорично відкидає ці претензії, посилаючись на тисячі позитивних відгуків.

Сексторшен описується як злочин, де шантажисти вимагають гроші, погрожуючи оприлюднити інтимні матеріали жертви, і DFC позиціонує себе як компанію-рятівника, обіцяючи відстежити злочинців і допомогти видалити вкрадений контент. Однак розслідування виявляє, що в контрактах компанії чітко вказано відсутність гарантій результатів через непередбачуваність дій шантажистів, що суперечить її агресивному маркетингу. DFC використовує двоетапну стратегію продажів: "Phase I" (початковий пакет від $1,499) і "Phase II" (дорожчий моніторинг акаунтів), що може коштувати клієнтам до $20,000. Ціни доповнюються можливістю розстрочки на шість років із відсотковою ставкою до 18%, а в разі несплати клієнти стикаються з агресивним стягненням боргів — наприклад, один чоловік отримав 35 дзвінків за чотири місяці після оголошення банкрутства.

Особливу увагу приділено тактикам залякування, які застосовує DFC. Внутрішні сценарії продажів, отримані USA TODAY, показують, як співробітники компанії використовують

[14] https://www.usatoday.com/story/life/health-wellness/2025/03/20/digital-forensics-sexortion-blackmail-recovery-services/81934584007/

емоційну вразливість жертв, залякуючи їх сценаріями, де шантажисти можуть опублікувати матеріали, сфабрикувати звинувачення в педофілії чи продати особисті дані на даркнеті. Клієнтам часто радять продовжувати спілкування з шантажистами, щоб DFC могла відстежити їх через спеціальні посилання, що суперечить рекомендаціям ФБР і експертів із кібербезпеки, які закликають блокувати злочинців і не вступати з ними в контакт. Компанія також погрожує судовими позовами за негативні відгуки та забороняє клієнтам їх публікувати в контрактах, що викликало критику з боку BBB, яка видала два попередження про DFC і отримала 92 скарги за три роки.

DFC на чолі з юрисконсультом Джеромі Сімоновичем захищає свою діяльність, стверджуючи, що працює прозоро, попереджаючи клієнтів про складність боротьби з кіберзлочинцями з країн третього світу, і спирається на позитивний досвід 2700 клієнтів із січня 2024 року. Сімонович пояснює тактики продажів як "пояснення наслідків" і зазначає, що шантажисти починають боятися компанії завдяки її репутації. Проте численні клієнти скаржаться, що DFC не надає доказів видалення контенту, а лише тимчасово зменшує їх тривогу.

Експерти та офіційні органи, зокрема ФБР (попередження від квітня 2023 року) і Департамент внутрішньої безпеки, застерігають від співпраці з комерційними фірмами на кшталт DFC, рекомендуючи безкоштовні ресурси, такі як Take It Down для неповнолітніх або StopNCII.org для дорослих. Вони зазначають, що повне видалення контенту з інтернету технічно неможливе без доступу до пристрою шантажиста, а методи DFC, як-от відправка листів із погрозами злочинцям, не мають юридичної сили.

Загалом розслідування викриває етичні та практичні проблеми в діяльності DFC, від агресивного тиску на клієнтів до завищених цін і неефективних методів, закликаючи жертв звертатися до правоохоронців і уникати комерційних компаній, які можуть погіршити їхнє становище.

Chainalysis Links NYC 2025: Інновації, Безпека та Співпраця у Майбутньому Криптовалют [15]

2 квітня 2025 року в Нью-Йорку відбулася конференція Chainalysis Links NYC 2025. Цей захід, організований компанією Chainalysis, зібрав представників урядових структур, правоохоронних органів, фінансових інститутів та криптоіндустрії для обговорення інновацій, безпеки та співпраці у сфері блокчейн-технологій і криптовалют. Документ охоплює доповіді, панельні дискусії, презентації нових продуктів і ключові меседжі, спрямовані на створення прозорої, безпечної та регульованої екосистеми цифрових активів. Основний акцент зроблено на тому, як технології, партнерства та регулювання можуть спільно сприяти розвитку глобальної фінансової інфраструктури, побудованої на блокчейні.

Конференція розпочалася з виступу генерального директора Chainalysis Джонатана Левіна, який підкреслив стрімке зростання криптоіндустрії та її вплив на світові фінанси. Він назвав цей момент найцікавішим за десять років своєї роботи в компанії, але водночас звернув увагу на виклики: зростання загроз від хакерів, пов’язаних із такими державами, як Північна Корея, та шахрайств, що використовують штучний інтелект (ШІ). Левін розповів про нещодавні

[15] https://www.chainalysis.com/blog/links-nyc-2025-day1/

придбання Chainalysis — компаній Hexagate і Alterya, які підсилюють безпеку смарт-контрактів і допомагають боротися з шахрайством, а також наголосив на необхідності співпраці між урядами, бізнесом і технологічними компаніями для створення безпечнішої крипто-екосистеми.

Далі віце-президент із продуктів Еммануель Маро представив низку нових інструментів Chainalysis, спрямованих на спрощення складних процесів і підвищення ефективності роботи з блокчейн-даними. Серед них — оновлений Reactor, який став швидшим і зручнішим для розслідувань, названий "найгіршим кошмаром злочинців", а також Rapid — інструмент на базі ШІ, що дозволяє проводити запити природною мовою. Було презентовано Chainalysis Data Solutions (DS) для кастомізованого моніторингу загроз і оновлення для комплаєнсу, такі як Compliance Insights Dashboard та Asset Intelligence, якими вже користуються 9 із 10 найбільших централізованих бірж. Маро також детально зупинився на Hexagate — інструменті для виявлення вразливостей смарт-контрактів за допомогою машинного навчання, і Alterya, яка допомагає виявляти шахрайство на ранніх етапах. Він підкреслив критичну роль відповідального використання даних у боротьбі з шахрайствами, що стрімко зростають через ШІ, і наголосив, що сама по собі прозорість блокчейну недостатня — потрібні інструменти для її ефективного використання.

Ще однією важливою темою стала політика нової адміністрації США щодо криптовалют, яку обговорили Бо Хайнс, виконавчий директор Ради президента з цифрових активів, і Сара Ворд, головна юрисконсультка Chainalysis. Хайнс окреслив амбітні плани щодо створення найбільш сприятливого для криптовалют середовища в США, включаючи законодавство про стейблкойни, модернізацію регулювання та формування стратегічного резерву біткойнів. Він підкреслив унікальність біткойна і наголосив на прагненні адміністрації зробити США глобальним лідером у цифрових фінансах, зберігаючи при цьому фінансову стабільність через співпрацю з Конгресом, агентствами та приватним сектором.

Панель, присвячена взаємодії криптовалют і правоохоронних органів, за модерацією Джима Лі з Chainalysis, об’єднала представників поліції Нью-Йорка, Лондона та Женеви. Meghann Teubner з NYPD зазначила, що головною проблемою в Нью-Йорку є фінансування насильства через криптовалюту, і наголосила на потребі навчання понад 30 000 офіцерів базовим поняттям, таким як "seed phrase". Філ Девіс із лондонської Met Police назвав державно-приватні партнерства основою успіху, а Патрік Гіон із поліції Женеви передбачив, що в майбутньому цифрове життя може стати важливішим за реальне, підкресливши значення міжнародного обміну інформацією. Учасники дійшли згоди, що для боротьби з дедалі складнішими злочинами необхідні партнерства, навчання та передові інструменти.

Сесія про життя блокчейн-хакера, яку провели Нів Єхезкель і Авів Шавіт із Chainalysis, розкрила методи атак на смарт-контракти в DeFi, демонструючи реальні приклади експлуатації вразливостей. Ця презентація підкреслила важливість проактивних заходів безпеки для захисту користувацьких коштів і показала технічну складність сучасних хакерських атак.

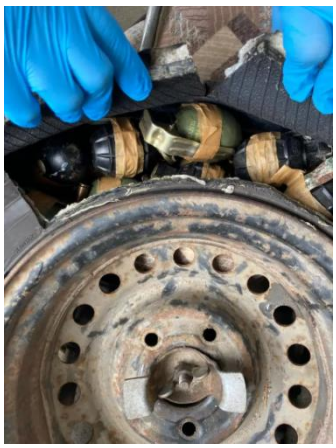
Інша панель, модерована Ліаною Різзі, зосередилася на інтеграції криптовалют у традиційні фінанси за участю представників Standard Chartered, Towerbank і MoraBanc. Учасники обговорили адаптацію до нових регуляцій, таких як MiCA, управління волатильністю та важливість орієнтації на клієнтів, підкресливши, що успішне впровадження залежить від прозорості, освіти та побудови довіри.

Окремо було розглянуто проблему шахрайств типу "pig butchering" на панелі під модерацією Адама Харта. Алана Кац із прокуратури Брукліна розповіла про блокування понад 300 шахрайських сайтів для "розриву зв'язку" між жертвами та шахраями, Ерін Фраколлі з Binance зазначила зростання випадків психологічних маніпуляцій та труднощів з порятунком жертв, які часто повертаються до шахраїв навіть після попереджень, а Елад Фоукс із Chainalysis описав масштаб проблеми через ШІ та "шахрайські набори", закликавши до використання ШІ для раннього виявлення загроз. Учасники наголосили на необхідності співпраці з соціальними мережами та ширшої просвітницької роботи.

Тема стейблкойнів стала центральною на ще одній панелі, модерованій JP Jednorski, за участю представників Circle, PayPal і 1Money. Учасники обговорили еволюцію стейблкойнів від торгових пар до платіжних інструментів, підкресливши важливість чітких правил AML, моніторингу та федерального законодавства для масового впровадження. Вони зазначили, що комплаєнс є конкурентною перевагою, яка сприяє довірі та залученню інвестицій.

Загалом конференція підкреслила, що криптовалютна індустрія перестала бути нішею і стала ключовою частиною фінансової інфраструктури. Успіх залежить від партнерств, інноваційних інструментів, прозорості та відповідального регулювання, а також від спільної роботи всіх зацікавлених сторін для подолання викликів і реалізації можливостей, які відкриває блокчейн.

Ліквідовано контрабанду вогнепальної зброї [16]



У квітні 2025 року Європол оголосив про успішне розкриття міжнародної мережі незаконної торгівлі вогнепальною зброєю, яка постачала автомати та гранати до Західної Європи, зокрема Франції. Операція, проведена у співпраці з правоохоронними органами кількох країн, призвела до арештів та вилучення значної кількості зброї, включаючи автомати Калашникова та вибухові пристрої.

Розслідування виявило складну логістичну мережу, яка використовувала легальні транспортні канали для переміщення зброї, маскуючи її серед звичайних вантажів. Цей випадок підкреслює зростаючу загрозу, яку становить незаконна торгівля зброєю для безпеки Європи, особливо в контексті можливого використання такої зброї терористичними організаціями.

Європол наголосив на необхідності посилення міжнародної співпраці та обміну розвідувальною інформацією для ефективної боротьби з подібними злочинними мережами. Важливою є також модернізація митного контролю та впровадження новітніх технологій для виявлення незаконних вантажів.

Цей успіх правоохоронних органів демонструє ефективність спільних зусиль у протидії транснаціональній злочинності та забезпеченні безпеки громадян.

[16] https://www.europol.europa.eu/media-press/newsroom/news/ak-rifles-and-grenades-seized-firearms-trafficking-route-france-dismantled?mtm_campaign=press-releases-just-published-20250411&utm_term=press-releases-just-published&mtm_source=newsletter&mtm_medium=email&mtm_content=title&mtm_group=news

У Франції перехоплено осередок водіїв, який переправляв мігрантів [17]

У квітні 2025 року правоохоронні органи Франції, за підтримки Європолу, успішно ліквідували організовану злочинну групу, яка спеціалізувалася на незаконному перевезенні мігрантів через територію країни. Операція, що отримала назву "ZIZOU", стала результатом тривалого розслідування та тісної міжнародної співпраці.

В рамках операції було проведено 24 обшуки та затримано 24 особи, підозрюваних у причетності до мережі перевізників. Під час обшуків вилучено три транспортні засоби, які використовувалися для перевезення мігрантів, а також інші докази, що підтверджують незаконну діяльність групи.

Розслідування виявило, що злочинна мережа діяла за чітко організованою схемою: водії, часто наймані за грошову винагороду, перевозили мігрантів через Францію, використовуючи різні маршрути та засоби маскування, щоб уникнути виявлення правоохоронцями. Мігранти, переважно з країн Близького Сходу та Північної Африки, сплачували значні суми за транспортування, що свідчить про високий рівень прибутковості цього незаконного бізнесу.

Європол наголосив на важливості цієї операції як прикладу ефективної міжнародної співпраці у боротьбі з транснаціональною злочинністю. Організація підкреслила необхідність подальшого зміцнення обміну інформацією між країнами-членами та посилення заходів з виявлення і припинення діяльності подібних мереж.

Для загального розвитку

Штраф у €1M для OKCoin Europe — системні провали, які мають стати уроком для всіх VASP [18]

У 2024 році OKCoin Europe була оштрафована на понад 1 мільйон євро після глибокої перевірки, проведеної Мальтійським підрозділом фінансової розвідки (FIAU). Цим рішенням було не лише покарано серйозні прогалини в роботі конкретного оператора, а й попереджено всю криптовалютну індустрію: базові вимоги AML не можуть залишатися другорядними.

Ось що саме пішло не так — і які уроки мають винести всі, хто працює з цифровими активами.

1. Недооцінка ризиків продуктів та сервісів. Фундаментальна проблема починалась з того, що оцінка ризиків компанії була надто загальною. OKCoin не врахувала специфічних ризиків, пов’язаних з такими інструментами, як:
    - приватні монети (privacy coins),
    - децентралізовані біржі (DeFi),
    - криптоміксери,
    - стейблкоїни.

[17] https://www.europol.europa.eu/media-press/newsroom/news/migrant-smuggling-driver-cell-intercepted-in-france?mtm_campaign=press-releases-just-published-20250410&utm_term=press-releases-just-published&mtm_source=newsletter&mtm_medium=email&mtm_content=title&mtm_group=news

[18] https://www.amlcube.com/post/lessons-from-okcoin-europe-s-1m-aml-penalty?utm_source=substack&utm_medium=email

Ці категорії давно асоціюються з високими ризиками відмивання коштів, однак компанія не інтегрувала ці фактори в свою рамку оцінки ризику. Це свідчить про відсутність продукт-орієнтованого підходу до управління ризиками.

2. Реактивна, а не проактивна оцінка клієнтів. Близько 50% перевірених файлів показали, що оцінка ризику клієнта проводилася вже після того, як клієнт здійснив депозит. У деяких випадках клієнти встигли внести значні суми без попередньої оцінки ризику — затримка тривала кілька місяців. Це означає, що клієнти могли активно використовувати платформу до того, як була сформована базова думка про рівень їхнього ризику.
3. Відсутність глибоких KYC-даних під час онбордингу. Дані при онбордингу були надто поверхневими. Компанія фіксувала такі формулювання, як “бізнес” чи “найманий працівник”, не вимагаючи подальшого підтвердження чи деталізації. Меню вибору в анкетах було вкрай обмеженим, що унеможливлювало розуміння джерел коштів, сфери діяльності клієнта або передбачуваних обсягів транзакцій.
4. Автоматичний моніторинг був, але не працював як слід. Система моніторингу транзакцій працювала формально — автоматично генерувала попередження. Але у понад 80% випадків ці попередження були або закриті без розслідування, або не отримали належної уваги. Один із найкричущіших фактів — понад 20 мільйонів доларів з діяльності клієнтів не було належним чином проаналізовано відповідно до ризик-орієнтованого підходу.
5. Відсутність посиленої перевірки для клієнтів високого ризику. Кілька клієнтів, яких було класифіковано як високоризикових, не пройшли посиленої перевірки (EDD). Компанія не запитувала жодних додаткових документів, які б допомогли зрозуміти походження активів або призначення транзакцій. У деяких випадках навіть не перевірялося, чи належить гаманець, з якого надходили великі криптовалютні депозити, саме цьому клієнту.
6. Відсутність повідомлення про підозрілу діяльність (STR). Один із клієнтів, який був класифікований як високоризиковий, вніс майже 1,2 мільйона доларів і вивів понад 1,4 мільйона — за кілька місяців. Водночас біржа мала дуже обмежену інформацію в онбордингових документах клієнта, а додаткова документація, подана під час EDD, була поверхневою та непідтвердженою. Хоча в компанії були внутрішні занепокоєння, жодного повідомлення до підрозділу фінансової розвідки не було подано.
7. AML-тренінги не відповідали бізнес-моделі. Так, співробітники компанії проходили навчання з ПВК. Але його зміст був загальним, теоретичним і не враховував специфіку ризиків, притаманних саме бізнес-моделі OKCoin Europe. На думку FIAU, ефективне навчання має відображати реальні продукти, сервіси і способи роботи компанії, а не лише загальні принципи AML.

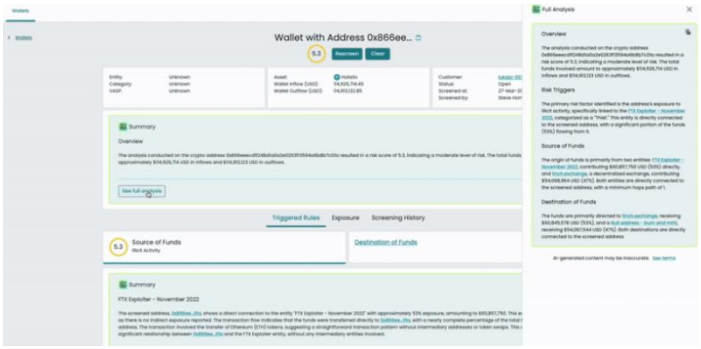
Це рішення — не просто приклад суворої регуляторної відповіді, а реальна дорожня карта того, чого робити не можна у сфері AML-комплаєнсу для VASP.

- ✓ Чітко структуруйте свої оцінки ризиків за продуктами.
- ✓ Не відкладайте клієнтську оцінку "на потім".
- ✓ Впровадьте системи, які не лише створюють алерти, але й змушують вас діяти.
- ✓ Навчайте команду з урахуванням ваших реальних ризиків.

Понад мільйон євро штрафу — це лише один з елементів наслідків. Репутаційні втрати, блокування партнерств і зменшення клієнтської довіри можуть коштувати значно більше.

Нова программа Elliptic для роботи комплаєнсу [19]

У квітні 2025 року компанія Elliptic представила свою нову розробку — Elliptic Copilot, інноваційний ШІ-асистент, призначений для трансформації процесів комплаєнсу у сфері криптовалют. Цей інструмент покликаний автоматизувати найбільш трудомісткі етапи перевірки транзакцій, зменшуючи час обробки з годин до хвилин.



Elliptic Copilot використовує агентну ШІ-архітектуру, яка імітує логіку дій аналітика: від збору даних до формування висновків. Він автоматично аналізує ризикові сигнали, відстежує рух коштів, ідентифікує залучені сторони та надає аналітику повну картину ризику у зручному форматі. Це дозволяє аналітикам зосередитися на стратегічних завданнях, замість витрачати час на рутинні перевірки.

Представлені результати впровадження Elliptic Copilot вражають:

- Зменшення часу на обробку ризикових сигналів на 50%.
- Економія до 25 хвилин на кожне розслідування.
- Скорочення загального часу від виявлення до закриття кейсу на 3 години щодня.

Ці показники свідчать про значне підвищення ефективності комплаєнс-команд.

Elliptic Copilot вже використовується провідними гравцями ринку, такими як BitGo. За словами Сема Робертса, старшого директора фінансового моніторингу в BitGo, впровадження Copilot дозволило значно прискорити процеси перевірки та розслідування.

Завдяки поєднанню ончейн-даних, поведінкових моделей та офчейн-інформації, Elliptic Copilot забезпечує глибокий аналіз ризиків у режимі реального часу. Це робить його корисним інструментом для фінансових установ, криптобірж та регуляторів, які прагнуть підвищити ефективність та точність своїх комплаєнс-процесів.

[19] https://www.elliptic.co/blog/from-hours-to-minutes-how-elliptics-copilot-is-disrupting-the-compliance-workflow

Ваша думка важлива!

1. Якою має бути роль України в міжнародних зусиллях із протидії російському впливу в Африці, зокрема в Лівії, щоб запобігти посиленню економічної та військової міці РФ?
2. Які механізми двосторонньої взаємодії між Україною та іноземними санкційними органами, зокрема OFSI, можуть бути задіяні для виявлення та заморожування активів осіб, причетних до фінансування збройної агресії, з урахуванням складних корпоративних структур і використання трастових схем?
3. Як штучний інтелект може змінити парадигму нагляду за фінансовим сектором у країнах із обмеженими ресурсами? Чи готові наші наглядові органи до використання технологій реального часу, хмарних рішень і пояснюваних моделей (XAI) для підвищення ефективності виявлення ризиків ВК/ФТ?
4. Як забезпечити баланс між інноваціями у сфері цифрових фінансів (віртуальні активи, стейблкоїни) та ефективним контролем з боку СПФМ і регуляторів? Чи є в нас достатньо методичних матеріалів та інструментів для розуміння природи таких активів і відповідного управління ризиками ПВК/ФТ?
5. Наскільки серйозною загрозою для санкційної політики є діяльність юридичних фірм і TCSPs, які не ідентифікують прихованих бенефіціарів або не повідомляють про порушення? Чи маємо ми достатній рівень міжвідомчої координації, щоб вчасно реагувати на подібні виклики в українському контексті?
6. Яким чином міжнародне співробітництво, зокрема із США, може бути посилене для протидії незаконному переміщенню та легалізації викрадених культурних цінностей, і які міжнародні інструменти слід удосконалити для ефективного переслідування транснаціональних схем торгівлі предметами культурної спадщини?

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-2025-15

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].