Методологічний бюлетень

Серійний номер: МінФін-AML-2025-30

Липень 2025

“Секрет успіху в тому, щоб діяти!”

Данте Аліг’єрі

Мета

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

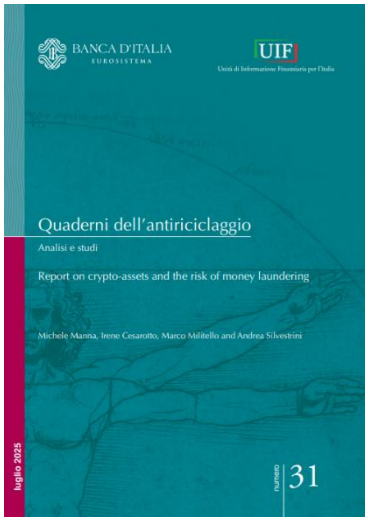
Містить актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

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

Звіти міжнародних організацій та окремих юрисдикцій

Звіт про криптоактиви та ризик відмивання грошей [1]

АУДІОПЕРЕКАЗ



Документ, підготовлений ПФР Італії, є міждисциплінарним дослідженням ризиків ВК, пов’язаних із використанням криптоактивів. Його ціль — надати всебічну оцінку технологічних, нормативних та ринкових аспектів криптоактивів з перспективи ПВК/ФТ. Структура документа охоплює п’ять розділів, що послідовно викладають природу криптоактивів, їхню класифікацію, механізми транзакцій, правову базу (включно з Регламентом MiCAR і новим Пакетом ЄС щодо ПВК), ринкову динаміку та практичні кроки у сфері ПВК.

На початку визначається гібридна природа криптоактивів. Автори вводять складну типологію, що включає центральні банківські гроші, банківські депозити, електронні гроші та криптовалюти. Ця класифікація критично важлива для розуміння обмеженості традиційного правила KYC у криптопросторі, а також необхідності окремого регуляторного підходу.

[1] https://uif.bancaditalia.it/pubblicazioni/quaderni/2025/quaderno-31-2025/index.html

Історичний огляд починається з появи Біткоїна в 2008 році і простежує еволюцію уваги міжнародних організацій (FATF, ЄС тощо) до тематики криптоактивів. Хоча перші нормативні кроки (наприклад, AMLD5) з'явилися лише у 2018 році, пізніше ЄС швидко активізував роботу, зокрема над MiCAR, у відповідь на волатильність ринку та спроби приватного сектора (як-от Libra) вийти на платіжний ринок.

Ключовим аспектом документа є пояснення високої вразливості криптоактивів до ризиків ВК: поєднання псевдоанонімності, відсутності потреби в посередниках, глобальної доступності, фрагментованості ринку та нерівномірного впровадження ПВК-регулювання в юрисдикціях.

У технологічному розділі пояснено базову архітектуру Біткоїна (через приклад користувача «Mark»): створення гаманців, проведення транзакцій, структура блоків, винагороди майнерів, механізми верифікації. Звертається увага на можливість деанонімізувати користувачів через кластери адрес, спостереження за змінами адрес, методи співвідношення входів і виходів транзакцій. Попри псевдоанонімність, аналітичні інструменти (як-от Chainalysis) дозволяють отримувати значний обсяг інформації, особливо у випадку співпраці з біржами.

Особливої уваги надано «приватним монетам» (наприклад, Monero), які використовують інструменти обфускації як-от кільцеві підписи, приховані адреси, Dandelion++. Хоча деякі атаки виявили слабкі місця, зокрема методи на основі аналізу «mixins», спільноти КА активно вдосконалюють захист.

У юридичному розділі подано глибокий аналіз нормативного ландшафту. Порівнюються визначення понять, що використовуються в MiCAR, 5AMLD, а також міжнародних стандартах (FATF, ЄЦБ, Європейської банківської асоціації), з акцентом на різницю між поняттями «віртуальні активи», «криптовалюти» та «токени». Особливо важливим є аналіз Регламенту MiCAR (EU 2023/1114), де приділено увагу ідентифікації та ліцензуванню постачальників послуг, пов'язаних з криптоактивами (CASP), класифікації токенів (utility, asset-referenced, e-money), механізмам white paper, а також вимогам до забезпечення надійності та прозорості емітентів. Окрема увага приділена взаємозв'язку MiCAR із Пакетом ЄС щодо ПВК: обговорюється, як нові вимоги щодо KYC, підходу, заснованого на ризиках, зберігання даних і транскордонної співпраці мають застосовуватися до CASPs у різних державах-членах. Розглянуто виклики для регуляторів, пов'язані з потенційним «регуляторним туризмом» та потребою в уніфікованому нагляді.

Висновки:

- **Необхідність спеціалізованого підходу до регулювання криптоактивів.** Криптоактиви мають гібридну природу, що не вкладається у традиційні категорії грошей або фінансових інструментів. Тому застосування стандартних ПВК-інструментів, зокрема KYC, вимагає адаптації та нових технологічних рішень.
- **Розширення використання аналітичних інструментів є критично важливим.** ПФР та правоохоронним органам слід інвестувати в інструменти, які дозволяють аналізувати транзакції, ідентифікувати кластери адрес і виявляти патерни ВК, включно в умовах обфускації.
- **Нерівномірність регулювання в різних країнах ЄС створює ризики обходу вимог ПВК.** Рекомендовано налагодити прямі обміни інформацією між органами ПВК і CASP у межах ЄС для зменшення простору для «регуляторного арбітражу».
- **Стрімке зростання ринку криптоактивів потребує прискореної реакції регуляторів.** З урахуванням переходу до фази масового прийняття криптоактивів, регулятори мають діяти на випередження, а не з реактивною логікою. Це включає підтримку досліджень, участь у спільнотах DeFi, і підвищення технічної обізнаності персоналу.

Ринковий розділ документа висвітлює структуру та поведінкові особливості ринку криптоактивів. Аналітика ринку демонструє, що він має високий рівень концентрації: переважають кілька токенів (Bitcoin, Ethereum, Tether), а основні біржі контролюють значну частину обсягів торгів. Також аналізуються поведінкові патерни — різка волатильність цін, вплив спекуляцій і повідомлень у медіа, реакція на регуляторні новини. Розглядається роль централізованих і децентралізованих бірж, а також ступінь їх інтеграції з традиційною фінансовою системою. Окремо описано практики ПВК на біржах, включно з прикладами обмежень на приватні монети, впровадження процедур верифікації клієнтів і виявлення підозрілої поведінки.

У завершальному розділі запропоновано низку практичних дій для суб'єктів ПВК, які мають сприяти зменшенню ризиків ВК у сфері криптоактивів. Насамперед, наголошується на необхідності інвестування в розвиток аналітичних інструментів для аналізу транзакцій з криптоактивами, включно з підтримкою академічних досліджень, закупівлею програмного забезпечення на кшталт Chainalysis та навчанням персоналу. Пропонується створити централізовану систему збору даних щодо транзакцій, біржової активності та взаємозв'язків між CASP. Серед ключових рекомендацій — розбудова двосторонніх каналів інформаційного обміну між ПФР держав-членів ЄС та CASP, які працюють в інших юрисдикціях, що дозволить ефективніше реагувати на транскордонні транзакції та уникати сліпих зон. Особлива увага приділена зміцненню компетенцій співробітників ПФР: пропонується створення програм навчання з акцентом на блокчейн-аналітику, децентралізовані платформи, стейблкоїни та DeFi. Зрештою, підкреслюється необхідність зберігати баланс між підтримкою інновацій (щоб не гальмувати розвиток фінансових технологій) і забезпеченням фінансової стабільності та доброчесності ринку.

Керівництво для постачальників послуг з криптоактивами, які пропонують нерегульовані послуги [2]

Європейський орган з цінних паперів та ринків (ESMA) оприлюднив заяву, яка має на меті надати вказівки CASP щодо уникнення хибних уявлень при наданні нерегульованих послуг. Ця заява видана лише через кілька місяців після початку застосування Регламенту про ринки криптоактивів (MiCA) до фірм, що надають послуги з криптоактивами. ESMA нагадує CASP про їхній обов'язок діяти чесно, професійно та в найкращих інтересах своїх клієнтів та потенційних клієнтів.

Основний зміст заяви зосереджений на ситуаціях, коли CASP пропонують як регульовані (згідно з MiCA), так і нерегульовані послуги. У таких випадках CASP зобов'язані уникати створення плутанини або введення в оману клієнтів або потенційних клієнтів щодо того, чи послуга користується захистом, передбаченим MiCA. ESMA застерігає, що практика пропонування CASP як регульованих MiCA, так і нерегульованих продуктів та послуг, які не підпадають під сферу дії MiCA або іншого секторального законодавства ЄС (наприклад, Директиви 2014/65/EU), створює ризики для захисту інвесторів.

Метою цієї заяви є визначення деяких ризиків, які можуть виникнути, та питань, на які CASP повинні звертати особливу увагу при наданні таких нерегульованих продуктів та/або послуг.

[2] https://www.esma.europa.eu/sites/default/files/2025-07/ESMA35-1872330276-2329_-_MiCA_Statement_Access_to_Unregulated_Activities.pdf

Там, де CASP надають як регульовані, так і нерегульовані продукти та/або послуги, існує значний ризик того, що клієнти та потенційні клієнти неправильно зрозуміють обсяг захисту, який їм надається. Це пов'язано з тим, що вони можуть не усвідомлювати, що захист, передбачений MiCA, не поширюється на нерегульовані продукти та/або послуги. Нерегульована діяльність, що здійснюється CASP, не пропонує таких самих гарантій, як послуги з криптоактивами, регульовані MiCA, зокрема щодо управління конфліктами інтересів, вимог до розгляду скарг, захисту активів клієнтів та постійного нагляду з боку національних компетентних органів.

Регульований статус CASP згідно з MiCA може створити "ефект ореолу", який часто може служити для потенційно хибного заспокоєння щодо нерегульованих продуктів та/або послуг, пропонованих цим CASP або пов'язаними особами, що пропонують нерегульовані продукти та/або послуги через ту саму платформу. Деякі CASP можуть навіть використовувати свій регульований статус згідно з MiCA як маркетинговий аргумент та заохочувати плутанину між регульованими та нерегульованими продуктами та послугами. Тому CASP повинні бути особливо пильними щодо уникнення будь-якої плутанини у клієнтів або потенційних клієнтів щодо захисту, пов'язаного з нерегульованими продуктами та/або послугами.

Висновки:

- **Обов'язкова прозорість регуляторного статусу:** CASP повинні прозоро та наочно повідомляти клієнтам про регуляторний статус кожної пропонованої послуги, чітко розмежовуючи регульовані та нерегульовані види діяльності у всіх комунікаціях, включаючи маркетингові матеріали та веб-сайти, щоб запобігти плутанині та хибним уявленням про захист MiCA.
- **Уникнення "ефекту ореолу" та оманливого маркетингу:** CASP не повинні використовувати свій регульований статус згідно з MiCA як маркетинговий аргумент для просування нерегульованих послуг або створювати "ефект ореолу", який може ввести клієнтів в оману щодо обсягу захисту, що поширюється на нерегульовані продукти та послуги.
- **Впровадження суворих механізмів підтвердження:** Перед наданням нерегульованих послуг CASP зобов'язані використовувати активні механізми підтвердження, такі як спливаючі вікна з вимогою згоди, щоб забезпечити чітке розуміння клієнтами нерегульованого статусу послуги та пов'язаних ризиків.
- **Особлива увага до управління конфліктами інтересів:** CASP повинні забезпечити належне управління конфліктами інтересів та чітке визначення юридичних осіб, що надають кожну послугу, щоб уникнути приховування ризиків та плутанини щодо відповідальності за нерегульовані послуги.

CASP зобов'язані діяти чесно, професійно та в найкращих інтересах своїх клієнтів та потенційних клієнтів. Крім того, вони повинні дотримуватися свого зобов'язання забезпечувати, щоб вся інформація, включаючи маркетингові комунікації, адресована клієнтам або потенційним клієнтам, була чесною, чіткою та не вводила в оману. Для зменшення ризиків, що клієнти або потенційні клієнти неправильно зрозуміють, чи є продукт або послуга регульованою згідно з MiCA, CASP повинні вжити всіх необхідних заходів для забезпечення повної обізнаності клієнтів та потенційних клієнтів про регуляторний статус продукту/послуги, яку вони отримують.

Що робити:

- Чітке та ефективне повідомлення про регуляторний статус: Регуляторний статус продукту та/або послуги повинен бути чітко та ефективно повідомлений у всіх взаємодіях з клієнтами та на кожному етапі процесу продажу. Наприклад, усі маркетингові комунікації повинні чітко вказувати, чи є продукт та/або послуга, пропонована CASP, регульованою чи

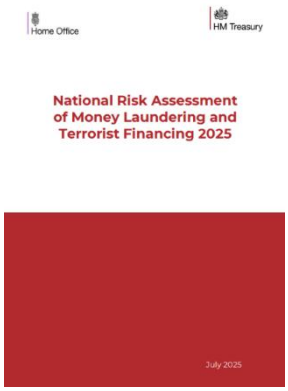
ні. Така вказівка має бути чітко видна клієнтам та потенційним клієнтам.

- Розмежування на веб-сайті та в документації: Будь-яка інформація на веб-сайті CASP, пов'язана з нерегульованою діяльністю, повинна бути чітко відрізнена від регульованої діяльності. CASPs повинні мати окремі розділи на будь-якому веб-сайті, який вони експлуатують, для регульованої діяльності та будь-якої іншої діяльності, яку вони здійснюють. Клієнтська документація повинна бути відповідно розрізнена, щоб забезпечити достатню обізнаність клієнтів про відмінності в захисті.
- Спливаючі вікна для нерегульованих послуг: Перш ніж клієнту будуть надані нерегульовані послуги та/або продукти, повинно з'являтися спливаюче вікно, що вказує на те, що це нерегульовані послуги/продукти. Це спливаюче вікно повинно включати підхід "поставте галочку", що вимагає, щоб клієнт прочитав інформацію, надану у спливаючому вікні, і визнав нерегульований статус послуги/продукту, перш ніж клієнт фактично зможе отримувати нерегульовані послуги та/або продукти.

Чого не робити:

- Не використовувати misleading термінологію: Не слід використовувати термінологію, яка натякає на те, що продукт або послуга, що не підпадає під сферу дії MiCA або іншого секторального законодавства ЄС, є регульованою.
- Не обмежувати інформацію про нерегульований статус: Інформація щодо нерегульованого статусу продукту або послуги не повинна бути видимою лише в Умовах та положеннях.
- Не використовувати регуляторний статус як промоційний інструмент для нерегульованої діяльності: Регуляторний статус CASP не повинен використовуватися як інструмент просування. При здійсненні нерегульованої діяльності інформація, що надається клієнту або потенційному клієнту, включаючи маркетингові матеріали та іншу документацію, не повинна містити посилання на те, що CASP авторизований/регулюється.
- Не допускати невизначеності щодо надавача послуг: Не повинно бути неясно, яка саме особа надає нерегульовані послуги та/або продукти на момент укладення відповідної угоди, а пов'язані ризики не повинні бути приховані.
- Не дозволяти нерегульованим особам пропонувати послуги через інтерфейс CASP: Нерегульовані особи (незалежно від того, чи є вони частиною тієї ж групи, що й CASP, чи ні) не повинні пропонувати послуги та/або продукти, регульовані або несанкціоновані згідно з MiCA, через інтерфейс CASP.

Національна оцінка ризиків Сполученого Королівства – 2025 [3]



Національна оцінка ризиків (НОР) відмивання коштів і фінансування тероризму 2025 року Сполученого Королівства є всеохопним стратегічним документом, який фіксує сучасний стан загроз, вразливостей і рівня протидії у сфері ПВК/ФТ у країні. Цей звіт розроблений відповідно до вимог Положення 16 Регламенту про відмивання коштів, фінансування тероризму та переказ коштів (MLR 2017), а також вимог FATF до країн щодо проведення національних оцінок ризиків. Документ оновлює попередні оцінки 2015, 2017 та 2020 років та інтегрує актуальні зміни у криміногенному середовищі, фінансових технологіях, геополітиці й нормативному регулюванні. Він

3 https://assets.publishing.service.gov.uk/media/6877be59760bf6cedaf5bd4f/National_Risk_Assessment_of_Money_Laundering_and_Terrorist_Financing_2025_FINAL.pdf

базується на аналізі понад 550 джерел, включно з відповідями з регульованого сектору, правоохоронних органів, академічних установ і відкритих даних, а сам ризик оцінюється за методологією MoRiLE, що враховує масштаб, вразливість і силу наявних контролів.

Основний зміст НОР полягає у встановленні того, що Сполучене Королівство залишається країною з високим рівнем вразливості до відмивання коштів через її глобальну фінансову відкритість, наявність потужного ринку професійних послуг, активне використання складних корпоративних структур і широке застосування нових фінансових технологій. Значну частину загроз становлять доходи від шахрайства (яке складає понад 43% усіх злочинів в Англії та Уельсі), кіберзлочинів (зокрема із застосуванням програм-вимагачів і криптовалют), незаконного обігу наркотиків, ухилення від сплати податків, а також від санкційного обходу, пов'язаного з війною росії проти України. Відзначається зростання ролі транскордонних злочинних мереж та поєднання схем ВК з корупцією, торгівлею людьми, організованою злочинністю і легалізацією доходів через законні сектори.

Особлива увага приділена готівці, яка, незважаючи на спад її використання в легальній економіці, залишається основним інструментом відмивання злочинних доходів. Поштові відділення, а також малі готівкові бізнеси — перукарні, автомийки, продуктові крамниці — використовуються для здійснення великої кількості дрібних депозитів, які далі переміщуються до банків або платіжних платформ. Щомісячно через поштові відділення проходить до £3 млрд готівки, з яких значна частина може бути пов'язана з нелегальними джерелами. Поряд з цим, у звіті фіксується активне використання, зокрема китайського підпільного банкінгу та hawala, для переказу грошей поза традиційними фінансовими каналами, особливо в етнічних громадах.

Криптоактиви визнано сектором з найдинамічнішим зростанням ризиків. У 2024 році вже 12% дорослого населення Британії володіло криптоактивами. Розповсюдженими залишаються випадки їх використання в шахрайстві, кіберзлочинах, шантажі, а також для обходу санкцій. Велика частина провайдерів криптопослуг знаходиться за межами юрисдикції FCA, що суттєво обмежує можливості контролю. У зв'язку з цим країна запровадила Travel Rule

Висновки:

- **Високий рівень ризику відмивання коштів через готівку зберігається, попри зниження її використання в легальній економіці.**
  Рекомендація: посилити нагляд за готівковими потоками, особливо через поштові відділення, нефінансові установи, і бізнеси з високими готівковими оборотами (перукарні, автомийки, тощо).
- **Інформаційно-аналітичні механізми (SARs, JMLIT) потребують подальшої цифровізації та автоматизації.**
  Результат: запуск нової цифрової SARs-системи сприятиме покращенню зворотного зв'язку з приватним сектором і розширить можливості виявлення підозрілих транзакцій.
- **Криптоактиви залишаються пріоритетним джерелом ризику, зростає обсяг злочинної активності, пов'язаної з DeFi, NFT, необанкінгом.**
  Рекомендація: забезпечити ефективну імплементацію Travel Rule для CASP, продовжити технічну підтримку правоохоронців у сфері розслідувань блокчейну.
- **Професійні посередники (адвокати, бухгалтери, надавачі послуг, пов'язаних зі створенням трастів) відіграють ключову роль у транснаціональних схемах ВК/ФТ, зокрема у санкційному обході.**
  Практичне рішення: реалізовано стратегію NECC та OPBAS щодо зниження ролі професійних посередників (2024), яку варто масштабувати на інші юрисдикції.

для надавачів послуг у сфері віртуальних активів (CASP), підвищила регуляторні вимоги, а правоохоронці отримали додаткові повноваження для арешту і конфіскації криптоактивів.

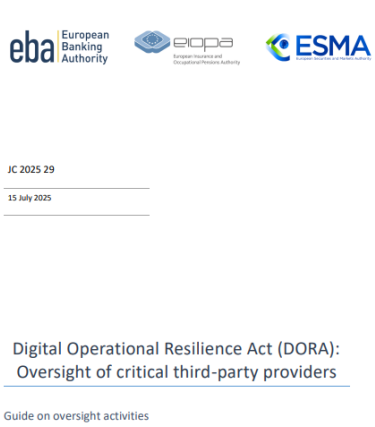
Окремо оцінено ризики фінансування тероризму, з акцентом на складність виявлення малих переказів, що здійснюються через платіжні платформи, благодійні організації або цифрові фінансові інструменти. Значну увагу приділено взаємозв'язку між фінансуванням тероризму, організованою злочинністю та іншими формами нелегального фінансування. Держава вжила низку заходів у межах стратегії CONTEST та співпраці з Tri Sector Group, яка поєднує уряд, фінансовий та недержавний сектор.

У відповідь на виявлені загрози, уряд запровадив низку інституційних і нормативних реформ. Прийняті два ключові акти: Economic Crime (Transparency and Enforcement) Act 2022, що передбачає створення реєстру бенефіціарних власників для нерезидентів і посилення судового припису невідомого походження активів (UWO), а також Economic Crime and Corporate Transparency Act 2023, який запровадив обов'язкову ідентифікацію осіб, пов'язаних із компаніями, розширення повноважень Companies House, впровадження обміну розвідувальною інформацією між приватними компаніями. Крім того, в рамках SARs Reform створено нову цифрову платформу подання підозрілих транзакцій, а також запроваджено Fusion Cell — аналітичну структуру, яка об'єднує державні та приватні дані для виявлення складних загроз.

Значну увагу приділено посиленню професійного нагляду, зокрема через діяльність OPBAS, підвищення ефективності роботи FCA, впровадження нових стратегій щодо професійних посередників, а також запуск Програми ПВК/ФТ та повернення активів (AMLAR). Фінансування заходів здійснюється за рахунок запровадженого у 2022 році збору за боротьбу з економічними злочинами, очікуваний дохід від якого становитиме £115 млн щорічно.

Таким чином, звіт HOP-2025 є не лише діагностичним документом, а й дорожньою картою для всіх учасників системи ПВК/ФТ. Він дає розгорнуту картину загроз, пропонує інституційні та технічні відповіді, визначає пріоритетні напрями для співпраці держави та приватного сектору і формує основу для адаптації механізмів ПВК/ФТ до нових викликів сучасного світу.

DORA в дії: як ЄС запроваджує ризик-орієнтований контроль за технологічними гігантами [4]



Документ є керівництвом, розробленим трьома європейськими наглядовими органами – EBA, ESMA та EIOPA – з метою пояснення та уніфікації процесів нагляду за критично важливими третіми сторонами (CTPPs), що постачають ІКТ-послуги фінансовим установам (ФУ) у Європейському Союзі. Документ слугує як практичний інструмент для реалізації повноважень, передбачених Регламентом (ЄС) 2022/2554 (DORA), і водночас забезпечує прозорість та передбачуваність дій наглядових органів для всіх зацікавлених сторін: CTPPs, ФУ, компетентних органів (CAs) та громадськості.

Основним предметом документа є створення скоординованої законодавчої рамки, яка забезпечує централізований, пропорційний та ризик-орієнтований

[4] https://www.eba.europa.eu/sites/default/files/2025-07/32044d65-455e-4fff-82d0-aa0d8ac2799f/JC%202025%2029%20%20DORA%20Oversight%20Guide.pdf

підхід до моніторингу та оцінки цифрової стійкості зовнішніх ІКТ-постачальників, критично важливих для безперебійного функціонування фінансових послуг у ЄС. Рамка не замінює обов'язки самих фінансових установ у сфері управління ІКТ-ризиками, а натомість їх доповнює. Вона також не дублює нагляд, що здійснюється CAs, а передбачає взаємодію і обмін інформацією на міжінституційному рівні.

Ключовим елементом рамки є процес щорічного визначення критичності ІКТ-постачальників на основі низки кількісних та якісних критеріїв (згідно зі ст. 31 DORA і відповідним делегованим актом). До уваги беруться системна важливість, масштаб використання послуг у фінансовому секторі, рівень замінності провайдера, кількість охоплених ФУ тощо. Після визнання постачальника критичним, за ним закріплюється головний наглядовий орган (LO), який відповідає за реалізацію наглядових повноважень на основі індивідуального річного плану і в межах багаторічної стратегії. LO діє у співпраці зі Спільною групою з перевірок (JET), Спільним об'єднанням з нагляду (JOV) та під егідою спільних структур — Спільної мережі з нагляду (JON) та Наглядового формуму.

У керівних настановах докладно описано види наглядової діяльності, які включають: регулярний моніторинг, запити на інформацію (RfI), тематичні та цільові розслідування, перевірки на місцях, а також процес видачі рекомендацій та подальший контроль за їх виконанням. Усі ці інструменти впроваджуються пропорційно рівню ризику, який той чи інший CTPP становить для фінансової системи. Описано, що спілкування з CTPP має бути структурованим і послідовним, а мова взаємодії — переважно англійська. Окремо наголошено на ролі комунікаційних точок, які мають бути створені як в межах ЄС, так і для дочірніх підприємств CTPPs з третіх країн — з належним рівнем організаційної спроможності та ресурсів для забезпечення ефективної взаємодії з LO.

Висновки:

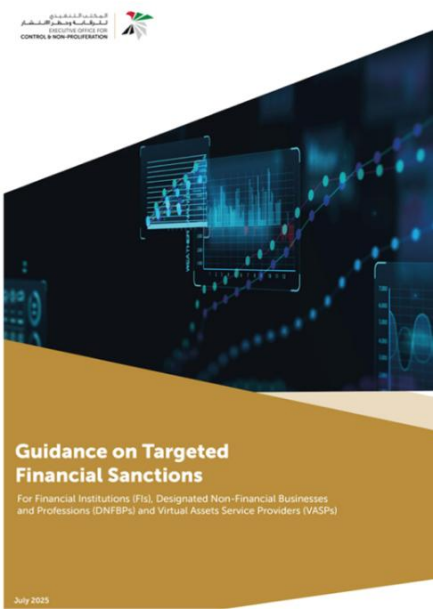
- **ESAs отримали реальні повноваження для нагляду за CTPPs, включаючи інспекції, запити даних, рекомендації та штрафи.** Практично це дозволяє фінансовим регуляторам ЄС централізовано реагувати на порушення цифрової безпеки критичними надавачами послуг, незалежно від юрисдикції їх юридичної реєстрації.
- **Фінансові установи мають готуватись до тісної координації з CAs та врахування наглядових висновків щодо їх ІКТ-партнерів.** Це передбачає перегляд підходів до управління ризиками третіх сторін, а також більш тісну інтеграцію з процесами оцінки цифрової стійкості контрагентів.
- **Для CTPPs встановлені чіткі очікування щодо корпоративної структури, звітності та взаємодії з LO/ESAs, включаючи вимогу щодо наявності координаційного центру в ЄС.** Це створює нову норму для глобальних ІКТ-постачальників: без локальної присутності, відповідної інфраструктури та процедур забезпечення нагляду — діяльність у фінансовому секторі ЄС може бути обмежена.
- **Порушення або невиконання рекомендацій призводить до репутаційних ризиків (публічне розкриття), а також до можливого припинення контрактів з ФУ.** Це стимулює добровільне дотримання вимог, водночас підсилює позицію наглядових органів для впливу навіть без прямого санкційного тиску.

Рекомендації, які видає LO, є формально необов'язковими, але можуть мати репутаційні наслідки у випадку відмови CTPP їх виконувати. У разі відмови від виконання або неналежної реалізації заходів з боку CTPP, LO може оприлюднити цю інформацію, звернутись до CAs, а ті — вжити наглядових заходів щодо ФУ, включно з вимогою розірвати контракт із ненадійним надавачем послуг. Документ також передбачає механізм діяльності за межами ЄС, якщо CTPP має інфраструктуру поза межами

Союзу, та встановлює умови для міжнародного співробітництва через Меморандум про взаєморозуміння (MoUs) з органами третіх країн.

Таким чином, цей документ відіграє роль навігаційної карти для реалізації DORA у частині нагляду за CTPPs, забезпечуючи операційну деталізацію всіх процедур, принципів, організаційної структури та очікуваних результатів. Він ґрунтується на ідеї про те, що централізований, ризик-орієнтований і прозорий нагляд за технологічною інфраструктурою критичної важливості є необхідною умовою цифрової стійкості фінансової системи ЄС.

Імплементація цільових фінансових санкцій в ОАЕ: оновлене керівництво EOCN (2025) як еталон для суб'єктів фінансового моніторингу [5]



Документ, розроблений Виконавчим офісом з контролю та нерозповсюдження (EOCN) ОАЕ, є оновленим нормативним посібником, який регламентує порядок імплементації цільових фінансових санкцій (ЦФС) на національному рівні. Його структура та зміст орієнтовані на забезпечення повної відповідності вимогам Резолюцій Ради Безпеки ООН, Рекомендаціям FATF (зокрема Р 6 та Р 7), а також правовим актам ОАЕ, включаючи Федеральний закон №20 від 2018 року та Постанову №74 від 2020 року.

Документ деталізує правову основу ЦФС, описує процеси та процедури, обов'язкові до виконання для фінансових установ (ФУ), визначених нефінансових установ і професій (ВНУП), а також надавачів послуг у сфері з віртуальних активів (VASPs), які визначаються як підзвітні суб'єкти. Центральною метою є запобігання наданню доступу до фінансових ресурсів та активів особам, організаціям чи структурам, визначеним як такі, що загрожують міжнародному миру, беруть участь у фінансуванні тероризму або сприяють розповсюдженню зброї масового знищення. У документі наголошується, що всі санкційні заходи мають застосовуватись «без затримки», що в інтерпретації нормативу означає не пізніше 24 годин з моменту публікації оновленого санкційного списку.

Синхронізація з міжнародними стандартами забезпечується шляхом зобов'язання суб'єктів до обов'язкової реєстрації у Національній системі повідомлень про оновлення санкційних списків (NAS), що адмініструється EOCN, та проведення регулярного скринінгу на предмет збігів із санкційними списками — як під час встановлення ділових відносин, так і в ході щоденного моніторингу. Документ чітко визначає критерії, за якими проводиться оцінка рівня збігу: повний збіг, частковий збіг, хибне співпадіння або відсутність збігу. Для кожного з результатів встановлено конкретний порядок дій, включаючи обов'язковість подання відповідного звіту (CNMR або PNMR) через платформу goAML або, у випадку непідконтрольних суб'єктів, електронною поштою до EOCN.

Особливої уваги надано трактуванню понять «власність», «контроль» і «діяльність за дорученням або в інтересах» санкціонованих осіб. У документі описано детальний підхід до визначення структури власності, що охоплює як більшість участі (більше 50%), так і випадки фактичного контролю незалежно від частки володіння — наприклад, через право підпису, повноваження з управління, контроль голосів або юридичні домовленості. Усі юридичні особи, що знаходяться під прямим чи опосередкованим контролем санкціонованих осіб,

[5] https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=1df781eb-3fe2-421c-9730-2b5fdcb7d2e4

прирівнюються до самих осіб із санкційного списку та підлягають замороженню. Також передбачено зобов'язання замороження активів осіб, які діють за дорученням або під контролем таких осіб, за наявності відповідних юридичних підтверджень (довіреності, угоди, рішення органів управління тощо).

У практичній площині керівництво містить численні приклади для різних типів суб'єктів (банків, страхових компаній, брокерів, рієлторів, дилерів дорогоцінних металів, компаній з управління активами, криптовалютних бірж, юридичних фірм тощо), з конкретними ситуаціями застосування ЦФС, формування звітів, вимог до документації, обсягів заморожених активів і строків подання звітності. Усі приклади ілюструють застосування підходу, орієнтованого на результат: повне замороження активів, заборона на надання послуг і чітка звітність із додатком підтверджувальних документів.

Окремий розділ присвячено обов'язковим внутрішнім політикам та процедурам, які мають бути запроваджені в кожній установі, включаючи заборону на розголошення клієнтам намірів про застосування санкцій, вимоги до технічного та кадрового забезпечення, регулярне навчання персоналу та внутрішній контроль за дотриманням процедур. Також передбачено положення щодо відповідальності: у разі порушення зобов'язань — штрафи до 5 млн AED або позбавлення волі до 7 років; у випадку дій, вчинених «у добрій вірі», — звільнення від адміністративної, цивільної та кримінальної відповідальності.

На завершення, документ надає розмежування між випадками, що потребують подання звітів CNMR/PNMR, і ситуаціями, які є предметом підозрілих транзакцій (STR/SAR), зокрема у випадках потенційного обходу санкцій, або якщо особа згадується у звітах Панелі експертів ООН чи фігурує в санкційних списках інших юрисдикцій (OFAC, ЄС, HMT тощо). У таких випадках ЦФС не застосовується, але суб'єкт повинен взаємодіяти зі своїм наглядовим органом і/або подавати STR/SAR до ПФР.

Висновки:

- **Уніфікована процедура ЦФС для всіх типів суб'єктів:** Всі фінансові установи, ВНУП і постачальники послуг з віртуальними активами зобов'язані в однаковому порядку здійснювати реєстрацію в Системі сповіщень про оновлення санкційних списків (NAS), щоденний скринінг, замороження активів і звітування у випадку збігів. Зокрема, застосування термінів CNMR (Звіт про підтверджене співпадіння імені) та PNMR (Звіт про часткове співпадіння імені) є обов'язковим стандартом.
- **«Без затримки» = 24 години на замороження:** Всі активи фізичних або юридичних осіб, внесених до списків санкцій (ЄС/OAE), мають бути заморожені не пізніше ніж через 24 години після внесення до списку. Забороняється будь-яке попередження клієнта або третіх осіб про заплановані дії.
- **Замороження поширюється на структури під контролем:** Активи компаній або структур, що прямо чи опосередковано контролюються санкційною особою (включаючи за ознаками більшості в управлінні або голосуванні), також підлягають замороженню навіть за наявності менш ніж 50% частки у власності. Також заморожуються активи осіб, що діють «від імені» санкційної особи (на підставі договорів, довіреностей тощо).
- **Санкційний комплаєнс має бути безперервним і документованим:** Усі результати скринінгу, дії щодо замороження, хибне співпадіння з особою із санкційного списку, PNMR або CNMR мають документуватись і зберігатись щонайменше 5 років. Крім того, ЦФС має бути інтегровано в політики та внутрішній контроль суб'єкта з обов'язковими навчаннями для персоналу.

Таким чином, це керівництво є всеосяжним нормативним та практичним інструментом, який встановлює єдиний стандарт реалізації цільових фінансових санкцій в ОАЕ, забезпечуючи

водночас відповідність міжнародним зобов'язанням та захист національної фінансової системи від зловживань у сфері тероризму, ФР та обходу санкцій.

Корупція як системна загроза сталому розвитку: стратегічна відповідь для країн G20 [6]

Документ, підготовлений UNODC, OECD і Світовим банком на запрошення Головування Бразилії в G20, є стратегічним аналітичним звітом, що досліджує, яким чином корупція системно підриває досягнення Цілей сталого розвитку (ЦСР) до 2030 року. Звіт базується на трьох ключових напрямах — соціальна інклюзія, економічне зростання та захист довкілля — і має на меті надати державам G20 практичні рекомендації для інтеграції антикорупційних підходів у політику сталого розвитку. В основі викладених тез — визнання того, що корупція є не лише моральною проблемою або юридичним правопорушенням, а фундаментальним викликом до ефективного управління, соціальної справедливості, справедливого розподілу ресурсів і екологічної безпеки.

У соціальному вимірі наголос зроблено на тому, що корупція поглиблює нерівність, обмежує доступ до основних послуг, посилює вразливість певних груп населення, зокрема жінок і бідних домогосподарств. Через зловживання у сферах охорони здоров'я, освіти, доступу до води, електроенергії та правосуддя, корупція стає основним чинником соціального відчуження. Зазначається, що гендерна нерівність має двосторонній зв'язок із корупцією: жінки частіше страждають від її проявів (у тому числі через сексуальну корупцію), а водночас збільшення кількості жінок на керівних посадах асоціюється зі зниженням рівня корупції. Системна корупція також сприяє політичній нестабільності, зменшує довіру до держави та провокує соціальні конфлікти, що особливо небезпечно для країн з низькою легітимністю влади.

З точки зору економіки, корупція істотно гальмує зростання за всіма основними каналами: вона послаблює макрофінансову стабільність, знижує ефективність публічних інвестицій, обмежує розвиток людського капіталу, створює дисбаланси в продуктивності та сприяє політичній дестабілізації. У звіті наводяться дані МВФ, згідно з якими держави з нижчим рівнем сприйняття корупції мають вищі податкові надходження (у середньому на 4% ВВП), менше марнотратства у бюджеті, більше прямих іноземних інвестицій і кращу якість публічної інфраструктури. Особливо наголошено на корупційних ризиках у системі державних закупівель, яка охоплює близько 13 трлн доларів щороку. Слабкі інститути, недостатній контроль і відсутність відкритих даних у цій сфері сприяють масштабним втратам. Пропонується використання цифрових технологій (е-закупівлі, штучний інтелект, відкриті дані), створення умов для обміну інформацією між податковими, антикорупційними та правоохоронними органами, а також посилення антикорупційних вимог у міжнародних інвестиційних угодах. Також відзначено важливість активної участі приватного сектору у створенні культури доброчесності — через впровадження комплаєнс-програм, прозорих політик лобізму та добровільного розкриття фактів корупції, особливо в контексті транснаціональних компаній та галузей із високими ризиками (енергетика, добувна галузь, інфраструктурні проєкти).

У сфері фінансів та оподаткування розкрито механізми, якими корупція підриває ефективність державної податкової політики, сприяє ухиленню від сплати податків з боку еліт і

[6] https://www.unodc.org/corruption/uploads/documents/Corruption_sustainable_development_C.pdf

транснаціональних компаній та зменшує податкову мораль серед громадян. Підкреслено цінність міжвідомчої взаємодії та обміну даними — зокрема щодо бенефіціарної власності, декларацій активів, транскордонних переказів — для виявлення ухилення від податків, незаконного збагачення та відмивання коштів.

Ще один важливий компонент — екологічний. У документі зазначено, що корупція є критичним чинником, який унеможливлює досягнення цілей у сфері боротьби зі змінами клімату, збереження біорізноманіття та боротьби із забрудненням. Відсутність ефективного регулювання, корупційна уразливість зелених закупівель, викривлення вуглецевих ринків і недостатній контроль за кліматичним фінансуванням призводять до неефективного витрачання ресурсів, зниження довіри до «зелених» ініціатив і нерівного розподілу вигод. Окрема увага приділяється зв'язку корупції з екологічними злочинами — зокрема незаконною вирубкою лісів, браконьєрством, торгівлею відходами — та використанням природних ресурсів у якості джерела незаконних прибутків. Зроблено акцент на необхідності прозорого управління природними ресурсами, включення екологічного ризик-менеджменту у стратегії державних компаній і надання пріоритету криміналізації екозлочинів як предикатних для відмивання коштів.

Висновки:

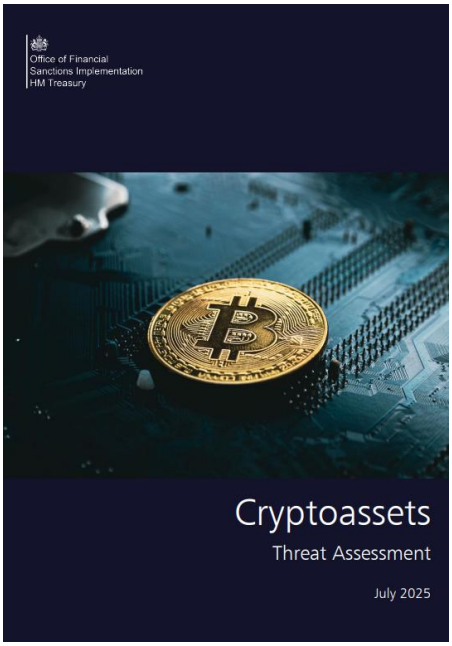
- **Корупція є системним бар'єром для досягнення ЦСР, який поглиблює нерівність, знижує якість державних послуг і призводить до втрати довіри до держави.** **Рекомендація:** G20 мають забезпечити посилення аудиту соціальних витрат, прозорість публічного управління та врахування гендерних аспектів у протидії корупції.
- **Інтеграція антикорупційних заходів у всі ланки економіки (держзакупівлі, оподаткування, фінансовий сектор) — ключ до зменшення втрат і мобілізації ресурсів для розвитку.** **Рекомендація:** впровадження електронних інструментів (е-закупівлі, аналітика, AI) і взаємодія податкових та антикорупційних органів мають стати пріоритетом.
- **Недостатнє врегулювання корупції від екологічних злочинів підриває глобальні зусилля у сфері клімату та збереження біорізноманіття.**
- **Рекомендація:** країни G20 мають інтегрувати антикорупційні індикатори у NDCs, підвищити прозорість у «зелених фінансах» та контролювати витрати, пов'язані з кліматом.
- **Повернення активів та боротьба з незаконними фінансовими потоками залишаються ключовими недоопрацьованими сферами у контексті фінансування розвитку. Рекомендація:** G20 мають активізувати використання цивільних / адміністративних конфіскацій, забезпечити прозорі угоди з повернення активів і гарантувати, що ці кошти спрямовуються на потреби сталого розвитку.

Окремим розділом розглядається питання повернення активів, наголошуючи на тому, що обсяг повернутих коштів наразі вкрай обмежений порівняно з тим, що було конфісковано, а тим паче — з фактичними обсягами викрадених активів. Підкреслюється необхідність активнішого використання некримінальних механізмів конфіскації (цивільних, адміністративних), розвитку міжнародного співробітництва у правових та фінансових процедурах, а також забезпечення прозорого використання повернених активів для підтримки соціального розвитку в країнах-отримувачах.

У висновках документа наголошується, що країни G20 мають моральний і політичний обов'язок діяти як глобальні лідери у сфері антикорупції, забезпечуючи як внутрішню реформу, так і підтримку іншим країнам шляхом технічної допомоги, обміну досвідом та участі в міжнародних ініціативах. Успішна реалізація

ЦСР є неможливою без фундаментальної боротьби з корупцією, і кожна країна повинна усвідомити, що антикорупційна політика — це не паралельна складова розвитку, а його основа.

Криптоактиви під прицілом санкцій: оцінка загроз для Сполученого Королівства у 2022–2025 роках[7]



Оцінка загроз, пов'язаних із криптоактивами, підготовлена Управлінням з реалізації фінансових санкцій Сполученого Королівства (OFSI) у липні 2025 року, є аналітичним документом, що ґрунтується на даних про підозрювані порушення санкційного законодавства у секторі криптоактивів за період з січня 2022 по травень 2025 року. Вона є частиною серії галузевих оцінок, які мають на меті підтримати суб'єктів, що працюють у Сполученому Королівстві, у запровадженні ризик-орієнтованого підходу до забезпечення відповідності фінансовим санкціям. В умовах після початку повномасштабного вторгнення росії в Україну і посилення санкційного тиску з боку Сполученого Королівства та її партнерів, криптоіндустрія зазнала суттєвого перегляду регуляторної уваги, зокрема у зв'язку з ризиками, пов'язаними з обходом санкцій та незаконним рухом цифрових активів у глобальному просторі.

Документ вказує, що з часу внесення криптофірм до переліку «відповідних осіб» у санкційному законодавстві у 2022 році, OFSI зафіксувало, що більш як 7% усіх звітів про підозрювані порушення стосуються саме цього сектора, причому понад 90% з них надійшли у 2024–2025 роках. При цьому OFSI майже напевно вважає, що значна частина порушень санкцій не була задекларована. Основними причинами такої недоподачі є ненавмисне порушення, затримка в атрибуції санкційних адрес, недостатнє використання блокчейн-аналітики, або ж недосконалі системи моніторингу транзакцій у компаніях. Звіт наголошує, що типові порушення відбуваються через як прямий, так і непрямий контакт із особами чи структурами, що підпадають під санкції. Наприклад, фірма може приймати кошти, що проходять через одну або кілька транзакційних «переходів» (hops) від гаманця, що належить підсанкційній особі, або надавати технічні чи операційні послуги контрагентам, які у свою чергу співпрацюють із підсанкційними особами.

Окрему увагу приділено впливу російської біржі Garantex, яка після внесення до санкційного списку у 2023 році продовжувала отримувати транзакції від британських криптофірм як безпосередньо, так і через посередників. OFSI стверджує, що майже всі виявлені перекази до підсанкційних осіб після 2022 року так чи інакше включали Garantex. Після міжнародної спецоперації у 2025 році, яка призвела до її закриття, діяльність Garantex продовжилася під брендом Grinex – новою платформою, зареєстрованою у Киргизстані, яка приймає платежі від російських користувачів, обслуговує ті ж самі адреси, що й Garantex, та використовує візуально ідентичний інтерфейс. Це створює ризики для британських компаній, які можуть несвідомо вступати у взаємодію з підсанкційною інфраструктурою.

Іншою суттєвою загрозою у звіті визначено діяльність кіберзлочинних груп, пов'язаних із Північною Кореєю. Йдеться як про прямі атаки на криптофірми з метою викрадення активів, так

7 https://assets.publishing.service.gov.uk/media/687e6362791bb4d8c309a06e/OFSI_Cryptoassets_Threat_Assessment.pdf

і про масштабні схеми відмивання коштів через багатоступеневі маршрути, що включають DeFi-протоколи, обмінники без KYC, позабіржові платформи у третіх юрисдикціях та використання стейблкоїнів. У звіті наведено приклади атак на британські фірми Merlin DEX та Lykke, в яких було викрадено мільйони доларів у криптоактивах. Також зазначено, що КНДР використовує IT-фахівців під прикриттям (фрилансерів), які влаштовуються на роботу до компаній і отримують доступ до критичної інфраструктури з метою подальшого компрометації або витоку коштів.

Ще одним важливим вектором загроз є операції, пов'язані з Іраном. Після узаконення криптомайнінгу та запуску цифрового ріалу, іранська інфраструктура активно використовує криптоактиви для обходу санкцій і зовнішньої торгівлі. OFSI зафіксувало перекази з Сполученого Королівства на іранські платформи, зокрема Nobitex, яка має імовірні зв'язки з Корпусом вартових ісламської революції (IRGC). Ці платформи не лише проводять фінансові операції, але й надають інструкції користувачам, як обійти міжнародні обмеження, включаючи використання документів з використанням діпфейків для проходження KYC.

Документ містить широкий перелік типових схем санкційного обходу, зокрема використання DeFi, неавторизованих обмінників, NFT, мемкоїнів, а також інструментів, які сприяють зникненню сліду транзакцій у блокчейні. Наведено детальні червоні прапорці, що вказують на потенційну участь у санкційних порушеннях: нетипова активність одразу після оголошення санкцій, нові гаманці з великими переказами, використання VPN, DEX-ів, P2P, а також публічний маркетинг послуг типу «санкційно-стійкий кешаут».

З практичного боку OFSI наголошує на обов'язку криптофірм повідомляти про підозрілі активності не лише до OFSI, але й до FCA та NCA, та рекомендує включати у звіти чітко атрибутовані адреси, трасу транзакцій, затримки у виявленні, використану аналітику, а також KYC-дані користувачів. Особлива увага приділяється історичним порушенням, які виявляються завдяки новим аналітичним інструментам, та правильному трактуванню їх у контексті дати санкційного призначення.

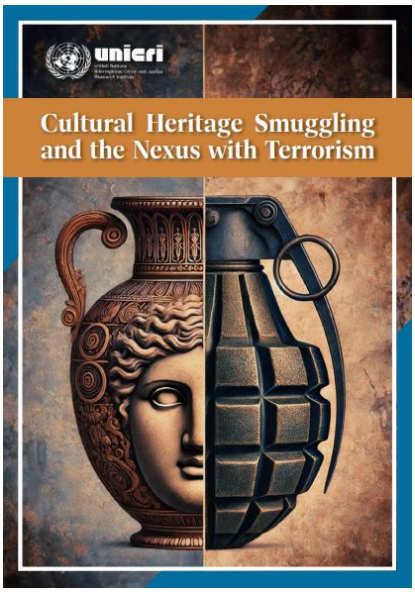
Висновки:

- **Британські криптофірми майже напевно системно недоповідають про підозри порушення санкцій.**
  Практична дія: запровадити регулярні ретроспективні перевірки всіх транзакцій, зокрема за допомогою блокчейн-аналітики.
- **Найпоширенішими причинами порушень є затримки в ідентифікації адрес, пов'язаних із санкційними особами, та неналежний моніторинг на кілька «переходи».**
  Рекомендація: установити контроль на глибину не менше 3–5 трансакцій (переходи) і постійно оновлювати аналітичні кластери адрес.
- **OFSI вважає високим ризик прямих і опосередкованих зв'язків із російською біржею Garantex та її наступником Grinex.**
  Практична дія: заблокувати будь-які адреси/платформи, пов'язані з цими суб'єктами, та оперативно повідомляти OFSI/NCA.
- **КНДР продовжує активно атакувати британський криптосектор для викрадення активів та відмивання коштів.**
  Рекомендація: проводити належну перевірку персоналу, уникати найму IT-фрилансерів без перевірок, а також негайно повідомляти про будь-яке викрадення або підозру на хакерське втручання.

У підсумку, OFSI закликає всі британські фірми, що взаємодіють із сектором криптоактивів, не лише дотримуватися поточних вимог, але й проводити активний внутрішній аудит, перегляд політик моніторингу, впровадження багаторівневої блокчейн-аналітики, перевірку контрагентів і навчання персоналу щодо ризиків обходу санкцій. Цей документ є не лише попередженням, а

й інструментом для запровадження кращих практик у сфері комплаєнсу на стику криптосектору та санкційного регулювання.

Контрабанда культурної спадщини та її зв’язок із тероризмом: глобальні виклики та стратегії протидії [8]



Документ, підготовлений Міжрегіональним дослідницьким інститутом ООН з питань злочинності та правосуддя (UNICRI) під авторством Крістіана Вієни де Азеведо, старшого наукового співробітника UNICRI та спеціального агента Федеральної поліції Бразилії, є всебічним дослідженням контрабанди культурної спадщини з особливим акцентом на її зв’язок із тероризмом.

Звіт має на меті не лише висвітлити масштаби та динаміку цього виду злочинної діяльності, але й підкреслити її перетин з організованою злочинністю та фінансуванням терористичних організацій. Документ спирається на історичний аналіз, академічні дослідження, звіти міжнародних організацій, таких як ООН та ЮНЕСКО, а також на напівструктуровані та неструктуровані інтерв’ю з експертами, правоохоронцями та особами, причетними до розслідувань. Окремо наголошується, що звіт не претендує на вичерпне охоплення всіх аспектів контрабанди культурної спадщини чи всіх маршрутів і методів злочинців, а фокусується на антикваріаті як ключовій складовій цього ринку.

Контрабанда культурної спадщини - це проблема, що має глибоке історичне коріння, сягаючи часів стародавніх імперій та колоніальної епохи, коли розграбування культурних цінностей було поширеним явищем. У сучасному світі цей ринок функціонує як складна мережа, що поєднує легальні та нелегальні операції, де легальність артефактів залежить від їхнього походження. Документ підкреслює, що ринок антикваріату характеризується високим рівнем секретності та анонімності, що робить його привабливим для таких злочинів, як відмивання грошей, ухилення від податків, торгівля людьми та фінансування тероризму. Артефакти, на відміну від інших незаконних товарів, таких як наркотики, можуть проходити процес "очищення", перетворюючись із контрабандних об’єктів у легальні предмети колекціонування, що ускладнює їх відстеження та притягнення винних до відповідальності.

Звіт детально описує, як контрабанда культурної спадщини пов’язана з тероризмом, зокрема через діяльність таких груп, як ІДІЛ, Аль-Каїда, Хезболла, Талібан, а також повстанські угруповання в Камбоджі, Колумбії, Лівії, Малі, Нігері та Сомалі. Ці організації використовують доходи від торгівлі антикваріатом для закупівлі зброї, вербування бійців, підтримки логістики та інших потреб. Наприклад, ІДІЛ створила спеціальний "Департамент цінних ресурсів" для управління розграбуванням і комерціалізацією артефактів в Іраку та Сирії, видаючи ліцензії на розкопки та стягуючи податки з брокерів. Резолюції Ради Безпеки ООН (2199 від 2015 року та 2347 від 2017 року) підтверджують участь ІДІЛ, Аль-Каїди та інших груп у незаконній торгівлі антикваріатом, що підкріплюється доказами, зібраними під час операцій, таких як рейд спецназу США в 2015 році на об’єкт ІДІЛ.

[8] https://unicri.org/sites/default/files/2024-07/Cultural%20Heritage%20Smuggling%20and%20the%20Nexus%20with%20Terrrorism.pdf

Документ також аналізує регіональні особливості контрабанди культурної спадщини. У Центральній Америці, зокрема в Белізі, Сальвадорі, Гватемалі та Гондурасі, наркокартелі з 1980-х років використовують доходи від торгівлі артефактами для фінансування наркоторгівлі та закупівлі зброї, часто поєднуючи контрабанду антикваріату з транспортуванням наркотиків. В Африці, зокрема в країнах Сахелю (Алжир, Лівія, Малі, Нігер, Нігерія, Туніс), місцеві жителі, так звані "копачі", розграбовують археологічні об'єкти для забезпечення базових потреб, але значна частина артефактів потрапляє до транснаціональних злочинних мереж, які експортують їх до Європи, США та країн Аравійського півострова. У Малі, наприклад, через триваючі конфлікти та нестабільність до 90% археологічних об'єктів було розграбовано. На Близькому Сході, в таких країнах, як Ірак, Сирія, Афганістан і Ємен, терористичні групи систематично розграбовують археологічні пам'ятки, використовуючи старі торговельні маршрути для транспортування артефактів через Туреччину, Йорданію чи ОАЕ. У Китаї масове розграбування стародавніх гробниць, де 80–90% об'єктів уже пограбовано, підживлюється попитом на міжнародному ринку, а в Камбоджі контрабанда артефактів до Таїланду стала серйозною проблемою, що потребувала міжнародних розслідувань.

Одним із ключових викликів у боротьбі з контрабандою культурної спадщини є непрозорість ринку антикваріату. Законодавство в багатьох країнах є недостатньо чітким або суперечливим, що дозволяє легалізувати незаконно отримані артефакти, особливо ті, що були вивезені в колоніальні часи. Відсутність паперового сліду в транзакціях, складність визначення походження та автентичності артефактів, а також брак спеціалізованих знань у митних служб, правоохоронних органів, прокурорів і суддів ускладнюють розслідування та судовий розгляд. Крім того, злочини, пов'язані з культурною спадщиною, часто сприймаються як "без жертв", що знижує їх пріоритетність для урядів порівняно з насильницькими злочинами чи наркоторгівлею. Іншою проблемою є тривале зберігання артефактів у схованках (іноді роками чи десятиліттями), що ускладнює їх відстеження та повернення до країн походження.

Документ пропонує низку практичних рекомендацій для протидії контрабанді культурної спадщини. По-перше, уряди, неурядові організації та академічні установи повинні посилити програми підвищення культурної обізнаності, залучаючи місцеві громади до збереження їхньої спадщини, особливо в бідних регіонах, де люди вдаються до розграбування через економічні труднощі. Такі програми мають поєднуватися з ініціативами створення робочих місць для зменшення економічної мотивації. По-друге, країни, які найбільше страждають від розграбування, повинні створювати міждисциплінарні мережі співпраці між правоохоронцями, прокурорами,

Висновки:

- **Вдосконалення законодавства та інфраструктури:** Африканським країнам слід терміново оновити правові рамки, гармонізуючи їх із міжнародними стандартами, та створити системи повідомлення про кіберінциденти, цифрові сховища доказів і бази даних кіберрозвідки для ефективної боротьби з кіберзлочинами.
- **Посилення співпраці:** Необхідно прискорити міжнародну співпрацю через оперативні мережі та спростити доступ до даних, розміщених за кордоном, а також налагодити чіткі канали взаємодії з приватним сектором для спільного розслідування кіберзлочинів.
- **Інвестиції в підготовку кадрів:** Правоохоронні органи потребують спеціалізованого навчання та доступу до сучасних інструментів, щоб подолати нестачу ресурсів і кваліфікації, про яку повідомили 95% країн.
- **Підвищення обізнаності громадян:** Розширення програм інформування про фішинг, програми-вимагачі та цифрове шахрайство допоможе зменшити кількість жертв і підвищити кіберстійкість суспільства.

суддями, культурними органами та академічними експертами для підвищення якості розслідувань. По-третє, необхідна тісніша співпраця між державним і приватним секторами, зокрема в країнах призначення, де власники галерей і працівники музеїв повинні проходити навчання для розпізнавання незаконних артефактів і розуміння їхнього зв'язку з фінансовими злочинами та тероризмом. По-четверте, країни походження, транзиту та призначення повинні укладати двосторонні та багатосторонні угоди для стандартизації процедур, обміну інформацією та створення спільних слідчих груп. Це включає використання технологій для моніторингу ринків антикваріату. Нарешті, звіт підкреслює необхідність додаткових академічних досліджень для кращого розуміння зв'язку між контрабандою культурної спадщини та фінансуванням тероризму, з акцентом на відстеження фінансових потоків і транснаціональних злочинних мереж.

Санкції

ЄС ухвалює 18-й пакет економічних та індивідуальних заходів [9]

18-й пакет санкцій Європейського Союзу проти росії, ухвалений 18 липня 2025 року, є суттєвим розширенням та посиленням існуючих обмежувальних заходів, спрямованих на підрив здатності росії фінансувати свою агресивну війну проти України. Цей пакет охоплює широкий спектр секторів, включаючи енергетичний, банківський, військово-промисловий комплекси та торгівлю, а також індивідуальні санкції, що свідчить про намір ЄС продовжувати тиск до повного припинення агресії.

Одним із ключових аспектів нового пакету є подальше обмеження доходів росії від енергоносіїв. Цінова стеля на сиру нафту знижується з 60 до 47,6 доларів США за барель, що відображає поточні світові ціни на нафту та має на меті подальше скорочення доходів росії від експорту нафти, які все ще становлять значну частину урядових надходжень. Вводиться автоматичний та динамічний механізм коригування цінової стелі, що забезпечить її ефективність та адаптацію до ринкових умов. Це доповнюється забороною на імпорт до ЄС нафтопродуктів, вироблених у третіх країнах з російської сирої нафти, за винятком тих, що походять з країн-партнерів (Канада, Норвегія, Швейцарія, Сполучене Королівство та США), що має перекрити шляхи обходу санкцій.

Значна увага приділяється протидії російському "тіньовому флоту", який використовується для обходу цінової стелі та транспортування нафти, військового обладнання та викраденого українського зерна. Додатково 105 суден підпадають під заборону доступу до портів та шлюзів ЄС, а також заборону на надання широкого спектру послуг, пов'язаних з морськими перевезеннями, збільшуючи загальну кількість таких суден до 444. Вперше під санкції потрапляє капітан судна "тіньового флоту" та приватний оператор міжнародного морського реєстру. Це посилює тиск на механізми, які росія використовує для приховування походження нафти та обходу санкцій, що безпосередньо впливає на її нафтові доходи. Крім того, вводиться повна заборона на будь-які транзакції, пов'язані з газопроводами Nord Stream 1 та Nord Stream 2, включаючи їх будівництво, експлуатацію, технічне обслуговування та будь-яке майбутнє

[9] https://www.consilium.europa.eu/en/press/press-releases/2025/07/18/russia-s-war-of-aggression-against-ukraine-eu-adopts-18th-package-of-economic-and-individual-measures/?utm_source=linkedin.com&utm_medium=social&utm_campaign=20250718-fac-meeting-russia-sanctions-18-package&utm_content=visual

використання. Це спрямовано на унеможливлення майбутніх надходжень від постачання газу через ці трубопроводи. Також припиняється тимчасове звільнення для Чехії щодо імпорту нафти трубопроводом з росії.

Банківський сектор зазнає подальших обмежень. Існуюча заборона на надання спеціалізованих фінансових послуг, що базуються в ЄС, певним російським банкам, розширюється до повної заборони транзакцій. Це стосуватиметься 22 додаткових російських банків, на додаток до 23 вже існуючих. Знижується поріг для накладення санкцій на фінансові та кредитні установи третіх країн, а також постачальників послуг з криптоактивами, які сприяють обходу санкцій, підтримують агресивну війну росії або пов'язані з російською системою передачі фінансових повідомлень (SPFS). Це розширення заборони транзакцій також охоплює фінансові установи третіх країн, які підтримують війну росії, зокрема шляхом обробки транзакцій або надання експортного фінансування для торговельних операцій, що обходять мету санкцій. Вводиться повна заборона на здійснення будь-яких транзакцій з російським фондом прямих інвестицій (RDIF) та його дочірніми компаніями та інвестиціями. Крім того, чотири російські компанії, в які RDIF здійснив значні інвестиції, також підпадають під цю заборону, що ще більше обмежує доступ росії до світових фінансових ринків та іноземної валюти. Також вводиться заборона на продаж, постачання, передачу та експорт програмного забезпечення для управління підприємствами, промислового дизайну та виробництва, а також програмного забезпечення з певними застосуваннями в банківському та фінансовому секторах.

Військово-промисловий комплекс росії зазнає подальших ударів. Вводяться повні санкції щодо постачальників російського ВПК, включаючи три організації з Китаю, які продають товари, що використовуються на полі бою. 26 нових організацій підпадають під більш жорсткі експортні обмеження щодо товарів та технологій подвійного призначення, включаючи ті, що можуть сприяти технологічному розвитку російського оборонного та безпекового сектору. Одинадцять з цих організацій розташовані в третіх країнах (сім у Китаї та Гонконзі, чотири в Туреччині), і були залучені до обходу експортних обмежень, у тому числі для безпілотних літальних апаратів (БПЛА). Розширено список обмежених товарів, які сприяють технологічному розвитку оборонного та безпекового сектору росії, включивши верстати з числовим програмним керуванням (ЧПК) та хімічні компоненти для палива. Існуюча заборона на транзит через територію росії також розширена, щоб охопити окремі економічно важливі товари, що використовуються для будівництва та транспорту.

Щодо Білорусі, пакет санкцій включає вісім нових індивідуальних обмежень, пов'язаних з білоруським військовим комплексом. Також посилюються заходи, що стосуються торгівлі з Білоруссю, які тепер відображають заходи, накладені на росію. Заборона на спеціалізовані послуги фінансових повідомлень посилюється до повної заборони транзакцій, а також вводиться ембарго на імпорт зброї з Білорусі.

Пакет також містить заходи, спрямовані на захист держав-членів від нелегітимних арбітражних розглядів у рамках двосторонніх інвестиційних угод (BIT), ініційованих російськими компаніями та особами, включаючи олігархів. Це включає положення про відшкодування збитків, які мають бути стягнуті державами-членами, положення про невизнання таких арбітражних розглядів у ЄС та зобов'язання для держав-членів діяти в судових процесах BIT.

Щодо впливу на російський бюджет та доходи, суворе дотримання цих санкцій, особливо щодо нафтогазового сектору, має на меті значно скоротити джерела фінансування російської агресії. Зменшення цінової стелі на нафту до $47,6 за барель, розширення списків суден "тіньового флоту" та заборона на імпорт нафтопродуктів з російської сировини, незважаючи на спроби росії використовувати нетрадиційні шляхи експорту, будуть тиснути на її енергетичні доходи.

За даними Міністерства фінансів рф, станом на 1 липня 2025 року, обсяг Фонду національного добробуту росії (ФНБ) становив близько $133,3 млрд, або 7,6% ВВП країни. Ліквідна частина

ФНБ (кошти, які можуть бути використані для покриття дефіциту бюджету) становила $87,5 млрд. Дефіцит російського бюджету за перше півріччя 2025 року, за попередніми даними, склав близько $17 млрд. Уряд росії прогнозує дефіцит на весь 2025 рік на рівні 0,9% ВВП, або близько $20 млрд. Однак міжнародні аналітичні центри та фінансові установи, такі як МВФ, прогнозують, що фактичний дефіцит може бути значно вищим, до 2,5-3% ВВП, або близько $50-60 млрд, враховуючи зростання військових витрат та падіння нафтогазових доходів на тлі санкцій.

Додаткові фінансові санкції, включаючи розширену заборону транзакцій з банками, та повну заборону на операції з RDIF, будуть обмежувати доступ росії до світових фінансових ринків та іноземної валюти, ускладнюючи фінансування дефіциту бюджету. Це може змусити росію звернутися до внутрішніх резервів, таких як ФНБ, що виснажить їх швидше, ніж очікувалося, особливо ліквідну частину. Довгостроковий вплив включатиме погіршення інвестиційного клімату, технологічну деградацію та подальшу ізоляцію російської економіки. За умов суворого дотримання санкцій, нафтові та газові доходи росії продовжать знижуватися, що створить додатковий тиск на бюджет та змусить уряд вдаватися до ще більших запозичень або скорочення соціальних програм. Це потенційно може призвести до значного збільшення дефіциту та подальшого зниження рівня ФНБ.

Висновки:

- **Цілеспрямоване зменшення енергетичних доходів росії:** Зниження цінової стелі на нафту до $47,6/барель та посилення контролю за "тіньовим флотом" є пріоритетом, що вимагає постійного моніторингу та адаптації для максимального скорочення фінансових надходжень, які є основою російського військового бюджету.
- **Повне відключення від світової фінансової системи:** Розширення банківських санкцій до повної заборони транзакцій та блокування операцій з RDIF критично важливе для обмеження доступу росії до іноземної валюти та капіталу, що змусить її покладатися на внутрішні, швидко виснажувані резерви, такі як ФНБ.
- **Припинення постачання для військово-промислового комплексу:** Санкції проти постачальників ВПК росії, особливо з третіх країн, та розширення списку заборонених технологій (ЧПК-верстати, хімічні компоненти для палива) є ключовими для підриву здатності росії виробляти та модернізувати військове обладнання.
- **Захист від правового шантажу та обходу санкцій:** Введення механізмів захисту від нелегітимних арбітражних позовів та обов'язок держав-членів активно протидіяти обходу санкцій у судовому порядку створює додатковий рівень захисту від спроб росії підірвати санкційний режим.

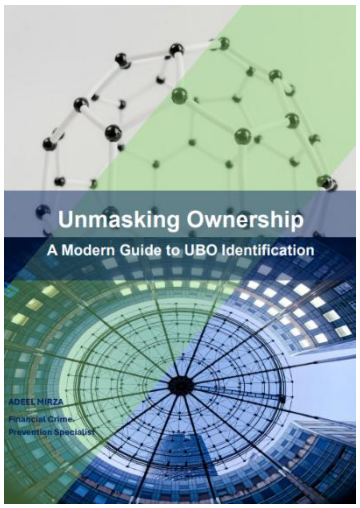
Звіти окремих інституцій та експертів

Розкриття власності [10]

Даний документ слугує всебічним посібником з ідентифікації кінцевих бенефіціарних власників (КБВ), що є фундаментальним та незамінним елементом ефективної системи ПВК/ФТ. Це не просто формальність дотримання вимог, а життєво важлива практика управління ризиками, спрямована на виявлення реальних осіб, що стоять за корпоративними механізмами,

[10] https://media.licdn.com/dms/document/media/v2/D4D1FAQGhW92he_jfZQ/feedshare-document-pdf-analyzed/B4DZf._r2VHAAY-/0/1752329804129?e=1754524800&v=beta&t=u_RzEiBDYe6doNwhCw97xEwQ5klayW8b2ftIZrByGME

підставними компаніями, трастами та багатошаровими структурами власності, навмисно розробленими для приховування бенефіціарної власності. Прозорість власності та контролю запобігає нецільовому використанню юридичних осіб для незаконних цілей, таких як відмивання коштів, фінансування тероризму, ухилення від сплати податків, корупція та фінансування організованої злочинності.



Глобально, важливість ідентифікації КБВ підкреслюється обов'язковими міжнародними стандартами, які вимагають від юрисдикцій та підзвітних організацій впровадження надійних заходів розкриття бенефіціарної власності. Ці стандарти, зокрема, Рекомендації FATF 10 і 24, 5-та Директива ЄС щодо боротьби з відмиванням коштів (5AMLD), вбудовані в національні закони по всьому світу, створюючи єдину основу для просування прозорості, підзвітності та ефективного зниження ризиків. Цей посібник призначений для допомоги командам комплаєнсу, ПВК/ФТ та онбордингу в ідентифікації КБВ у різних структурах власності, включаючи приватні компанії, публічні компанії, трасти, холдингові компанії та транскордонні юридичні особи.

КБВ – це не просто акціонер чи зареєстрований директор, а особа, яка прямо або опосередковано здійснює значний контроль над юридичною особою. Це може включати володіння певною часткою власності або правом голосу (зазвичай 25% або більше, хоча пороги можуть відрізнятися залежно від юрисдикції), або наявність повноважень впливати на рішення, призначати вище керівництво чи отримувати економічну вигоду від активів юридичної особи. Якщо жодна фізична особа не відповідає порогу власності чи контролю, або якщо є сумніви щодо достовірності наданої інформації, КБВ може бути визначений як старший керівний службовець або фізична особа, яка контролює іншими засобами. У трастах та подібних утвореннях КБВ включають засновника трасту, довірену особу та будь-яку іншу фізичну особу, що здійснює кінцевий контроль над трастом. Механізми контролю охоплюють частки в капіталі, права голосу, домінуючий вплив, право призначати/знімати більшість членів правління.

Розуміння того, як ідентифікувати КБВ у різних типах юридичних осіб та складних утвореннях, є фундаментальною складовою ефективної належної перевірки клієнтів (CDD) та зменшення ризиків фінансових злочинів. У сучасному глобальному фінансовому середовищі, де злочинці, особи, що ухиляються від сплати податків, та особи, що перебувають під санкціями, все частіше експлуатують юридичні структури для приховування своєї особистості, простої ідентифікації юридичного власника недостатньо. Ідентифікація КБВ дозволяє установам заглянути за межі формальної структури та виявити фізичних осіб, які дійсно володіють, контролюють або отримують вигоду від компанії, трасту чи іншого правового утворення. Підхід до ідентифікації КБВ повинен бути ретельно адаптований до типу залученої організації, оскільки права власності, механізми контролю та права на вигоду значно відрізняються між організаційними структурами. Ця структурна складність вимагає складного та розважливого підходу до розслідування, що поєднує глибокі регуляторні знання з ретельними аналітичними навичками. Ефективна ідентифікація КБВ передбачає ретельне відстеження власності через заплутані, багатошарові рамки, навігацію транскордонними організаціями та перевірку номінальних акціонерів або директорів, які можуть служити лише прикриттям. Такі структури часто навмисно створюються для приховування справжніх бенефіціарних власників та перешкоджання прозорості.

Посібник деталізує процеси ідентифікації для різних структур власності. Для прямої власності (прості структури), де фізичні особи безпосередньо володіють акціями, кроки включають перевірку особи та власності фізичної особи, а також реєстрацію та скринінг даних КБВ. У випадку непрямих/складних структур власності, де власність є багатошаровою через кілька

юридичних осіб, необхідно скласти корпоративну структуру з відсотками акцій на кожному рівні, розрахувати кінцеву власність шляхом множення, ідентифікувати фізичних осіб з ≥25% непрямої власності та перевірити права контролю, якщо власність розподілена. Багатоюрисдикційна власність, що охоплює кілька країн (часто з використанням офшорних компаній), вимагає запиту сертифікованих або апостильованих корпоративних документів, використання інструментів для відстеження транскордонних ланцюгів (наприклад, OpenCorporates або Orbis), застосування рейтингу ризиків юрисдикції (списки FATF, податкові гавані) та проведення перевірок джерела походження багатства для КБВ з високим ризиком.

Виявлення "червоних прапорців" у структурах КБВ є ключовим для виявлення потенційних спроб приховати справжню власність та уникнути регуляторного контролю. До таких "червоних прапорців" належить використання складних, багатошарових ланцюгів власності, особливо коли юридичні особи охоплюють кілька юрисдикцій, що вважаються високоризиковими або непрозорими. Наявність номінальних акціонерів або директорів, які, схоже, займають посади без чіткого економічного обґрунтування, часто свідчить про спробу приховати справжню контролюючу сторону. Аналогічно, часті зміни у власності або контролі, особливо напередодні значних фінансових операцій, можуть вказувати на спроби уникнути виявлення. КБВ, які є політично значущими особами (PEP), або ті, що мають зв'язки з офшорними фінансовими центрами, вимагають посиленої перевірки через підвищений ризик. Ще одним "червоним прапором" є ситуація, коли КБВ юридичної особи важко перевірити або він не бажає надавати ідентифікаційні документи, або коли КБВ є фізичною особою без чіткого зв'язку з бізнес-операціями чи географічною присутністю організації. Ці індикатори, окремо або разом, повинні спровокувати заходи посиленої належної перевірки (EDD), оскільки вони можуть вказувати на відмивання коштів, ухилення від сплати податків або нецільове використання юридичних осіб для незаконних цілей. EDD запускається, якщо КБВ знаходиться у високоризиковій юрисдикції, складна структура власності приховує контроль, є розбіжності у документах, офшорні компанії не мають видимого економічного обґрунтування, або залучено PEP. В кінцевому підсумку, ефективна ідентифікація КБВ виходить за рамки простої

Висновки:

- **Стратегічна необхідність:** Ідентифікація КБВ є фундаментальним елементом ефективних систем ПВК/ФТ, що дозволяє виявляти реальних осіб, які стоять за корпоративними структурами, та запобігати використанню юридичних осіб для фінансових злочинів, таких як відмивання коштів, фінансування тероризму та ухилення від сплати податків. Це вимагає адаптованого та складного підходу до розслідування.
- **Комплексний підхід до ідентифікації:** Процес ідентифікації КБВ повинен бути гнучким, враховуючи різноманітні структури власності (прямі, непрямі, багатоюрисдикційні) та типи юридичних осіб (компанії, трасти), з визначенням порогів контролю (як правило, 25% власності/голосів) та застосуванням правила "старшого керівника" як резервного варіанта.
- **Життєво важлива роль "червоних прапорців" та EDD:** Установи повинні бути особливо пильними до "червоних прапорців", таких як складні багатошарові структури, використання номінальних осіб, часті зміни власності або залучення PEP, оскільки ці індикатори вимагають негайної посиленої належної перевірки для розкриття прихованої власності та зниження ризиків фінансових злочинів.
- **Професіоналізм та скептицизм:** Ефективна ідентифікація КБВ — це не лише перевірка документів, а й критичний, ризик-орієнтований процес, що вимагає глибокого аналізу юрисдикцій, ретельної оцінки складних структур та пильного професійного скептицизму для розкриття справжніх бенефіціарів за навмисно замаскованими схемами.

процедурної формальності; це критичний, заснований на ризиках, дослідницький процес, який вимагає надійного поєднання документальної перевірки, ретельного аналізу юрисдикцій та пильної професійної скептичності.

Використання терористами посередників з надання послуг з віртуальними активами [11]

Документ, підготовлений Еллісон Оуен у межах проєкту CRAAFT II, є глибоким і емпірично обґрунтованим аналізом того, як терористичні організації — зокрема ХАМАС, Хезболла та ІДІЛ — поступово інтегрують віртуальні активи (ВА) у свою фінансову діяльність, насамперед через використання посередницьких сервісів. До таких посередників належать позабіржові (OTC) брокери, платформи peer-to-peer (P2P) і малі сервіси з конвертації активів, які сприяють обміну ВА на фіатні кошти та навпаки. У дослідженні використано дані блокчейн-аналізу від компанії Crystal Intelligence, а також інтерв'ю з експертами державного й приватного сектору, відкриті джерела і накази Ізраїлю про адміністративні вилучення активів.

Хоча традиційні методи фінансування тероризму — наприклад, перевезення готівки чи використання системи хавала — залишаються домінуючими, автори фіксують зростання експериментів із ВА, особливо у країнах із прогалинами в регулюванні, високим рівнем тіньової економіки та обмеженим доступом до офіційної фінансової інфраструктури. Наприклад, ХАМАС організовував напівструктуровані кампанії зі збору пожертв через Telegram із використанням TRON-адрес USDT. Ці кампанії передбачали регулярну зміну криптогаманців, інструкції з використання офісів обміну валют та інші засоби, що ускладнюють ідентифікацію донорів і відстеження ланцюжків транзакцій правоохоронцями.

Окрему увагу приділено малим сервісам із конвертації активів та OTC-брокерам, які часто діють у сірій зоні або взагалі поза межами регуляторного поля. Два кейси з Лівану ілюструють, як такі сервіси можуть використовуватись терористами: йдеться, зокрема, про вже закриту платформу "Cashout.lb" і анонімний конвертаційний пункт, транзакції якого свідчать про незареєстровану обмінну діяльність. Обидва випадки були безпосередньо пов'язані з діяльністю терористичних організацій, що підтверджується адміністративними ордерами на вилучення активів з боку Ізраїлю.

Згідно з аналітикою Crystal Intelligence, не всі посередники свідомо сприяють терористичним фінансовим потокам, проте їхня діяльність часто є критичною ланкою завдяки відсутності або слабкості заходів ПВК/ФТ. Часто такі брокери функціонують як пулові гаманці або агрегатори, що переводять великі обсяги транзакцій через великі криптобіржі, які виступають джерелом ліквідності. Унаслідок цього терористичні кошти можуть «вбудовуватись» у легальну фінансову систему. Автори звіту закликають до посилення контролю як на рівні таких брокерів, так і на рівні великих бірж, які зобов'язані впроваджувати заходи підвищеної обачності при ідентифікації клієнтів і моніторингу транзакцій.

[11] https://www.projectcraaft.eu/research-briefings/https/static1squarespacecom/static/5e399e8c6e9872149fc4a041/t/681ccf124419647df74eb0ac/1746718484160/594-craaft-ii-bp1-terrorist-financingpdf-sebw9

Окремо розглядається роль третіх осіб, які забезпечують готівкову конвертацію віртуальних пожертв, зокрема через неформальні системи грошових переказів типу хавала у Лівані та Сирії. Особливе занепокоєння викликає використання стейблкоїнів (зокрема USDT у мережі TRON) для зведення балансів між такими структурами, що значно ускладнює виявлення таких схем через їх децентралізований і непрозорий характер. Автор також звертає увагу на злиття терористичного фінансування з іншими формами фінансових злочинів: окремі суб'єкти, ідентифіковані у терористичних схемах, одночасно брали участь у криптовалютних шахрайствах на кшталт «pump-and-dump».

У заключному розділі висвітлюються ключові вразливості і формулюються рекомендації для подальшого регуляторного реагування. Зокрема, підкреслюється доцільність не забороняти сервіси з конвертації ВА, а регулювати їхню діяльність, щоби не сприяти витісненню в тінь. Також рекомендовано запровадити моніторинг вкладених послуг (nested providers), підвищити вимоги до криптобірж щодо ідентифікації клієнтів і транзакційного аналізу, а також системно відстежувати обіг стейблкоїнів у неформальних трансфертних мережах. У якості пріоритетних дій виділено також необхідність детального відображення фінансових потоків і посилення транскордонної співпраці — враховуючи мобільність таких послуг і дедалі складніші схеми приховування фінансових операцій.

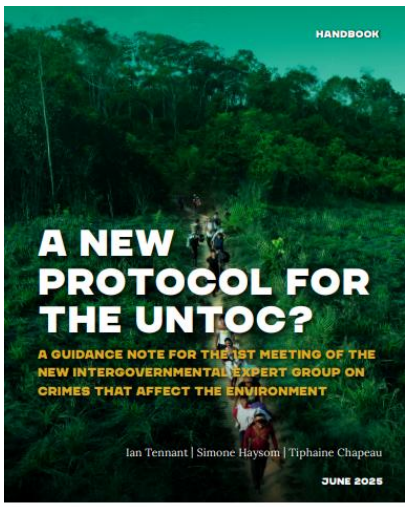
Висновки:

- **Посередницькі сервіси (OTC-брокери, малі пункти обміну, P2P-платформи) є ключовими каналами для доступу терористів до фіатної ліквідності.** Регуляторам варто в першу чергу ідентифікувати, легалізувати та контролювати такі сервіси в юрисдикціях із низьким рівнем ПВК/ФТ-нагляду.
- **Терористичні групи свідомо ускладнюють простеження криптовалютних пожертв через ротацію адрес і анонімні канали комунікації.** Необхідно розробити процедури розпізнавання фрагментованих потоків, зокрема у співпраці з блокчейн-аналітичними компаніями.
- **Стейблкоїни, особливо USDT у мережі TRON, дедалі активніше використовуються в системах типу хавала.** Слід посилити нагляд за потоками стейблкоїнів у країнах із розвиненими неформальними трансфертними мережами.
- **Великі біржі мають запровадити підвищені заходи обачності стосовно дрібних брокерів, що можуть бути неусвідомленими посередниками ФТ.** Зокрема, варто вдосконалити процедури ідентифікації, моніторингу транзакцій і виявлення схем «наповнення» та інтеграції злочинних коштів.

Новий протокол UNTOC: Шлях до посилення боротьби з екологічними злочинами [12]

Документ, підготовлений Global Initiative Against Transnational Organized Crime (GI-TOC), є ґрунтовним аналізом сучасного стану боротьби з екологічними злочинами та пропозицією щодо створення нового протоколу до Конвенції ООН проти транснаціональної організованої злочинності (UNTOC). Цей документ створений для підтримки роботи міжурядової експертної групи (IEG), перше засідання якої відбулось 30 червня – 2 липня 2025 року у Відні, з метою оцінки прогалин у міжнародному правовому полі, визначення необхідності нового протоколу та розробки рекомендацій для його ефективного впровадження. Він підкреслює нагальну потребу

[12] https://globalinitiative.net/wp-content/uploads/2025/06/Ian-Tennant-Simone-Haysom-Tiphaine-Chapeau-A-new-protocol-for-the-UNTOC_-GI-TOC-June-2025.v2.pdf



в оновленні міжнародної правової бази для боротьби з екологічними злочинами, які мають руйнівний вплив на екосистеми, здоров'я людини, економіки та глобальну стабільність.

Документ розпочинається з контексту, нагадуючи, що у жовтні 2024 року Бразилія, Франція та Перу внесли резолюцію на 12-й сесії Конференції UNTOC, яка закликала оцінити, як Конвенція застосовується до злочинів, що впливають на довкілля, та виявити прогалини в чинних міжнародних правових механізмах. Ця ініціатива є частиною багаторічного руху за посилення боротьби з екологічними злочинами, які виходять за межі регулювання Конвенції про міжнародну торгівлю видами дикої фауни і флори, що перебувають під загрозою зникнення (CITES). Зокрема, документ відзначає, що поточна міжнародна правова база є фрагментованою, а координація між різними ініціативами, організаціями (такими як UNODC, INTERPOL, IUCN) та форумами залишається недостатньою. Перше засідання IEG у Відні стало ключовою платформою для багатосторонніх дискусій, спрямованих на створення нового інструменту для боротьби з цими злочинами.

Екологічні злочини, такі як незаконний видобуток природних ресурсів, торгівля дикими видами, забруднення довкілля та маніпуляції фінансовими механізмами, такими як ринки вуглецевих кредитів чи біорізноманіття, мають серйозні та різноманітні наслідки. За оцінками Світового банку, незаконне полювання, вирубка лісів та торгівля дикими видами завдають глобальній економіці збитків на суму від 1 до 2 трильйонів доларів США щорічно. Ці злочини погіршують якість води, повітря та ґрунту, сприяють пандеміям, порушують права людини, зокрема корінних народів, та підривають економічну стабільність, відбираючи доходи у держав. Особливо вразливими є захисники довкілля, які дедалі частіше зазнають переслідувань, погроз і навіть убивств від злочинних мереж та корумпованих чиновників. Документ підкреслює, що ці злочини є глибоко глобалізованими, що вимагає скоординованої міжнародної відповіді.

Основна частина документа присвячена аналізу прогалин у чинному правовому полі. По-перше, міжнародні угоди, такі як CITES, Базельська, Роттердамська, Стокгольмська та Мінаматська конвенції, зосереджені переважно на регулюванні торгівлі, а не на криміналізації екологічних злочинів. UNTOC є єдиною універсальною угодою з положеннями кримінального права, але вона не має специфічного протоколу для екологічних злочинів, на відміну від протоколів щодо торгівлі людьми, контрабанди мігрантів чи незаконного обігу зброї. Це призводить до того, що законодавство є фрагментованим і не гармонізованим між країнами, що ускладнює боротьбу з найбільш шкідливими формами екологічних злочинів. По-друге, відсутність єдиних стандартів ускладнює міжнародну співпрацю, а низька обізнаність суддів і правоохоронців щодо використання UNTOC ще більше погіршує ситуацію. По-третє, у країнах Глобального Півдня бракує ресурсів, спроможностей і політичної волі для ефективного розслідування та судового переслідування екологічних злочинів, тоді як у країнах Глобальної Півночі ці злочини часто не є пріоритетними порівняно з традиційними загрозами безпеці. Корупція є ключовим фактором, що сприяє екологічним злочинам на всіх етапах – від незаконного видобутку до торгівлі та утилізації, і становить серйозну перешкоду для посилення законодавства та правозастосування. Крім того, приватний сектор, зокрема технологічні компанії, недостатньо залучений до боротьби з онлайн-торгівлею незаконними товарами, хоча технології могли б значно полегшити відстеження злочинів. Нарешті, екологічні злочини порушують права людини, особливо корінних народів та захисників довкілля, які потребують захисту та визнання їхньої ролі у протидії злочинам.

Документ пропонує бачення нового протоколу до UNTOC, який має базуватися на чотирьох принципах: спільній відповідальності, цілісному підході, підході, заснованому на шкоді, та залученні всього суспільства й уряду. Спільна відповідальність передбачає, що країни повинні співпрацювати, враховуючи глобальний характер екологічних злочинів, подібно до підходу в боротьбі з наркотиками. Цілісний підхід має охоплювати всі види екологічних злочинів, щоб уникнути фрагментації та передбачити появу нових незаконних ринків. Підхід, заснований на шкоді, фокусується на впливі злочинів на екосистеми та здоров'я людини, а не лише на окремих кримінальних ринках, таких як торгівля дикими тваринами. Підхід залучення усього суспільства ґрунтується на об'єднанні зусиль урядових інституцій, громадянського суспільства, бізнесу та науково-освітнього середовища. Пропоновані елементи протоколу включають криміналізацію широкого спектру екологічних злочинів, захист жертв і захисників довкілля, посилення міжнародної співпраці через навчання, обмін інформацією та технічну допомогу, а також створення загальної дефініції екологічних злочинів, яка охоплює дії, що завдають значної шкоди екосистемам або здоров'ю людини.

Особливу увагу приділено необхідності ефективного механізму огляду. Чинний механізм огляду UNTOC є неефективним через обмежену прозорість, низьку участь громадянського суспільства та повільний прогрес – лише два огляди було проведено з 2020 року. Новий протокол потребує окремого, амбітного механізму огляду, який забезпечить критичну оцінку, прозорість, активну участь громадянського суспільства, гнучкість для реагування на нові виклики, ефективне використання ресурсів і координацію в межах системи ООН. Такий механізм може не лише підвищити ефективність протоколу, а й пожвавити загальну імплементацію UNTOC.

У висновках документ наголошує, що, незважаючи на геополітичну фрагментацію та конкуруючі пріоритети, новий протокол може стати каталізатором для посилення глобальної відповіді на екологічні злочини. IEG має оцінити ефективність чинного правового поля, визначити цілі нового протоколу та усунути недоліки в його реалізації. Рекомендації включають посилення співпраці в рамках існуючих угод, покращення правоохоронної та судової співпраці, боротьбу з корупцією та незаконними фінансовими потоками, розширення досліджень та обміну інформацією, а також активне залучення громадянського суспільства, корінних громад і захисників довкілля.

Висновки:

- **Створення нового протоколу до UNTOC:** Розробити новий протокол до UNTOC, який криміналізує широкий спектр екологічних злочинів, включаючи незаконний видобуток, торгівлю та утилізацію, з чіткою дефініцією, що охоплює дії, які завдають значної шкоди екосистемам або здоров'ю людини. Протокол має бути гнучким, щоб адаптуватися до нових ринків та викликів.
- **Посилення міжнародної співпраці:** Гармонізувати законодавство для полегшення міжнародної співпраці, спрощуючи вимоги для екстрадиції та взаємної правової допомоги. Створити мережі для обміну інформацією та провести тренінги для суддів і правоохоронців щодо використання UNTOC.
- **Залучення громадянського суспільства та захист прав:** Забезпечити активну участь корінних громад і захисників довкілля у розробці та реалізації протоколу. Створити механізми захисту для жертв і свідків екологічних злочинів, гарантуючи їхні права та компенсацію.
- **Боротьба з корупцією та залучення приватного сектору:** Розробити антикорупційні заходи, включаючи прозорість фінансових потоків і розкриття бенефіціарної власності. Залучити технологічні компанії до боротьби з онлайн-торгівлею незаконними товарами та посилити відповідальність за корпоративні злочини.

Як іноземні шахраї використовують американські банки для обману громадян: Механізми, прогалини та наслідки [13]

Стаття, опублікована ProPublica за авторством Цезаря Подкула, розкриває масштабну проблему використання американських банківських установ для здійснення шахрайських схем, зокрема так званих «pig-butchering» афер (спосіб шахрайства, що передбачає встановлення довіри з жертвою перед виманюванням грошей), які проводяться переважно азійськими злочинними синдикатами. Ці схеми, що щорічно призводять до втрат на суму приблизно 4 мільярди доларів, базуються на складному процесі відмивання грошей, отриманих шахрайським шляхом, через банківські рахунки в США з подальшим їх переведенням у криптовалюту для виведення за кордон. Стаття висвітлює як конкретні випадки шахрайства, так і системні проблеми в банківській системі, які дозволяють злочинцям безперешкодно діяти.

Стаття розпочинається з історії Брайана Малоні молодшого, власника сімейного бізнесу Middlesex Truck and Coach у Бостоні, який несподівано виявив, що його компанію звинуватили у причетності до шахрайської схеми на суму 333,565 доларів. Жертва з Нью-Джерсі переказала ці кошти на рахунок у Chase, який, як виявилося, був відкритий шахраями від імені компанії Малоні без його відома. Малоні, який не мав жодного відношення до цього рахунку і навіть не був клієнтом Chase, зіткнувся з позовом від жертви, яка намагалася повернути свої гроші. Цей випадок ілюструє, як шахраї використовують назви легітимних бізнесів як прикриття для створення фіктивних банківських рахунків, через які проходять кошти жертв. Перевірка банку показала, що невідома особа відкрила рахунок онлайн, не надавши жодних документів для підтвердження особи чи зв'язку з його компанією, що вказує на серйозні прогалини в банківських процедурах перевірки клієнтів.

Цей інцидент є лише частиною глобальної проблеми, яка охоплює банківську систему США. Стаття детально описує механізми, за допомогою яких шахраї використовують американські банки для відмивання грошей. Зокрема, на платформах на кшталт Telegram діють китайськомовні канали, де пропонуються в оренду банківські рахунки в американських банках, таких як PNC, Chase, Citi та Bank of America. Ці рахунки рекламуються як «автомобілі» або «флоти» – сленгові терміни, які в китайському кримінальному жаргоні позначають інструменти для відмивання грошей. Одне з таких оголошень, яке згодом було видалене, обіцяло можливість фізичного доступу до банків для здійснення переказів, що робить такі рахунки особливо привабливими для шахраїв. Ці пропозиції дозволяють злочинцям швидко отримувати доступ до банківської інфраструктури США, обходячи традиційні перевірки.

Одним із ключових прикладів системних недоліків є випадок із Bank of America, де, за даними прокурорів, банк дозволив відкрити сотні рахунків без належної верифікації. Зокрема, 176 клієнтів вказали одну й ту саму адресу – невеликий будинок, що явно не могло відповідати реальності. Це свідчить про серйозні порушення в процедурах «знай свого клієнта» (Know Your Customer, KYC) та протидії відмиванню грошей (Anti-Money Laundering, AML). Стаття також звертає увагу на слабкість законодавчого регулювання в США: Закон про банківську таємницю (Bank Secrecy Act) вимагає від банків знати своїх клієнтів і повідомляти про підозрілі транзакції,

[13] https://www.propublica.org/article/pig-butchering-scam-cybercrime-us-banks-money-laundering

але не встановлює чітких стандартів ефективності таких програм. Це дає банкам значну свободу в обсязі перевірок, і багато з них уникають ретельного моніторингу, оскільки це пов'язано з додатковими витратами та сповільненням бізнес-процесів.

Стаття також висвітлює міжнародний масштаб проблеми. Значна частина шахрайських операцій координується з Сіануквіля, Камбоджа, де розташовані комплекси, що слугують базами для злочинних синдикатів. Китайські працівники, які беруть участь у цих схемах, використовують Telegram для координації банківських рахунків, отримуючи комісії за посередництво. Навіть відома камбоджійська фінансова компанія Huione Group, за даними Міністерства фінансів США, сприяє таким операціям через свої онлайн-ринки, хоча стверджує, що працює над запобіганням зловживанням. Гроші, отримані від жертв, часто переводяться в криптовалюту, що дозволяє шахраям швидко виводити їх за кордон, зокрема через офшорні рахунки, наприклад, у Багамах.

Стаття наводить приклад особи на ім'я Чжу, яка відігравала ключову роль у відмиванні грошей. Упродовж одного тижня в листопаді 2022 року Чжу отримав шість переказів на загальну суму майже 1 мільйон доларів, які потім консолідував і перевів на рахунок у Багамах, контрольований іншою особою, ймовірно, пов'язаною зі злочинним синдикатом. Дані від аналітичної компанії Crystal Intelligence показують, що криптогаманець, пов'язаний із цією схемою, обробив транзакції на суму 41 мільйон доларів між квітнем 2021 та квітнем 2024 року. Чжу був заарештований у березні 2023 року за звинуваченням у банківському шахрайстві, але його виправдали, оскільки захист стверджував, що він не знав про злочинне використання рахунків. Проте згодом його знову звинуватили у відмиванні грошей, і на момент написання статті він вважається втікачем.

Висновки:

- **Регуляторним органам США необхідно встановити чіткі стандарти ефективності** для програм KYC та AML, щоб змусити банки проводити ретельнішу перевірку клієнтів і моніторинг транзакцій у реальному часі.
- **США та країни, такі як Камбоджа, повинні співпрацювати** для закриття шахрайських центрів і блокування платформ, таких як Telegram, які використовуються для реклами нелегальних послуг банківських рахунків.
- **Банки та уряд мають інвестувати в освітні кампанії,** щоб навчити громадян розпізнавати афери та уникати переказів на невідомі рахунки.
- **Потрібно розробити механізми, які полегшують жертвам шахрайства притягнення банків до відповідальності** за недбалість, наприклад, через спрощення судових процедур або введення штрафів за порушення AML.

Інший приклад стосується жертви на ім'я Кевін, який втратив значні суми через такого роду аферу. Після втрати сина від передозування фентанілом Кевін перебував у стані емоційної вразливості, що зробило його легкою мішенню для шахраїв. Він здійснив кілька переказів на суму 344,000 доларів на різні рахунки, зокрема в Chase та Cathay Bank, сподіваючись розблокувати неіснуючий прибуток у 4 мільйони доларів. Незважаючи на спроби Кевіна скасувати перекази через свій банк TD, Chase не відреагував на запити, а зворотні перекази виявилися неможливими через політику банків. Лише один раз банк PNC зупинив підозрілий переказ, але це не врятувало Кевіна від подальших втрат.

Жертви шахрайства починають подавати позови проти банків, звинувачуючи їх у недбалості щодо виконання вимог KYC та AML. Наприклад, житель Каліфорнії, який втратив майже 1 мільйон доларів, подав позов проти DBS та інших банків, а професор із Айови, що втратив 200,000 доларів, позивався до Hang Seng Bank у Гонконзі. Проте такі позови рідко бувають успішними через складність доведення, що банки знали чи мали знати про шахрайство. Водночас банки визнають масштаб проблеми: за даними опитування, проведеного Wells Fargo, майже третина

американців стикалися з шахрайством або кіберзлочинністю. Президент Американської банківської асоціації Роб Ніколс наголосив, що банки роблять більше за інші галузі для захисту клієнтів, але визнав, що шахрайство залишається значним тягарем для суспільства.

На міжнародному рівні інші країни вживають більше рішучих заходів. Наприклад, у Сполученому Королівстві з жовтня 2023 року банки зобов'язані відшкодовувати жертвам шахрайства до 415,000 фунтів (приблизно 520,000 доларів) за транзакцію, навіть якщо клієнт сам санкціонував переказ. Австралія також розробляє подібні ініціативи. У США ж банки поки що покладаються на добровільні ініціативи, такі як створення програм протидії шахрайству, але брак чітких регуляторних вимог гальмує прогрес.

Інші новини

Розкіш і злочини: як молодий росіянин використовував нерухомість для відмивання коштів [14]

Стаття, опублікована Compliance Correlated за авторством Рашель Волкотт, детально висвітлює справу Семена Куксова, молодого росіянина, який очолював організовану злочинну групу, що займалася відмиванням значних сум грошей через операції з розкішною нерухомістю у Сполученому Королівстві. Семен, син надзвичайно багатого російського бізнесмена Володимира Куксова, використав своє привілейоване походження, сімейні зв'язки та доступ до значних ресурсів для створення складної схеми, яка дозволяла відмивати готівку, отриману злочинним шляхом. У статті розкриваються подробиці діяльності злочинної мережі, судового процесу, а також спроби захисту пом'якшити вирок, посилаючись на медичні діагнози, зокрема ADHD, аутизм та інші психологічні й фізіологічні стани.

Семен Куксов разом із партнером Андрієм Дзекцером керував групою, до якої входило щонайменше дев'ять осіб, включаючи молодшого брата Семена, Олександра Куксова. Злочинна діяльність розпочалася в червні 2022 року і тривала до арешту Семена 27 вересня 2023 року. Група займалася збором і транспортуванням великих сум готівки по всій Англії, використовуючи для цього фургони Mercedes Vito. Операції охоплювали міста, такі як Олдхем і Ньюпорт Пагнелл, а також мали міжнародний характер, зокрема в Ірландії, де один із кур'єрів був затриманий із €50,000 у Дубліні. Інший кур'єр був спійманий із £188,154. Гроші відмивалися через орендовані об'єкти розкішної нерухомості, зокрема квартиру в Кенсінгтоні вартістю £1 млн і Collingwood House у Лондоні, які слугували "рахунковими центрами". Під час обшуків у Collingwood House правоохоронці вилучили £887,029, сейф і машини для підрахунку грошей, що свідчить про масштаб і організацію операції.

У суді Семен Куксов визнав себе винним за двома пунктами обвинувачення у відмиванні грошей на суми £1,923,040 та €188,950. Його захист, очолюваний відомим адвокатом Кіраном Воганом, намагався зменшити вирок, акцентуючи на медичних діагнозах. Адвокат стверджував, що Семен страждає на ADHD, аутизм, пухлину мозку та кісти шишкоподібної залози, які нібито потребують постійного медичного нагляду і вплинули на його поведінку. Воган описав злочинну діяльність Куксова як "еволюційний" шлях, що почався з амфетамінової залежності, перейшов у азартні ігри з високими ставками, пережив передозування і завершився відмиванням грошей.

[14] https://www.compliancecorylated.com/news/wealthy-gen-z-russian-laundered-money-in-luxury-properties-claimed-adhd-caused-offending/

Захист також намагався представити Семена як жертву ізоляції в інтернаті та суворого виховання батьком, якого адвокат характеризував як "сильного дисциплінара". Проте суд відхилив ці аргументи, наголосивши, що ADHD не є "злочинним геном" і не призводить до втрати морального компасу. Хоча точний термін ув'язнення не уточнюється, згадується, що вирок було скорочено з початкових семи з половиною років після врахування визнання провини.

Значну роль у справі відіграла сім'я Куксова. Батько Семена, Володимир Куксов, є головою ради директорів російської компанії AKROS, яка співпрацює з підсанкційними компаніями, такими як "Лукойл" і "Газпром". Володимир володіє контрольним пакетом акцій AKROS через кіпрську компанію Vienoy Limited, але, за даними слідства, не був причетний до злочинної діяльності сина. Незважаючи на це, він надавав Семену значну підтримку, зокрема був присутній на судовому слуханні разом із матір'ю Семена та дядьком із Канади. Семен також виступав директором кількох компаній у Сполученому Королівстві та Росії, де кінцевим бенефіціаром був його батько, зокрема Collingwood House Investment Limited, яка володіла однойменною нерухомістю в Лондоні. У 2018 році Семен і Володимир були помічені разом на морській регаті у Сполученому Королівстві, спонсорованій AKROS, а в 2022 році обоє отримали британські паспорти за програмою "золотої візи", що підкреслює їхні фінансові можливості та зв'язки.

Молодший брат Семена, Олександр Куксов, також був залучений до операції, виконуючи вказівки Дзекцера щодо збору та доставки готівки. Під час арешту 19 жовтня 2022 року в нього вилучили £155,650 у квартирі в Кенсінгтоні. Однак не уточнюється, чи був Олександр офіційно звинувачений або чи проходив судовий процес. На 9 липня 2023 року він перебував на свободі та відвідав Дублін, щоб дізнатися про долю іншого заарештованого спільника. Сім'я Куксова активно підтримувала Семена під час судового процесу, найнявши адвоката Амаю (Джабу) зі Stokoe Partnership Solicitors у Лондоні, який представляв його інтереси під час арештів кур'єрів. Крім того, сім'я замовила психіатричну експертизу у доктора Алі Аяза, який діагностував у Семена ADHD та аутизм, хоча ці висновки не вплинули на рішення суду.

Стаття також звертає увагу на ширші проблеми, пов'язані зі справою. Операція Куксова мала транскордонний характер, що вказує на необхідність посилення міжнародної співпраці між правоохоронними органами Сполученого Королівства, Ірландії та інших країн. Використання розкішної нерухомості як інструменту для відмивання грошей підкреслює вразливість цього сектору, що вимагає від регуляторних органів посилення перевірок походження коштів і прозорості бенефіціарної власності. Спроба захисту використати медичні діагнози для пом'якшення вироку виявилася невдалою, що може вплинути на майбутні судові стратегії в подібних справах. Крім того, програма "золотих віз", яка дозволила сім'ї Куксових отримати британське громадянство, викликає питання щодо ризиків відмивання грошей через подібні схеми, особливо для осіб, пов'язаних із підсанкційними структурами.

Темні ринки Telegram: Як конкуренти заповнюють нішу Huione Guarantee [15]

Стаття від Elliptic, присвячена діяльності темних ринків у месенджері Telegram після закриття платформи Huione Guarantee. Документ висвітлює складну екосистему нелегальних ринків, що діють переважно в Південно-Східній Азії та Китаї, їхню роль у глобальній системі шахрайства, а також

[15] https://www.elliptic.co/blog/telegram-dark-markets-expand-to-fill-the-gap-left-by-huione-guarantee

пов’язані з ними виклики, такі як торгівля вкраденими даними, відмивання грошей і шахрайські схеми.

Стаття розпочинається з опису впливу закриття Huione Guarantee, яка була однією з провідних платформ у сфері нелегальних онлайн-ринків. Ця подія, що сталася навесні 2025 року, спричинила значний резонанс у середовищі шахраїв, брокерів вкрадених даних і осіб, що займаються відмиванням грошей, які активно використовували цю платформу для своїх операцій. Закриття Huione Guarantee описується як "шокові хвилі" для екосистеми темних ринків, що підкреслює її центральну роль у підтримці злочинної діяльності. Однак замість припинення таких операцій, нішу, що звільнилася, швидко заповнили інші Telegram-канали та ринки, які продовжують процвітати завдяки анонімності та доступності месенджера.

Особлива увага приділяється діяльності таких платформ, як Tudou Guarantee, яка після закриття Huione Guarantee значно розширила свою аудиторію. Згідно з даними, кількість користувачів Tudou Guarantee подвоїлася, а обсяги криптовалютних надходжень досягли рівня, порівнянного з тими, що раніше спостерігалися на Huione Guarantee. Багато торговців, які раніше працювали на Huione Guarantee, перейшли на Tudou, пропонуючи аналогічні послуги: продаж вкрадених даних, інструменти для шахрайства (зокрема для схем так званого "pig butchering" – обману, що передбачає встановлення довіри з жертвою перед виманюванням грошей), а також послуги з відмивання грошей. Цікаво, що Huione Guarantee мала 30% частку в Tudou Guarantee, придбавши її в грудні 2024 року, що вказує на тісний зв’язок між цими платформами та можливу координацію їхньої діяльності.

Документ також підкреслює використання криптовалют, зокрема стейблкойну USDT (Tether), як основного інструменту для транзакцій на цих ринках. Криптовалюти забезпечують анонімність і ускладнюють відстеження фінансових потоків, що робить їх привабливими для злочинців. Elliptic, яка спеціалізується на аналізі блокчейн-транзакцій, відстежує понад 30 активних Telegram-ринків, що вказує на масштабність проблеми. У тексті згадується, що екосистема темних ринків є складною мережею, яка включає не лише справжні платформи, але й численні шахрайські ринки, що обманюють навіть своїх клієнтів, додаючи додатковий рівень складності для правоохоронних органів.

Щодо географічного аспекту, стаття акцентує увагу на Південно-Східній Азії та Китаї як основних регіонах, де зосереджена діяльність цих ринків. Це пов’язано з відносною слабкістю регуляторних механізмів у цих регіонах, а також із великою кількістю технологічно підкованих злочинців, які використовують Telegram для координації своєї діяльності. Звіт зазначає, що серед товарів і послуг, які пропонуються на таких ринках, є вкрадені дані для цільового шахрайства, інструменти для відмивання грошей, а також інші незаконні пропозиції, включаючи проституцію.

Одним із ключових висновків документа є необхідність ширшого та систематичного видалення подібних ринків із Telegram. Закриття однієї платформи, як Huione Guarantee, виявилося недостатнім для припинення діяльності екосистеми, оскільки конкуренти швидко адаптуються та заповнюють прогалину. Це вказує на потребу в скоординованих діях між технологічними платформами, правоохоронними органами та регуляторами для боротьби з цією проблемою. Крім того, необхідно підвищувати обізнаність про загрози, які становлять темні ринки, через поширення інформації в соціальних мережах та інших каналах.

Ваша думка важлива!

1. Які кроки мають зробити українські регулятори для усунення прогалин між технічною складністю криптоактивів та обмеженістю традиційних інструментів KYC?
2. Наскільки готові СПФМ в Україні до активного використання інструментів блокчейн-аналітики? Які перепони ви бачите на цьому шляху?
3. Які механізми нагляду за діяльністю професійних посередників (зокрема, адвокатів, бухгалтерів, аудиторів, суб'єктів, що надають послуги зі створення або управління юридичними особами) можуть бути ефективно імплементовані в українській юрисдикції з урахуванням міжнародної практики (зокрема стратегії OPBAS та підходів FATF)?
4. Які галузі в Україні (енергетика, видобування, інфраструктура) мають найвищі ризики корупції у контексті екологічних злочинів і відмивання коштів?
5. Які механізми міжнародної співпраці Україна могла б використати для посилення боротьби з транскордонними екологічними злочинами, такими як незаконний експорт бурштину чи відходів?
6. Чи достатньо ефективними є нинішні механізми перевірки походження коштів в Україні для виявлення транскордонних злочинних схем, і які зміни необхідні для їх удосконалення?
7. Чи повинна Україна запровадити власну рамку нагляду за критичними ІКТ-постачальниками у фінансовому секторі за зразком DORA, і які ризики та переваги це матиме для кіберстійкості державних і приватних фінансових установ?
8. Як забезпечити баланс між свободою приватної власності та вимогами негайного замороження активів у рамках ЦФС — чи існує ризик зловживань або неправомірного блокування активів?

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-2025-30

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

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