ДЕРЖАВНА СЛУЖБА ФІНАНСОВОГО МОНІТОРИНГУ УКРАЇНИ

THE STATE FINANCIAL MONITORING SERVICE OF UKRAINE

Україна

Серійний номер: ДСФМУ-ДК-2024-037
Грудень 2024

Методологічний Бюлетень

Мета

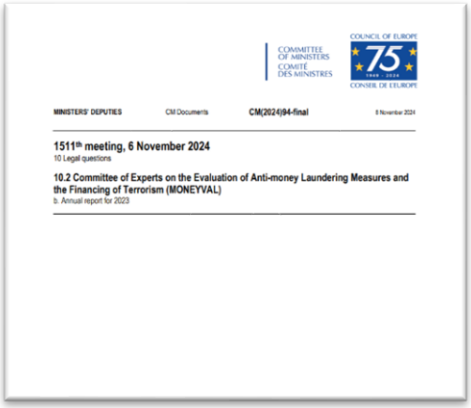
Методологічний Бюлетень видається Держфінмоніторингом на регулярній основі починаючи з квітня 2024 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для суб'єктів первинного фінансового моніторингу (СПФМ), регуляторів та правоохоронних органів.

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Річний звіт MONEYVAL[1]


COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES
COUNCIL OF EUROPE
75
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES CM Documents CM(2024)94-final

1511th meeting, 6 November 2024
10 Legal questions

10.2 Committee of Experts on the Evaluation of Anti-money Laundering Measures and the Financing of Terrorism (MONEYVAL)
b. Annual report for 2023

Річний звіт MONEYVAL підсумовує досягнення та виклики в оцінюванні й вдосконаленні систем ПВК/ФТ/ФР у 35 країнах-учасницях організації. У звіті наголошується, що, попри суттєві успіхи у розумінні ризиків ПВК/ФТ/ФР, міжнародному співробітництві та використанні фінансової розвідки, залишаються значні проблеми, пов'язані з недостатнім наглядом за приватним сектором, прозорістю юридичних осіб та низьким рівнем конфіскацій і переслідувань за злочини, пов’язані з відмиванням коштів. Ці виклики значною мірою обумовлені недостатньою ефективністю регуляторних і правозастосовних органів, а також слабким впровадженням ризик-орієнтованих підходів у наглядових процесах.

[1] https://rm.coe.int/0900001680b25d1c

У 2023 році MONEYVAL завершила чергові взаємні оцінки для Північної Македонії, Румунії, Азербайджану та Чорногорії, виявивши значні відмінності в ефективності реалізації стандартів FATF. У звітах підкреслено успіхи в міжнародній кооперації та розумінні ризиків, однак вказано на необхідність покращення розслідувань і конфіскацій активів, пов'язаних із відмиванням коштів, та впровадження санкційних механізмів. Наприклад, Північна Македонія продемонструвала позитивні результати у розумінні ризиків, але потребує посилення контролю за секторами, які наражаються на високий ризик, такими як нерухомість і казино. Румунія, у свою чергу, продемонструвала прогрес у міжнародній співпраці, але стикається з труднощами у впровадженні наглядових заходів для ВНУП і боротьбі з ризиками фінансування тероризму.

Окремо MONEYVAL підкреслює роль високопрофільних заходів, зокрема зустрічі міністрів у Варшаві у квітні 2023 року, де була ухвалена нова стратегія організації на 2023–2027 роки. Ця стратегія визначає основні напрями розвитку: посилення моніторингу, інтеграція інноваційних підходів до оцінювання ризиків та зміцнення співпраці з міжнародними організаціями, такими як FATF, і регіональними органами. MONEYVAL також розпочала підготовку до 6-го раунду оцінювання, розробивши нові правила, шаблони та методики, що дозволяють забезпечити більшу точність і ефективність оцінок.

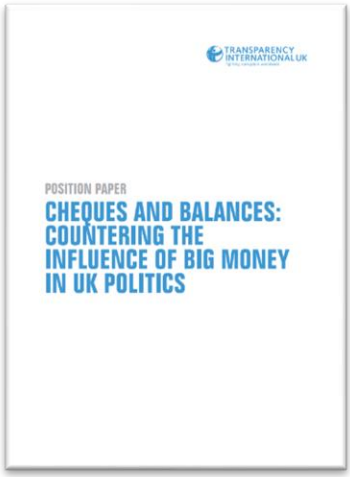
Висновки:

- **Пріоритети нового раунду оцінювання:** MONEYVAL готує 6-й раунд взаємних оцінок, запроваджуючи вдосконалені процедури для підвищення ефективності оцінювання систем ПВК/ФТ/ФР.
- **Необхідність посилення контролю:** Більшість країн-учасниць потребують вдосконалення у сферах нагляду за ВНУП, конфіскації активів та впровадження фінансових санкцій.
- **Успіхи в міжнародному співробітництві:** 80% країн демонструють високий рівень відповідності у міжнародному обміні інформацією, що підкреслює сильну позицію MONEYVAL у глобальній мережі.
- **Рекомендації щодо покращення:** Країни мають забезпечити прозорість юридичних осіб, підвищити рівень обізнаності про ризики серед суб'єктів фінансового моніторингу та зміцнити заходи із запобігання фінансуванню тероризму.

Звіт підкреслює важливість взаємодії з міжнародними партнерами, зокрема у сфері розробки стандартів FATF, що стосуються прозорості юридичних осіб, запобігання зловживанням у неприбутковому секторі та повернення кримінальних активів. MONEYVAL також ініціювала нові дослідження, спрямовані на аналіз впливу військових конфліктів на фінансові злочини та матеріальність ризиків у різних секторах.

Попри прогрес, MONEYVAL вказує на необхідність посилення ресурсної бази організації, залучення нових експертів і забезпечення ефективної співпраці між державним і приватним секторами. Звіт також акцентує увагу на важливості прозорості юридичних осіб, кращого використання фінансової розвідки та вдосконалення національних стратегій боротьби з відмиванням коштів і фінансуванням тероризму.

Стримування і противага: протидія впливу великих грошей у політиці Великобританії[2]



Документ підготовлений Transparency International UK, є ґрунтовним аналізом проблеми впливу великих фінансових пожертвувань на політичні процеси у Великій Британії. Автори описують ключові загрози для демократичної системи, спричинені надмірною залежністю політичних партій від великих донорів, непрозорістю походження коштів та недостатньою ефективністю чинних регуляторних механізмів. В основі проблеми лежить сучасна система фінансування політики, яка дозволяє приватним інтересам, часто з сумнівним походженням, отримувати доступ до процесів ухвалення політичних рішень.

Однією з основних проблем є те, що за останні роки у Великій Британії політичні пожертвування зросли до рекордних рівнів, причому значна їх частина надійшла від невідомих або сумнівних джерел. Наприклад, £115 мільйонів було пожертвувано від невідомих або непрозорих донорів, що приховує справжнє походження коштів. £48,2 мільйони пов’язані з донорами, яких звинувачують у купівлі привілейованого доступу або впливу, а £42 мільйони – від осіб, які причетні до корупції, шахрайства або відмивання коштів. Крім того, £38,6 мільйонів було надано через непрозорі об'єднання, які дозволяють приховувати джерела фінансування. У той час, як чинне законодавство спрямоване на запобігання корупції та зловживанням у політичному фінансуванні, воно неадекватно реагує на нові виклики.

Висновки:

- **Система регулювання фінансування політики у Великій Британії не справляється з викликами сучасності:** Залежність від великих донорів і відсутність жорстких правил створюють ризики корупції, політичного захоплення та втрати довіри виборців.
- **Необхідність обмежень пожертвувань:** Введення ліміту у £10,000 на рік може значно знизити вплив великих грошей на політичні процеси та підвищити довіру суспільства.
- **Прозорість як ключ до реформ:** Посилення правил звітності та прозорості дозволить відслідковувати походження коштів і зменшить ризики маніпуляцій.
- **Інституційні реформи:** Виборча комісія повинна отримати повноваження для ефективного контролю та застосування санкцій, що дозволить зробити політичні процеси більш підзвітними.

Однією з ключових загроз є залежність політичних партій від невеликої групи заможних донорів. У 2023 році 66% усіх пожертвувань було забезпечено лише 19 донорами, що суттєво підриває принцип рівності доступу до політичних процесів. Відсутність обмежень на максимальну суму пожертвувань посилює ризики політичного захоплення, коли фінансово потужні донори фактично отримують можливість впливати на державну політику. Ця проблема також ускладнюється практиками, пов’язаними з дарунками, гостинністю та фінансуванням закордонних поїздок політиків, які нерідко фінансуються іноземними урядами або приватними інтересами.

[2] https://www.transparency.org.uk/sites/default/files/pdf/publications/TI-UK%20MoneyInPolitics%20PositionPaper.pdf

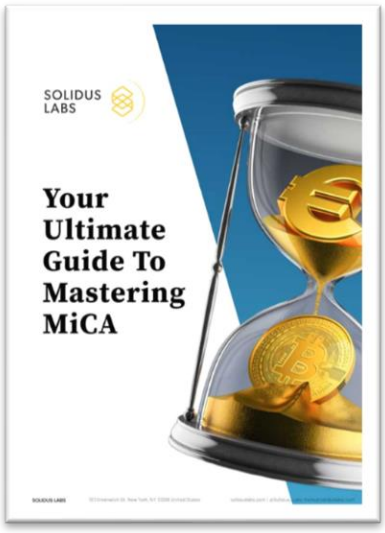
Чинна система регулювання має низку недоліків. Виборча комісія, яка відповідає за моніторинг і забезпечення прозорості політичних фінансів, обмежена у своїх повноваженнях і не може ефективно розслідувати кримінальні порушення. Збільшення витрат на виборчі кампанії та високі пороги для звітності про пожертвування створюють додаткові ризики непрозорості та зловживань. У 2023 році виборчі витрати політичних партій досягли рекордних £34,1 мільйонів, що створило безпрецедентний тиск на їхні фінанси та збільшило залежність від великих донорів. Такі тенденції посилюють громадське сприйняття того, що політика стає інструментом для забезпечення приватних інтересів.

Документ пропонує 15 реформ, які мають на меті змінити цю ситуацію. Серед ключових заходів пропонується встановити ліміт на річні пожертвування у розмірі £10,000, що дозволить зменшити вплив великих донорів на політичні рішення. Зниження порогів для звітності про пожертвування до £500 дозволить підвищити прозорість і запобігти приховуванню джерел фінансування. Автори також наполягають на зменшенні лімітів виборчих витрат, що знизить тиск на партії у залученні значних фінансових ресурсів. Пропонується законодавчо забезпечити незалежність Виборчої комісії, наділивши її правом розслідувати порушення та накладати санкції.

Крім того, документ акцентує на необхідності запровадження жорсткіших правил для прийняття дарунків, гостинності та фінансування закордонних поїздок політиків, щоб уникнути конфліктів інтересів і впливу зовнішніх гравців на політичні рішення. Пропонується запровадити політику "знай свого донора", яка вимагатиме від політичних партій перевіряти та публікувати інформацію про джерела своїх фінансів. Усі ці заходи спрямовані на те, щоб захистити демократію у Великій Британії, підвищити рівень довіри громадськості до політичних процесів і забезпечити доброчесність політичного фінансування.

Регулювання

Посібник із опанування MiCA[3]



Документ є детальним посібником для розуміння регуляторної бази Markets in Crypto-Assets (MiCA), яка найближчим часом набуде обов'язкової сили. MiCA стане першим всеосяжним регламентом для криптоактивів у межах Європейського Союзу, спрямованим на створення єдиного регуляторного середовища для ринку криптоактивів. Документ розкриває основні аспекти MiCA, що охоплюють ліцензування, прозорість, боротьбу зі зловживаннями на ринку та регулювання послуг, пов'язаних із криптоактивами.

MiCA буде застосовуватись безпосередньо у 27 країнах-членах ЄС, а також у Норвегії, Ліхтенштейні та Ісландії, що усуває необхідність у додатковому національному законодавстві. Її положення охоплюють як емітентів криптоактивів, так і постачальників послуг з криптоактивами (CASPs). Для CASPs передбачено обов'язкове ліцензування, що забезпечує їхню легальну діяльність у межах ЄС. Важливо, що ліцензія, отримана в одній державі-члені, надає право працювати в усіх інших країнах блоку завдяки механізму «паспортування».

[3] https://report.soliduslabs.com/hubfs/MiCA%20Factsheet%20-%20Solidus%20Labs.pdf

Одна з ключових дат — 30 грудня 2024 року, коли положення MiCA повністю набудуть чинності для всіх криптоактивів і CASPs. Для компаній, які вже діють під національними рамками регулювання, передбачено перехідний період до червня 2026 року. Однак для заходів щодо запобігання маніпуляціям на ринку та зловживанням цей період не діє, і всі CASPs повинні дотримуватися цих вимог із дня вступу MiCA в силу.

Документ також висвітлює суворі вимоги до CASPs, включаючи:

- Заборону маніпуляцій на ринку, інсайдерської торгівлі та незаконного розкриття внутрішньої інформації.
- Вимогу до реального моніторингу транзакцій, впровадження систем комплаєнсу та регулярної звітності до національних компетентних органів (NCA).
- Підготовку співробітників через регулярне навчання щодо виявлення і запобігання зловживанням.

Висновки:

- **Дедлайн для виконання ключових вимог:** CASPs повинні повністю відповідати заходам MiCA щодо запобігання маніпуляціям на ринку та зловживанням до 30 грудня 2024 року. Недотримання може призвести до серйозних санкцій і втрати ліцензії.
- **Єдина ліцензія для всього ЄС:** Ліцензування за MiCA дозволяє CASPs працювати у всіх державах-членах через механізм «паспортування», що значно спрощує доступ до ринку.
- **Прозорість і відповідальність:** CASPs повинні впровадити суворі системи моніторингу, регулярну звітність і дотримання вимог Travel Rule для забезпечення прозорості транзакцій.
- **Необхідність стратегічного планування:** Підготовка до MiCA включає аналіз прогалин у політиках компанії, адаптацію до вимог Digital Operational Resilience Act (DORA) та інтеграцію інструментів для моніторингу і комплаєнсу.

Особливу увагу приділено прозорості та підзвітності, зокрема необхідності CASPs надавати дані про всі транзакції, розкривати джерела коштів та забезпечувати жорстке дотримання правил, пов'язаних із Travel Rule. Регламент також акцентує на управлінні ризиками, зокрема пов'язаними з аутсорсингом і конфліктами інтересів, які можуть впливати на доброчесність послуг.

Для компаній, які планують отримати ліцензію MiCA, документ пропонує детальну дорожню карту підготовки: від аналізу прогалин і адаптації нових регуляторних вимог до стратегічного планування операцій і взаємодії з регуляторами.

Ефективне управління ризиками шахрайства та помилок: Аналіз впливу на державні фінанси Великобританії у 2023–2024 роках [4]

Документ, підготовлений Національним аудиторським офісом Великобританії (NAO), надає вичерпний аналіз масштабів, наслідків і методів протидії шахрайству та помилкам у державному секторі. Основна увага приділяється управлінню публічними фінансами, мінімізації втрат і підвищенню ефективності урядових програм.

Шахрайство та помилки становлять значну загрозу для державних ресурсів, завдаючи шкоди в розмірі від 55 до 81 мільярда фунтів стерлінгів лише у 2023–2024 фінансовому році. При

[4] https://www.nao.org.uk/wp-content/uploads/2024/11/fraud-overview-2023-24.pdf

цьому виявлено та відновлено лише малу частину цих коштів. Згідно з оцінками Public Sector Fraud Authority (PSFA), реальні втрати можуть бути ще більшими через недоліки в оцінці ризиків і вимірювання рівня шахрайства в окремих урядових програмах. Особливий вплив на збільшення випадків шахрайства мав період пандемії COVID-19, коли через спрощені процедури підтримки економіки та населення урядом було втрачено понад 10,5 мільярда фунтів.

Документ систематизує типи шахрайства, які включають зловживання грантовими коштами, шахрайство в державних закупівлях, ухилення від сплати податків, внутрішню корупцію та регуляторні зловживання. Однією з основних проблем, що розглядаються, є недостатня спроможність багатьох державних установ ефективно оцінювати та управляти ризиками шахрайства, що обмежує їхню здатність впроваджувати превентивні заходи.

Документ підкреслює важливість профілактики шахрайства як найефективнішого методу боротьби. Запобігання втратам не тільки економить ресурси, але й мінімізує репутаційні ризики для урядових органів. Використання циклічного підходу до управління ризиками шахрайства, запропонованого NAO, передбачає оцінку ризиків, розробку превентивних заходів, впровадження контролю, моніторинг і постійне вдосконалення систем. Зазначається, що більшість існуючих ініціатив зосереджені на виявленні шахрайства, а не на запобіганні, що потребує зміни підходів.

Висновки:

- Значна частина шахрайства залишається непоміченою. Підвищення якості аналізу даних та розширення оцінки ризиків в інших відомствах можуть значно знизити втрати.
- Профілактика є найбільш ефективним методом боротьби з шахрайством. Розробка попереджувальних механізмів, таких як аналітика ризиків та перевірка даних, дозволяє уникати втрат до їх виникнення.
- Необхідно розвивати професійну компетентність державних службовців, підвищувати прозорість діяльності та запроваджувати технологічні рішення.
- Урядові установи повинні впроваджувати постійний цикл управління ризиками шахрайства, включаючи розробку стратегій, оцінку контролю та моніторинг результатів.

Технологічні рішення займають важливе місце в боротьбі з шахрайством. Документ описує використання аналітики даних і штучного інтелекту для ідентифікації ризикових транзакцій та розробки превентивних заходів. Наприклад, інноваційні моделі аналізу даних, такі як автоматичне порівняння документів чи прогнозування ризикових випадків, вже демонструють ефективність у таких сферах, як соціальні виплати та податковий контроль. Проте бар'єрами для впровадження цих технологій є низька якість даних, нестача кадрів і нормативні обмеження щодо обміну інформацією між відомствами.

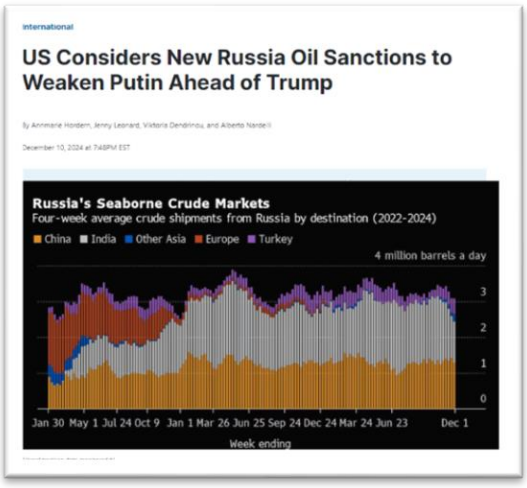
Крім того, значна увага приділяється податковій прогалині – різниці між теоретично належними до сплати та фактично отриманими податками, яка у 2023–2024 році становила майже 39,8 мільярда фунтів. Найбільший внесок у цю прогалину роблять малий бізнес і помилки через недотримання законодавства. HMRC впроваджує заходи для зменшення прогалин, але відзначається потреба в удосконаленні цифрових послуг і зміцненні податкових правил.

Документ також аналізує вплив шахрайства на соціальні виплати, зокрема на програми, що реалізуються Департаментом праці та пенсій (DWP). Рівень помилок і шахрайства в цих програмах залишається стабільно високим, що щорічно призводить до значних втрат бюджету. У зв'язку з цим рекомендується використовувати більш цілеспрямований підхід до перевірки ризикових випадків і покращення аналітичних моделей.

Загалом, документ наголошує на важливості створення сильної антикорупційної культури, підвищення професійної компетентності працівників державного сектору та забезпечення прозорості урядових операцій. Він пропонує структурований підхід до боротьби з шахрайством, що базується на використанні технологій, превентивних заходах і міжвідомчій співпраці для зниження втрат державних коштів.

Санкції

США вважають, що нові нафтові санкції проти Росії послаблять Путіна перед приходом Трампа[5]



Адміністрація президента Джо Байдена розглядає можливість запровадження нових, жорсткіших санкцій проти російської нафтової галузі з метою посилення тиску на Кремль у контексті війни в Україні. Ці заходи можуть бути впроваджені за кілька тижнів до інавгурації Дональда Трампа, запланованої на 20 січня 2025 року.

Хоча конкретні деталі санкцій ще не визначені, обговорюються обмеження, які можуть торкнутися певних аспектів експорту російської нафти. Раніше адміністрація Байдена утримувалася від таких кроків через побоювання щодо можливого зростання цін на енергоносії, особливо напередодні президентських виборів. Однак, з огляду на зниження цін на нафту та прогнози глобального надлишку в 2025 році, адміністрація тепер готова до більш агресивних дій.

Одним із можливих напрямків санкцій є обмеження діяльності так званого "тіньового флоту" танкерів, які Росія використовує для транспортування своєї нафти. Ці судна часто працюють

[5] https://www.bnnbloomberg.ca/business/international/2024/12/11/us-mulls-new-russia-oil-sanctions-to-weaken-putin-ahead-of-trump/?utm_source=newsletter.illicitedge.com&utm_medium=newsletter&utm_campaign=klarna-clocked-tehran-treasury-and-china-on-campus

з невідомими страховиками або власниками, що дозволяє Росії обходити існуючі обмеження. Європейський Союз також планує вжити подібних заходів щодо цього флоту до кінця року.

Ці ініціативи відображають прагнення адміністрації Байдена посилити економічний тиск на Росію перед передачею влади. Водночас, існують побоювання, що адміністрація Трампа може прагнути швидкого врегулювання конфлікту між Росією та Україною, що може вплинути на подальшу підтримку України з боку США.

Ці події відбуваються на тлі зусиль США щодо надання додаткової військової та фінансової підтримки Україні, а також обговорень щодо подальших кроків у сфері санкційної політики проти Росії.

Звіти окремих інституцій та експертів

Виклики та підходи до секторальної оцінки ризиків віртуальних активів[6]


RUSI

POLICY BRIEFS

Making a Sectoral Virtual Asset Risk Assessment: Challenges and Approaches

Alison Owen and Samantha Sheen

28 November 2024

Long Read

This policy brief, written for authorities responsible for the risk-assessment process, aims to offer insight on five key challenges that jurisdictions face with a sectoral virtual asset risk assessment, and suggests potential considerations for overcoming these barriers.

In June 2024, the Financial Action Task Force (FATF) – the international standard setter for anti-financial crime measures – reported that 29% of jurisdictions had yet to conduct a virtual asset (VA) risk assessment.[1] Furthermore, based on FATF's expectations, 75% of jurisdictions had not conducted adequate VA risk assessments.[2] In view of the centrality of the risk assessment process to the effective application of a risk-based approach – that is, the method of assessing risk exposure and tailoring mitigation controls – FATF's concerns should not be overlooked.

A sectoral VA risk assessment – evaluating sector-specific risks – is key for jurisdictions to understand their financial crime risk exposure. This information can be relayed to the private sector and supervisors so they can effectively implement a risk-based approach. If carried out in a robust manner, this process points the jurisdiction in a more informed direction and allows it to prioritise where and in what order vulnerabilities need to be addressed. However, as can be seen in FATF's finding, challenges persist for authorities responsible for leading the VA risk-assessment process.

To compound the challenge, criminal networks and state actors constantly adapt their approaches and exploit emerging avenues in the VA industry. This problem requires jurisdictions to update a sectoral VA risk assessment regularly to take account of new threats. By taking this initiative, jurisdictions can work towards a safer environment for the VA industry and consequently the whole financial system.

This policy brief, written for authorities responsible for the risk-assessment process, aims to offer insight on five key challenges that jurisdictions face with a sectoral VA risk assessment, and suggests potential considerations for overcoming these barriers. These problems, which have to do with development of the methodology, data collection and risk mitigation, are outlined, along with responses to each.

У червні 2024 року FATF повідомила, що 29% юрисдикцій ще не провели оцінку ризиків, пов'язаних з віртуальними активами (ВА), а 75% не здійснили адекватних оцінок таких ризиків. Це викликає занепокоєння, оскільки процес оцінки ризиків є центральним для ефективного застосування ризик-орієнтованого підходу. Секторальна оцінка ризиків ВА дозволяє юрисдикціям зрозуміти свій вплив на фінансові злочини та передати цю інформацію приватному сектору та наглядовим органам для ефективного впровадження ризик-орієнтованого підходу.

Матеріал RUSI визначає п'ять ключових викликів, з якими стикаються юрисдикції під час проведення секторальної оцінки ризиків ВА, та пропонує можливі шляхи їх подолання:

1. Плутанина щодо методології: Існує багато методологій для проведення секторальної оцінки ризиків ВА, опублікованих різними міжнародними інституціями, що може призвести до розгубленості при виборі найкращої. Юрисдикції можуть обрати одну з існуючих методологій або розробити власну, адаптовану до їхнього регуляторного середовища. Наприклад, Словацька Республіка адаптувала методологію Європейської Комісії, тоді як Люксембург зосередився лише на внутрішніх ризиках, аналізуючи загрози та вразливості сектора.
2. Обмеженість даних: Відсутність достатніх даних є значною перешкодою для оцінки ризиків. Юрисдикції можуть не враховувати широкий спектр доступної інформації та покладатися лише на звіти про підозрілу діяльність від приватного сектора. Однак існують інші корисні джерела, такі як скарги споживачів, дані від митних агентств, інформація від розвідувальних служб та аналітичні інструменти блокчейну.

[6] https://rusi.org/explore-our-research/publications/policy-briefs/making-sectoral-virtual-asset-risk-assessment-challenges-and-approaches

Наприклад, в Естонії фінансова розвідка оцінювала кількість запитів від іноземних правоохоронних органів, що допомогло виявити ризики, пов'язані з ВА.

3. Визначення ризиків для фінансових установ та ВНУП: ВА є додатковим засобом переміщення коштів, і, як і всі форми передачі вартості, вони можуть бути використані зловмисниками за відсутності належних засобів контролю. Оцінка ризиків повинна враховувати вплив ВА на фінансові установи та ВНУП. Наприклад, оцінка ризиків у Маврикії виявила, що відсутність правових обмежень дозволяє особам отримувати доступ до віртуальних платформ для ставок, що приймають платежі у ВА.
4. Недостатня співпраця між державними та приватними секторами: Ефективна оцінка ризиків вимагає тісної співпраці між державними органами та приватним сектором. Відсутність комунікації може призвести до неповного розуміння ризиків та неефективних заходів з їхнього пом'якшення.
5. Швидкий розвиток технологій та методів ухилення: Кримінальні мережі та державні актори постійно адаптують свої підходи та використовують нові можливості в індустрії ВА. Це вимагає регулярного оновлення секторальної оцінки ризиків ВА для врахування нових загроз.

Висновки:

- **Розробка гнучкої методології:** Юрисдикціям слід обрати або розробити методологію оцінки ризиків ВА, яка відповідає їхньому регуляторному середовищу та дозволяє ефективно ідентифікувати та пом'якшувати ризики.
- **Розширення джерел даних:** Використання різноманітних джерел інформації, включаючи скарги споживачів, дані митниці та аналітичні інструменти блокчейну, може покращити розуміння ризиків, пов'язаних з ВА.
- **Інтеграція ризиків ВА у загальну оцінку ризиків фінансових установ:** Фінансовим установам та ВНУП слід враховувати ризики, пов'язані з ВА, у своїх внутрішніх оцінках ризиків та впроваджувати відповідні заходи контролю.
- **Підвищення співпраці між державними та приватними секторами:** Сприяння обміну інформацією та співпраці між державними органами та приватним сектором є ключовим для ефективної оцінки та управління ризиками ВА.

Вплив Директиви про платіжні послуги[7]

Документ детально описує очікувані зміни та вплив, які внесе третя Директива про платіжні послуги (PSD3) і пов’язаний Регламент про платіжні послуги (PSR). Основна мета цих змін полягає в еволюції існуючої регуляторної бази PSD2 для вирішення сучасних викликів у сфері фінансових технологій, захисту споживачів, управління ризиками шахрайства та інтеграції новітніх технологій у платіжні системи.

PSD3 пропонує гармонізувати режими електронних грошей (EMI) та платіжних послуг (PSP), створюючи єдиний підхід до питань ліцензування, моніторингу транзакцій, розподілу відповідальності та підвищення прозорості. Нові вимоги включають:

- Зобов’язання EMI реєструвати всіх своїх дистриб’юторів.
- Посилення режиму захисту коштів, зокрема скорочення строків збереження.

[7] https://www.paperturn-view.com/?pid=ODg8847488&v=1.1

- Обов’язкове проведення аналізу впливу на захист даних для обміну інформацією між PSP, відповідно до GDPR.

Зміни також торкнуться підходів до управління ризиками шахрайства, таких як:

- Введення єдиних платформ обміну даними для виявлення підозрілих транзакцій.
- Вимоги до інформування споживачів про ризики, пов’язані із шахрайськими транзакціями.
- Посилення відповідальності PSP за підтвердження імені отримувача платежу та вирішення випадків шахрайства, пов’язаного з підробкою.

Особливу увагу приділено доступу третіх сторін (TPP) до платіжних систем. Всі PSP повинні будуть забезпечити інтерфейси, які дозволяють доступ TPP до рахунків користувачів, а також надавати споживачам інструменти управління їх згодами через так звані "інформаційні панелі".

Ще одна ключова зміна — введення обов’язкової сильної аутентифікації клієнтів (SCA), яка враховує доступність для осіб з обмеженими цифровими навичками або без доступу до смартфонів. Директива також змінює підходи до розрахунків, впроваджуючи механізми прозорості та спрощуючи регуляторну звітність для PSP.

Висновки:

- **Покращення управління ризиками шахрайства:** Введення централізованих платформ обміну даними та зобов’язання для PSP проводити аналізи впливу захисту даних значно підвищать безпеку платіжних систем.
- **Підвищення прозорості для користувачів:** Вимога створення інтерфейсів для управління згодами TPP забезпечить кращий контроль для споживачів над доступом до їх фінансової інформації.
- **Уніфікація вимог для EMI та PSP:** Новий підхід до захисту коштів і реєстрації дистриб’юторів створить стандартизовану базу для всіх суб’єктів платіжних послуг, що сприятиме зменшенню регуляторних прогалин.
- **Розширення відповідальності PSP:** Нові правила стосовно боротьби з шахрайством і підтвердження імені отримувача покладають значну частину відповідальності на платіжні установи, мотивуючи їх удосконалювати системи виявлення загроз.

Небезпека відеоігор[8]

Документ розглядає зростаючі ризики ВК у відеоігровій індустрії, яка стала багатомільярдним глобальним ринком (понад $196 мільярдів у 2023 році) завдяки технологічним інноваціям, онлайн-платформам і мікротранзакціям. Незважаючи на очевидну розважальну природу, ця

[8] https://www.canva.com/design/DAGMyTCozrg/d-bK2bfiVupugzm008haQw/view?utm_content=DAGMyTCozrg&utm_campaign=designshare&utm_medium=link&utm_source=editor

галузь все частіше привертає увагу злочинців, які використовують її для фінансових злочинів, зокрема ВК.

З розвитком моделі "pay-to-win" (де гравці купують ігрові предмети чи переваги за реальні гроші) відкрилися нові можливості для незаконної діяльності. Через анонімність і віртуальну природу транзакцій, злочинці можуть:

- Використовувати незаконні кошти для купівлі віртуальних активів (валюти, предметів).
- Переводити ці активи між рахунками, приховуючи походження коштів.
- Продавати активи на вторинних ринках, повертаючи "відмиті" гроші в реальну економіку.

Окремо аналізуються особливості використання популярних ігор (наприклад, Fortnite чи EA FC) і платформ, таких як GTA Role Play, де віртуальні валюти використовуються для легалізації коштів або навіть організації нелегальних транзакцій (торгівля наркотиками чи зброєю). Документ також звертає увагу на стрімінгові платформи, такі як Twitch, де донати та підписки можуть бути використані для ВК за допомогою викрадених кредитних карток або підроблених облікових записів.

Відсутність належного регулювання у відеоігровій сфері створює додаткові ризики, оскільки багато платформ працюють без суворого нагляду з боку фінансових регуляторів. Вторинні ринки, де здійснюється торгівля віртуальними активами, часто функціонують поза контролем розробників і служать ідеальним середовищем для приховування нелегальних коштів.

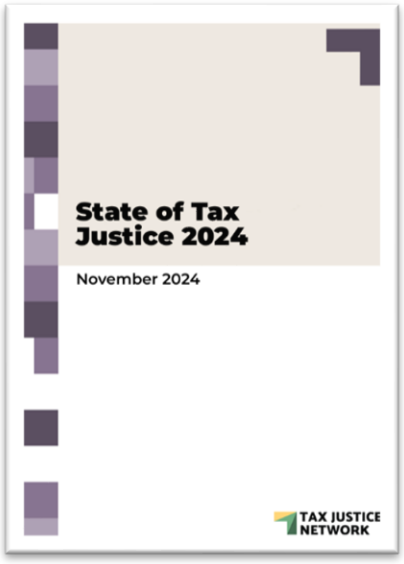
Особливу увагу приділено залученню молоді: більшість гравців віком до 35 років знайомі з онлайн-платформами, що робить їх потенційними "віртуальними мулами", які несвідомо беруть участь у ВК, створюючи багатоступеневі схеми обміну активів.

Документ закликає до більш активної співпраці регуляторів, розробників ігор і батьків, щоб запобігти фінансовим злочинам у цій сфері. Потрібно посилити контроль за вторинними ринками, удосконалити моніторинг транзакцій та підвищити обізнаність про ризики.

Висновки:

- **Регулювання індустрії:** Відсутність нагляду у відеоігровому секторі створює ідеальні умови для ВК. Необхідно впровадити стандарти фінансового моніторингу для платформ та вторинних ринків.
- **Зловживання мікротранзакціями:** Віртуальні валюти та активи використовуються для приховування незаконних коштів через багатоступеневі схеми. Рекомендовано обмежити можливості анонімних транзакцій.
- **Захист молоді:** Молоді гравці часто стають несвідомими учасниками схем ВК. Потрібно впровадити освітні програми, які підвищать обізнаність про ці ризики.
- **Технологічний моніторинг:** Необхідно впровадити алгоритми для виявлення підозрілих транзакцій і активностей, особливо на платформах із великим обігом віртуальних активів (як-от Twitch).

Глобальна битва за податкову справедливість: виклики, втрати та можливості згідно зі State of Tax Justice 2024 [9]



Звіт, опублікований Tax Justice Network, є фундаментальним аналізом глобальних викликів у сфері податкової справедливості. Він охоплює різноманітні аспекти податкових зловживань, включно з ухилянням від сплати корпоративних податків та офшорними схемами багатих фізичних осіб. Основний акцент зроблено на масштабах втрат, механізмах їх виникнення, ролі ключових держав та міжнародних інституцій, а також можливих шляхах розв'язання проблеми.

У центрі уваги звіту — значні глобальні втрати податкових надходжень, які становлять 492 мільярди доларів США на рік. З цієї суми 348 мільярдів доларів припадає на корпоративні податкові зловживання, що викликані штучним перенесенням прибутків міжнародних корпорацій до юрисдикцій із низьким оподаткуванням. Ще 145 мільярдів доларів втрачається через ухиляння від сплати податків багатими фізичними особами, які використовують офшорні рахунки для приховування своїх доходів. Ці втрати мають масштабний вплив на економіки країн, особливо тих, що розвиваються, де вони еквівалентні значній частці бюджетів охорони здоров'я та інших життєво важливих сфер.

Звіт критикує роль країн Організації економічного співробітництва та розвитку (ОЕСР) у формуванні міжнародного податкового порядку. Зокрема, незважаючи на впровадження ініціативи BEPS (Base Erosion and Profit Shifting) у 2015 році, результати її реалізації демонструють обмежену ефективність. ОЕСР не вдалося забезпечити суттєве зменшення масштабів податкових зловживань, а запропоновані нею рішення, такі як Глобальний мінімальний податок, виявилися недостатньо амбітними та вигідними для податкових гаваней. Це підкреслює необхідність переходу до інклюзивного та прозорого процесу під егідою ООН, який передбачає розробку міжнародної податкової конвенції.

Висновки:

- Введення глобального інструменту під егідою ООН дозволить забезпечити інклюзивність і прозорість у прийнятті рішень.
- Потрібно вдосконалити стандарти автоматичного обміну інформацією (CRS) та розширити їх охоплення для уникнення лазівок.
- Податки на надприбутки та багатство здатні компенсувати втрати бюджету та зменшити нерівність.
- Країни ОЕСР, які є основними джерелами втрат, повинні взяти на себе провідну роль у впровадженні ефективних міжнародних правил.

Особливу увагу звіт приділяє ролі конкретних країн у податкових зловживаннях. Велика Британія та її мережа заморських територій («друга імперія») разом із такими юрисдикціями, як Нідерланди, Люксембург і Швейцарія, складають так звану «вісь ухиляння від податків», яка відповідальна за третину глобальних втрат від корпоративного податкового зловживання. Водночас ці країни отримують непропорційну вигоду від залучення прибутків через низьке оподаткування, створюючи значний

[9] https://taxjustice.net/wp-content/uploads/2024/11/State-of-Tax-Justice-2024-English-Tax-Justice-Network.pdf

дисбаланс у глобальному податковому середовищі.

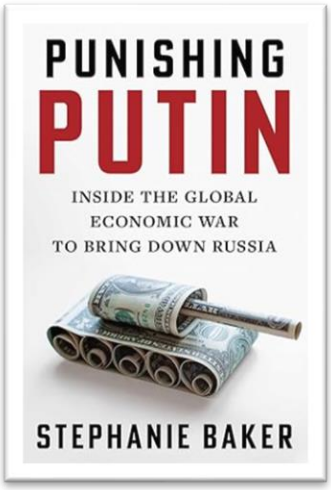
Ще одним ключовим аспектом звіту є аналіз ефективності стандарту CRS (Common Reporting Standard), який впроваджений для автоматичного обміну фінансовою інформацією. Хоча CRS зменшив масштаби офшорного ухиляння, його обмежена юрисдикційна та інструментальна охопленість залишають численні лазівки для тих, хто прагне приховати свої активи.

На цьому тлі звіт наголошує на необхідності впровадження податків на надприбутки та багатство як засобу зменшення нерівності та забезпечення додаткових бюджетних надходжень. Також пропонується створення глобального реєстру активів, що охоплює інформацію про реальних власників компаній і офшорних структур, для забезпечення прозорості та підвищення підзвітності.

Ключовою політичною рекомендацією є підтримка переговорів щодо міжнародної податкової конвенції під егідою ООН, які мають розпочатися у 2025 році. Ця ініціатива має потенціал створити глобальну податкову архітектуру, яка буде ефективною, інклюзивною та прозорою, зосереджуючись на інтересах країн, що зазнають найбільших втрат. Успішна реалізація цього проєкту дозволить зменшити глобальні дисбаланси, підвищити доходи державних бюджетів та сприяти досягненню соціальної справедливості.

Рекомендовані матеріали

Punishing putin[10]



"Punishing Putin" Стефані Бейкер — це авторитетне й ґрунтовне дослідження безпрецедентної економічної війни, розгорнутої США та їхніми європейськими союзниками проти Росії після її повномасштабного вторгнення в Україну 24 лютого 2022 року. Ця книга, написана досвідченою журналісткою з глибоким доступом до західних і російських джерел, розкриває причини, перебіг та наслідки цієї глобальної фінансової кампанії, яка не лише змінила баланс сил у світі, але й ризикувала спровокувати серйозну економічну рецесію.

Авторка описує, як Захід швидко мобілізував економічні інструменти, щоб нанести удар по російській економіці, яка колись входила до одинадцяти найбільших у світі, і послабити військову машину Путіна. Вона досліджує масштабні операції, починаючи з заморожування 300 мільярдів доларів золотовалютних резервів Росії, захоплення супер'яхт та накладання санкцій на олігархів, і закінчуючи маніпуляціями світовими цінами на нафту та блокуванням доступу Росії до військових технологій.

Бейкер відтворює атмосферу напружених переговорів у кулуарах Вашингтона, Лондона та Брюсселя, де ухвалювалися доленосні рішення. Вона показує, як створювалася ціла армія аналітиків, слідчих у сфері фінансових злочинів і міжнародних юристів, щоб ефективно застосовувати нову форму "економічного державного управління". Ці зусилля спрямовані на те, щоб обмежити доступ Росії до фінансів і стратегічних ресурсів, які могли б підтримувати її агресивну політику.

[10] https://www.amazon.com/Punishing-Putin-Inside-Global-Economic/dp/1668050587

Попри значні втрати для Росії, авторка не приховує, що санкції не досягли миттєвого ефекту, на який сподівалися західні лідери. Вона аналізує, як Москва адаптується до санкційного тиску, шукаючи нові шляхи обходу обмежень і використовуючи підтримку з боку держав, що не приєдналися до санкцій, як-от Китай і Індія. Це висвітлює складність глобальної санкційної політики і показує, що навіть наймасштабніші економічні заходи потребують широкої міжнародної підтримки для досягнення максимального ефекту.

Книга підкреслює ключовий парадокс сучасного конфлікту: хоч санкції спрямовані проти Росії, обмеження на передачу передових технологій Україні можуть мати не менш значний вплив на хід війни. Авторка звертає увагу на те, що саме технологічна перевага Заходу може стати вирішальним фактором у великих конфліктах тепер і в майбутньому.

"Punishing Putin" — це не лише аналіз сучасної санкційної стратегії, а й важливий внесок у розуміння глобальних змін у світовій економічній і політичній системі. Книга пропонує багатогранний погляд на те, як санкції впливають на глобальні альянси, сприяють розподілу світу на нові блоки інтересів і створюють нову еру "економічного державного управління", наслідки якої відчуватимуться десятиліттями.

Поради та найкращі практики щодо відповідності MiCA[11]

Подкаст "MiCA Masters", організований Solidus Labs, представив 22-й епізод, в якому ведуча спілкується з Еоїном Кернсом, Головою з питань комплаєнсу та відповідальним за звітність щодо відмивання коштів (MLRO) у MoonPay.

Тема епізоду: Основна увага приділена практичним підходам до впровадження регуляторних вимог згідно з Регламентом ЄС MiCA (Markets in Crypto-Assets), а також побудові ефективних комплаєнс-фреймворків у криптоіндустрії.

Ключові аспекти епізоду

1. *Підготовка до MiCA:*

Еоїн Кернс детально описує, як компанії можуть адаптувати свої бізнес-моделі до нових вимог MiCA, враховуючи регуляторний вплив на всі аспекти діяльності, від операцій до управління ризиками.

2. *Аутсорсинг та конфлікти інтересів:*

11 https://open.spotify.com/episode/22L4amjfHriHdCyvNmHPMj?si=b58b022472af438f&nd=1&dlsi=130f624471af4fde
https://podcasts.apple.com/us/podcast/mica-masters-tips-and-best-practices-for-mica-and/id1627530972?i=1000678421707

Особливу увагу приділено управлінню аутсорсингом і уникненню конфліктів інтересів у відповідності до нових нормативних вимог. Важливі інструменти включають чітке документування процедур і регулярні аудити.

3. *Виклики та можливості Travel Rule:*

Огляд правил FATF і EU Travel Rule, які вимагають збору та передачі інформації про відправників і отримувачів транзакцій. Еоїн пояснює, як компанії можуть інтегрувати ці вимоги у свої системи безпеки та моніторингу.

4. *Практичні поради для комплаєнс-офіцерів:*

В епізоді висвітлюються конкретні поради для комплаєнс-фахівців, щоб вони могли оперативно реагувати на зміни регуляторного ландшафту. Особливий акцент зроблено на використанні автоматизованих інструментів моніторингу та розвитку професійної мережі.

5. *Значення участі в галузевих об'єднаннях:*

Еоїн наголошує на важливості взаємодії з регуляторами та співпраці з колегами через індустріальні групи для обміну досвідом та впливу на формування регуляторної політики.

Значення для аудиторії

Епізод стане корисним для:

- Комплаєнс-фахівців: пропонує практичні рекомендації для щоденної роботи в умовах швидкоплинного регуляторного середовища.
- Бізнесу в криптоіндустрії: надає приклади побудови ефективних стратегій відповідності регуляторним вимогам.
- Ентузіастів криптовалют: допомагає зрозуміти складність регуляторного ландшафту в ЄС

Еволюція фінансування терористів-бойовиків: виклики та сучасні тренди 2014–2024 років [12]

12 листопада 2024 року на віртуальному заході, організованому Контр-терористичним виконавчим директоратом ООН (UNCTED) було представлено звіт "Trends Tracker: Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014–2024" та обговорено ключові зміни у фінансуванні діяльності іноземних терористичних бойовиків (ІТБ) за останнє десятиліття. Документ відображає еволюцію фінансових потоків, пов'язаних із операціями та логістикою ІТБ, та демонструє, як терористичні організації адаптуються до нових обставин і використовують різноманітні технології.

[12] https://www.un.org/securitycouncil/ctc/news/cted-holds-virtual-launch-event-%E2%80%9Ctrends-tracker-evolving-trends-financing-foreign-terrorist

Основним висновком звіту є те, що фінансові схеми ІТБ зазнали суттєвих змін: від простих методів, таких як готівкові перекази, до більш складних і технологічно вдосконалених підходів. Сучасні терористичні групи, зокрема після втрати територій ІДІЛ у 2019 році, дедалі більше покладаються на децентралізовані моделі фінансування. Географічні зрушення, такі як зміни у маршрутах, нові конфліктні зони та розширення регіональних фінансових хабів в Африці та Азії, відіграють вирішальну роль у трансформації цих схем. Це відображає багатовимірний характер загрози, яка більше не є лінійною, а охоплює широкий спектр способів залучення і використання коштів.

Технології стали важливим інструментом для обох сторін: терористи активно використовують криптовалюти для збору та переміщення коштів, тоді як правоохоронні органи використовують блокчейн-аналітику для відстеження фінансових потоків. Водночас традиційні методи, такі як фізичне транспортування готівки або неформальні системи передачі вартості, залишаються актуальними, часто використовуються паралельно з новими технологіями для максимізації ефективності і приховування фінансових слідів.

Звіт також звертає увагу на зміну характеру витрат ІТБ. Якщо раніше кошти переважно витрачалися на подорожі й основну логістику, то тепер їх використовують для створення нових мереж, хабарів, контрабанди, повернення та реінтеграції бойовиків, а також для підтримки зв'язку з тими, хто залишився у зонах конфліктів. Важливим аспектом стало зростання ролі жінок у фінансуванні та логістиці терористичних організацій. Цей феномен часто ігнорується в національних оцінках ризиків, що може призводити до неефективної протидії.

Успішні державні практики, представлені на заході, включають криміналізацію фінансування тероризму, що охоплює діяльність ІТБ, розробку механізмів заморожування активів, підвищення обізнаності серед населення про ризики фінансування тероризму та активну співпрацю з приватним сектором. Особливий акцент зроблено на міжвідомчій взаємодії та публічно-приватному партнерстві, що дозволяє більш ефективно відстежувати фінансові потоки та виявляти порушення.

Криптовалютний трилер: Як уряд США розкрив найбільше в історії Bitcoin пограбування [13]

Епізод подкасту Smithsonian Sidedoor досліджує одну з найбільших криптовалютних крадіжок в історії – злам біржі Bitfinex у 2016 році та подальшу роботу федеральних агентів США, що привела до повернення викрадених коштів у 2022 році. Це історія про технології, злочинність і методи розслідування в цифрову еру, яка виявила, що навіть, здавалося б, анонімні транзакції у криптовалюті можуть бути простежені.

Історія починається із викрадення понад $70 мільйонів у біткоїнах із криптовалютної біржі Bitfinex, яка базувалась у Гонконгу. Хакери перевели ці кошти до свого цифрового гаманця, адресу якого могла побачити уся світова спільнота завдяки прозорості блокчейну. Унікальна структура блокчейну, де кожна транзакція записується у публічний реєстр,

[13] https://www.si.edu/sidedoor/bitcoin-bank-heist

унеможливлювала швидке використання викрадених коштів, адже кожен рух криптовалют був видимим для аналітиків і зацікавлених сторін.

Злочинці зіткнулися з парадоксальною ситуацією: вони мали величезну суму, яка збільшувалася у вартості через зростання ціни біткоїна, але не могли витратити ці кошти без ризику викриття. Вони почали вживати складних заходів для відмивання грошей, зокрема розбивання суми на дрібніші частини, використання даркнет-маркетів, міксерів (сервісів, що "змішують" транзакції) і фальшивих акаунтів на криптобіржах. Проте кожна транзакція залишала цифровий слід.

Справу взявся розслідувати спеціальний агент Кріс Янчевскі із кіберпідрозділу IRS. Використовуючи аналітику блокчейну, він відстежував пересування викрадених коштів через складні схеми транзакцій. Розслідування було не лише технічно складним, а й креативним, адже вимагало розуміння не лише того, як пересувалися гроші, але й чому це робилося саме так.

Протягом кількох років команда федеральних агентів аналізувала дані і, врешті-решт, змогла пов’язати віртуальні гаманці із реальними людьми – подружжям Іллею Ліхтенштейном та Хезер Морган. Остання була відома своїми дивними витівками у соціальних мережах під псевдонімом Razzlekhan, що іронічно сприяло її викриттю. Детальні відео у соцмережах стали джерелом доказів, адже вони містили кадри, які підтверджували використання певних пристроїв та давали підказки про стиль життя підозрюваних.

У січні 2022 року агенти провели обшук у квартирі пари в Нью-Йорку, намагаючись знайти приватні ключі до криптовалютних гаманців. Після ретельного пошуку ключі були виявлені у хмарному сховищі. Це дозволило агенціям повернути вкрадені біткоїни загальною вартістю $4,5 мільярда – найбільшу суму, коли-небудь вилучену урядом США.

Цей випадок став поворотним моментом у боротьбі з криптозлочинами. Він продемонстрував, що навіть найскладніші схеми відмивання грошей залишають цифрові сліди, які можна простежити. Справа також розвіяла міф про абсолютну анонімність криптовалют, підкресливши важливість прозорості та належної перевірки (KYC/AML) у фінансових сервісах. Завдяки цьому розслідуванню криптозлочинці зрозуміли, що навіть найскладніші маніпуляції не є гарантією безкарності.

На завершення, ноутбук, за допомогою якого проводилося це розслідування, тепер став частиною експозиції в Національному музеї американської історії у Смітсонівському інституті. Він символізує перехід до нової ери боротьби із фінансовими злочинами у цифровому світі.

Інші новини

Стан нелегальної тютюнової промисловості у Канаді[14]

Незаконна торгівля тютюновими виробами в Канаді досягла масштабів, які перевищують обсяги легальних продажів у деяких провінціях. Це зростання пояснюється високими податками на тютюнову продукцію, недостатнім контролем з боку правоохоронних органів і

[14] https://nationalpost.com/news/canada/canadas-illegal-tobacco-industry-now-surpassing-legal-sales-in-parts-of-the-country-report

активною діяльністю організованих злочинних угруповань. Високі акцизи роблять легальні сигарети менш доступними для споживачів, що стимулює їх купувати дешевші нелегальні аналоги. Водночас, правоохоронним органам бракує ресурсів для боротьби з цією проблемою, а організовані злочинні мережі використовують нелегальну торгівлю для фінансування інших кримінальних операцій.

Поширення нелегального ринку тютюнових виробів призводить до значних економічних втрат для державного бюджету через недоотримані податкові надходження, зростання рівня злочинності, а також створює серйозні ризики для здоров'я населення, оскільки нелегальні сигарети часто не відповідають стандартам безпеки. Для подолання цієї проблеми необхідно переглянути податкову політику, зменшивши податковий тиск на тютюнову продукцію, посилити правозастосування шляхом збільшення фінансування правоохоронних органів і покращення координації між ними, а також організувати інформаційні кампанії, спрямовані на зменшення попиту на нелегальну продукцію. Лише спільні зусилля уряду, правоохоронців і громадськості дозволять ефективно боротися з незаконною торгівлею тютюном.

Злочин як послуга: нові виклики для фінансової безпеки у цифрову епоху [15]

Стаття аналізує зростаючу загрозу феномену "злочин як послуга" (Crime as a Service (CaaS)), який дедалі більше впливає на фінансові системи та безпеку суспільства. У тексті підкреслюється, що CaaS є новою моделлю злочинної діяльності, в якій технологічні інструменти та послуги надаються злочинцями через підпільні платформи, зокрема даркнет і месенджери, такі як Telegram. Ці інструменти дозволяють користувачам, які не мають глибоких технічних знань, здійснювати широкий спектр злочинів, зокрема шахрайство, відмивання коштів, фінансування тероризму та створення фіктивних компаній.

Одним із ключових аспектів є використання фальшивих документів, таких як рахунки за комунальні послуги, паспорти та водійські посвідчення, які створюються з високою точністю та пропонуються за надзвичайно низькими цінами. Наприклад, підроблений паспорт можна придбати за $12, а селфі для верифікації – за $15. Такі документи використовуються для обходу процедур KYC/AML, реєстрації фіктивних компаній або доступу до банківських послуг. Їх складно або навіть неможливо відрізнити від справжніх, що створює значні виклики для фінансових установ.

Документ також висвітлює функціонування платформ, які спеціалізуються на обході систем перевірки особистості. Наприклад, ProKYC пропонує інструменти, що дозволяють обходити відеоверифікацію з 100% успішністю, використовуючи технології штучного інтелекту та deep-fake. Ці інструменти значно знижують ефективність традиційних систем перевірки Bitfinex чи Binance.

[15] https://en.paperjam.lu/article/crime-as-a-service-a-threat-to

Ще однією загрозою є активне використання злочинцями "мулових" схем. Фінансові "мули" — це люди, які добровільно або через примус погоджуються надавати свої банківські рахунки для переказу незаконних коштів. У документі підкреслюється, що ці схеми використовуються для відмивання доходів, отриманих від кіберзлочинності, часто за допомогою криптовалют. Учасники цих схем можуть отримувати невеликі комісії, тоді як організатори створюють складні ланцюги транзакцій, які ускладнюють виявлення кінцевих бенефіціарів.

Висновки:

- Низька вартість і висока якість підроблених документів створюють серйозну загрозу системам верифікації особистості. Фінансові установи мають інвестувати у вдосконалені механізми перевірки, включаючи біометричні дані.
- Інструменти на кшталт ProKYC сприяють масовим зловживанням. Потрібно впроваджувати нові технології виявлення, такі як аналіз відеопотоків на наявність маніпуляцій.
- Для боротьби із цим явищем необхідно розробляти спільні ініціативи із запобіганням залучення вразливих осіб до таких схем.
- Рекомендовано посилити співпрацю між державними органами, фінансовими установами та технологічними компаніями для відстеження транзакцій, ідентифікації злочинців і закриття незаконних платформ.

Важливим аспектом документа є підкреслення необхідності боротьби з CaaS через впровадження новітніх технологій та посилення співпраці між державними і приватними структурами. Наприклад, пропонується використовувати технології для розпізнавання deep-fake, такі як FakeCatcher від Intel, а також проводити моніторинг даркнет-форумів і підозрілих платформ. Важливим інструментом протидії є блокчейн-аналітика, яка допомагає виявляти транзакції, пов’язані з незаконною діяльністю.

Окрему увагу приділено репутаційним і фінансовим ризикам для фінансових установ. У документі зазначається, що участь у відмиванні коштів, навіть ненавмисна, може призвести до втрати ліцензій, штрафів і пошкодження репутації. У підсумку автори акцентують на необхідності інвестувати в інноваційні рішення для забезпечення безпеки фінансових операцій та активізації міжнародної співпраці у протидії CaaS.

Для загального розвитку

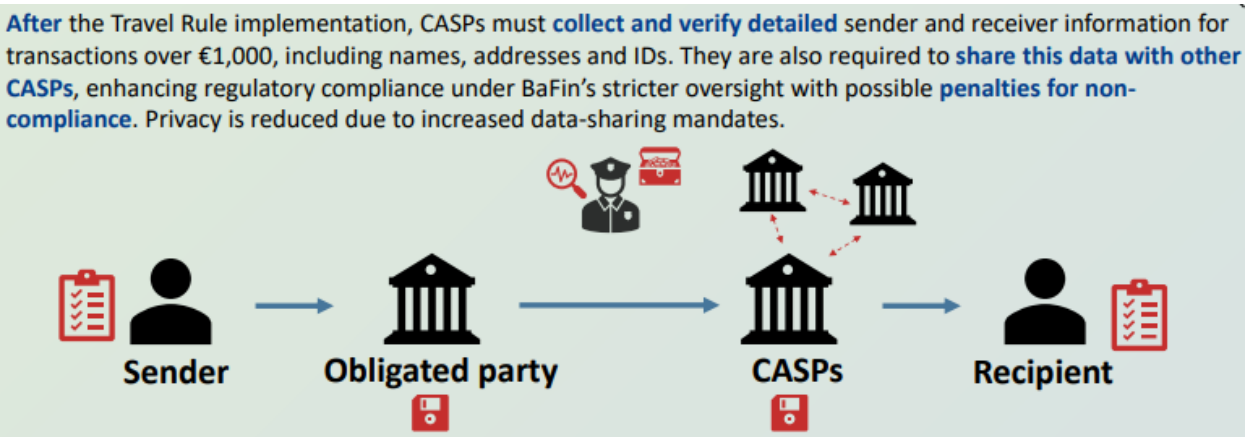
Практичні наслідки Travel Rule[16]

Документ аналізує вимоги, виклики та наслідки впровадження Travel Rule, яке було розроблено FATF для боротьби з ВК/ФТ. Спочатку це правило стосувалося традиційних фінансових транзакцій, але з 2019 року його дія була поширена на криптовалюти та постачальників послуг, пов’язаних з криптоактивами (CASPs), щоб зменшити ризики анонімності та децентралізації. У ЄС Travel Rule було стандартизовано через "Regulation (EU) 2023/1113", що набуде обов'язкової сили з 30 грудня 2024 року.

[16] https://media.licdn.com/dms/document/media/v2/D4D1FAQHZcMjOuJX1Kw/feedshare-document-pdf-analyzed/feedshare-document-pdf-analyzed/0/1731486572690?e=1735171200&v=beta&t=rvpgpmuu2rg7jPc8nn6RnqBZThquGNGcqaDZ3SXUv6s

Головна мета Travel Rule – підвищення прозорості криптовалютних транзакцій через обов'язкове збирання, зберігання та передачу інформації про відправників і отримувачів транзакцій. Це також сприяє зниженню ризиків злочинної діяльності та підвищенню рівня довіри до криптовалютного ринку. Проте, впровадження цього правила стикається з низкою викликів, серед яких технічна інтероперабельність між різними системами CASPs, забезпечення кібербезпеки й захисту персональних даних клієнтів відповідно до Регламенту із загального захисту даних (GDPR), а також значні витрати на впровадження необхідних технічних рішень.

Порівняння ситуації до і після впровадження Travel Rule показує значні зміни в регуляторних вимогах: від мінімального збору даних і обмеженого нагляду до обов'язкової ідентифікації та верифікації транзакцій на суму понад €1,000 з передачею цих даних між CASPs. Це знижує рівень конфіденційності транзакцій, але підвищує їхню прозорість і підзвітність.



Для ефективного дотримання нових вимог CASPs рекомендується адаптувати свої процеси, включаючи автоматизацію збору й передачі даних, посилення моніторингу транзакцій, забезпечення безпеки даних та навчання персоналу. Особливо важливим є готовність до дотримання регуляторних вимог до зазначеного дедлайну, оскільки недотримання може призвести до значних штрафів і репутаційних втрат. Travel Rule відіграє ключову роль у формуванні більш безпечного та прозорого криптовалютного середовища, сприяючи боротьбі з фінансовими злочинами.

Що таке токенізація

Токенізація — це процес перетворення прав на актив у цифровий токен на блокчейн. Ці токени представляють власність або доступ до активу та можуть включати будь-що від нерухомості та мистецтва до інтелектуальної власності та фінансових інструментів.

Токенізація змінює спосіб інвестування та володіння активами, перетворюючи предмети реального світу на цифрові токени в блокчейні. Це спрощує торгівлю, купівлю або продаж часток високоцінних активів, підвищуючи ліквідність і знижуючи транзакційні витрати. Токенізація - це не просто модне слово, і вона трансформує такі галузі, як нерухомість, предмети розкоші та фінансові ринки.

Процес токенізації починається з перетворення вартості активу в цифровий токен, який представляє частину цього активу. Потім ці токени надійно зберігаються в блокчейні, децентралізованому та прозорому реєстрі. Блокчейн гарантує, що записи про власність та транзакції є незмінними та доступними для всіх учасників, забезпечуючи безпечний та ефективний спосіб керування активами.

Наприклад, у токенізації нерухомості право власності на майно розбивається на цифрові частки. Замість того, щоб купувати цілу нерухомість, інвестори можуть придбати частки, дозволяючи зменшити мінімальні інвестиції та отримати доступ до цінних об'єктів, які раніше були недоступні. Ця трансформація відкриває ринок нерухомості для набагато ширшого кола інвесторів, від фізичних осіб до установ.

Популярні активи, що токенізуються:

- Нерухомість: за допомогою токенізації майно можна розділити на цифрові акції, що дозволить дрібним інвесторам володіти частиною дорогої нерухомості.
- Предмети розкоші: дорогоцінні метали, мистецтво та предмети колекціонування тепер можна токенізувати, що робить їх більш ліквідними та доступними для ширшої аудиторії.
- Фінансові активи: акції та облігації переходять на блокчейн, що робить торгівлю швидшою та прозорішою.

Токенізація відкриває нові інвестиційні можливості, роблячи ринки доступнішими для всіх, а не лише для багатих чи інституційних інвесторів. Оскільки ця тенденція зростає, розуміння юридичних аспектів є ключовим для орієнтування в цьому середовищі, що розвивається.

Контактуйте щодо цього документу з Держфінмоніторингом:

- **Email:** bulletin@fiu.gov.ua
- **Поштова адреса:** Державна служба фінансового моніторингу України, Україна, 04050 м. Київ, вул. Білоруська, 24
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № ДСФМУ-ДК-2024-037

Бюллетень є волонтерською розробкою методологічної команди Державної служби фінансового моніторингу України відповідно до пункту 18 частини 2 статті 25 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

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