Методологічний бюлетень

Серійний номер: МінФін-AML-2025-18

Травень 2025

“Маленькі справи, зроблені наполегливо, сильніші за великі задуми без дій”

Пітер Маршалл

Мета

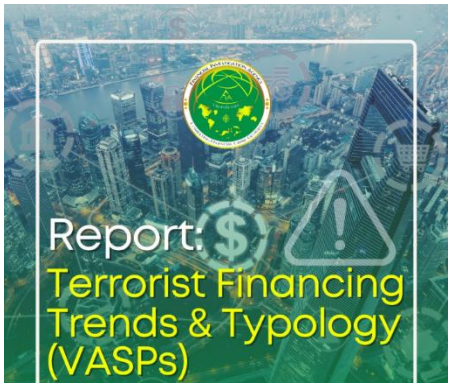
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено 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, зокрема навчання та координації дій між різними установами для забезпечення належної співпраці та обміну інформацією.

Звіти міжнародних організацій та окремих юрисдикцій

Звіт про виявлені типології фінансування тероризму [1]



Документ, підготовлений Агентством фінансових розслідувань Британських Віргінських Островів (BVI FIA), присвячений аналізу типологій фінансування тероризму (ФТ) з використанням віртуальних активів та ролі місцевих постачальників послуг у сфері віртуальних активів (VASPs) у період з січня по серпень 2024 року. Головна увага приділяється способам, якими терористичні мережі використовують інфраструктуру BVI VASPs для міжнародного переміщення коштів, обходу санкцій і маскування джерел фінансування, з особливим наголосом на використанні стейблкоїна USDT у мережі TRON.

[1] https://www.fiabvi.vg/Portals/0/DNNGalleryPro/uploads/2025/4/10/ReportonTFTrendsandTypologyforPublicUse(VASPs)(November2024).pdf

У звіті детально описано основні криптовалюти, що фігурували у підозрілих транзакціях, із домінуванням Tether (USDT), що обумовлено його стабільністю, низькою вартістю переказу та можливістю здійснення транзакцій через різні блокчейн-мережі. Інші популярні активи — Ethereum (ETH), Bitcoin (BTC), MATIC (Polygon), Solana (SOL) та Monero (XMR). Значна частина коштів проходила через гаманці, асоційовані з TRON, завдяки високій швидкості обробки та низьким комісіям. Це дозволяло створювати багатошарові схеми з використанням проміжних гаманців і таким чином ускладнювати відслідковування походження коштів.

Встановлено, що VASPs не використовувались як кінцева точка, а діяли як транзитні вузли у схемах фінансування. У ряді випадків операції прямо або опосередковано були пов'язані з адресами, що належать терористичним угрупованням, включно з "Hezbollah", "Hamas", "Gaza Now" та іншими псевдоблагодійними структурами, такими як "The Whispers of the Forgotten" чи "Dusty Path". Використання транзакційних коментарів на кшталт "Father Shaheed" свідчить про навмисну передачу меседжів і усвідомлений намір підтримати ФТ-структури.

У звіті також представлено географічний аналіз транзакцій, у якому домінують Швеція (21%), Німеччина та Франція (по 13%), Палестина (9%), а також Туреччина, Кувейт, Саудівська Аравія, Сомалі, Росія та інші. Це підкреслює транснаціональний характер таких операцій і необхідність міжнародної координації у сфері ПВК/ФТ.

Зазначено, що окремі компанії, включаючи MSB (постачальників платіжних послуг) і онлайн-казино, зареєстровані за межами BVI, використовували місцеві VASP для переміщення коштів, пов'язаних з терористичними структурами. Встановлено щонайменше один випадок прямого переказу з адреси, пов'язаної з "Hezbollah", на рахунок клієнта BVI VASP. Також ідентифіковано численні спроби обходу міжнародних санкцій з боку резидентів юрисдикцій під санкційним тиском — зокрема Росії, Туреччини, Палестини, Сомалі — через використання криптовалютних інструментів.

У висновках наголошено на необхідності впровадження низки конкретних заходів, серед яких — удосконалення регуляторної рамки для VASPs, впровадження новітніх технологій блокчейн-моніторингу, підвищення прозорості транзакцій (включно з вимогами щодо звітності за проміжними гаманцями), посилення санкційного нагляду та міжнародної співпраці між наглядовими і правоохоронними органами. Запропоновано також навчальні програми для фахівців, які зможуть ідентифікувати приховані сигнали в транзакціях (наприклад, словесні коди або специфічну структуру переказів).

Висновки:

- **Tether (USDT) мережі TRON активно використовується для фінансування тероризму через BVI VASPs**, що дозволяє обійти традиційні фінансові системи завдяки низьким комісіям, швидкості та можливості створення проміжних гаманців.
- **BVI VASPs виступають транзитними ланками у міжнародних схемах ФТ**, не зберігаючи кошти, але сприяючи їхньому переміщенню, що потребує підвищеної уваги з боку регулятора до ролі платформи у глобальних ланцюгах руху коштів.
- **Встановлено зв'язки між підозрілими транзакціями та конкретними терористичними організаціями**, включно з випадками переказів на адреси, афілійовані з "Hezbollah" та "Hamas", що свідчить про усвідомлений і цілеспрямований характер операцій.
- **Рекомендується впровадити нові технології моніторингу блокчейн-активності та підвищити вимоги до звітності VASPs**, включно з обов'язковим фіксуванням шляхів коштів через проміжні гаманці, щоб запобігти використанню BVI як юрисдикції для обходу санкцій та фінансування тероризму.

Переломний момент: Глобальні наслідки шахрайських центрів, підпільного банкінгу та незаконних онлайн-майданчиків у Південно-Східній Азії [2]

Цей звіт Управління ООН з наркотиків і злочинності (UNODC) є масштабним дослідженням транснаціональної злочинності, яка виникла у Південно-Східній Азії, проте вже має глобальні наслідки для фінансової безпеки, кіберстійкості та протидії відмиванню коштів. Його основний фокус – взаємозв'язок між шахрайськими центрами, підпільним банкінгом, нелегальними онлайн-платформами, цифровими фінансовими інструментами та організованими злочинними угрупованнями, що координують цю діяльність через розгалужені ланцюги вразливих юрисдикцій.

Звіт починається із загальної оцінки ситуації: понад 200,000 осіб, включно з жертвами торгівлі людьми, були залучені до роботи в шахрайських центрах, часто розміщених у спеціальних економічних зонах Камбоджі, М'янми, Лаосу та на території прикордонних міст Китаю. Ці центри спеціалізуються на масовому онлайн-шахрайстві (investment scams, romance scams, pig-butchering), де жертв вводять у оману щодо можливостей інвестування у криптовалюти, акції, тощо, а згодом — викрадають кошти через низку шахрайських платформ.

Ключовим інструментом такої злочинної діяльності є паралельна фінансова інфраструктура, яка включає:

- нелегальні обмінні точки, які працюють на основі принципів неформальних систем переказу (аналог hawala/fei qian);
- фінансові брокери, які конвертують фіатні кошти у криптовалюти або стейблкоїни (переважно USDT), часто через OTC-дески або Telegram;
- онлайн-платформи з функцією "гаранта", такі як Huione Guarantee, що формально пропонують сервіс ескроу, але фактично є "підпільними банками", які обслуговують нелегальні гральні сайти, шахрайські сервіси, постачальників фейкових ID та кіберінструментів для атак.

Звіт демонструє, як стейблкоїни (особливо USDT на мережі TRON) стали валютою для організованих злочинних груп: завдяки швидкості, дешевизні переказів, відсутності банківського посередництва та низькому регуляторному нагляду. Платформи Huione Guarantee у 2023 році обробили понад $11 млрд у вигляді тіньових транзакцій, і навіть почали випускати власні "токени-купони", номіновані у юанях.

Крім онлайн-шахрайства та обслуговування грального бізнесу, звіт виявляє поширену практику «білих етикеток» (white-labelling) — постачання готових платформ для шахрайств, які можуть використовуватись будь-якою групою злочинців за ліцензією, включно з власним бекендом, чатами, підробленими портфелями і т.д. Цей кримінальний SaaS (software-as-a-service) масштабував індустрію до регіонів Кавказу, Центральної Азії, Східної Африки та навіть Європи, включно з відкриттям центрів у Батумі (Грузія) та Сейшельських островах.

[2] https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

Ще одна частина звіту присвячена шкідливому програмному забезпеченню та кіберінструментам, таким як "U Browser", що подається як легітимний китайський браузер, але насправді здійснює:

- приховану реєстрацію екрану користувача;
- скриншотинг;
- встановлення бекдорів;
- пересилання даних на IP-адреси, зареєстровані в Китаї.

Звіт наголошує на глибокій інтеграції підпільного банкінгу з цифровими злочинними екосистемами, де переплетено гральний бізнес, фіктивні аукціони, подарункові карти, QR-коди, ескроу-сервіси, криптобіржі, Telegram-боти, і навіть криптопроєкти, які рекламуються як DeFi або NFT.

На завершення, UNODC попереджає, що ця злочинна екосистема вже вийшла далеко за межі Південно-Східної Азії та потребує глобальної відповіді. Пропонується низка системних заходів: впровадження спільних чорних списків гаманців і проєктів, аналіз підозрілих платформ, які пропонують "гарантовану конверсію USDT", обов'язкове повідомлення про великі транзакції зі стейблкоїнами, криміналізація використання тіньових фінансових платформ та синхронізація національних Оцінок ризиків із реаліями онлайн-фінансових злочинів.

Висновки:

- **Криптоплатформи типу Huione активно використовуються для відмивання коштів, обходу санкцій та розвитку нелегальних ринків, включно з емісією стейблкоїна, орієнтованого на обхід валютного контролю**. Це вимагає від країн встановлення регуляторних бар'єрів для необлікованих та позаліцензійних VASP.
- **Синдикати, як-от Suncity Group, використовують мережу гральних сайтів, фіктивних турнірів і нелегальних банківських сервісів як механізм системного ВК**. Національні органи фінансової розвідки мають зосередити увагу на транзакціях, пов'язаних із азійськими ігровими платформами та "junket" системами.
- **Застосування шкідливого ПЗ під виглядом браузера (наприклад, "U Browser") дозволяє кіберзлочинцям вести приховану діяльність зі збору даних і викрадення коштів у глобальному масштабі**. Рекомендовано включити моніторинг таких програм до списку червоних прапорців ПФР.
- **Регіони за межами Південно-Східної Азії, зокрема Грузія, перетворюються на нові хаби для кіберзлочинних схем**. Уряди країн повинні включати в Оцінки національних ризиків ризики ВК/ФТ/ФР, пов'язані з гральним, крипто та кіберсектором, і враховувати географічне розширення транснаціональних злочинних груп.

Керівні принципи щодо наглядової практики для компетентних органів для запобігання та виявлення зловживань на ринку відповідно до MiCA [3]

Фінальний звіт Європейського органу з цінних паперів і ринків (ESMA) містить офіційно затверджені настанови для національних компетентних органів (NCAs) країн ЄС щодо запобігання та виявлення маніпулювання ринками криптоактивів у межах регламенту MiCA (Регламент (ЄС) 2023/1114). Ці настанови спрямовані на забезпечення узгодженості наглядових підходів у державах-членах, створення єдиної культури нагляду, адаптацію перевірених практик з традиційних фінансових ринків до специфіки крипторинку, а також врахування нових викликів,

[3] https://www.esma.europa.eu/sites/default/files/2025-04/ESMA75-453128700-1408_Final_Report_MiCA_Guidelines_on_prevention_and_detection_of_market_abuse.pdf

пов'язаних із технологічними інноваціями та транснаціональним характером обігу криптоактивів.

Документ базується на статті 92(3) MiCA та визначає наглядові дії щодо виявлення таких правопорушень, як інсайдерська торгівля, неправомірне розкриття інсайдерської інформації, а також ринкова маніпуляція. Розробка ESMA враховує досвід впровадження Регламенту Європейського Союзу про зловживання на ринку (Регламент ЄС 596/2014), але водночас адаптується до особливостей середовища криптоактивів — використання соцмереж, блокчейн-технологій, максимального вилучення цінності (MEV), взаємодії майнерів і валідаторів, впливу стейблкоїнів та децентралізованих майданчиків.

Щоб забезпечити ефективне впровадження цих положень, ESMA визначила 12 ключових настанов, які формують логічну рамку для наглядової діяльності компетентних органів:

1. **Пропорційність у застосуванні (Guideline 1):** регулятори повинні оцінювати ризики, пов'язані з діяльністю кожного суб'єкта ринку, зокрема CASPів, трейдерів, майнерів, з урахуванням обсягу їх операцій, впливу на ринок і типу ризиків. Також очікується врахування нових моделей зловживань і технологічних змін, а нагляд має постійно еволюціонувати разом із ринком.
2. **Загальний підхід до запобігання і виявлення (Guideline 2):** передбачено ризик-орієнтований і прогностичний підхід до моніторингу, із швидким реагуванням на виявлені загрози. Стратегії нагляду мають бути стратегічно прив'язані до виявлення нових маніпуляцій.
3. **Інтеграція наявного досвіду (Guideline 3):** регулятори повинні аналізувати, чи підходять чинні механізми виявлення маніпуляцій з традиційних ринків до світу криптоактивів, і за потреби адаптувати їх — зокрема у частині MEV, маніпуляцій пропозицією токенів, маніпуляцій через соцмережі тощо.
4. **Єдина наглядова культура (Guideline 4):** NCA повинні обмінюватися досвідом, поширювати найкращі практики, брати участь у групах ESMA, зокрема для обговорення складних випадків нагляду, і за можливості — координуватися з органами захисту прав споживачів та протидії відмиванню коштів.
5. **Адекватність ресурсів (Guideline 5):** держави-члени повинні виділяти окремі ресурси та команди для моніторингу крипторинків. Персонал повинен володіти знаннями про технології блокчейну, консенсусні механізми, особливості ончейн-даних тощо. Рекомендовано залучення до програм безперервного навчання, таких як EU-SDFA.
6. **Відкритий діалог зі стейкхолдерами (Guideline 6):** слід організовувати комунікацію з експертами, компаніями, які надають технічні рішення, громадськими організаціями, провайдерами даних та особами, які виконують функції моніторингу за контрактом з CASPами.
7. **Поширення культури ринкової доброчесності (Guideline 7):** NCA повинні реалізовувати інформаційні та освітні заходи — подкасти, блоги, відповіді на запитання, пояснення типових зловживань, навчання, а також сприяти впровадженню добровільних стандартів доброчесності серед учасників ринку.
8. **Моніторинг і нагляд на основі даних (Guideline 8):** мають використовуватись як відкриті, так і регуляторні дані (ордери, транзакції), із поєднанням офчейн- і ончейн-аналізу, включаючи автоматизований моніторинг соцмереж та новин. Рекомендується використання систем виявлення шаблонів, ключових слів, підозрілих трендів.

9. **Нагляд за внутрішніми системами PPAET (Guideline 9):** регулятори повинні регулярно перевіряти, чи дійсно CASPи та інші PPAET мають системи та процедури запобігання маніпуляціям, і наскільки ці системи відповідають змінюваним ризикам. Частота перевірок має узгоджуватись із масштабом і ризик-профілем суб'єкта.
10. **Реакція на STOR (Guideline 10):** у кожного регулятора має бути чітка, поетапна процедура обробки повідомлень про підозрілі транзакції, включаючи призначення відповідальних осіб, критерії класифікації за серйозністю і частотою, та протоколи реагування.
11. **Координація з ESMA (Guideline 11):** у складних транскордонних випадках (2 і більше юрисдикції, ризик дублювання дій, додаткове навантаження на учасників ринку) NCA можуть ініціювати координовані перевірки або розслідування під егідою ESMA.
12. **Бар'єри з боку третіх країн (Guideline 12):** якщо CASP працює через платформи або суб'єктів, розташованих у країнах з низьким рівнем прозорості або співпраці, NCA повинна повідомити про це ESMA та інших учасників, ініціювати координацію і погодити стратегію реагування.

Висновки:

- **Регулятори країн ЄС мають впровадити ризик-орієнтований і пропорційний нагляд за ринками криптоактивів**, адаптуючи практики до таких особливостей, як технології блокчейну, роль валідаторів/майнерів, соцмережі та токеноміка.
- **Моніторинг ринкових зловживань має охоплювати як фінансові, так і інформаційні потоки**, включаючи соцмережі, блоги, вебплатформи, а також офчейн- та ончейн-дані про транзакції і ордери.
- **Регулятори зобов'язані розвивати системи внутрішнього аналізу STOR, налагоджувати механізми обміну інформацією з іншими NCA та ESMA**, а також реагувати на транскордонні загрози злагоджено та координаційно.
- **Рекомендовано створити спеціалізовані команди нагляду за ринками криптоактивів із відповідною IT-кваліфікацією та знаннями**, впровадити навчальні програми, автоматизовані системи аналізу ризиків і механізми навчання учасників ринку щодо ринкової доброчесності.

Ці 12 настанов створюють структуровану методологію, яка покликана забезпечити ефективне, скоординоване та ризик-орієнтоване регулювання ринків криптоактивів у ЄС. Вони також є дороговказом для третіх країн, які прагнуть гармонізувати свій підхід до нагляду за крипторинками згідно з європейськими стандартами.

Розкриття вразливостей біометричних систем: Посилення стійкості правоохоронних органів [4]

Документ, підготовлений Europol Innovation Lab у співпраці з провідними експертами у сфері біометричних технологій, пропонує всесторонній аналіз вразливостей біометричних систем, які використовуються для ідентифікації осіб, та стратегій їх захисту в контексті правоохоронної діяльності. Звіт має на меті підвищити обізнаність правоохоронних органів щодо потенційних загроз, пов'язаних із біометричними системами, та підготувати їх до протидії злочинним атакам, які можуть підірвати надійність цих технологій. Документ охоплює широкий спектр тем, від

[4] https://www.europol.europa.eu/cms/sites/default/files/documents/Biometric-vulnerabilities.pdf

технічних аспектів біометричних систем до етичних і правових рамок їх використання, пропонуючи конкретні рекомендації для зміцнення систем ідентифікації.

Звіт розпочинається з підкреслення критичної ролі біометричних технологій у правоохоронній діяльності, де вони застосовуються для ідентифікації осіб у розслідуваннях, пов'язаних із тероризмом, шахрайством, торгівлею людьми, кіберзлочинністю та іншими видами злочинів. Біометричні системи, що використовують відбитки пальців, обличчя, райдужної оболонки ока та голосу, стали невід'ємною частиною сучасних методів верифікації особи завдяки їхній точності та зручності. Проте зростання популярності біометричних технологій, зокрема у віддаленій ідентифікації та комерційних додатках, зробило їх привабливою мішенню для злочинців, які розробляють дедалі складніші методи атак. Документ наголошує на необхідності відповідального використання біометричних даних, що має відповідати суворим етичним і правовим стандартам, таким як Загальний регламент захисту даних (GDPR), Регламент захисту даних ЄС (EUDPR) та Директива про правоохоронну діяльність (LED).

Основна увага звіту зосереджена на атаках, які передбачають подання фальшивих або змінених біометричних даних до пристроїв захоплення, таких як сканери, камери чи мікрофони, з метою обману системи. Ці атаки поділяються на активні атаки, спрямовані на імітацію особи, відомої системі, та атаки приховування ідентичності, які мають на меті уникнути розпізнавання.

Звіт детально аналізує вразливості чотирьох ключових біометричних характеристик. Для підробки відбитків пальців, злочинці створюють силіконові репліки, використовують відбитки із поверхонь або цифрово згенеровані відбитки у 2D, 2.5D чи 3D форматах, а також навмисно пошкоджують відбитки для уникнення розпізнавання. Щодо обличчя, зловмисники можуть використовувати фотографії з соціальних мереж, маски (від простих до високоякісних силіконових), макіяж, морфінг облич (комбінування рис двох осіб для обману систем видачі документів) або діпфейки, які дозволяють імітувати особу навіть у реальному часі. Для обману систем розпзнавання райдужної оболонки ока, характерні атаки з використанням роздрукованих зображень, штучних очей, текстурованих контактних лінз або повторного відтворення зображень, а також методи уникнення розпізнавання шляхом зміни пози очей. Голосові атаки включають відтворення записів, синтетичну мову, створену за допомогою систем штучного інтелекту, або конверсію голосу, причому діпфейкові голоси стають дедалі доступнішими через прості додатки, що створює додаткові загрози, зокрема для шахрайства.

Для протидії атакам звіт пропонує методи виявлення атак (PAD), які поділяються на апаратні, що використовують додаткові датчики для перевірки ознак життя, та програмні, що аналізують сліди атак у захоплених даних. Виявлення "живості" (liveness detection) є ключовим елементом PAD, оскільки воно підтверджує, що біометрична характеристика належить живій людині.

Звіт також підкреслює важливість стандартів ISO/IEC, зокрема ISO/IEC 30107, які гармонізують визначення, методології тестування та оцінку ефективності PAD. Ці стандарти вводять метрики, такі як Attack Presentation Classification Error Rate (APCER) та Bona Fide Presentation Classification Error Rate (BPCER), які вимірюють помилки класифікації атак і справжніх даних. Для голосових систем ініціатива ASVspoof пропонує спільну оцінку PAD та біометричних компараторів, що підвищує надійність захисту.

Окремий розділ присвячений захисту біометричних шаблонів — цифрових представлень біометричних характеристик, які є чутливими особистими даними. Хоча раніше вважалося, що

шаблони неможливо відновити, сучасні дослідження показують, що зловмисники можуть реконструювати зображення відбитків або райдужної оболонки. Для захисту даних пропонується використовувати крипто-біометрію та біометрію в зашифрованому домені з гомо-морфним шифруванням, які відповідають принципам незворотності, невідстежуваності та оновлюваності, визначеним у ISO/IEC 24745. Звіт наголошує на загрозі крадіжки біометричних даних, оскільки викрадені дані з однієї системи можуть бути використані для атак на інші, навіть якщо ті мають високий рівень захисту.

Для зміцнення біометричних систем звіт пропонує низку заходів. Правоохоронці повинні регулярно проходити навчання, щоб бути в курсі нових методів атак і технологій PAD. Впровадження передових алгоритмів і машинного навчання для виявлення атак є критично важливим, як і інтегрований підхід, який захищає всі етапи біометричного процесу — від збору до зберігання даних.

Висновки:

- **Підвищення обізнаності через навчання:** Правоохоронні органи повинні впровадити регулярні тренінги та семінари для офіцерів, щоб ознайомити їх із новими методами атак і технологіями PAD, що дозволить оперативно виявляти та реагувати на спроби шахрайства з біометричними даними.
- **Впровадження живої реєстрації (live enrolment):** Для мінімізації ризиків морфінгу або використання синтетичних даних необхідно запровадити живу реєстрацію біометричних даних під час видачі документів, наприклад, паспортів, із контролем умов захоплення даних.
- **Стандартизована міжнародна звітність:** Створити єдину міжнародну систему кодування та збору даних про біометричні атаки, щоб оцінити їх масштаби, визначити пріоритетні загрози та спрямувати ресурси на розробку контрзаходів.
- **Інвестиції в захист шаблонів:** Пріоритетно інвестувати в дослідження та впровадження гомо-морфного шифрування та крипто-біометричних даних, щоб забезпечити незворотність і невідстежуваність біометричних шаблонів, знижуючи ризик їх крадіжки та зловживання ними.

Співпраця між експертами з біометрії, кібербезпеки, криміналістики та академічними дослідниками сприятиме обміну знаннями про нові атаки та методи захисту. Звіт також закликає до створення міжнародної системи кодування та збору даних про біометричні атаки, щоб оцінити їх масштаби та визначити пріоритети. Безпечна обробка даних, включаючи шифрування, токенізацію та живу реєстрацію (live enrolment), має мінімізувати ризики маніпуляцій.

У висновках звіт наголошує, що біометричні системи, попри їхню надійність, залишаються вразливими до нових атак, які стають дедалі складнішими через доступність таких технологій, як діпфейки та 3D-друк. Правоохоронні органи повинні постійно оцінювати PAD-системи та інвестувати в захист даних, щоб забезпечити надійність ідентифікації та захист прав громадян. Стандартизація, етичне використання та міждисциплінарна співпраця є основою для безпечного впровадження біометричних технологій, що дозволяє правоохоронцям ефективно боротися зі злочинністю, зберігаючи довіру суспільства.

Нові ризики відмивання коштів та фінансування тероризму у сфері азартних ігор [5]

Документ, опублікований Комісією з азартних ігор Великобританії, є вичерпним посібником для ліцензіатів та компаній у секторі азартних ігор, спрямованим на протидію новим і триваючим

[5] https://www.gamblingcommission.gov.uk/licensees-and-businesses/guide/page/emerging-money-laundering-and-terrorist-financing-risks-from-april-2025/

ризикам відмивання грошей (ML) та фінансування тероризму (TF). Він детально описує вразливості в гральній індустрії, зокрема в казино, платіжних системах і нових технологіях, надаючи практичні рекомендації для забезпечення відповідності законодавству про протидію відмиванню коштів (AML) та умовам ліцензій. Документ структуровано так, щоб висвітлити конкретні зони ризику, їхні наслідки та необхідні дії для операторів, спираючись на нормативні акти, попередні оцінки ризиків і зовнішні джерела, такі як HMRC, Національне агентство з боротьби зі злочинністю (NCA), HM Treasury та Financial Action Task Force (FATF).

Документ звертає увагу на ризики, пов'язані з діяльністю грошових сервісів (MSB) у онлайн та офлайн казино, що включають обмін валют, виплату чеків через третіх осіб і грошові перекази. Особливий акцент зроблено на високому ризику відмивання грошей через використання великих номіналів іноземних валют, зокрема банкнот €500, які часто приваблюють злочинців. Хоча кількість MSB-транзакцій зменшилася, ця діяльність залишається високоризиковою через такі фактори, як платежі від політично значущих осіб (PEPs) або осіб із санкційних списків, залежність від даних сторонніх постачальників для належної перевірки, а також перекази з невідомих або неліцензованих джерел. Операторам рекомендується проводити ретельні оцінки ризиків, впроваджувати надійні заходи контролю, застосовувати посилену перевірку клієнтів (EDD) для користувачів MSB-послуг і дотримуватися рекомендацій HMRC щодо MSB.

Значну увагу приділено новій загрозі – використанню штучного інтелекту (ШІ) для обходу перевірок клієнтів. Зростає кількість складних спроб створення фіктивних акаунтів за допомогою ШІ-генерованих фальшивих документів. За даними NCA, акаунти, створені такими методами, частіше використовуються для ML або TF. Для протидії цьому операторам радять ретельно перевіряти документи клієнтів, навчати персонал виявляти ШІ-генеровані підробки та подавати звіти про підозрілу діяльність (SAR) до NCA, вказуючи код 0752 NECC.

Ще одна серйозна проблема – експлуатація споживачів через пропозиції фінансових винагород за надання особистих даних для створення численних гральних акаунтів. Такі схеми можуть бути пов'язані з діяльністю неліцензованих посередників або муловими акаунтами, що використовуються для відмивання грошей. Операторам доручено посилити процеси верифікації особи, забезпечити відповідність умовам ліцензії (зокрема, умові 17.1.1 LCCP) і оперативно усувати виявлені прогалини, щоб запобігти створенню фіктивних акаунтів.

Документ також аналізує ділові відносини з третіми сторонами, зокрема партнерства та інвестиції, які класифікуються як високоризикові в оцінці ризиків Комісії за 2023 рік. Недостатня перевірка таких відносин може наражають операторів на ризики ML/TF, особливо якщо партнери працюють у високоризикових юрисдикціях або займаються незаконною діяльністю. Операторам необхідно оцінювати юрисдикційні, транзакційні ризики та походження коштів партнерів, забезпечувати законність ділових відносин і враховувати ширші цілі ліцензування під час оцінки діяльності партнерів за межами Великобританії.

Відкриті платіжні системи, які дозволяють переказувати кошти між різними методами оплати, визнано значною вразливістю для ML, оскільки вони можуть приховувати походження чи призначення коштів. Документ наполегливо рекомендує впроваджувати закриті платіжні системи, де виведення коштів здійснюється тим самим методом, що використовувався для депозиту, щоб мінімізувати ці ризики. Оператори, які продовжують використовувати відкриті системи, повинні включити ці ризики до своїх оцінок ризиків ML/TF і впровадити суворі заходи контролю для запобігання їхнього злочинного використання.

Поява ігор, розроблених ліцензованими постачальниками програмного забезпечення, на неліцензованих вебсайтах, доступних британським споживачам, є ще однією проблемою. Такі дії створюють ризик прийняття коштів, отриманих злочинним шляхом, і підривають цілі ліцензування. Операторам, включно з тими, хто має ліцензії на програмне забезпечення для азартних ігор, наказано активно моніторити ділові відносини, припиняти партнерства з невідповідними суб'єктами та негайно повідомляти Комісію, надаючи чіткий план дій для вирішення виявлених порушень.

Криптоактиви, які набирають популярності в гральній індустрії, визнано високоризиковим методом оплати через їхню вразливість до ML/TF. Оператори повинні повністю розуміти послуги своїх платіжних провайдерів, оцінювати ризики нових платіжних методів, повідомляти про зміни в методах оплати як ключові події відповідно до умови ліцензії 15.2.1 і вважати клієнтів, які використовують криптоактиви, високоризиковими, застосовуючи до них EDD.

Платіжні термінали в офлайн казино виділено як слабке місце, оскільки депозити через ці методи часто перевіряються менш ретельно. Операторам наказано включати термінали до своїх оцінок ризиків, перевіряти походження коштів і забезпечувати, щоб використання терміналів впливало на загальний ризик-профіль клієнта, а не покладатися виключно на сторонніх постачальників для перевірок.

Краш-ігри, які стали популярними в неліцензованих крипто-казино і тепер з'являються в легальних казино, створюють унікальні виклики через їхню високу волатильність і швидкі виплати, що можуть маскувати підозрілу поведінку. Оператори повинні оцінювати ризики ML таких продуктів, впроваджувати заходи для виявлення незвичайних моделей ставок і включати використання краш-ігор до ризик-профілю клієнтів, подаючи SAR за необхідності.

Нарешті, документ звертається до списку юрисдикцій, що перебувають під посиленим моніторингом FATF, оновленому у лютому 2025 року. Оператори зобов'язані виявляти клієнтів і відносини, пов'язані з високоризикованими юрисдикціями (як із "чорного", так і з "сірого" списків), і застосовувати надійну EDD для пом'якшення ризиків ML, TF і фінансування розповсюдження. Головна мета – щоб оператори азартних ігор залишалися пильними, проактивними та відповідними у запобіганні використанню їхніх бізнесів для ML/TF, захищаючи цілісність гральної індустрії та суспільство.

Висновки:

- **Посилення перевірок для MSB та криптоактивів:** Оператори повинні вважати клієнтів, які використовують MSB-послуги чи криптоактиви, високоризиковими, застосовувати посилену перевірку (EDD) і перевіряти походження коштів.
- **Боротьба з ШІ-підробками:** Необхідно навчати персонал виявляти ШІ-генеровані фальшиві документи, подавати SARs із кодом 0752 NECC до NCA та регулярно оновлювати процеси верифікації.
- **Впровадження закритих платіжних систем:** Рекомендується використовувати закриті платіжні системи для зменшення ризиків відмивання грошей; для відкритих систем – включати ці ризики до оцінки та впроваджувати суворі заходи контролю.
- **Моніторинг ділових відносин:** Проводити ретельну перевірку третіх сторін, припиняти співпрацю з партнерами, що діють нелегально, та повідомляти Комісію з планом дій.

Протидія шахрайству в США: Аналіз зусиль федеральних агенцій та бізнесу [6]

Документ, підготовлений Рахунковою палатою США (Government Accountability Office, GAO), є ґрунтовним звітом, що аналізує зусилля федеральних агенцій та приватного сектору у протидії шахрайству, зокрема так званим "скамам" – виду шахрайства, яке базується на обмані чи маніпуляціях з метою отримання фінансової вигоди.

Звіт створено на запит комітетів Конгресу, зокрема Комітету з банківської справи, житлової політики та міських справ і Спеціального комітету з питань старіння, з метою оцінки ефективності заходів для запобігання та реагування на шахрайство, а також для розробки рекомендацій щодо вдосконалення координації, звітності та інформування споживачів. Документ охоплює широкий спектр питань, включаючи діяльність федеральних агенцій, аналіз даних про скарги, ефективність освітніх програм, ініціативи приватного сектору та реагування на скарги споживачів, з акцентом на захист вразливих груп, таких як літні люди.

Звіт розпочинається з опису природи шахрайства, яке еволюціонувало разом із технологіями, стаючи дедалі складнішим і більш поширеним. Шахрайство часто передбачає контакт з жертвою через телефон, соціальні мережі, електронну пошту чи текстові повідомлення, після чого шахрай застосовує різні сценарії, щоб переконати жертву здійснити платіж через P2P-програми, подарункові картки, банківські перекази чи навіть готівку.

GAO підкреслює, що шахрайство завдає значних фінансових збитків, іноді призводячи до втрати всіх заощаджень жертви, а також спричиняє емоційні травми. Хоча точної урядової оцінки загальних втрат немає, експерти оцінюють збитки у мільярди доларів щорічно. Документ також звертає увагу на глобальний масштаб проблеми, зокрема діяльність транснаціональних злочинних організацій, які використовують call-центри за кордоном та примусову працю в "скам-комплексах", де жертви змушені проводити шахрайські операції.

GAO дослідило діяльність 13 федеральних агенцій, серед яких ключовими є Бюро захисту прав споживачів у фінансовій сфері (CFPB), Федеральне бюро розслідувань (FBI), Федеральна торгова комісія (FTC), Федеральна резервна система та Мережа боротьби з фінансовими злочинами (FinCEN). Ці агенції займаються різними аспектами боротьби з шахрайством, включаючи інформування споживачів, прийом скарг, розслідування та правоохоронні дії.

Проте звіт виявляє критичну прогалину: відсутність єдиної урядової стратегії, яка б координувала ці зусилля. Наявні стратегії, наприклад, щодо кіберзагроз чи відмивання коштів, не охоплюють шахрайство комплексно, а міжвідомча координація залишається фрагментарною. FBI розробляє стратегію щодо кібершахрайства, яка могла б стати основою для ширшої урядової ініціативи, але на момент підготовки звіту жодна агенція не взяла на себе лідерство у створенні такого плану. GAO наголошує, що скоординована стратегія дозволила б оптимізувати ресурси, уникнути дублювання зусиль і підвищити ефективність боротьби з шахрайством.

Особливу увагу звіт приділяє збору та аналізу даних про скарги, пов’язані з шахрайством. CFPB, FBI (через Центр скарг на інтернет-злочини, IC3) та FTC є основними агенціями, які отримують скарги від споживачів. Наприклад, у 2023 році FBI повідомило про 589 400 скарг, пов’язаних із шахрайством, із загальними втратами у $10,55 мільярда. Проте через обмеження в методах збору даних, таких як нестандартизовані категорії чи відсутність єдиної термінології, агенції не

[6] https://www.gao.gov/assets/gao-25-107088.pdf

можуть точно оцінити загальну кількість шахрайств чи їх фінансові наслідки. Відсутність урядової оцінки масштабів проблеми ускладнює розуміння її серйозності та розробку цільових заходів. GAO також зазначає, що різні агенції використовують власні визначення "шахрайства" та "скаму", що ускладнює порівняння даних і координацію зусиль. Наприклад, FTC не розрізняє шахрайство та сками у своїх звітах, оскільки їхня правова база фокусується на нечесних практиках, незалежно від того, чи був платіж авторизованим.

Освітні ініціативи для споживачів є ще одним важливим аспектом звіту. CFPB, FBI та FTC надають широкий спектр матеріалів, що пояснюють типи шахрайств і способи їх уникнення. Проте GAO виявило, що жодна з цих агенцій не проводить систематичного оцінювання ефективності своїх освітніх програм. Без таких оцінок неможливо визначити, наскільки ці ініціативи допомагають споживачам розпізнавати шахрайство чи захищатися від нього, або як можна вдосконалити матеріали для різних груп населення, зокрема літніх людей, які є особливо вразливими. Звіт підкреслює, що літні люди (60+) зазнають більших фінансових втрат і рідше повідомляють про шахрайство, що вимагає спеціалізованих освітніх підходів.

У сфері приватного сектору, GAO проаналізувало зусилля семи компаній, включаючи постачальників P2P-програм, емітентів подарункових карток, фінансові установи та компанії, що надають послуги грошових переказів. Ці бізнеси застосовують різні методи для запобігання шахрайству, такі як попереджувальні повідомлення в додатках, навчання персоналу, уповільнення транзакцій для перевірки їх легітимності та розміщення попереджувальних знаків у торговельних точках. GAO провело 68 неанонсованих візитів до роздрібних магазинів у восьми штатах, щоб оцінити наявність і видимість попереджувальних знаків про шахрайство з подарунковими картками. Результати показали значну розрізненість: у деяких магазинах знаки були відсутні, приховані за товарами або недостатньо помітні, що вказує на потребу в стандартизації та посиленні таких заходів. Звіт також зазначає, що федеральне законодавство не зобов’язує фінансові установи відшкодовувати втрати від шахрайських платежів, якщо вони були ініційовані власником рахунку, що ускладнює повернення коштів жертвам.

Для оцінки реагування на скарги GAO провело інсценування, імітуючи скарги від споживачів, включаючи літніх людей, до CFPB, FBI, FTC, а також до емітентів подарункових карток і компанії з грошових переказів. Результати показали різноманітність підходів. Федеральні агенції зазвичай реєструють скарги, можуть перенаправляти їх до інших установ або використовувати для розслідувань, але рідко надають пряму допомогу у поверненні коштів. Бізнеси, такі як емітенти подарункових карток, часто відмовляються відшкодовувати втрати, посилаючись на авторизацію транзакцій. GAO підкреслює, що обмежена можливість повернення коштів залишається значною проблемою для жертв шахрайства, особливо вразливих груп.

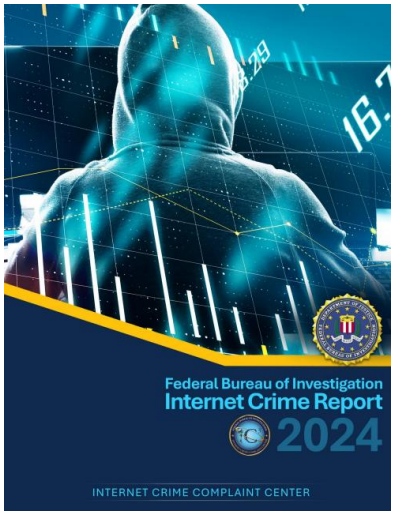
На основі аналізу GAO пропонує 16 рекомендацій, спрямованих на вдосконалення боротьби з шахрайством. Ключові рекомендації включають розробку урядової стратегії для координації зусиль, створення єдиного визначення шахрайства, розробку національної оцінки масштабів шахрайства та оцінювання ефективності освітніх програм. FBI не погодилося з трьома рекомендаціями, стверджуючи, що вони виходять за межі їхньої компетенції або є складними для реалізації через обмеженість ресурсів. FTC висловила занепокоєння щодо єдиного визначення "скаму", оскільки воно може не відповідати їхнім правовим повноваженням, і зазначила, що створення такого визначення може відволікати ресурси від правоохоронної діяльності. Інші агенції, такі як Національна адміністрація кредитних спілок, визнали спостереження GAO, але не отримали конкретних рекомендацій.

Звіт завершується висновками, що підкреслюють необхідність системного підходу до боротьби з шахрайством, який би поєднував зусилля уряду, бізнесу та споживачів. Документ наголошує на глобальному характері шахрайства, його зростаючій складності через використання технологій, таких як штучний інтелект і deepfake, та особливій вразливості літніх людей. GAO закликає до посилення координації, стандартизації даних і оцінювання ефективності заходів, щоб зменшити фінансові та емоційні втрати від шахрайства та підвищити захист споживачів у США.

Висновки:

- **Розробка урядової стратегії:** Федеральні агенції повинні розробити комплексну міжвідомчу стратегію для координації зусиль у протидії шахрайству. FBI, враховуючи їхній досвід у кібершахрайстві, має очолити цей процес, щоб забезпечити ефективне використання ресурсів та уникнення дублювання зусиль.
- **Стандартизація даних про шахрайство:** CFPB, FBI та FTC повинні співпрацювати для створення єдиного визначення "скаму" та розробки національної оцінки кількості шахрайств і фінансових втрат. Це передбачає вдосконалення методів збору даних та врахування неповідомлених випадків.
- **Оцінювання освітніх програм:** Агенції мають впровадити систематичне оцінювання ефективності своїх освітніх ініціатив, використовуючи метрики, такі як рівень розпізнавання шахрайства споживачами, щоб адаптувати матеріали до потреб різних груп, зокрема літніх людей.
- **Покращення бізнес-практик:** Роздрібні торговці та фінансові установи повинні стандартизувати попереджувальні повідомлення про шахрайство (наприклад, на подарункових картках) та впровадити заходи для уповільнення підозрілих транзакцій, щоб дати споживачам час перевірити їхню легітимність.

Економіка шахрайства: чому криптовалюта стала головним інструментом кібершахраїв[7]



Звіт Федерального бюро розслідувань США є ґрунтовним аналітичним документом, що охоплює масштабну картину кіберзлочинності у 2024 році та підсумовує двадцятип'ятирічну діяльність Internet Crime Complaint Center (IC3). Основний фокус звіту зосереджений на кількісному та якісному аналізі скарг на інтернет-злочини, тенденцій, втрат, вікових і географічних характеристик постраждалих, а також інструментів реагування, які використовує уряд США, зокрема ФБР. За 2024 рік IC3 отримала 859 532 скарги із загальними задекларованими втратами у розмірі 16,6 мільярда доларів США, що на 33% більше, ніж у 2023 році. В середньому кожна скарга супроводжувалась втратою у 19 372 долари. Більшість втрат пов'язана з інвестиційним шахрайством ($6,57 млрд), компрометацією бізнес-електронної пошти ($2,77 млрд), техпідтримкою ($1,46 млрд), крадіжками персональних даних, а також шахрайством у сфері криптовалют. Особливу загрозу становлять так звані «pig butchering scams» — складні соціально-інженерні схеми, в яких шахраї входять у довіру до жертви в онлайн-просторі і поступово спонукають до інвестування у фейкові криптоплатформи. У звіті також наголошується, що понад 83% всіх втрат спричинені саме кіберзлочинами з

[7] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

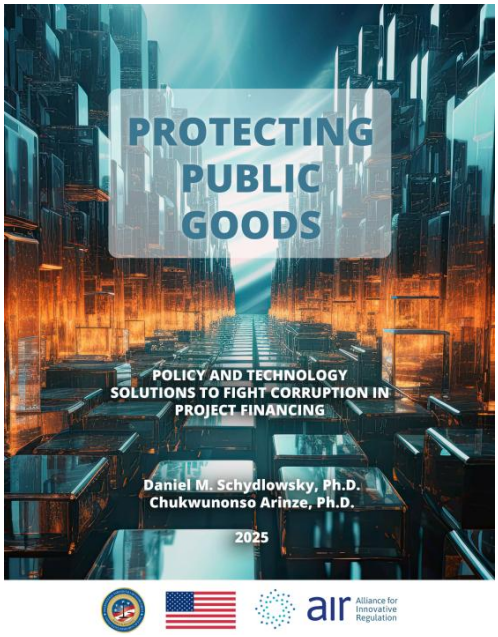
елементом обману або маніпуляції, які активно експлуатують цифрові платформи, мобільні додатки, електронну пошту та онлайн-банкінг. Серед інструментів шахрайства найпопулярнішими залишаються фішинг, фальшиві веб-сайти, підроблені особи техпідтримки, маніпулятивні оголошення в соціальних мережах та інші методи соціальної інженерії. Значне занепокоєння викликає зростання атак на критичну інфраструктуру — понад 4,800 організацій у США з секторів водопостачання, охорони здоров'я, енергетики тощо повідомили про інциденти, здебільшого з використанням програм-вимагачів (ransomware) та зламів баз даних. Найактивнішими виявились варіанти Akira, LockBit, RansomHub, FOG і PLAY. Однією з найбільш ефективних відповідей з боку ФБР стало посилення діяльності Recovery Asset Team (RAT), що оперує механізмом Financial Fraud Kill Chain — системою оперативної взаємодії з фінансовими установами для заморожування коштів, що пересилаються шахраям. У 2024 році IC3 RAT вдалося ініціювати 3 020 процедур замороження на суму $848,4 млн, з яких понад $561 млн було успішно заблоковано. У цьому контексті звіт демонструє приклади успішної міжвідомчої та міжнародної взаємодії, включаючи співпрацю з правоохоронними органами Індії для ліквідації транскордонних кол-центрів-шахраїв. Водночас важливою новацією звітного року стала ініціатива «Operation Level Up» — проєкт із виявлення та повідомлення жертв криптоінвестиційного шахрайства, що дозволив поінформувати понад 4 300 осіб, з яких 76% навіть не знали, що стали жертвами шахрайства, та попередити втрати на суму понад $285 млн. Значну увагу звіт приділяє вразливості громадян похилого віку. Особи 60+ років подали 147 127 скарг із загальними втратами $4,88 млрд, тобто майже третина всіх втрат — саме у цій віковій групі. Найпоширенішими схемами для них були шахрайства з техпідтримкою, романтичні афери, інвестиційні схеми та фальшиві дзвінки від урядових структур. Вікова аналітика також показує, що найвищі середні втрати на одну скаргу припадають на старші вікові групи, особливо у сферах, де застосовуються методи довготривалого впливу та маніпуляції (наприклад, романтичне шахрайство). У географічному розрізі найвищі показники за кількістю скарг та розміром втрат продемонстрували штати Каліфорнія, Техас, Флорида, Нью-Йорк та Іллінойс. Найбільші втрати спостерігались через криптовалюту, банківські перекази та транзакції через P2P-платформи. Загалом, звіт чітко ілюструє, як масштаби та складність кіберзлочинів еволюціонують, а також підкреслює важливість постійного партнерства між правоохоронцями, фінансовим сектором, технологічними компаніями та громадськістю для ефективного стримування цифрових загроз.

Висновки:

- **Різке зростання криптозлочинів:** Збитки від шахрайства з криптовалютою зросли на 66% у 2024 році (до $9,3 млрд), а особи 60+ років стали основною цільовою групою. Необхідні термінові просвітницькі кампанії для захисту літніх людей.
- **Фінансове шахрайство через email-компрометацію (BEC):** IC3 успішно відновила понад $560 млн завдяки фінансовому ланцюгу блокування (FFKC), що підтверджує ефективність міжвідомчої координації. Рекомендовано розвивати аналогічні механізми в інших юрисдикціях.
- **Рекордна кількість атак на критичну інфраструктуру:** Зафіксовано понад 4,800 випадків уразливості, з них більшість — через програми-вимагачі. Це вимагає зміцнення кіберзахисту державних і приватних структур.
- **Інституційна відповідь дає результати:** Ініціативи FBI (наприклад, Operation Level Up, співпраця з Індією щодо кол-центрів) демонструють практичну ефективність і можуть бути масштабовані на міжнародному рівні.

Звіти окремих інституцій та експертів

Захист суспільних благ: Інноваційні технології та політика проти корупції в інфраструктурному фінансуванні [8]



Документ підготовлений Альянсом за інноваційне регулювання (AIR) у співпраці з Державним департаментом США, є всебічним дослідженням проблеми корупції в фінансуванні інфраструктурних проєктів та пропонує інноваційні технологічні й політичні рішення для її подолання. Документ спирається на результати двох TechSprints (2022 та 2024 років), які об'єднали експертів для розробки інструментів, спрямованих на зменшення корупційних ризиків у секторі інфраструктури — одному з найбільш вразливих через великі обсяги фінансування та складність дозвільних процедур. Документ аналізує життєвий цикл інфраструктурних проєктів, точки вразливості до корупції, її економічні та суспільні витрати, а також традиційні й новітні методи виявлення та запобігання, пропонуючи конкретні рекомендації для урядів, фінансових установ і міжнародних організацій.

Документ розпочинається з окреслення глобальної проблеми корупції, яка підриває розвиток, іноземні інвестиції, демократію та стабільність. За оцінками, до 30% коштів, виділених на інфраструктурні проєкти, відводяться через корупційні схеми, що зменшує ресурси для суспільних благ і послаблює довіру до державних інститутів.

Як приклад наводиться скандал із бразильською компанією Odebrecht, яка виплатила $788 млн хабарів для отримання контрактів у 12 країнах, що призвело до значного завищення вартості проєктів. Цей випадок ілюструє системний характер проблеми та необхідність комплексного підходу. Документ розроблений в рамках ініціативи ASET (Anti-Corruption Solutions Through Emerging Technologies), яка використовує формат TechSprints для стимулювання інновацій через інтенсивні сесії вирішення проблем.

Автори детально описують типовий життєвий цикл інфраструктурного проєкту — від концептуального розвитку до фінального завершення, включаючи етапи профілювання, попередніх і детальних інженерних досліджень, розробки тендерної документації, залучення учасників, оцінки пропозицій, укладання контрактів, виконання робіт і остаточного огляду. Вони також аналізують фінансові потоки в проєктах, що фінансуються багатонаціональними банками розвитку, зазначаючи, що корупція найчастіше проявляється на етапах нижче рівня підрядників, хоча домовленості можуть укладатися раніше.

Вразливості до корупції включають маніпуляції з вибором місця проєкту для підвищення вартості прилеглих земель, включення специфічних технічних вимог для обмеження конкуренції, штучне обмеження учасників тендерів через завищені кваліфікаційні критерії, змову між учасниками, низькі пропозиції кошторису з подальшим збільшенням витрат через контрактні зміни, а також використання арбітражу для завищення цін за винагороду. Окремо розглядаються неоднозначні ситуації, такі як лобіювання, конфлікти інтересів, кумівство та «капіталізм друзів», які ускладнюють визначення корупції через культурні, правові чи політичні відмінності.

[8] https://regulationinnovation.org/wp-content/uploads/2025/04/Protecting-Public-Goods-White-Paper.pdf

Економічні та суспільні втрати від корупції є значними: прямі втрати охоплюють надмірні ціни контрактів, хабарі та витрати на посередників, тоді як непрямі включають спотворення розподілу ресурсів, зниження ефективності, пошук ренти та демотивацію працівників. За оцінками, корупція коштує світовій економіці $3,6 трлн щорічно (5% ВВП), причому непрямі втрати перевищують прямі, стаючи системними та загрожуючи демократичному врядуванню.

Традиційні методи запобігання корупції включають забезпечення прозорості через публікацію тендерних документів і протоколів, обмеження участі в тендерах на основі репутації та досвіду, вимогу фінансових гарантій від підрядників і захист викривачів, які розкривають корупційні схеми. Проте ці методи мають обмеження: надмірні вимоги до учасників можуть зменшувати конкуренцію, а викривачі стикаються з серйозними ризиками, як-от переслідування чи навіть смерть, як у випадку з викривачем Odebrecht у Колумбії.

Для подолання цих обмежень документ пропонує низку технологічних інновацій. Open Banking API дозволяють моніторити фінансові транзакції в реальному часі, виявляючи відхилення від узгоджених графіків виплат. Блокчейн-технології забезпечують створення анонімних, захищених платформ для викривачів через децентралізовані месенджери з кінцевим шифруванням, що знижує ризик переслідування. Геопросторові зображення, зокрема зроблені низькоорбітальними радариами (SAR), дозволяють відстежувати фізичний прогрес будівництва, порівнюючи виплати з фактичною роботою. Штучний інтелект може використовуватися для створення «калькулятора витрат», який оцінює бюджети проєктів на основі даних завершених проєктів, допомагаючи виявляти завищені пропозиції. Впровадження цих технологій вимагає модернізації апаратного й програмного забезпечення, підвищення експертизи і переходу до хмарних обчислень.

Політичні рекомендації включають міжнародну стандартизацію підходів до боротьби з корупцією, створення уніфікованих шаблонів контрактів для зменшення маніпуляцій, збільшення кількості учасників тендерів шляхом ширшої публікації, розробку реєстрів надійності та ефективності підрядників, рандомізацію й інтернаціоналізацію тендерних механізмів для ускладнення підкупу, одночасне присудження контрактів на виконання та нагляд, стандартизацію поводження з PEP, розширення вимог до AML-ланки у ланцюзі постачання, рівне ставлення до хабародавців і одержувачів та інтеграцію антикорупційних заходів із діяльністю ПФР/FATF. Ці заходи спрямовані на підвищення прозорості, конкуренції та відповідальності в фінансуванні інфраструктури.

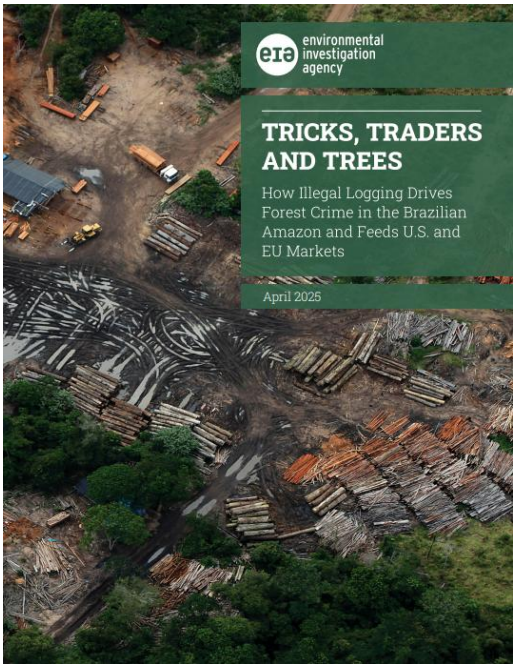
Висновки:

- **Впровадження реального моніторингу через Open Banking API:** Урядам і фінансовим установам слід інвестувати в інтеграцію Open Banking API для реального аудиту транзакцій інфраструктурних проєктів, що дозволить виявляти відхилення від графіків виплат і зменшить можливості для розкрадання коштів.
- **Створення блокчейн-платформ для захисту викривачів:** Необхідно розробити та впровадити децентралізовані месенджери з кінцевим шифруванням для анонімного повідомлення про корупцію, що підвищить безпеку викривачів і заохотить їх до співпраці.
- **Використання геопросторових зображень для нагляду:** Організації-донори та уряди повинні застосовувати низькоорбітальні радари для моніторингу фізичного прогресу будівництва, забезпечуючи відповідність виплат фактичній роботі та зменшуючи ризик нецільового використання коштів.
- **Розробка AI-калькулятора для бюджетування:** Міжнародні банки розвитку повинні створити репозиторії даних завершених проєктів і використовувати прогнозний ШІ для оцінки бюджетів, що допоможе виявляти завищені пропозиції та підвищить прозорість у тендерах.

У заключній частині документ наголошує на необхідності адаптації до швидкої технологічної еволюції, яка одночасно створює можливості для прозорості та нові виклики, такі як кібератаки (ransomware), що в 2023 році принесли зловмисникам понад $1 млрд у криптовалютах. Потенційна конвергенція корупції та кіберзлочинності, наприклад, через встановлення підрядниками пристроїв для майбутнього шантажу в інфраструктурних об'єктах, вимагає попереджувальних заходів.

Автори закликають до подальших досліджень ризиків, пов'язаних із новими технологіями, і розробки політик для їх пом'якшення, підкреслюючи важливість TechSprints для співпраці між урядами, приватним сектором і громадянським суспільством.

Як незаконна вирубка в бразильській Амазонії живить ринки США та ЄС [9]



Звіт, опублікований Environmental Investigation Agency (EIA) у співпраці з CCCA, є детальним розслідуванням незаконних практик вирубки лісів у штаті Пара, найбільшому регіоні Бразилії з виробництва деревини в Амазонії. Документ розкриває складні схеми видобутку цінних порід деревини, таких як іпе та кумару, без належних дозволів, їх легалізацію через фальшиві документи та експорт на ринки США і Європейського Союзу, де ця деревина використовується для створення розкішних настилів, меблів та знакових громадських проєктів, таких як High Line Park у Нью-Йорку. Поєднуючи передові технології, свідчення інсайдерів та аналіз публічних даних, звіт викриває масштаби екологічної шкоди, системної корупції та глобальних ланцюжків постачання, які підтримують лісові злочини.

Дослідження зосереджується на штаті Пара, де, за оцінками, майже третина деревини, видобутої в Амазонії, є незаконною. Звіт підкреслює стрімке зростання площі незаконно вирубаних лісів: з 17 800 гектарів між 2021 і 2022 роками до 28 000 гектарів, що свідчить про поглиблення кризи, яка загрожує екосистемам, підживлює організовану злочинність та підриває верховенство права. EIA разом із CCCA застосували комплексну методологію, що включає аналіз великих даних, супутникові зображення від таких джерел, як Planet і Google Earth, та інструмент Normalized Difference Fraction Index (NDFI) для виявлення втрат лісового покриву. Ці дані доповнені інтерв'ю з офіційними особами, інсайдерами та юристами, а також публічними записами про вирубку лісів, штрафи та ембарго. Крім того, звіт спирається на внутрішні розслідування EIA, що включають фотографії, аудіо- та відеоматеріали, а також інформацію від партнерів.

У центрі звіту — п'ять детальних кейсів, які ілюструють витончені методи маскування незаконної вирубки. Один із прикладів показує, як деревина видобувається без дозволів, але легалізується через законні ділянки, звідки, згідно з офіційними документами, вона нібито транспортується. Інший кейс викриває ділянки, де супутникові зображення не показують жодних ознак вирубки, але деревина все одно реєструється як така, що походить із цих місць, що вказує на підробку документів. Третій випадок розкриває продовження експорту деревини з ділянок, на які накладено офіційні заборони через порушення. Четвертий кейс пов'язує вирубку з незаконним видобутком золота та штучним завищенням обсягів іпе для прикриття деревини, отриманої з

[9] https://eia.org/wp-content/uploads/2025/04/EIA_US_Brazil_Timber_Report_0325_FINAL_SPREADS.pdf

інших джерел. Особливо показовим є приклад ділянки Sitio Santo Antonio, де дозвіл на вирубку стверджував наявність 4,4 м³ іпе-амарело на гектар — значно більше за типові показники 0,2–0,5 м³/га, що свідчить про навмисну фальсифікацію для легалізації незаконно видобутої деревини. Ці кейси підкреслюють два основні методи «відмивання» деревини: реєстрація деревини з ділянок, де немає видимих ознак вирубки, та завищення обсягів із частково вирубаних ділянок для легалізації незаконно отриманої сировини.

Звіт простежує шлях цієї незаконної деревини від штату Пара до міжнародних ринків, демонструючи, як фальшиві документи дозволяють їй уникати перевірок і потрапляти в ланцюжки постачання США та ЄС. Бразильський іпе, відомий своєю міцністю, використовується для розкішних застосувань, але розслідування показує, що ці продукти часто пов'язані з екологічними та юридичними порушеннями. Розділ під назвою «Туман корупції» досліджує системні проблеми, які уможливлюють ці практики, включаючи хабарництво посадовців, підробку документів та слабке виконання заборон. Ця глибоко вкорінена корупція, разом із недостатнім наглядом, дозволяє незаконній деревині безперешкодно потрапляти в глобальні торговельні мережі.

Документ завершується закликом до термінових дій, наголошуючи на необхідності посилення міжнародних і національних регулювань для боротьби з лісовими злочинами. Він пропонує запровадити суворіші аудити ланцюжків постачання, використовувати технології, такі як супутниковий моніторинг, для перевірки походження деревини, а також застосовувати санкції до компаній, причетних до незаконної торгівлі. Рекомендації включають поглиблення співпраці між Бразилією, США та ЄС для вдосконалення механізмів правозастосування, таких як Бразильський лісовий кодекс і Регламент ЄС щодо деревини (EUTR), а також покращення систем сертифікації деревини для забезпечення прозорості.

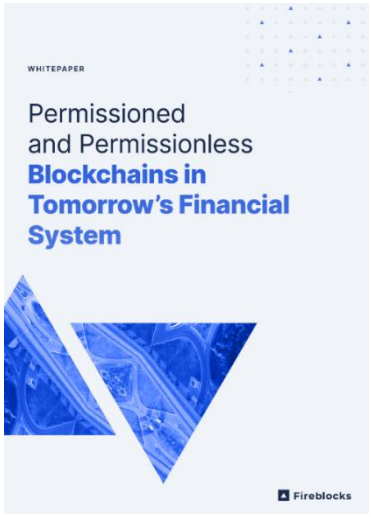
Висновки:

- **Посилення моніторингу ланцюжків постачання:** США та ЄС повинні запровадити обов'язкові перевірки походження деревини з використанням супутникових зображень і технологій, таких як NDFI, для виявлення фіктивних документів. Імпортери мають вимагати сертифікати, підтверджені незалежними аудиторами.
- **Санкції проти порушників:** Впровадити цільові санкції проти бразильських компаній, причетних до «відмивання» деревини, та міжнародних покупців, які свідомо чи несвідомо купують незаконну деревину, включаючи штрафи та заборону на імпорт.
- **Міжнародна співпраця:** Бразилія, США та ЄС мають створити спільну робочу групу для обміну даними про незаконну вирубку, координації розслідувань та вдосконалення механізмів правозастосування.
- **Технологічне вдосконалення:** Розширити використання супутникового моніторингу та великих даних у Бразилії для відстеження вирубки лісів у реальному часі, порівнюючи заявлені обсяги деревини з реальними даними.

Від закритих мереж до відкритої інфраструктури: як блокчейн змінює глобальне фінансування[10]

Документ є ґрунтовним аналітичним дослідженням, яке розкриває трансформацію фінансової системи під впливом блокчейн-технологій, з особливим акцентом на взаємодію між публічними (permissionless) та приватними (permissioned) мережами.

[10] https://richturrin.substack.com/api/v1/file/b08b2ba5-e273-40cb-8171-85d3902ee53b.pdf



Починаючи з огляду історичної еволюції блокчейну — від запуску біткоїна у 2009 році до сучасних децентралізованих платформ із високим рівнем масштабованості, документ демонструє, як permissionless-мережі (Bitcoin, Ethereum, Solana, Polygon та інші) стали каталізаторами розвитку інноваційних фінансових сервісів, таких як DeFi, NFT, DAO та токенізація активів. При цьому підкреслюється, що попри потужні переваги відкритих блокчейнів — прозорість, відсутність цензури, глобальна доступність та децентралізація — вони створюють серйозні виклики для фінансових установ: зокрема, у сферах контролю, конфіденційності, відповідності вимогам регуляторів та управління ризиками. Через це традиційні фінансові інститути, включно з центральними банками, переважно віддають перевагу permissioned-блокчейнам, які забезпечують закриту архітектуру, чітке управління доступом, контроль за транзакціями, можливість модифікації або видалення даних, що критично важливо в контексті законодавств типу GDPR або Basel III.

Автори документа пропонують не обирати між двома моделями, а формувати симбіотичну екосистему, в якій публічні та приватні мережі співіснують і взаємодіють. Така модель дозволяє використовувати permissioned-блокчейни для первинних фінансових ринків (емісія активів, управління ними, KYC/AML), а permissionless — для вторинних ринків, де важливими є прозорість, ліквідність та відкритий доступ.

Висновки:

- **Фінансові установи повинні впроваджувати гібридну блокчейн-архітектуру:** permissioned-блокчейни мають використовуватись для контролю, управління ризиками, KYC/AML, а permissionless — для масштабування, ліквідності та залучення глобальних користувачів.

  Рекомендація: розробити внутрішню стратегію переходу до гібридної інфраструктури з чітким поділом зон відповідальності та типів активів.

- **Інтероперабельність має стати пріоритетом при проєктуванні цифрових фінансових систем:** механічне переміщення токенів без збереження функціональності є недостатнім — потрібна повна програмна компоновка (composability).

- **Рекомендація:** інтегрувати міжмережеві протоколи (Axelar, Chainlink CCIP, LayerZero) у свої платформи та оцінити їхню сумісність з EVM.

- **RegTech і інструменти комплансу потребують оновлення для роботи з permissionless-блокчейнами:** поточне регулювання (наприклад, GDPR, DORA, SAB121) недостатньо адаптоване до особливостей публічних реєстрів.

  Рекомендація: використовувати zero-knowledge докази, псевдоанонімізацію, інтеграцію з KYC-рішеннями та розробити процедури відповідності до нових моделей ризиків.

- **Токенізація активів — не майбутнє, а теперішній тренд, який слід масштабувати:** більшість провідних банків та фінансових груп вже реалізували попередні апробації з токенізації фондів, облігацій, стейблкоїнів.

- **Рекомендація:** розпочати із MVP для окремого фінансового активу (фонду, облігації або платіжного токена) із чіткою схемою дистрибуції через permissioned-платформи та подальшою інтеграцією в permissionless-мережі.

Окреме місце у документі займає питання інтероперабельності — здатності мереж комунікувати між собою на рівні логіки, активів та смарт-контрактів. Звіт демонструє, що поточні рішення (мости, кросчейн-меседжінг) є недостатніми і пропонує концепцію «композабельності» — повної програмної взаємодії між блокчейнами, яка дозволяє створювати комплексні фінансові продукти, що охоплюють кілька мереж одночасно. У цьому контексті ключову роль відіграють протоколи типу Axelar, Chainlink CCIP, LayerZero, Ownera, які забезпечують надійне, безпечне та масштабоване міжмережеве з'єднання. Значна частина документа присвячена кейсам реального використання блокчейнів у фінансовому секторі — від запуску цифрового фонду BlackRock на Ethereum, стейблкоїн-платформи HSBC на Hyperledger Besu, токенізованих облігацій ABN AMRO на Stellar до проєкту Project Mariana, який демонструє міжнародну координацію між центральними банками щодо кроскордонних транзакцій із використанням CBDC. Автори висвітлюють також технічні особливості — роль EVM як стандарту, який домінує у проєктах з токенізації, та зростаючу популярність мульти-чейнової розробки серед розробників (87% використовують хоча б одну EVM-сумісну мережу).

Загалом, документ наголошує, що майбутнє фінансової інфраструктури неможливе без комплексної інтеграції permissionless і permissioned систем, і саме на цій точці перетину — з урахуванням вимог до контролю, регуляторної відповідності, прозорості, масштабованості й програмованості — формується нова парадигма цифрових фінансів.

SEPA Instant у дії: як миттєві платежі змінюють фінансову інфраструктуру Європи [11]

Документ є комплексним аналітичним гідом, орієнтованим на бізнес, фінтех-компанії та розробників, які прагнуть інтегрувати миттєві платежі у рамках зони SEPA за допомогою SCT Inst (SEPA Instant Credit Transfer). У фокусі документа — як регуляторний, так і операційно-технічний контекст, що охоплює впровадження нових платіжних практик у відповідності до європейського законодавства, включно з Регламентом ЄС щодо обов'язкової підтримки SEPA Instant.

Автори підкреслюють, що SCT Inst є надзвичайно перспективним інструментом, який забезпечує переказ коштів у межах 10 секунд, 24 години на добу, 365 днів на рік, за фіксованих умов, передбачених схемою Європейської платіжної ради. Документ надає глибокий огляд сучасного стану інфраструктури: платіжні системи RT1 від EBA Clearing та TIPS від Європейського центрального банку виступають основними механізмами здійснення платежів для миттєвих транзакцій у євро.

У звіті детально розглянуто варіанти підключення бізнесу до SEPA Instant — через пряме підключення до RT1/TIPS, через банків-партнерів або через технологічних провайдерів, таких як Numeral. Пояснюється роль BIC (Bank Identifier Code) для участі в системі, важливість налаштування повідомлень ISO 20022 та наявності шлюзу до національного чи європейського клірингового механізму. Особлива увага приділена практичним кейсам використання SEPA

[11] https://25739848.fs1.hubspotusercontent-eu1.net/hubfs/25739848/Guides/Numeral%20Guide%20to%20SEPA%20Instant%20Credit%20Transfer.pdf?utm_campaign=Indirect%20SEPA%20Guide&utm_medium=email&_hsmi=75009302&utm_content=75009302&utm_source=hs_automation

Instant у комерційній діяльності: миттєва виплата зарплат працівникам, компенсації водіям і кур'єрам у гіг-економіці, виплати постачальникам, розрахунки між компаніями на маркетплейсах.

Документ містить ринкову аналітику: зокрема, наголошується на тому, що лише 11% SEPA-переказів у 2022 році були миттєвими, однак очікується суттєве зростання цього показника завдяки новим регуляторним вимогам та підтримці з боку провідних європейських банків. Також акцент зроблено на важливості API як зручного інструменту інтеграції, що дозволяє скоротити час виходу на ринок і уникнути складнощів прямого підключення до банківських систем. Компанія Numeral позиціонує себе як провайдера з прозорим API, повною документацією та підтримкою, що робить її привабливим вибором для компаній, які хочуть швидко та ефективно реалізувати SEPA Instant у своїх продуктах. У документі також наведено порівняння витрат, часових рамок впровадження, складності інтеграції та можливих сценаріїв використання.

Окремо представлено посилання на джерела, які дозволяють отримати додаткову інформацію про ринок миттєвих платежів, серед яких дані SWIFT, Deloitte, PwC та Європейської комісії. Таким чином, цей гід є водночас методологічним посібником, стратегічним орієнтиром і технічним мануалом для будь-якого бізнесу, що прагне вийти на європейський платіжний ринок із сучасним, відповідним до регуляторних вимог, фінансовим рішенням.

Висновки:

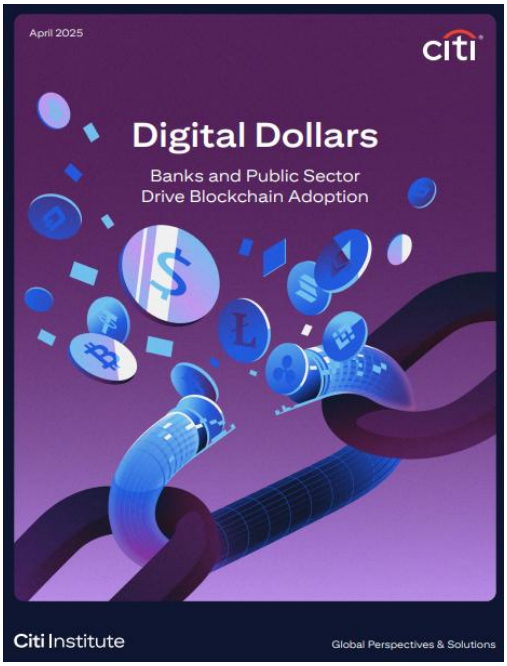
- **Ринок SEPA Instant буде обов'язковим:** Європейське законодавство вводить обов'язковість підтримки SCT Inst для банків, що створює нове середовище, у якому всі учасники повинні адаптуватися до 24/7 платежів. Українським платіжним установам варто вже зараз адаптувати процеси під цю модель.
- **Інтеграція через API спрощує впровадження:** Використання сучасних API-рішень (як у Numeral) дозволяє уникнути складної інфраструктурної інтеграції з банками та пришвидшує вихід на ринок.
- **Миттєві платежі — ключ до гіг-економіки та маркетплейсів:** SCT Inst особливо важливий для сегментів, де швидкість переказу критична — зарплати фрілансерам, виплати постачальникам, гейміфіковані сервіси тощо.
- **Вибір правильного маршруту підключення критично важливий:** Організації мають обрати між прямим доступом до RT1/TIPS, підключенням через банк або використанням провайдера (BaaS/TPP), залежно від обсягів, типу діяльності та наявних технічних ресурсів.

Блокчейн у дії: як банки та держави формують нову архітектуру цифрових фінансів [12]

Звіт Citigroup є масштабним дослідженням, що охоплює трансформаційний потенціал блокчейн-технологій та стейблкоїнів у фінансовому та державному секторі. У центрі аналізу — оцінка чинників, які сприяють активнішому залученню банків і держав до цифрових фінансів, зокрема через стейблкоїни, децентралізовану інфраструктуру обліку, токенізацію активів і цифрову ідентичність. Автори розглядають 2025 рік як потенційний переломний момент — «ChatGPT-момент» — для масового прийняття блокчейну у державному управлінні та фінансах. Основними драйверами виступають зростання попиту на прозорість і підзвітність, розвиток

[12] https://www.citigroup.com/rcs/citigpa/storage/public/GPS_Report_Blockchain_Digital_Dollar.pdf

законодавства в США та ЄС (зокрема регулювання MiCA), технологічна зрілість стейблкоїнів і участь великих фінансових установ, включно з центральними банками та багатосторонніми організаціями.



Документ детально розкриває механіку роботи стейблкоїнів, акцентуючи на їхньому зв'язку з резервами в доларах США та короткострокових держоблігаціях, що зумовлює їхню роль як нового джерела попиту на державний борг. Прогнозується, що до 2030 року ринок стейблкоїнів може досягти $1,6 трлн у базовому сценарії і до $3,7 трлн у оптимістичному, при цьому близько 90% обсягу залишатиметься деномінованим у доларах США. Одночасно документ аналізує ризики: геополітичне протистояння, небезпеку девальвації прив'язки (de-pegging), надмірну концентрацію ринку, ризики використання для відмивання коштів і системні загрози через недовіру до забезпечення резервів.

Увага також приділена порівнянню стейблкоїнів із CBDC (цифровими валютами центральних банків), зазначаючи відмінності у моделі управління, ризиках, механізмах використання та регуляторному статусі. У звіті окреслено, що держави дедалі частіше розглядають блокчейн як інструмент модернізації державних послуг, зокрема в сфері фінансів, управління реєстрами, розподілу субсидій, гуманітарної допомоги, токенізації боргових зобов'язань та запровадження цифрової ідентичності. Як приклад ефективного застосування технології у державному секторі, наводиться досвід Естонії, яка застосовує KSI-блокчейн як додатковий рівень захисту довіри до своїх інформаційних систем. Крім того, Світовий банк у співпраці з EY реалізує проєкт FundsChain, що забезпечує прозору трасування витрат і використання міжнародних коштів у пілотних проєктах у Молдові, Кенії, Бангладеш тощо.

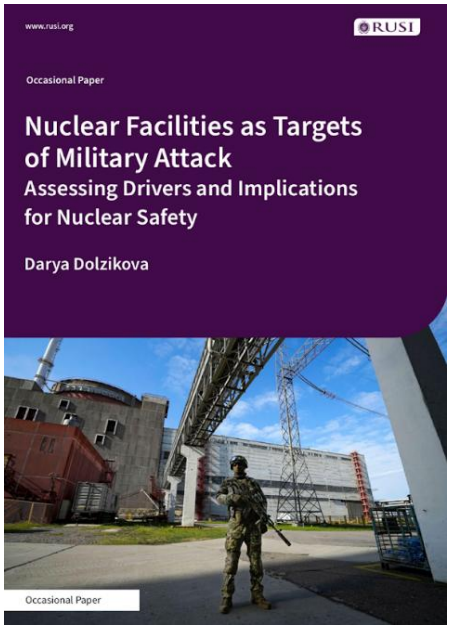
Висновки:

- **Розробка законодавства щодо стейблкоїнів є критичним фактором масштабного впровадження.** США та ЄС повинні створити чіткі законодавчі рамки, які легітимізують стейблкоїни як інструмент цифрової економіки. Україні доцільно ініціювати аналогічний нормативний процес з урахуванням MICA та американських стандартів.
- **Блокчейн-технології можуть суттєво зменшити рівень шахрайства та неефективності в публічному секторі.** Доцільно впроваджувати блокчейн у сферах субсидій, реєстрів, гуманітарної допомоги та токенізації публічних активів. Україна могла б використати досвід Естонії, Грузії та Світового банку для запуску експерементальних цифрових ініціатив.
- **Стейблкоїни створюють нові можливості для банків, але також несуть ризики відтоку депозитів.** Банкам слід проактивно інтегруватися у стейблкоїнову інфраструктуру через кастодіальні послуги, випуск токенів, платіжні рішення та управління ліквідністю. Національний банк України має оцінити макрофінансові наслідки таких інновацій.
- **Національна стратегія цифрової політики має включати блокчейн як інструмент підзвітності.** Уряди, зокрема України, повинні створити посади «цифрових уповноважених», які координуватимуть розвиток цифрової ідентичності, реєстрів, фінансових технологій і кібербезпеки з урахуванням можливостей DLT.

Звіт містить аналітику щодо токенізації активів і перспектив використання смарт-контрактів для автоматизації та скорочення посередників, що має особливу актуальність для державних інституцій. Розглянуто потенціал цифрової ідентичності, як-от приклад Швейцарії та Бразилії, де цифрові ID на базі блокчейну сприяють безпечному зберіганню та захисту персональних даних. Автори також підкреслюють потребу в гармонізації міжнародних стандартів, забезпеченні сумісності рішень, розбудові довіри серед користувачів і створенні нормативної бази, яка враховує специфіку децентралізованих технологій.

Загалом, звіт пропонує всебічне бачення того, як блокчейн та стейблкоїни можуть змінити підходи до управління державними фінансами, прискорити інновації у банківському секторі та стати основою для нової ери цифрової довіри в економіках, що розвиваються, та розвинених країнах. У документі послідовно демонструється, що успіх цифрової трансформації залежить не лише від технологій, а й від політичної волі, стратегічного бачення, співпраці між державними і приватними суб'єктами, а також здатності створити інклюзивну, захищену та прозору цифрову екосистему.

Воєнна загроза для ядерної інфраструктури: логіка атак, наслідки та шляхи мінімізації ризиків[13]



Аналітичний документ, підготовлений RUSI, є однією з найбільш системних та ґрунтовних спроб дослідити логіку і наслідки використання військової сили проти ядерної інфраструктури в умовах сучасних збройних конфліктів. Центральною відправною точкою дослідження стало повномасштабне вторгнення Російської Федерації в Україну та її військова окупація Запорізької атомної електростанції (ЗАЕС), що стало безпрецедентним прикладом захоплення діючої АЕС під час активної фази війни. Разом з тим, у документі підкреслюється, що загроза нападу на ядерні об'єкти не є новим явищем — приклади таких дій простежуються ще з часів Другої світової війни, а їх кількість та складність зростають на фоні ерозії норм ядерного нерозповсюдження та поширення ядерної енергетики як елемента «зеленої трансформації».

Документ ґрунтується на аналізі великої кількості історичних кейсів — від ударів по іракських, іранських та сирійських ядерних об'єктах до військових планів щодо ядерної інфраструктури Північної Кореї, Японії чи Ізраїлю — а також на результатах польових досліджень в Україні у 2024 році, включно з інтерв'ю з енергетиками, військовими, експертами з ядерної безпеки та парламентарями. У фокусі роботи — спроба відповісти на запитання: чому держави вирішують атакувати або загрожувати атаками на ядерні об'єкти; які наслідки це має для безпеки, довкілля, політичної стабільності; та як можна зменшити ці ризики.

У документі виокремлено п'ять ключових типів стратегічної та оперативної логіки, яка може лежати в основі рішень про застосування сили щодо ядерних об'єктів: контрпроліферація (зупинка або затримка розвитку ядерної програми супротивника), енергетичне виснаження (виведення з ладу джерел енергії), зональне стримування або заборона доступу (через створення забрудненої території), ескалація та примус (використання загроз як інструменту політичного тиску), а також тактичне проходження території, де розташовані ядерні об'єкти, без

[13] https://static.rusi.org/nuclear-facilities-as-targets-of-military-attack.pdf

цільового їх ураження. Кожен із цих типів розглянуто в історичному контексті, з прикладами, ризиками та правовими оцінками.

Особливу увагу приділено аналізу наслідків вивільнення ядерних матеріалів — як радіологічних, так і хімічно-токсичних. Детально розглядаються ризики, пов'язані з різними типами об'єктів паливного циклу — від збагачувальних заводів до сховищ відпрацьованого палива. Авторка пояснює, що ступінь шкоди залежить не лише від характеру об'єкта, а й від метеоумов, щільності населення, рівня готовності аварійних служб та поведінки населення. Окремо досліджуються психологічні ефекти загрози радіаційного зараження, які часто перевищують фактичні ризики для здоров'я, спричиняючи масову тривогу, евакуації, соціальну дестабілізацію та навіть другорядні людські втрати (зокрема серед вразливих груп під час евакуацій), як це було у випадках Чорнобиля, Фукусіми та Гоянії.

Документ також включає аналіз нормативно-правового поля. Окреслено, що чинне міжнародне гуманітарне право (зокрема додаткові протоколи до Женевських конвенцій) загалом забороняє атаки на цивільну інфраструктуру, зокрема об'єкти, які містять «небезпечні сили». Водночас подвійне (dual-use) призначення багатьох ядерних об'єктів, складність визначення «військової необхідності», а також політична воля окремих держав залишають поле для інтерпретацій. Різноманітні резолюції МАГАТЕ та ООН, хоча й фіксують засудження атак на АЕС, не мають зобов'язуючої сили. Авторка стверджує, що відсутність нових заборон — це результат свідомої політики окремих держав збереження опції воєнного удару по ядерній інфраструктурі як одного з інструментів стримування або тиску.

У практичному вимірі робота містить рекомендації щодо чотирьох основних напрямів зниження ризиків. По-перше, це — посилення дотримання і деталізація існуючих норм міжнародного права, включаючи розробку оперативних інструкцій для збройних сил щодо дій біля ядерних об'єктів. По-друге — інженерно-фізичне підсилення захисту, з урахуванням ресурсних

Висновки:

- **Контрпроліферaційні удари залишаються політично привабливими, але стратегічно сумнівними:** військові атаки на ядерні об'єкти рідко повністю зупиняють ядерні програми, проте можуть слугувати засобом політичного сигналу.

  Рекомендація: на міжурядовому рівні розробити чіткі критерії оцінки ефективності та допустимості таких дій, враховуючи гуманітарні наслідки.

- **Зростає ризик «опосередкованих» атак — на допоміжну інфраструктуру:** у майбутньому об'єктами ураження можуть ставати водозабори, енергоживлення, логістика, що критичні для безпечної роботи АЕС, без прямого ураження реактора.

  Рекомендація: модернізувати концепцію безпеки, інтегрувавши захист допоміжних систем в інженерне та охоронне проєктування.

- **Психологічний ефект радіаційної загрози використовується як засіб тиску:** паніка, спричинена навіть загрозою атаки на ядерний об'єкт, може мати стратегічну цінність для агресора.

  Рекомендація: впроваджувати заздалегідь підготовлені та довірені кризові комунікаційні протоколи, аби уникати дестабілізації та масової тривожності

- **Системний захист ядерної інфраструктури потребує децентралізації та міжсекторальної взаємодії:** ризики зменшуються через розосередження об'єктів (зокрема перехід до SMR — малих модульних реакторів) та підвищення суспільної стійкості (resilience).

  Рекомендація: проводити стрес-тести суспільної готовності та інвестувати у цивільні й військові CBRN-можливості.

обмежень і можливого зворотного ефекту від мілітаризації. По-третє — створення інституційної та технічної надлишковості і розосередженості, зокрема шляхом переходу до малих модульних реакторів, що зменшують привабливість об'єкта як стратегічної цілі. І, нарешті, розвиток загальносуспільної стійкості: впровадження програм підвищення обізнаності, підготовки громадськості до надзвичайних ситуацій, формування довіри до офіційної комунікації та боротьба з дезінформацією.

Загалом, цей звіт є не лише глибоким теоретичним і прикладним дослідженням, а й потужним закликом до переосмислення системи глобальної безпеки навколо ядерної інфраструктури в умовах епохи зростаючих загроз, збройних конфліктів і ерозії міжнародного права. Його значущість для України є особливо високою, з огляду на безпрецедентний ризик, створений окупацією ЗАЕС, і потребу в розробці національної політики безпеки АЕС, з урахуванням викликів гібридної та конвенційної війни.

ВНУП

Індивідуальний підхід до ПВК/ФТ для ВНУП та VASP: як збудувати ефективну систему управління ризиками[14]

Документ є комплексним аналітичним оглядом стратегій зменшення ризиків відмивання коштів (ВК) для визначених нефінансових установ і професій (ВНУП) та постачальників послуг з віртуальними активами (VASPs). Він надає детальне роз'яснення ключових загроз, пов'язаних із використанням цих суб'єктів для легалізації злочинних доходів, а також практичні інструкції щодо впровадження ефективних програм протидії відмиванню коштів і фінансуванню тероризму (ПВК/ФТ). На початку документа викладено загальне розуміння феномену ВК — зокрема, пояснено три основні стадії процесу: розміщення, розшарування (або «layering») та інтеграція. Докладно описано, яким чином кошти, отримані злочинним шляхом, можуть проникати в легальну фінансову систему через ВНУП та VASPs — з огляду на слабший регуляторний нагляд, відсутність належної підготовки персоналу та обмежений доступ до інструментів верифікації клієнтів.

Особливу увагу приділено ролі ВНУП, які включають юристів, бухгалтерів, рієлторів, торговців коштовностями та трастових/корпоративних постачальників послуг. Пояснюється, що ці суб'єкти вразливі до зловживань через нерегульований характер своєї діяльності, мультиюрисдикційні зв'язки та взаємодію з клієнтами з юрисдикцій, що перебувають у сірому або чорному списку FATF. Також підкреслюється, що більшість з них мають недостатню обізнаність щодо процедур належної перевірки клієнтів (CDD/EDD), що ускладнює виявлення високоризикових операцій і клієнтів. Для ілюстрації наведено приклад схеми, за якою відмивання коштів може відбуватися через купівлю-продаж дорогоцінного каміння, що дозволяє легко переміщати цінності через кордони без слідів походження.

У другій частині документа акцент зроблено на VASPs — суб'єктах, які обслуговують операції з віртуальними активами (наприклад, криптовалюти). Пояснюється, що їх діяльність пов'язана з надзвичайно високими ризиками ВК/ФТ у зв'язку з притаманною анонімністю транзакцій,

[14] https://rapidaml.com/wp-content/uploads/2024/08/Money-Laundering-Risk-Mitigation-Strategy-for-DNFBPs-and-VASPs-1.pdf

легкістю створення децентралізованих платформ, відсутністю вимог до ідентифікації сторін та поширеним використанням технологій для приховування слідів (наприклад, міксерів і тамблерів). Значну загрозу становить і незнання або ігнорування правил FATF, таких як «Travel Rule», що вимагає передачі ідентифікаційної інформації про відправника й отримувача транзакцій.

Центральне місце в документі займає розкриття концепції підходу, заснованого на оцінці ризиків (Ризик-орієнтований підхід, РОП), яка є обов'язковою вимогою для ВНУП і VASPs згідно з рекомендаціями FATF та законодавством ОАЕ. Документ докладно описує, як цей підхід дозволяє адаптувати політики та контрольні механізми відповідно до рівня ризику конкретного клієнта, транзакції або виду діяльності. Наголошується, що універсальна модель ПВК не може ефективно працювати, оскільки кожен суб'єкт має різну структуру клієнтської бази, географію діяльності, бізнес-модель та канали доставки. Правильно реалізована модель РОП передбачає проведення ризик-профілювання клієнтів, визначення рівнів ризику, застосування відповідних процедур CDD або EDD та ведення прозорої документації всього процесу.

Окремий розділ присвячений структурі ефективної ПВК-програми для ВНУП та VASPs. Для ВНУП наголошується на потребі чіткого процесу перевірки клієнтів, моніторингу транзакцій та поглибленої перевірки у випадках високого ризику, із залученням вищого керівництва до ухвалення рішень про співпрацю з такими клієнтами. Для VASPs запропоновано спеціалізовані інструменти цифрової верифікації, включно з розпізнаванням обличчя, перевіркою IP-адрес і верифікацією гаманців, що дозволяє підвищити точність клієнтської ідентифікації. Зазначено, що VASPs повинні формалізувати взаємодію з регулятором, надсилати повідомлення про підозрілі транзакції через ПФР (через goAML), і впроваджувати інструменти постійного моніторингу поведінки клієнтів.

Завершальна частина документа описує вимоги до побудови стійкої системи AML-комплаєнсу, де ключову роль відіграє внутрішня культура, навчання персоналу, ефективна система звітності, використання автоматизованих рішень для моніторингу та управління ризиками, а також належна організація ведення обліку. Підкреслено, що без активної участі керівництва, створення відповідального відділу з комплаєнсу та залучення персоналу до процесів виявлення підозрілих дій, ефективність програми буде низькою.

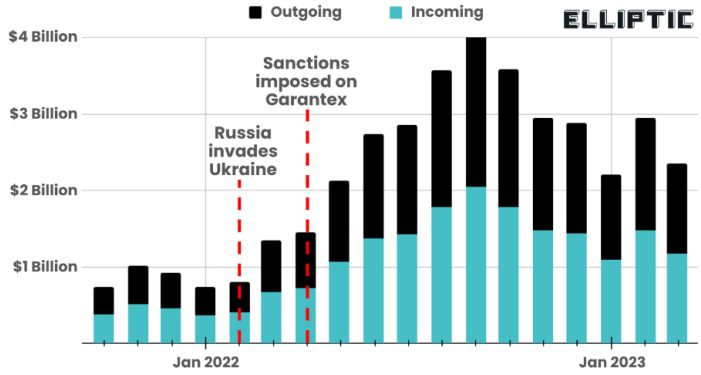
У підсумку автори наголошують, що ВНУП і VASPs не просто мають обов'язок дотримуватися формальних процедур, але повинні стратегічно підходити до аналізу своїх ризиків, розуміти динаміку регуляторного середовища та проактивно впроваджувати технології, що дозволяють знижувати ймовірність використання їх у схемах ВК/ФТ.

Висновки:

- **ВНУП і VASPs є особливо вразливими до зловживання з боку злочинців,** і їм необхідно впровадити ризик-орієнтовані заходи контролю, що враховують специфіку бізнес-моделі, географії та типів клієнтів.
- **Один підхід для всіх у питаннях ПВК не працює:** програма ПВК/ФТ має бути індивідуалізована з урахуванням типу послуг, структури транзакцій, рівня ризику клієнтів та регуляторного середовища.
- **VASPs повинні забезпечити верифікацію цифрової ідентичності клієнтів,** впровадити Travel Rule, моніторинг гаманців, IP-адрес та транзакційних аномалій, що відповідає вимогам FATF і дозволяє знижувати ризики анонімності.
- **Ефективна система ПВК/ФТ включає не лише технічні рішення, а й культуру комплаєнсу:** керівництво має бути залучене до формування політик, а персонал — проходити постійне навчання та звітувати про підозрілі дії.

Інші новини

Elliptic у дії: Розкриття Garantex [15]



Cryptocurrency transactions through Garantex surged following sanctions against the exchange, imposed by the U.S. Treasury.

У березні 2025 року компанія Elliptic оприлюднила результати масштабного розслідування діяльності російської криптовалютної біржі Garantex, яка, незважаючи на санкції OFAC, продовжувала активно функціонувати як платформа для відмивання коштів, фінансування тероризму та ухилення від санкцій. Завдяки використанню передових аналітичних інструментів, Elliptic змогла ідентифікувати понад $60 мільярдів транзакцій, здійснених через Garantex після введення санкцій у 2022 році, що свідчить про масштаб порушень та ефективність застосованих методів приховування діяльності.

Garantex, на яку були накладені санкції OFAC у квітні 2022 року за участь у відмиванні коштів, пов'язаних із даркнет-ринками та кіберзлочинними угрупованнями, зокрема російськими олігархами, продовжувала обслуговувати клієнтів, використовуючи складні методи маскування своєї присутності в блокчейні. Elliptic розробила власні технології для виявлення гаманців, контрольованих Garantex, що дозволило надати цінну інформацію слідчим органам та користувачам інструментів перевірки санкцій.

Розслідування Elliptic виявило, що Garantex активно використовувалася для відмивання коштів, отриманих від різних злочинних джерел. Зокрема, було встановлено, що понад $30 мільйонів, викрадених хакерською групою Lazarus Group з Північної Кореї під час зламу Horizon Bridge, були переказані через Garantex у лютому 2023 року. Крім того, біржа обслуговувала транзакції, пов'язані з різними програмами-вимагачами, такими як Conti, Lockbit та Black Basta, а також з даркнет-ринками, включаючи Blacksprut, Solaris, Mega та OMG!OMG!.

Завдяки співпраці з Elliptic, Секретна служба США змогла заморозити криптоактиви на суму $26 мільйонів, що належали Garantex, та провести подальші дії щодо припинення її діяльності. Цей випадок підкреслює важливість використання передових аналітичних інструментів для виявлення та протидії фінансовим злочинам у сфері криптовалют.

Для загального розвитку

Фінансування тероризму та некомерційний сектор[16]

Стаття, присвячена оновленій Рекомендації 8 FATF, є ґрунтовним аналізом еволюції підходів до запобігання зловживанню неприбутковими організаціями (НПО) з метою фінансування тероризму, вказуючи як на причини її неодноразового перегляду, так і на фундаментальні зміни, ухвалені в листопаді 2023 року. Автори аргументовано пояснюють, чому саме Рекомендація 8 посіла особливе місце серед стандартів FATF, демонструючи її трансформацію з інструменту, що часто застосовувався у спосіб, непропорційний реальним ризикам, до інструменту, в основі якого чітко закладено принципи фокусування, пропорційності та ризик-орієнтованості.

[15] https://www.elliptic.co/blog/elliptic-in-action-garantex?li_fat_id=7f6321a8-7401-46fd-a5ae-52ea6ff2d04b
[16] https://www.global-amlcft.eu/terror-financing-fatf-rec-8/?cn-reloaded=1

Перший розділ статті підкреслює, що Рекомендація 8 виникла у відповідь на практику використання терористичними угрупованнями, зокрема Аль-Каїдою, неприбуткових структур для акумуляції та перерозподілу коштів. Однак надмірна увага до сектора НПО як такого призвела до поширеної хибної практики – визнання всього сектору як "особливо вразливого", що спричинило хвилю надмірного регулювання та обмеження доступу до фінансових послуг. Зокрема, у низці держав це створило підґрунтя для зловживань, коли рекомендація використовувалася для обмеження діяльності правозахисних організацій під прикриттям заходів протидії фінансуванню тероризму.

В оновленій редакції FATF, як визнає стаття, вперше чітко артикулює як добрі, так і погані практики, включаючи ті, що прямо суперечать її намірам. Центральним меседжем документу стало твердження, що заходи в межах Рекомендації 8 повинні бути зосередженими, пропорційними та ризик-орієнтованими. Більше того, вони не повинні «надмірно перешкоджати або стримувати легітимну діяльність НПО», інакше такі заходи не вважаються відповідними Рекомендації.

Окрема увага в тексті приділяється докладному поясненню, що НПО не є суб’єктами фінансового моніторингу у класичному розумінні — на відміну від фінансових установ і ВНУП. Тому вимоги щодо належної перевірки клієнтів (customer due diligence) не можуть автоматично поширюватися на НПО. Замість цього держава має реалізовувати підхід «нагляду і моніторингу», а не «нагляду і контролю», що є принципово відмінним за своєю суттю. Такий підхід спрямований на превенцію та підтримку, а не на покарання.

Автори статті також наголошують на важливості дотримання міжнародного права та прав людини у впровадженні заходів протидії ФТ, зокрема в контексті гуманітарного винятку, закріпленого в Резолюції Ради Безпеки ООН 2664 (2022) та продовженого через 2671 (2024). Це означає, що гуманітарна діяльність, навіть якщо передбачає обіг коштів, не повинна вважатися порушенням санкційних режимів, якщо здійснюється згідно з умовами винятку. У цьому контексті оновлена Рекомендація 8 підкреслює, що заходи, які перешкоджають такій діяльності, прямо суперечать її положенням.

Не менш важливою є ідея тристороннього співробітництва, де держава, фінансовий сектор і самі НПО мають співпрацювати у питаннях оцінки ризиків та формування заходів у сфері ПВК/ФТ. Це визнає важливість досвіду та контекстуальної експертизи самих НПО у виявленні вразливостей та побудові дієвих стратегій захисту.

Підсумовуючи, стаття є вичерпним і чітко структурованим викладом сутності та практичної спрямованості оновленої Рекомендації 8 FATF. Вона демонструє важливий зсув у парадигмі регулювання — від обтяжливого, однозначного нагляду до підходу, який враховує різнорідність сектора, реальний рівень загроз та необхідність забезпечення простору для легітимної громадської активності. Очевидно, що така трансформація має значний вплив як на політику, так і на майбутню ефективність взаємних оцінок держав.

Ваша думка важлива!

1. Як балансувати між свободою діяльності благодійних організацій та необхідністю посиленого контролю задля запобігання їх використання у схемах ФТ?
2. Наскільки ефективно система фінансового моніторингу України інтегрує ВНУП у національну модель протидії відмиванню коштів, і які інституційні прогалини ще залишаються?
3. Чи достатньо уваги приділяється в Україні нагляду за ВНУП, такими як адвокати та податкові консультанти, у контексті протидії ВК/ФТ?
4. Як Україна може збалансувати впровадження біометричних технологій у правоохоронній діяльності з необхідністю захисту особистих даних громадян, враховуючи виклики воєнного часу та обмежені ресурси?
5. Які заходи може вжити Україна для захисту вразливих груп населення, таких як, наприклад, біженці, від експлуатації в схемах шахрайства у сфері азартних ігор, і як це може вплинути на розвиток легального грального ринку?
6. Як забезпечити захист викривачів корупції у контексті політичного тиску та слабкої правової системи?
7. Як Україна може посилити свою роль у міжнародних ініціативах боротьби з незаконною вирубкою лісів, враховуючи власні проблеми з нелегальним лісозаготівлею в Карпатах та зростаючий експорт деревини до ЄС?
8. Як Україна, в умовах воєнного стану та післявоєнної відбудови, може використати гібридну блокчейн-архітектуру для створення прозорої фінансової системи та залучення міжнародних інвесторів?
9. Яку роль має відігравати Національний банк України та Міністерство фінансів України у створенні нормативної та технологічної інфраструктури для масштабного впровадження блокчейну у державному управлінні?

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-2025-18

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

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