Методологічний бюлетень

Серійний номер: МінФін-AML-2025-44

Жовтень 2025

“Роби все, що в твоїх силах. Більше не може зробити ніхто”

Джон Вуден

Мета

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

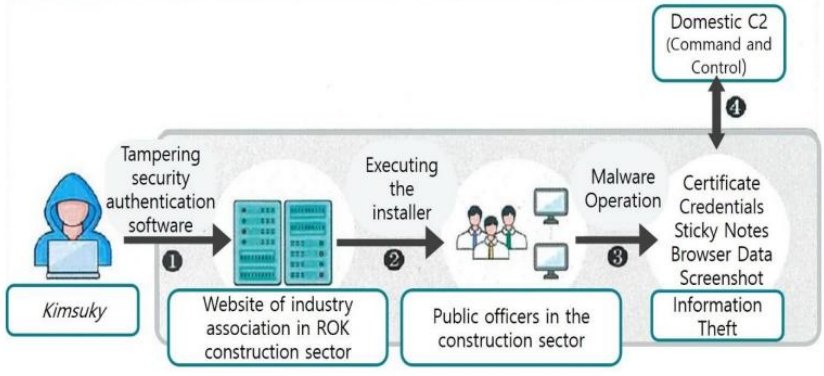
Містить актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

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

Звіти міжнародних організацій та окремих юрисдикцій

Порушення та ухилення КНДР від санкцій ООН через діяльність працівників кібербезпеки та інформаційних технологій [1]

Figure 25: Kimsuky's Cyber Operations Against the ROK Construction Sector in January 2024



Source: MSMT Participating State

Даний документ є звітом Багатосторонньої групи з моніторингу санкцій (MSMT), який охоплює діяльність Корейської Народно-Демократичної Республіки (КНДР) з кіберзлочинності та використання IT-працівників для порушення та обходу санкцій ООН у період із січня 2024 року по вересень 2025 року.

[1] https://www.mofa.go.jp/files/100922718.pdf

Основний зміст документа полягає в детальному описі того, як КНДР систематично використовує свої кіберможливості та розгалужену мережу IT-працівників за кордоном для генерації значних доходів, які безпосередньо спрямовуються на фінансування її незаконних програм озброєнь масового знищення (ЗМЗ) та балістичних ракет, що є прямим порушенням відповідних резолюцій Ради Безпеки ООН (РБООН). Загальний обсяг викрадених КНДР криптовалют лише за звітний період (січень 2024 – вересень 2025) склав щонайменше 2,8 мільярда доларів США, включаючи крадіжку 1,46 мільярда доларів з криптобіржі Bybit у лютому 2025 року.

Кібероперації КНДР здійснюються під контролем і на користь структур, що перебувають під санкціями ООН, включаючи Генеральне розвідувальне бюро (RGB, KPe.031), Міністерство атомної енергетичної промисловості (MAEI, KPe.027), Департамент військової промисловості (MID, KPe.028) та Офіс 39 Робочої партії Кореї (КРПК). Ці організації використовують висококваліфіковані групи, такі як TraderTraitor (найбільш витончена), CryptoCore та Citrine Sleet. Зловмисники активно застосовують методи соціальної інженерії, часто видаючи себе за рекрутерів або бізнесменів, щоб обманом змусити жертв (особливо в криптоіндустрії) завантажити шкідливе програмне забезпечення (наприклад, використовуючи фальшиві тестові завдання або маніпулюючи інтерфейсами багатопідписних гаманців). Спостерігається значна тенденція до атак на ланцюги постачання, спрямованих на сторонніх постачальників послуг зберігання цифрових активів, що дозволяє отримати доступ до даних великих криптобірж. Крім того, кіберактивність включає використання програм-вимагачів (ransomware, наприклад, Andariel, Moonstone Sleet), іноді в співпраці з російськомовними кіберзлочинцями (як-от Qilin або Play ransomware). Представники КНДР також активно використовують інструменти штучного інтелекту (LLM-чатботи), щоб покращити якість фішингових повідомлень та прискорити розробку шкідливого коду.

Після успішної крадіжки фінансовий пріоритет КНДР зміщується на відмивання коштів та їхню конвертацію у фіатну валюту. Процес відмивання є складним і включає до дев'яти етапів: обмін викрадених токенів на ETH, BTC або стейблкоїни (USDT, USDC), використання міксерів (Tornado Cash, Wasabi Wallet) та крос-чейн мостів (THORChain, SWFT) для заплутування слідів, а потім конвертацію через позабіржових (OTC) брокерів. КНДР надзвичайно залежить від китайської фінансової інфраструктури та розташованих у Китаї посередників для цих операцій; відомо про використання щонайменше п’ятнадцяти китайських банків та ідентифіковано конкретних OTC-трейдерів (зокрема, У Хуейхуей (Wu Huihui), Є Діньжун (Ye Dinrong) та Чен Хун Мань (Cheng Hung Man)), які сприяють обходу санкцій та переведенню вкрадених активів у фіат. Окрім використання криптовалюти як засобу крадіжки, КНДР (зокрема, через KOMID/221 Генеральне бюро) використовує стейблкоїни (USDT) як форму прямого платежу для закупівель, пов'язаних із військовим обладнанням та сировиною, такою як мідь, що є ще одним способом обходу санкцій.

У частині IT-працівників, звіт констатує порушення резолюцій РБООН 2375 та 2397, які вимагають репатріації північнокорейських громадян, що отримують дохід за кордоном, та забороняють видачу нових дозволів на роботу. Більшість IT-працівників (1000–1500) базуються в Китаї, хоча значна кількість також знаходиться в Росії, а також у Лаосі, В’єтнамі та країнах Африки. IT-працівники КНДР є високооплачуваними (мета — $10 000 до $100 000 на місяць за особу), а їхні доходи (оцінювані в $350–800 мільйонів у 2024 році) частково перераховуються безпосередньо на фінансування діяльності підсанкційних організацій КНДР. Вони активно використовують витончені тактики, методи та процедури для створення фальшивих особистостей (synthetic personas), включаючи генерацію штучних облич за допомогою GAN, маскування номерів телефонів через проксі-сервіси, використання VPN, а також купівлю та оренду верифікованих акаунтів на фріланс-платформах (Upwork, Freelancer) та платіжних системах (Payoneer, PayPal, Wise). IT-працівники активно націлюються на компанії в Європі та

США у секторах з високою цінністю, таких як оборонно-промислова база (DIB), штучний інтелект (AI), блокчейн та веб-розробка. Важливу роль у цій схемі відіграють іноземні посередники (фасилітатори), зокрема в Україні, Аргентині та США, які надають "ферми ноутбуків" (laptop farms), створюють фіктивні компанії (LLCs) та допомагають у верифікації особистості, щоб приховати справжнє місцезнаходження працівників та забезпечити їм доступ до західних банківських систем (наприклад, ACH-рахунків). Звіт також фіксує конвергенцію між місіями IT-працівників та кіберакторами, оскільки IT-працівники, отримуючи доступ до корпоративних мереж, можуть сприяти подальшим шпигунським або зловмисним фінансовим операціям.

Крім того, КНДР продовжує цільові кібероперації проти оборонно-промислової бази (DIB) та критичної інфраструктури, зокрема в Республіці Корея, з метою крадіжки інтелектуальної власності та чутливої технічної інформації для просування своїх програм ЗМЗ.

Основні аспекти участі України як транзитної або допоміжної ланки у схемах КНДР деталізовані в документі наступним чином:

Використання Українських Посередників (Фасилітаторів)

- *Надання інфраструктури та маскування розташування:* Фасилітатори, які базуються в Україні, надають комп'ютери, що фізично розташовані в Україні. Північнокорейські IT-працівники, які фактично знаходяться в інших країнах (наприклад, у Лаосі, як у випадку делегації Chonsurim), отримують віддалений доступ до цих українських комп'ютерів. Це дозволяє IT-працівникам КНДР маскувати своє справжнє географічне розташування.
- *Сприяння ідентифікації та працевлаштуванню:* Українські посередники надають північнокорейським розробникам облікові дані (credentials) українських громадян, які використовуються для отримання роботи.
- *Створення хибної ідентичності (Synthetic Personas):* З 2023 року спостерігається значне зростання випадків, коли IT-працівники КНДР вдаються до використання українських ідентифікаційних даних на фріланс-платформах. Передбачається, що КНДР обирає українські дані, оскільки компанії в західних країнах можуть бути більш схильні наймати українців, щоб надати підтримку Україні після вторгнення Росії у 2022 році.
- *Масштабування послуг:* Ринок українських продавців ідентифікаційних даних та акаунтів, орієнтований на потреби IT-працівників КНДР, значно розширився у 2024 році та продовжує зростати у 2025 році. Цей ринок еволюціонував від індивідуальних продавців до організованих мереж українських брокерів, які пропонують комплексні пакети послуг.
- *Комплексні пакети послуг:* Стандартний пакет послуг, пропонований брокерами, зазвичай включає верифіковані акаунти на фріланс-платформах, LinkedIn, Payoneer та PayPal, а також не верифіковані акаунти на Gmail, GitHub та різних криптовалютних біржах (часто MEXC та Binance). Деякі брокери також пропонують послуги з реєстрації акаунтів на інших платіжних системах (як-от Wise, Genomo, Zen та Paysera), місцевих телефонних провайдерах та в українських фінансових установах.
- *"Ферми ноутбуків":* Українські брокери відомі тим, що створюють великомасштабні "ферми ноутбуків" у своїх помешканнях або орендованих офісних приміщеннях, де одночасно працює понад 50 пристроїв. Для уникнення виявлення, вони використовують мобільні маршрутизатори та декілька SIM-карток.
- *Фінансове заохочення для українців:* Брокери рекрутують українців, які гостро потребують доходу, пропонуючи їм "сірі" схеми заробітку, щоб ті надавали свої ідентифікаційні документи, банківські виписки та фото. Існують бізнес-тренери, які просувають "пасивний дохід" шляхом здачі ноутбуків в оренду клієнтам, яких описують як "китайців" (хоча насправді це можуть бути IT-працівники КНДР).

- *Оплата та криптотранзакції:* Операції з IT-працівниками КНДР здійснюються переважно через криптовалюту. Більшість продавців фріланс-акаунтів зосереджені на українському ринку.
- *Приклад посередника:* У 2024 році у Польщі був заарештований один із відомих українських фасилітаторів — Олександр Діденко (Oleksandr Didenko). До арешту Діденко надавав підтримку щонайменше 300 північнокорейським IT-працівникам, керуючи "фермами ноутбуків" та створюючи фальшиві акаунти. Арешт Діденка спричинив значний збій у роботі IT-працівників, яких він підтримував.

Зв'язок із підсанкційними угрупованнями КНДР

- *Делегація Chonsurim:* IT-працівники делегації Chonsurim Trading Corporation (підпорядкована Департаменту 53 Міністерства національної оборони КНДР, MND), що базувалися в Лаосі, використовували послуги українських фасилітаторів для маскування свого розташування та отримання облікових даних українських громадян для працевлаштування.
- Делегація SANS FAB/Sangsin: IT-працівник Han Kwang Hyok (пов'язаний із Sangsin/SANS FAB) також використовував послуги українського фасилітатора, який надавав йому комп'ютер, розташований в Україні, для віддаленого доступу.

Таким чином, Україна, як і інші країни (Китай, Росія, Аргентина, ОАЕ), використовується як юрисдикція, де іноземні посередники активно допомагають IT-працівникам КНДР отримувати роботу та здійснювати фінансові операції, що порушують санкції ООН.

Висновки:

- **Посилення заходів щодо заморожування та арешту криптовалют:** Необхідно терміново розробити та впровадити правові та технічні можливості для ефективного відстеження, заморожування та конфіскації криптовалют (включаючи BTC, ETH, USDT), викрадених або відмитих КНДР, щоб забезпечити виконання режиму заморожування активів, передбаченого резолюціями РБ ООН. Особливу увагу слід приділити ідентифікації та нагляду за послугами, які систематично використовуються для обфускації транзакцій, зокрема, крос-чейн агрегаторами, міксерами та мостами.
- **Дієвий моніторинг та протидія китайській фінансовій інфраструктурі:** Державам-членам слід посилити пильність та застосувати контрзаходи відповідно до заклику FATF щодо КНДР, особливо щодо фінансових транзакцій, пов’язаних із китайськими банками та позабіржовими (OTC) трейдерами. Необхідно вживати оперативних заходів щодо виявлених посередників та припиняти кореспондентські та інші бізнес-відносини, які використовуються для конвертації викраденої криптовалюти у фіат.
- **Впровадження суворих протоколів Due Diligence при віддаленій роботі:** Компанії, особливо у високоризикових секторах (AI, DIB, фінтех), повинні негайно впровадити посилені заходи належної перевірки для всіх віддалених IT-працівників, включаючи багаторівневу верифікацію особистих даних, заборону використання комерційних VPN для доступу до корпоративних мереж, а також ретельний аналіз банківської інформації та запитів на оплату праці в криптовалюті або на рахунки, що не відповідають ідентифікаційним документам.
- **Виявлення та припинення діяльності іноземних фасилітаторів:** Необхідно систематично виявляти та притягати до відповідальності іноземних посередників (зокрема, в США, Аргентині, Україні, Росії), які надають IT-працівникам КНДР фальшиві або орендовані ідентифікаційні дані, створюють "ферми ноутбуків" та допомагають в отриманні доступу до міжнародних платіжних систем, оскільки їхня діяльність є критично важливою для успіху схем КНДР.

Проект Керівних принципів щодо спільних процедур та методологій для процесу наглядового огляду та оцінки (SREP) та наглядового стрес-тестування відповідно до Директиви 2013/36/ЄС [2]

Представлений документ є проєктом консультаційного документу Європейської банківської асоціації (EBA/CP/2025/21 від 24 жовтня 2025 року), який пропонує третій значний перегляд Керівних настанов щодо загальних процедур та методологій процесу наглядового огляду та оцінки (SREP) і наглядового стрес-тестування. Основна мета цього оновлення — привести наглядову практику у відповідність до суттєвих змін у регуляторному ландшафті, зокрема імплементації "банківського пакету" (CRD VI / CRR III), нового Регламенту про цифрову операційну стійкість (DORA) та нових вимог до процентного ризику банківського портфеля (IRRBB) і ризику кредитного спреду (CSRBB). Документ також консолідує майже десятирічний практичний досвід застосування SREP та виконує специфічні мандати CRD VI щодо розробки SREP для філій третіх країн (TCBs) та операціоналізації взаємодії між вимогами Pillar 2 та новим механізмом мінімального рівня достатності капіталу ("output floor"). Структурно, проєкт суттєво раціоналізує наглядовий процес: він об'єднує всі положення SREP в єдину комплексну рамкову структуру та, що важливо, скасовує окремі Керівні настанови EBA щодо оцінки ІКТ-ризиків у рамках SREP (EBA/GL/2017/05), інтегруючи оновлені вимоги (з урахуванням DORA) безпосередньо в оцінку операційного ризику. Ключовою методологічною зміною є підхід до нових типів ризиків: замість створення окремих модулів, такі "наскрізні" (cross-cutting) ризики, як ESG та операційна стійкість, тепер інтегровані в усі існуючі елементи SREP — від аналізу бізнес-моделі до оцінки управління та ризиків капіталу.

З точки зору боротьби з фінансовими злочинами, цей проєкт знаменує собою фундаментальне посилення зв'язку між пруденційним наглядом та ризиками відмивання коштів і фінансування тероризму (ВК/ФТ). Документ чітко закріплює, що пруденційні наглядові органи зобов'язані розглядати ризики ВК/ФТ з пруденційної точки зору , оскільки нездатність установ управляти ними може мати прямий згубний вплив на їхню фінансову стійкість та стабільність ринку. Ця вимога інтегрована в ключові елементи SREP: по-перше, в Аналіз бізнес-моделі (BMA), який тепер вимагає від наглядових органів ідентифікувати вразливості, що виникають через ризики ВК/ФТ, пов'язані з бізнес-моделлю установи (наприклад, діяльність з криптоактивами або операції у високоризикових юрисдикціях); по-друге, в Оцінку внутрішнього врядування, де введено спеціальний розділ 5.8 "Ризики ВК/ФТ та пруденційні занепокоєння". Цей розділ вимагає від наглядовців оцінювати, чи включає загальна система управління ризиками установи управління ризиками ВК/ФТ та чи виконує керівний орган свої обов'язки у цій сфері. Встановлюється чіткий механізм двосторонньої взаємодії: пруденційні наглядові органи повинні використовувати інформацію, отриману від органів з питань ПВК/ФТ , і, що критично важливо, у разі виявлення недоліків у системах врядування чи контролю, які можуть бути пов'язані з ПВК/ФТ, вони зобов'язані негайно повідомляти про це відповідний орган з ПВК/ФТ.

[2] https://www.eba.europa.eu/sites/default/files/2025-10/c5f0c511-b9cc-44fb-bb8a-bf8892953db4/Consultation%20paper%20on%20revised%20Guidelines%20on%20SREP%20and%20supervisory%20stress%20testing.pdf

Висновки:

- **Обов'язкова інтеграція ПВК/ФТ у пруденційний SREP.** Наглядові органи тепер зобов'язані систематично оцінювати пруденційні наслідки ризиків ВК/ФТ. Це має відбуватися під час аналізу бізнес-моделі, щоб виявити вразливості, пов'язані з продуктами чи географією , та під час оцінки внутрішнього врядування. Практичним наслідком є вимога двосторонньої співпраці: пруденційний наглядовий орган повинен використовувати дані від органу ПВК/ФТ та обов'язково повідомляти його про виявлені суттєві недоліки в системах контролю.
- **Впровадження нових рамок для SREP філій третіх країн (TCB) та ескалації нагляду.** Документ вводить два ключові практичні інструменти: 1) Нова, окрема методологія SREP для філій третіх країн, що фокусується на їхній бізнес-моделі, управлінні, капітальному забезпеченні, ліквідності та процедурах букінгу (booking arrangements). 2) Нова "високорівнева рамка ескалації" , яка надає наглядовим органам чіткий, але гнучкий алгоритм дій (від діалогу до примусових заходів) для забезпечення своєчасного усунення установами виявлених недоліків.
- **Горизонтальна інтеграція ризиків (ESG та DORA) замість окремих модулів.** Проєкт відмовляється від створення нових ізольованих процесів для ризиків. Натомість ризики ESG та ризики цифрової операційної стійкості (DORA) розглядаються як "наскрізні" (cross-cutting) фактори. Наглядові органи повинні оцінювати їхній вплив у контексті всіх існуючих елементів SREP — бізнес-моделі , внутрішнього врядування та операційного ризику. Це вимагає від установ більш глибокої інтеграції цих ризиків у їхні загальні системи управління.

Ця взаємодія також формалізована для транскордонних груп та філій третіх країн, де підозра у ВК/ФТ вимагає негайного повідомлення EBA та наглядового органу з ПВК/ФТ.

Окрім цього, документ впроваджує нову високорівневу та гнучку "рамку ескалації" (escalation framework) для наглядових дій , яка має на меті підвищити ефективність нагляду, надаючи чіткі кроки від посиленого діалогу до застосування обов'язкових заходів. Також значно посилюється принцип пропорційності: наглядові органи отримують більшу гнучкість щодо частоти та інтенсивності SREP, особливо для "малих та нескладних установ", для яких мінімальна частота повної оцінки SREP може бути подовжена з трьох до п'яти років за умови стабільного низькоризикового профілю. Нарешті, проєкт детально описує методологію взаємодії між вимогами Pillar 2 та "output floor", щоб запобігти подвійному врахуванню ризиків. Очікується, що нові Керівні настанови набудуть чинності з 1 січня 2027 року.

Прибуткові стейблкоїни як виклик традиційному банкінгу: аналіз регуляторних підходів ЄС, США, Сінгапуру та Гонконгу [3]

Аналітичний звіт Банку міжнародних розрахунків (BIS), підготовлений експерткою Деніз Гарсія Окампо у жовтні 2025 року, зосереджується на аналізі та порівнянні регуляторних підходів до явища прибуткових стейблкоїнів, тобто цифрових активів, пов’язаних із фіатними валютами, за якими користувачам нараховується певний дохід. Хоча більшість стейблкоїнів створені як платіжні засоби, їх використання як інвестиційних продуктів через криптовалютних посередників, біржі та DeFi-платформи спричинило появу нового фінансового феномену, що стирає межі між платіжним інструментом і депозитом, але без відповідного рівня регуляторного контролю, прозорості та захисту споживачів. У цьому контексті документ BIS пропонує

[3] https://www.bis.org/fsi/fsibriefs27.pdf

всебічний аналіз ринку, його механізмів і регуляторних реакцій у ключових юрисдикціях, а також оцінює наслідки для фінансової стабільності.

На початку звіту наголошується, що питання винагороди за володіння стейблкоїнами стало одним із центральних у політичних дебатах навколо криптоактивів. Регулятори зосереджують увагу не лише на емітентах, а й на третіх сторонах — криптосервіс-провайдерах (CASPs), які пропонують користувачам можливість заробляти відсотки або винагороди, попри те що самі стейблкоїни не створені для цього. Це створює певну асиметрію між банківським сектором, що діє в межах суворих пруденційних вимог і страхування депозитів, і криптосектором, який залишається менш контрольованим. Банківські лобісти застерігають, що дозвіл на виплату доходу за стейблкоїнами може спричинити відтік депозитів, зменшити кредитну ліквідність і підвищити нестабільність банківського фінансування. Водночас представники криптоіндустрії апелюють до конкуренції та прав споживачів на вибір фінансових продуктів. Проте BIS підкреслює, що головним фокусом мають бути не комерційні інтереси, а питання фінансової стабільності, прозорості та захисту споживачів.

У другому розділі окреслюється структура ринку. Станом на вересень 2025 року капіталізація стейблкоїнів перевищила 280 млрд доларів, і аналітики прогнозують її зростання до 1,9 трлн до 2030 року. Водночас сегмент прибуткових стейблкоїнів зріс із менш ніж 1 млрд до понад 19 млрд доларів, а лідерами стали проєкти Ethena (sUSDe), Sky (sUSDS) та BlackRock (BUIDL). Попри те, що «платіжні» стейблкоїни, такі як USDT і USDC, не генерують прибутку «на ланцюгу», провайдери використовують різні механізми для створення дохідності. Вони включають повторне кредитування користувацьких активів інституційним трейдерам і маркетмейкерам (як у програмі Gemini Earn, де кошти переказувалися Genesis), надання ліквідності у маржинальні пули (Bitfinex), використання DeFi-протоколів (Aave) або фінансування програм лояльності (Coinbase USDC Rewards). Водночас у більшості таких схем користувачі юридично не є власниками своїх токенів, а мають лише договірне право вимоги до посередника, що створює ризики втрати коштів у разі його неплатоспроможності — як це сталося у справі Celsius Earn, де суд визнав активи клієнтів власністю банкрута.

Звіт детально аналізує регуляторні режими чотирьох юрисдикцій, які стали орієнтирами у сфері нагляду за стейблкоїнами — Європейського Союзу, Гонконгу, Сінгапуру та США. ЄС запровадив сувору модель у межах Регламенту MiCA (2023/1114), який категорично забороняє емітентам та криптопосередникам нараховувати будь-які відсотки або винагороди, пов’язані з триманням токенів EMT або ART. Гонконгський «Stablecoins Ordinance» 2025 року дотримується аналогічного підходу, забороняючи будь-які форми прибутковості як для емітентів, так і для ліцензованих бірж та фінансових посередників. Натомість Сінгапур обрав більш гнучку модель: у межах свого «Single-Currency Stablecoin (SCS) Framework» 2023 року він дозволяє операції лише емітентам, які відповідають суворим вимогам, але обмежує виплату доходів і стейкінг роздрібним інвесторам, залишаючи можливість для професійних користувачів за умови розкриття ризиків. США, у свою чергу, ухвалили «GENIUS Act» (Guiding and Establishing National Innovation for US Stablecoins) 2025 року, який забороняє емітентам платити відсотки, але не встановлює прямої заборони для CASPs. Американська модель залишається неповною: поки що відсутній єдиний наглядовий режим, а регулювання CASPs здійснюється фрагментарно — через закони SEC, CFTC, FinCEN і на рівні окремих штатів. У підготовці перебуває законопроєкт «Digital Asset Market Clarity Act» (CLARITY Act), покликаний усунути регуляторні прогалини між SEC і CFTC.

У завершальній частині звіт підкреслює, що швидке зростання ринку стейблкоїнів і зростання їх зв'язків із банківською системою створює три взаємопов'язані категорії ризиків: споживчі, фінансово-стабілізаційні та етичні. По-перше, користувачі часто сприймають CASPs як безпечні депозитні сервіси, не усвідомлюючи, що їхні кошти не підпадають під систему страхування, а правовий статус токенів не гарантує відшкодування. По-друге, масові вилучення коштів або збої у виплаті відсотків можуть спровокувати ефект «набігу» (масове одночасне вилучення вкладниками або інвесторами своїх коштів із певної фінансової установи чи інструменту через втрату довіри або страх перед її неплатоспроможністю), який поширюється на емітентів і банки, що обслуговують резерви. По-третє, мультифункціональність CASPs створює конфлікти інтересів, адже платформи одночасно виконують ролі кастодіанів, кредиторів, маркетмейкерів і торгових посередників, що у традиційній фінансовій системі суворо розмежовується законом.

BIS доходить висновку, що чинне регулювання недостатньо охоплює нові ризики, пов'язані з продуктами доходу на базі стейблкоїнів, і закликає держави до вироблення цілісних законодавчих рамок, які поширювалися б не лише на емітентів, але й на криптосервіс-посередників. Пропонується низка стратегічних напрямів: обмеження доступу роздрібних інвесторів до таких продуктів, підвищення вимог до корпоративного управління, ліквідності та розкриття інформації про джерела прибутковості, розроблення єдиних стандартів звітності, класифікація «стейблкоїнів, що приносять дохід» як інвестиційних інструментів, а також посилення міжнародної координації та обміну даними між регуляторами. Таким чином, BIS підкреслює, що стейблкоїни, хоч і мають потенціал для розвитку цифрових платежів, у разі безконтрольного поширення механізмів отримання доходу, вони можуть стати джерелом системних ризиків, порівнянних із тими, що існують у традиційному банківському секторі, але без відповідних запобіжників. У цьому сенсі регулювання прибутковості за стейблкоїнами є не лише технічним, а й фундаментальним питанням для майбутньої архітектури глобальної фінансової стабільності.

Висновки:

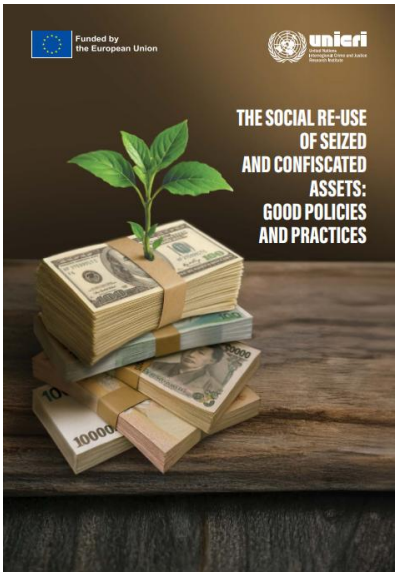
- **Регулювання має охоплювати не лише емітентів, а й посередників (CASPs) —** саме через них формується більшість ризиків, пов'язаних із продуктами доходу.
- **Виплата прибутковості за стейблкоїнами повинна бути або заборонена, або суворо ліцензована,** із чітким поділом між платіжними й інвестиційними токенами.
- **Роздрібним користувачам слід обмежити доступ до прибуткових продуктів на базі стейблкоїнів,** оскільки вони не розуміють повною мірою ризиків непокритих зобов'язань та юридичних наслідків.
- **Потрібна узгоджена глобальна рамка для CASPs,** яка б встановлювала вимоги до прозорості, звітності, управління ризиками та міждержавного нагляду — аналогічно до банківського чи інвестиційного сектору.

Від злочину до користі: як перетворити конфісковані активи на ресурс розвитку [4]

Документ UNICRI є комплексним міжнародним дослідженням, спрямованим на систематизацію кращих практик у сфері соціального повторного використання арештованих і конфіскованих активів. Підготовлений за фінансової підтримки Європейського Союзу у межах програми «Support to Eastern Partnership Countries to Enhance Asset Recovery II», він має на меті допомогти урядам, зокрема країнам Східного партнерства, адаптувати ефективні моделі прозорого управління вилученим майном, забезпечити його повернення суспільству та зміцнити довіру громадян до верховенства права. Видання розглядає соціальне повторне використання як

[4] https://unicri.org/sites/default/files/2025-10/Social-Reuse-of-Seized-and-Confiscated-Assets-Good-Policies-and-Practices-Oct-2025.pdf

завершальну або проміжну стадію циклу повернення активів, коли конфісковане майно спрямовується не лише на задоволення бюджетних потреб, а безпосередньо на користь громад — через фінансування соціальних, освітніх, медичних чи інфраструктурних програм, відновлення довіри у громадах, які постраждали від організованої злочинності.



В основі підходу UNICRI лежить розуміння, що процес конфіскації має не каральний, а відновлювальний характер, і що боротьба зі злочинністю повинна передбачати повернення суспільству тих ресурсів, які злочинці вилучили через корупцію, шахрайство або відмивання коштів. Саме тому соціальне повторне використання розглядається як елемент відновлення справедливості та репарації шкоди, заподіяної суспільству. Він сприяє не лише підвищенню ефективності антикорупційних та кримінально-правових заходів, а й зміцненню соціальної єдності, законності державних інституцій і виконанню міжнародних зобов'язань, визначених Ціллю сталого розвитку 16 («Мир, правосуддя та сильні інституції»).

У вступній частині документа детально аналізуються міжнародні стандарти та нормативно-правові орієнтири, що формують рамкове поле для соціального повторного використання активів. Серед ключових джерел — Конвенція ООН проти корупції (UNCAC), яка у статті 57 передбачає, що повернені активи повинні спрямовуватися на досягнення антикорупційних і соціально-економічних цілей; Принципи Глобального форуму з повернення активів (GFAR), які наголошують на важливості того, щоб відновлені кошти приносили користь громадянам країн, що постраждали від корупції; Рекомендовані принципи ООН з прав людини та повернення активів (OHCHR, 2022), що встановлюють вимогу прозорого, підзвітного та спільного використання поверненого майна; а також Директива ЄС 2014/42/ЄС і нова Директива (ЄС) 2024/1260, які заохочують держави-члени спрямовувати конфісковані активи на суспільні чи соціальні цілі, зокрема через їх використання місцевими органами влади або громадськими організаціями. Важливе місце посідають Керівні настанови Ради Європи щодо управління арештованими активами, які розрізняють пряме соціальне використання (наприклад, перетворення майна на соціальні центри) та непряме (використання доходів від продажу активів для фінансування програм розвитку).

Документ підкреслює, що соціальне повторне використання — це не лише механізм управління активами, а насамперед інструмент відновлення довіри громад до правосуддя. Там, де суспільство бачить, що держава не просто конфіскує майно, а повертає його для користі громади, зміцнюється віра у справедливість і державність. Це особливо важливо для регіонів, які історично зазнавали впливу організованої злочинності або системної корупції. Водночас реалізація такого підходу потребує інституційної спроможності, прозорих механізмів розподілу, правової визначеності та залучення громадянського суспільства.

Основна частина звіту присвячена узагальненню практик із понад двадцяти країн світу, кожна з яких розробила власну модель управління конфіскованими активами. Серед найуспішніших прикладів виділяється Італія, яка створила найповнішу систему соціального використання майна, конфіскованого у мафіозних структур. Її модель базується на законі №109/1996 та діяльності Національного агентства ANBSC, що забезпечує передачу активів місцевим громадам для створення соціальних підприємств, освітніх і культурних центрів, соціальні фермерські господарства, створені на базі конфіскованого майна, спортивних шкіл і соціальних кооперативів. Італійська практика перетворила конфіскацію на символ справедливості й відновлення: будівлі, що належали мафії, стали просторами громадського життя, а доходи від конфіскованих компаній фінансують програми працевлаштування та освіти.

Великий інтерес становить і досвід Франції, де Агентство AGRASC управляє активами, а з 2021 року проводить відкриті конкурси Appels à manifestation d'intérêt, завдяки яким НУО можуть безоплатно отримувати конфісковане майно для соціальних проєктів. Серед прикладів — передача конфіскованої вілли в Марселі для розміщення центру допомоги жінкам, які стали жертвами насильства, або перетворення об'єктів нерухомості в соціальні хаби та притулки для вразливих груп. Французька модель вирізняється прозорістю, конкуренцією і довгостроковим плануванням використання активів.

Албанія запропонувала практичний приклад партнерства між державними інституціями, ЄС і громадянським сектором. Її Агентство з управління арештованими активами (AAPSK) реалізувало низку соціальних ініціатив у межах програм CAUSE і TWIST: колишні кримінальні об'єкти були перетворені на кав'ярні, культурні простори, майстерні для соціального підприємництва. У рамках цих проєктів працюють вразливі групи населення, жінки, які постраждали від насильства, колишні ув'язнені, а отримані прибутки спрямовуються на розвиток місцевих громад.

Документ також висвітлює приклади Болгарії, де законодавчо передбачено, що щонайменше 30% вартості конфіскованого майна має використовуватися для соціальних цілей, і Боснії та Герцеговини, де конфісковані автомобілі, готелі чи житло передаються для потреб поліції, цивільного захисту чи постраждалих від стихійних лих. У Канаді діє децентралізована модель — провінційні уряди (Онтаріо, Британська Колумбія, Саскачеван) інвестують конфісковані кошти у програми для жертв насильства, молодіжні ініціативи та безпеку громад. Ірландія створила Community Safety Fund, з якого фінансуються освітні та профілактичні програми протидії злочинності, а Казахстан ухвалив закон, який гарантує, що всі повернуті активи спрямовуються у державний фонд соціального розвитку.

Особливу увагу UNICRI приділяє питанням прозорості, підзвітності й залучення громадянського суспільства. У документі наголошується, що саме громадські організації мають бути залучені до процесів розподілу і моніторингу використання активів, оскільки це забезпечує довіру, зменшує ризики повторного зловживання коштами та робить управління більш сталим. Крім того, для забезпечення прозорості рекомендується укладати міждержавні угоди (наприклад, між країнами-донорами та реципієнтами повернутих коштів), які регулюють механізм контролю, нагляду й аудиту, а також публічну звітність.

Документ завершується набором рекомендацій для країн Східного партнерства. UNICRI закликає ці держави розробити законодавчі рамки, які б передбачали чіткі механізми соціального використання активів — визначення

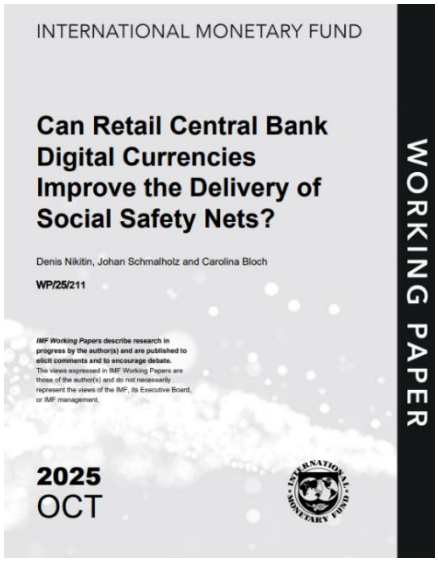
Висновки:

- **Соціальне повторне використання активів є невід'ємною частиною політики протидії організованій злочинності й корупції,** що реалізує принцип «повернення цінності суспільству», а не лише покарання злочинців.
- **Ефективність процесу залежить від законодавчого закріплення, інституційної спроможності та участі громадянського суспільства.** Успішні моделі (Італія, Албанія, Франція) показують, що найкращі результати досягаються за наявності чіткого законодавчого повноваження та громадського контролю.
- **Для країн Східного партнерства, включно з Україною, рекомендовано створення чітких механізмів соціальної реінтеграції конфіскованих активів,** зокрема через квотування частки для соціальних проєктів, розвиток міжвідомчих платформ та залучення НУО до моніторингу.
- **Соціальне повторне використання — інструмент стійкого розвитку,** який поєднує цілі антикорупційної політики з гуманітарними та економічними пріоритетами держави, сприяючи реалізації ЦСР-16 та формуванню культури доброчесності.

відповідальних інституцій, створення спеціальних фондів, квотування частки конфіскованих активів для соціальних проєктів і забезпечення участі громад у визначенні пріоритетів їх використання. У контексті України особливу роль відведено АРМА як центральному органу з управління арештованими активами, для якого запропоновано зміцнити принципи прозорості, моніторингу й комунікації з громадами, а також створити практику спрямування частини активів на підтримку соціальних ініціатив, відновлення громад, освіту й антикорупційні програми.

Загалом документ формує нове бачення процесу повернення активів — як інструменту соціального відновлення, а не просто економічного механізму. Він показує, що справедливість не завершується на конфіскації, а починається тоді, коли викрадене повертається суспільству. Соціальне повторне використання активів стає символом того, що держава здатна не лише покарати злочинців, а й перетворити злочинні ресурси на інструмент добра, розвитку та відновлення довіри громад до влади.

Від готівкових виплат до цифрових трансфертів: роль CBDC у модернізації соціальних гарантій [5]



Документ МВФ присвячено системному аналізу того, яким чином роздрібні цифрові валюти центральних банків (CBDC) можуть вплинути на механізми надання державної соціальної допомоги — соціальних гарантій і програм підтримки вразливих груп населення (SSN). Дослідження, підготовлене експертами Денісом Нікітіним, Йоханом Шмальгольцом і Кароліною Блох, окреслює концептуальні, технологічні та управлінські аспекти впровадження CBDC у сфері соціальної політики, фокусуючись на порівнянні з існуючими платіжними системами, такими як швидкі платіжні системи (FPS) чи мобільні фінансові сервіси. Центральна теза роботи полягає в тому, що просте використання CBDC як платіжного інструменту для перерахування коштів не надає суттєвих переваг порівняно з уже наявними рішеннями. Натомість потенціал CBDC може проявитися лише тоді, коли вони функціонуватимуть як платформа адміністрування соціальних виплат, що дозволяє урядам автоматизувати управління, забезпечити прозорість, безпосередній моніторинг та мінімізувати участь приватних фінансових посередників.

У вступі наголошується, що станом на 2024 рік 94 % центральних банків світу проводили дослідження або пілотні проєкти CBDC, і близько третини вже тестували пілотні версії цифрових валют. Країни, що першими впровадили CBDC, — Багамські острови, Ямайка, Нігерія — продемонстрували різний рівень ефективності, що зумовлює потребу у порівняльному аналізі їхнього потенціалу для державних програм соціальної підтримки. Автори підкреслюють, що навіть у разі технологічної досконалості CBDC їхня корисність залежить від цілей, які вони покликані обслуговувати: для системи соціальних виплат головне не швидкість чи дешевизна платежів, а можливість точно і своєчасно доставляти допомогу конкретним отримувачам соціальної допомоги, уникаючи витоків, дублювань та зловживань.

[5] https://www.imf.org/en/Publications/WP/Issues/2025/10/24/Can-Central-Bank-Digital-Currencies-Improve-the-Delivery-of-Social-Safety-Nets-568447#:~:text=However%2C%20leveraging%20CBDCs%20as%20payment,intermediaries%2C%20and%20monitor%20transactions%20directly.

В аналітичному розділі МВФ пропонує двокомпонентну методологічну рамку: поєднання моделі ланцюга доставки соціальних виплат з типовою архітектурою роздрібного CBDC. Ланцюг доставки охоплює п’ять основних етапів — ідентифікацію потенційних отримувачів, відбір отримувачів соціальної допомоги за критеріями вразливості, безпосереднє здійснення виплат, адміністрування й оновлення даних, а також використання коштів за цільовим призначенням. Відповідно, типова архітектура CBDC включає дворівневу систему розподілу (центральний банк і фінансові посередники), цифрові токени, ідентифіковані гаманці, дозвільний розподілений реєстр і механізми програмованості через смарт-контракти. Автори підкреслюють, що CBDC може впливати на кожну ланку цього процесу: від автоматизації перевірки права на допомогу до забезпечення повної прозорості використання бюджетних коштів.

Особливу увагу приділено функціональним характеристикам CBDC, які потенційно здатні змінити систему соціальних трансфертів. По-перше, CBDC є безризиковими зобов’язаннями центрального банку, що усуває ризик дефолту приватних банків. По-друге, вони, як правило, не приносять відсотків, що дозволяє уникнути відтоку депозитів із банківської системи. По-третє, гаманці CBDC мають ліміти на залишки й операції, що може впливати на розмір соціальних переказів. По-четверте, CBDC передбачають проведення процедур ідентифікації та перевірки клієнтів (CDD) з прив’язкою до національної системи ідентифікації, що підвищує сумісність із державними базами даних. По-п’яте, програмованість і смарт-контракти відкривають можливості для автоматичного виконання умовних платежів, цільового використання допомоги та моніторингу ефективності програм.

У роботі детально розглянуто практичні кейси впровадження CBDC та блокчейн-технологій у соціальному секторі. Досвід Австралії (використання блокчейну для управління виплатами особам з інвалідністю) показав, що програмована логіка платежів дозволяє суттєво скоротити адміністративні витрати й підвищити прозорість. У Казахстані пілот проєкту “Digital Tenge” демонструє можливість автоматизованих умовних платежів у шкільній системі харчування, коли транзакція ініціюється лише після підтвердження факту отримання послуги. Бразильські приклади токенізації сільськогосподарських активів і адміністрування пільгових кредитів за допомогою смарт-контрактів свідчать про перспективність CBDC як інструменту для фінансової підтримки фермерів і малих підприємців. Водночас досвід Нігерії з e-Naira виявив обмеження, пов’язані з низьким рівнем охоплення населення посвідченнями особи та відсутністю стимулів для переходу користувачів на вищі рівні CDD, що призвело до мізерного рівня активних гаманців.

На основі цих прикладів автори роблять висновок, що потенційні переваги CBDC у сфері соціальної політики не можуть бути реалізовані без паралельного розвитку інституційної інфраструктури — насамперед систем ідентифікації громадян, соціальних реєстрів, міжвідомчого обміну даними та кіберзахисту. CBDC можуть виступати каталізатором розвитку таких систем, адже вимога наявності посвідчення особи для відкриття цифрового гаманця здатна стимулювати масову ідентифікацію населення. Водночас на початковому етапі така вимога може обмежити охоплення соціальних виплат, якщо національна ID-система не є універсальною.

Великий розділ присвячено аналітичній оцінці впливу CBDC на кожен елемент ланцюга доставки соціальної допомоги. У сфері ідентифікації та відбору отримувачів соціальної допомоги CBDC можуть забезпечити точніше оцінювання добробуту громадян за рахунок доступу до агрегованих транзакційних даних, однак це створює ризики надмірного державного контролю й потребує чітких рамок конфіденційності. У частині безпосереднього здійснення виплат ключовою перевагою є можливість створення постійних державних гаманців для кожного громадянина, що усуває потребу у повторному зборі реквізитів і знижує адміністративні затрати. Доступ до розподіленого реєстру дозволяє автоматизувати звірку платежів, виявлення помилок та аналіз ефективності витрат у реальному часі. У сфері

адміністрування й управління програмами CBDC забезпечують автоматичне виконання умовних платежів через смарт-контракти, що дозволяє синхронізувати виплати з фактичним наданням послуг — наприклад, вакцинацією дітей чи відвідуванням школи. Програмованість гаманців може також забезпечити контроль за цільовим використанням коштів, хоча це породжує етичні дилеми та потребує правового врегулювання.

Разом із тим, автори зазначають, що більшість функціональних можливостей, які приписують CBDC, можуть бути досягнуті за допомогою удосконалення вже існуючих платіжних рішень — зокрема, впровадження систем відкритого банкінгу, розширення API-інтеграцій між банками та соціальними реєстрами, або використання гібридних моделей із поєднанням блокчейну та традиційних платіжних систем. Таким чином, переваги CBDC стають очевидними лише тоді, коли вони виконують роль комплексної адміністративної платформи, а не просто цифрового платіжного каналу.

У висновку документа підкреслено, що ефективне використання CBDC для соціальних програм вимагатиме скоординованої політики, взаємодії центральних банків, органів соціального захисту та технологічних регуляторів. Необхідно забезпечити баланс між прозорістю і захистом приватності, визначити чіткі стандарти відповідності у сфері ПВК/ФТ, а також гарантувати технічну стійкість і кібербезпеку. Лише за таких умов CBDC можуть стати інструментом, який не лише спрощує платіжну логістику, а й трансформує саму філософію соціального забезпечення — від реактивної допомоги до проактивного, автоматизованого й адресного управління соціальними ресурсами.

Висновки:

- **CBDC як платіжна адміністративна платформа (а не лише інструмент виплат)** може кардинально підвищити ефективність соціальних програм — через автоматизацію, прозорість і прямий моніторинг транзакцій.
- **Інтеграція з національними ID-системами —** критичний чинник успіху: без масової ідентифікації CBDC не зможе забезпечити інклюзивність і точну цільову ідентифікацію отримувачів.
- **Програмованість і доступ до реєстру операцій** відкривають нові можливості для аналітики, контролю та перевірки умовних виплат (CCT), але вимагають правових гарантій приватності.
- **CBDC не є панацеєю —** багато переваг можна досягти шляхом вдосконалення існуючих платіжних рішень (відкритий банкінг, API, національні швидкі платежі); доцільність CBDC виправдана лише за наявності чіткої порівняльної переваги.

У підсумку МВФ доходить до висновку, що CBDC мають потенціал значно покращити ефективність і прозорість соціальних програм, однак лише у випадку ретельної інтеграції з наявними системами, чіткого розуміння їхніх переваг і ризиків, а також поступового впровадження на основі пілотних програм. Інакше існує ризик, що CBDC залишаться лише технологічним експериментом, який дублює можливості традиційних платіжних інструментів, не приносячи суттєвої користі для державної соціальної політики.

Витрати на цифровий євро: ЄЦБ визначає реальні масштаби інвестицій для банків Єврозони [6]

Документ Європейського центрального банку є комплексним аналітичним дослідженням, присвяченим оцінці інвестиційних витрат, які може понести банківський сектор Єврозони у

6 https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.deprep251010_a_view_on_recent_assessments_of_digital_euro_investment_costs_for_the_euro_area_banking_sector.en.pdf

зв'язку з впровадженням цифрового євро. Його підготовлено на запит законодавців ЄС з метою створення збалансованої та обґрунтованої основи для політичних і регуляторних дискусій навколо законодавчої пропозиції щодо запровадження цифрової валюти центрального банку (CBDC) у межах єврозони. У документі відображено узагальнений погляд ЄЦБ на результати досліджень, проведених приватними та галузевими структурами (зокрема PwC, Європейською банківською федерацією, національними банківськими асоціаціями та окремими банками), а також запропоновано власний розрахунок витрат з урахуванням системних синергій, ефектів взаємного використання інфраструктури та реалістичних параметрів дизайну цифрового євро.

ЄЦБ наголошує, що хоча попередні галузеві оцінки (зокрема PwC, 2025 рік) передбачали загальні інвестиційні витрати у розмірі близько €18 мільярдів для банків Єврозони, ці цифри були отримані без урахування ключових факторів, здатних суттєво знизити навантаження. Насамперед, ідеться про синергії та взаємне використання витрат, які відображають можливість банків спільно користуватися технологічними рішеннями, провайдерами, платформами, сервісами та інфраструктурою. Врахування таких чинників у моделі ЄЦБ дозволяє зменшити реалістичні оцінки до діапазону €4–5,77 мільярда загалом за чотири роки (або €1–1,44 мільярда на рік), що збігається з оцінкою Європейської комісії, викладеною у її Оцінці впливу 2023 року, де передбачалося від €2,8 до €5,4 мільярда. Таким чином, навіть за консервативного підходу витрати на впровадження цифрового євро будуть співмірними з масштабом минулих нормативних ініціатив — таких як Директива PSD2 або гармонізація платіжних систем у рамках SEPA, і суттєво меншими за витрати на останню.

Документ роз'яснює, що аналітична модель ЄЦБ спирається на комбінацію емпіричних даних, опитувань експертів, оцінок національних центральних банків, матеріалів банківського нагляду та зовнішнього консалтингу. Вона диференціює два основних рівні синергії — внутрішньогрупові (характерні для банківських груп, об'єднаних в інституційні схеми захисту (IPS)) та ринкові (які виникають між незалежними банками на рівні країни або Єврозони через спільних IT-постачальників та інфраструктуру). Для банків, які належать до великих кооперативних чи ощадних груп (наприклад, німецькі Sparkassen або Volksbanken, австрійські Raiffeisen чи іспанські Caja Rural), очікувана економія завдяки спільному використанню IT-платформ і централізованому управлінню становить від 90 % до 98 % витрат порівняно з індивідуальним впровадженням у кожній установі. Для незалежних банків у межах ринку (поза IPS-групами) синергетичний потенціал оцінюється на рівні 30 % у середньому, із варіацією від 25 % у консервативному сценарії до 40 % у випадку високої концентрації провайдерів або спільних національних рішень. Ці показники підтверджуються практичними прикладами таких міжбанківських ініціатив, як італійська CBI Globe, іспанська Redsys, португальська SIBS Multibanco, французька STET або нідерландська Geldmaat, які вже забезпечили економію витрат у діапазоні 35–50 %.

ЄЦБ також проводить корекцію початкових оцінок PwC для врахування реального дизайну цифрового євро. У результаті аналізу було знижено частину витрат на створення або оновлення інфраструктури, яка вже існує у сучасних платіжних системах. Наприклад, вартість розробки карткових інструментів зменшено на €6 мільйонів, оскільки фізичні картки цифрового євро не вимагатимуть нової технологічної архітектури; витрати на модернізацію POS-терміналів знижено на €7 мільйонів завдяки природній заміні за життєвим циклом і переходу до smartPOS і SoftPOS-рішень; інвестиції у банкомати скориговано вниз на €5,1 мільйона через поширення

NFC і QR-кодних функцій у нових пристроях, а також розвиток незалежних ATM-мереж (IADs). Загальна економія після корекцій становить приблизно 16 %, що знижує середні витрати для банків різних кластерів: для найбільших — до €152 млн, для великих — €89 млн, для середніх — €24 млн, для малих — €8 млн за чотири роки.

Методологія екстраполяції охоплює 1 929 банківських установ Єврозони, з яких 115 визнані значущими, а решта — менш значущі. До розрахунку включено лише ті кредитні установи, які мають роздрібний бізнес і будуть зобов'язані надавати послуги цифрового євро відповідно до майбутнього Регламенту. Виключено інвестиційні та спеціалізовані банки без платіжної діяльності. Врахування структури ринку дозволило ЄЦБ зробити висновок, що навіть у разі реалізації базового сценарію витрати цифрового євро становитимуть менше 1 % сукупного річного прибутку банків Єврозони або близько 3,4 % середніх IT-інвестицій великих банків у розрізі чотирьох років. Це свідчить про відсутність системного фінансового навантаження та про економічну здійсненність проєкту.

У розділі про синергетичні сценарії ЄЦБ детально розглядає три варіанти розвитку подій — низький, базовий та високий. У базовому випадку, який вважається найімовірнішим, групові синергії становлять 90–98 %, а ринкові — 30 %. Це дає загальні інвестиційні витрати в обсязі €5,77 млрд (або €1,44 млрд на рік), що відповідає верхній межі оцінки Єврокомісії. Якщо ж до уваги беруться інші галузеві дослідження (менш публічні, але більш помірковані), загальні витрати знижуються до €4–4,2 млрд. Навіть у разі песимістичного сценарію, коли синергії не реалізуються в повному обсязі, інвестиційне навантаження не перевищує €6 млрд і залишається в межах, порівнянних з попередніми трансформаціями європейської платіжної інфраструктури.

У висновку документ підкреслює, що представлена оцінка не включає потенційних позитивних ефектів цифрового євро для бізнес-моделей банків, які можуть компенсувати інвестиційні витрати. Серед них – запровадження механізмів компенсації, відсутність комісій міжнародних схем, можливість створення європейських банківських платіжних рішень на базі стандартів цифрового євро, а також покращення позицій банків у конкуренції з великими технологічними компаніями. ЄЦБ закликає до подальшої технічної співпраці та координації з банківською галуззю, щоб максимально використати синергетичний потенціал, узгодити технічні стандарти, мінімізувати дублювання процесів і забезпечити повторне використання стандартів цифрового євро в інших європейських платіжних ініціативах.

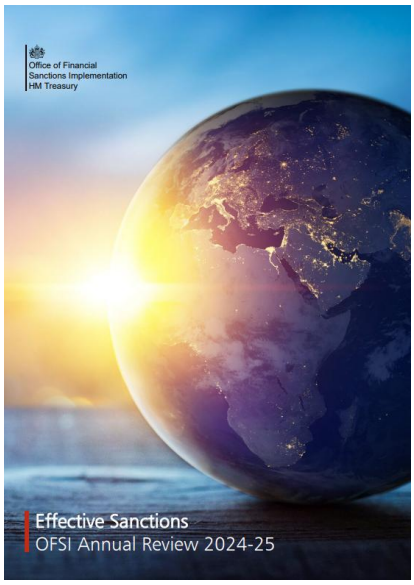
Таким чином, документ формує виважену позицію ЄЦБ щодо економічної доцільності впровадження цифрового євро. Він демонструє, що за умови системного підходу, спільного використання технологій та централізованого управління впровадженням цифрового євро інвестиційні витрати для банківського сектору залишаться контрольованими, не створюючи макрофінансових ризиків, і водночас відкриють

Висновки:

- **Реалістичний рівень інвестиційних витрат** на впровадження цифрового євро становить €4–5.77 млрд (€1–1.44 млрд на рік), що узгоджується з оцінками Єврокомісії та суттєво нижче початкових галузевих прогнозів PwC (€18 млрд).
- **Синергії та спільне використання інфраструктури** можуть зменшити витрати на 30–90 % залежно від ринку та структури банківських груп, особливо завдяки централізованим IT-провайдерам.
- **Адаптація існуючих стандартів (PSD2, SEPA, SCT Inst)** і природне оновлення обладнання дозволяють уникнути великих капітальних інвестицій у POS, ATM та карткові рішення.
- **ЄЦБ закликає до тісної співпраці між банківським сектором і регуляторами** для досягнення максимальної ефективності та своєчасного ухвалення законодавчої бази, що стане ключовою умовою успішного запуску цифрового євро.

можливості для довгострокової трансформації платіжної екосистеми Європи. Цей документ не лише узгоджує економічні очікування з фактичними технологічними реаліями, а й задає методологічну основу для подальших обговорень між ЄЦБ, національними регуляторами, законодавцями та банківським сектором, забезпечуючи перехід від теоретичного до практичного етапу реалізації цифрового євро.

Санкції нового покоління: британський підхід до ефективності, прозорості та міжнародної координації [7]



Річний звіт Управління з реалізації фінансових санкцій Великої Британії (OFSI) за 2024–2025 роки є системним аналітичним оглядом діяльності цього органу в межах стратегії «Ефективних санкцій», яка спрямована на забезпечення максимальної дієвості фінансових санкцій Великої Британії як інструменту зовнішньої політики, національної безпеки та міжнародного правопорядку. Документ підкреслює, що головним принципом роботи OFSI залишається ефективність у поєднанні з пропорційністю: санкції мають бути цілеспрямованими та результативними, завдаючи максимального впливу на об'єкти обмежень, але при цьому мінімізуючи шкоду для законного бізнесу, фінансових інститутів і громадянського сектору. У звіті зафіксовано суттєвий прогрес у трьох ключових напрямах — підвищенні рівня дотримання вимог, розвитку спроможностей та посиленні примусу, що разом забезпечують стратегічну ефективність санкційного режиму Сполученого Королівства.

Період 2024–2025 років став знаковим для OFSI, оскільки продемонстрував перехід від адміністративної реалізації санкцій до проактивної, аналітично керованої моделі управління, заснованої на співпраці з бізнесом, міжнародними партнерами та правоохоронними органами. Загальна вартість активів, заморожених відповідно до санкційного законодавства Великої Британії, досягла 37,08 мільярда фунтів стерлінгів, що на понад 50 % більше, ніж у попередньому році. Найбільшу частку становлять активи, пов'язані з росією — 22,5 мільярда фунтів, що відображає стратегічний пріоритет для уряду Великої Британії у протидії російській агресії. OFSI також зазначає зростання кількості виявлених порушень та підвищення результативності своєї системи розслідувань, що є наслідком переходу до ризик-орієнтованого та розвідувально-аналітичного підходу.

Підвищення рівня дотримання санкційного режиму розглядається як основа ефективності системи. OFSI активно розвиває інституційні канали комунікації з бізнесом та громадськістю, сприяючи кращому розумінню вимог санкційного законодавства. Протягом року відбулося понад тридцять галузевих зустрічей та конференцій за участі представників фінансового, юридичного, криптоактивного, морського, благодійного секторів, а також професійних спільнот, які нещодавно були охоплені вимогами звітності — агентів із нерухомості, арбітражних керуючих, учасників арт-ринку та торговців коштовностями. Значною ініціативою стало створення оновленої системи електронних сповіщень у співпраці з Міністерством закордонних справ (FCDO) та Офісом з реалізації торгівельних санкцій (OTSI), яка охопила понад 56 тисяч користувачів і забезпечує миттєве інформування про нові обмеження, ліцензії та зміни до санкційних списків. Відзначено й запуск нової платформи «Поширені запитання», яка містить 145 докладних роз'яснень і практичних інструкцій, що допомагають бізнесу уникати

[7] https://assets.publishing.service.gov.uk/media/68ef7ec68427701993d5e0d9/OFSI_Annual_Review_2024-25.pdf

непорозумінь і підвищують прозорість регулювання. У межах блоку дотримання вимог OFSI також здійснило 904 окремі рішення щодо ліцензування (на противагу 1401 роком раніше), що свідчить про підвищення оперативності процесів, та видало 19 загальних ліцензій, зокрема для врегулювання питань арбітражних витрат, персональних переказів і спрощення транзакцій із низьким рівнем ризику. Таким чином, регуляторна політика набула більш передбачуваного та бізнес-орієнтованого характеру без шкоди для санкційної строгості.

Другим важливим напрямом є розвиток спроможностей OFSI, спрямований на підвищення аналітичної, технічної та міжнародної потужності санкційного механізму. На кінець звітного періоду консолідований список санкцій налічував 4733 суб'єкти — 3750 фізичних осіб, 968 юридичних осіб та 15 суден. Найбільшу частку займають російські підсанкційні особи — 2113 позицій, або 44,6 % від загальної кількості. У межах контртерористичного напрямку OFSI вперше застосувало автономні національні санкції, зокрема проти фінансиста ірландської терористичної організації New IRA та праворадикальної групи Blood and Honour, що засвідчує розширення санкційного інструментарію для боротьби з новими типами загроз. Посилено міжнародну співпрацю — проведено понад 210 заходів у 44 юрисдикціях, а стратегічним проривом стало підписання Меморандуму про взаєморозуміння з Міністерством фінансів США (OFAC), що заклало основу для регулярного обміну аналітичними даними, спільних розслідувань і уніфікації стандартів санкційного нагляду. Не менш значущим стало поглиблення взаємодії з Європейським Союзом, включно з регулярними зустрічами з DG FISMA, координацією позицій щодо обмежень на експорт російської нафти та проведенням спільних інформаційних сесій у ключових портових центрах світу. На законодавчому рівні уряд ухвалив зміни до «Sanctions (EU Exit) (Miscellaneous Amendments) (No.2) Regulations 2024», які розширили коло «релевантних фірм», посилили повноваження OFSI у сфері ліцензування та примусу, а також запровадили нові виключення, що спрощують здійснення регуляторних платежів. Важливим напрямом стала реалізація урядової «Ініціативи економічного стримування», у межах якої OFSI впровадило нові стандарти управління даними, вдосконалило моніторинг ліцензій, запровадило систему післяліцензійного супроводу, розширило юридичну підтримку та значно підвищило кадрову компетенцію шляхом проведення понад 50 спеціалізованих тренінгів.

У напрямі забезпечення виконання OFSI продемонструвало значний прогрес у побудові сучасної, інтелектуально-керованої системи примусу, що базується на аналітиці, партнерстві та пропорційності. У 2024–2025 роках управління здійснило 57 заходів примусу, серед яких два гучних штрафи — £465 000 проти юридичної фірми «Herbert Smith Freehills LLP» за порушення санкційних обмежень у період згортання московського офісу та £15 000 проти «Integral Concierge Services Limited». На момент завершення звітного року OFSI вело 240 активних розслідувань, причому зросла частка справ, виявлених не в результаті самозвітування (151 випадок проти 108 роком раніше), що свідчить про якісне зростання аналітичної спроможності та інтеграції розвідувальної інформації. Найбільше порушень зафіксовано у фінансовому та юридичному секторах, а також у сфері криптоактивів, страхування, житла, морських перевезень і неприбуткових організацій. Вперше створено спеціалізовану команду Compliance Enforcement, яка займається моніторингом дотримання умов ліцензій та виявленням зловживань у цій сфері. Такі кроки дозволили скоротити терміни реагування, забезпечити більш рівномірний підхід до різних секторів і водночас зміцнити довіру бізнесу до справедливості санкційного режиму.

Щорічний звіт «Огляд заморожених активів» засвідчив не лише масштабність, а й підвищену якість аналітичного контролю за замороженими активами: загальна сума перевищила 37 мільярдів фунтів, з яких 13 мільярдів припадає на Лівію, 1,17 мільярда — на Білорусь, 384 мільйони — на Сирію. Окремо зазначено, що з лютого 2022 року у зв'язку з російським вторгненням OFSI зафіксував повідомлення про замороження активів на суму понад 28,7 мільярда фунтів. Попри спроби обходу санкцій через переміщення активів із Національного

депозитарію рф, британські установи забезпечили повне документування таких випадків, зберігаючи достовірність статистики. У розділі «Подальші кроки» зазначено стратегічні орієнтири на 2025–2026 роки: оновлення загальної стратегії до 10-річчя створення OFSI, розвиток цифрових інструментів звітності (нові онлайн-форми для повідомлень і ліцензій), запровадження освітнього відеоциклу «Фінансові санкції: основи» для малого бізнесу, удосконалення процедур цивільного примусу, а також впровадження механізмів захисту викривачів відповідно до Наказу про розкриття інформації в суспільних інтересах 2025 року. Крім того, передбачено продовження співпраці з міжнародними партнерами щодо зміцнення дії «Механізму граничної ціни на нафту» і подальшого посилення тиску на російські джерела фінансування війни.

Звіт завершується висновком, що ефективність санкційної політики Великої Британії нині ґрунтується на трьох взаємопов'язаних чинниках — зрозумілому та відкритому діалозі з бізнесом, зміцненні аналітичних і міжнародних спроможностей, а також системному підході до примусу, який забезпечує невідворотність відповідальності за порушення. OFSI послідовно трансформується з адміністративного підрозділу у стратегічний центр санкційної політики держави, який поєднує гнучкість сучасного управління, суворість правозастосування та орієнтацію на результат. Саме завдяки цьому санкційна система Сполученого Королівства, за оцінкою OFSI, залишається однією з найефективніших у світі, а її досвід стає зразком для партнерів по G7, ЄС і інших країн, що протистоять загрозам глобальної безпеки.

Висновки:

- **Санкційна ефективність значно зросла:** обсяг заморожених активів зріс до £37 млрд (+50 % р/р), що підтверджує дієвість британської системи фінансових обмежень, зокрема проти рф.
- **Зміщення до інтелектуально-керованої моделі примусу:** створення Команди з забезпечення дотримання санкцій (Compliance Enforcement Team) і використання OSINT-та розвідданих методів для виявлення порушень без самостійного повідомлення суб'єктів (151 випадок у 2024–25).
- **Посилена міжнародна координація:** підписання Меморандуму про взаєморозуміння з OFAC, спільна робота з ЄС та G7+ щодо механізму граничної ціни на нафту, розширення зв'язків із 44 юрисдикціями, включаючи Британські Віргінські острови та Кайманові острови.
- **Підвищення прозорості й доступності:** запуск 145 роз'яснень у форматі «Поширені запитання» (FAQ), оновленого вебпорталу та системи електронних сповіщень (e-alerts), якою користуються понад 56 тисяч суб'єктів. Це створює єдине інформаційне середовище для бізнесу, забезпечує своєчасне отримання оновлень щодо санкцій і підвищує рівень дотримання вимог у сфері фінансового моніторингу.

Проект регуляторних технічних стандартів щодо ризику коригування кредитної оцінки операцій з фінансування цінних паперів [8]

Цей документ, розроблений Європейським банківським органом (EBA), є імплементацією переглянутих вимог до власних коштів для покриття ризику коригування кредитної оцінки (CVA), що встановлені в Регламенті (ЄС) № 575/2013 (CRR), зміненому CRR3. Основний зміст та ключові аспекти проєкту полягають у визначенні чітких умов і критеріїв, які фінансові установи повинні

[8] https://www.eba.europa.eu/sites/default/files/2025-10/ed09f5f3-babd-44bb-a721-5e7a72a13e06/Final%20Report%20on%20draft%20RTS%20on%20CVA%20risk%20of%20SFTs.pdf

використовувати для об'єктивної оцінки суттєвості (матеріальності) ризику CVA, що виникає внаюнслідок операцій з фінансування цінних паперів (SFTs), які оцінюються за справедливою вартістю. Згідно зі статтею 382(2) CRR, установа повинна включати такі SFTs до розрахунку власних коштів для покриття ризику CVA, якщо ризик, що виникає від них, є суттєвим.

Проєкт RTS впроваджує кількісний підхід для визначення цієї суттєвості. Цей підхід був обраний як кращий варіант (порівняно з якісним або змішаним) для забезпечення об'єктивності, єдиних правил гри та узгодженості практик між установами в усьому ЄС, що, як очікується, знизить необхідність посиленого наглядового контролю. Методологія ґрунтується на метриці вимог до власних коштів для покриття ризику CVA, оскільки вона найбільш релевантна для оцінки ризику, що є предметом регулювання.

Для оцінки суттєвості використовується спеціальний коефіцієнт (Ratio), який кількісно визначає відсоткове збільшення ризику CVA внаслідок включення SFTs, оцінених за справедливою вартістю, до загального обсягу вимог до власних коштів. Коефіцієнт розраховується за формулою: Ratio = (a – b) / b, де «a» — це загальні вимоги до власних коштів для покриття ризику CVA, включаючи оцінені за справедливою вартістю SFTs, а «b» — це загальні вимоги до власних коштів для CVA ризику, виключаючи ці SFTs. Цей підхід, що оцінює маргінальний вплив, був обраний з урахуванням нелінійності формул спрощеного та стандартизованого підходів (SA-CVA та BA-CVA).

Поріг суттєвості встановлений на рівні 5%. Якщо розрахований коефіцієнт дорівнює або перевищує 5%, то ризик CVA, що виникає від цих SFTs, вважається суттєвим, і такі операції повинні бути включені до розрахунку капітальних вимог. Важливо, що оцінка суттєвості проводиться на основі сукупного ризику CVA від усіх SFTs, оцінених за справедливою вартістю; якщо поріг перевищено, всі такі SFTs включаються до розрахунку капіталу.

Щодо частоти оцінки, проєкт RTS встановлює її на щоквартальній основі. Це рішення прийнято для забезпечення узгодженості з регулярним циклом розрахунку та звітності щодо власних коштів. Конкретні звітні дати для оцінки — 31 березня, 30 червня, 30 вересня та 31 грудня. EBA переглянула початкові пропозиції щодо «стабілізаційних механізмів» (які вимагали б капіталізації на основі минулих кварталів) і вирішила, що оцінка повинна ґрунтуватися виключно на співвідношенні, що стосується поточної звітної дати. Це забезпечує відповідність принципу капіталізації ризику CVA лише тоді, коли він дійсно є суттєвим на даний момент (point-in-time assessment).

Також необхідно відзначити, що ці RTS та вимоги до капіталу для CVA ризику не застосовуватимуться до SFTs, які підпадають під встановлені винятки згідно зі статтею 382(3) та (4) CRR (наприклад, операції з нефінансовими та суверенними контрагентами), якщо тільки установа не вирішить добровільно їх включити. Це підтверджує, що ЄС вже має певні конкурентні переваги у своєму регуляторному полі, незважаючи на розбіжності у підході з регуляторами США чи Великої Британії, які застосовують якісні або повні виключення. При

розрахунку коефіцієнта установи повинні використовувати ті самі підходи та вимоги CRR щодо визнання забезпечення (collateral) та хеджування CVA, які вони застосовували б у будь-якому випадку. Загалом, EBA вважає, що очікувані переваги від встановлення єдиного, об'єктивного, кількісного підходу перевищують потенційні витрати, які можуть понести установи.

Висновки:

- **Запровадження щоквартального моніторингу суттєвості:** Установи повинні негайно інтегрувати кількісну методологію розрахунку коефіцієнта (Ratio = (a – b) / b) у свої внутрішні системи для фінансового та наглядового звітування. Оцінка суттєвості повинна проводитися щоквартально (31 березня, 30 червня, 30 вересня, 31 грудня), забезпечуючи готовність до синхронізації з циклом звітності COREP.
- **Дотримання порогового значення 5%:** Керівництву з ризик-менеджменту необхідно сфокусувати увагу на критичному порозі у 5%. Якщо розрахований коефіцієнт, що відображає маргінальний вплив SFTs на вимоги до CVA-капіталу, дорівнює або перевищує цей поріг на поточну звітну дату, необхідно невідкладно включити всі SFTs, оцінені за справедливою вартістю, до розрахунку регуляторних вимог до власних коштів для покриття ризику CVA.
- **Узгодження методології розрахунку CVA:** Для забезпечення достовірності коефіцієнта, установам слід використовувати ті ж самі підходи (наприклад, SA-CVA або BA-CVA) та правила визнання забезпечення і хеджування, які вони застосовують для розрахунку загальних вимог до CVA ризику згідно з CRR. Це вимагає єдності внутрішніх даних та методологій для уникнення розбіжностей між регуляторними розрахунками та оцінкою суттєвості.
- **Управління регуляторним периметром:** Враховуючи, що RTS не застосовуються до SFTs, які підпадають під винятки CRR (наприклад, операції з суверенними контрагентами), необхідно забезпечити чітку класифікацію SFTs та їхнє виключення з чисельника коефіцієнта, якщо вони законно звільнені від вимог CVA-капіталу.

Звіти окремих інституцій та експертів

Робоча група RUSI з кіберсанкцій: протидія кіберзагрозам, що підтримуються державою [9]

Стаття аналізує роль санкцій як інструмента реагування кіберзагрози, які походять від держав, виходячи з роботи Royal United Services Institute (RUSI) та їхньої ініціативи Cyber Sanctions Taskforce. Автори підкреслюють, що сучасні кібероперації держав (чи їхніх проксі) часто ведуться не у формі великих вибухових атак, а як тривала діяльність — інфільтрація, «pre-positioning», збір розвідданих, підготовка майбутніх ударів. Така модель означає, що реагування тільки після події не є достатнім: необхідно системне, перманентне стримування. На цьому базується аргумент про те, що санкції мають

[9] https://www.rusi.org/explore-our-research/publications/insights-papers/rusi-cyber-sanctions-taskforce-countering-state-backed-cyber-threats

бути не просто символічними чи одиничними заходами, а частиною стратегії, яка робить здійснення кібероперацій для супротивника дорожчим, повільнішим, ризикованішим.

У статті детально порівнюються підходи трьох ключових юрисдикцій — США, ЄС і Великої Британії. Сполучені Штати мали найтривалішу практику застосування санкцій проти кіберзагроз (наприклад, за виконавчим указом Executive Order 13694 від 2015 р.). Їхня стратегія включає іменні лістинги виконавців чи посередників, жорсткий технологічний/фінансовий тиск, кримінальні обвинувачення, що підсилює мультидоменний підхід. Водночас відповідь і ефект значною мірою залежать від типу супротивника (Іран, КНДР, РФ) і наявності відповідних важелів. ЄС, із запуском горизонтального режиму санкцій у 2019 році, застосував його обережно — імовірно через вимогу одностайності, обмежену публічність доказової бази та складність моніторингу ефекту. У Великій Британії після виходу з ЄС автономна санкційна політика також розвивається, з акцентом на координацію із союзниками, але без такої глибинної кримінальної складової, як у США.

Ключовий акцент статті — на тому, що санкції мають бути застосовані в межах кампанії, а не як розрізнені заходи. Це означає, що обмеження активів, замороження, публічна атрибуція, технічні попередження, дипломатичні демарші та кримінальні обвинувачення мають працювати синхронно. Лише так можна не просто покарати, а змінити поведінку, ускладнити бізнес-моделі, підвищити ризики і витрати участі у зловмисних операціях. Водночас автори зазначають, що для максимального ефекту задля цілей стримування важливо таргетувати не тільки виконавців атак, але й інфраструктурних посередників — криптобіржі, міксери, хостинг-послуги, технологічні постачальники, брокери — тобто ті, хто забезпечує бізнес-модель.

У статті також наголошується на потребі підвищення прозорості, збільшення змістовності публічних повідомлень про санкції та забезпечення моніторингу їхнього впливу. Автори радять створювати публічні «методички» чи технічні довідники для приватного сектору, щоб компанії могли краще зрозуміти механіку включення до списків, а регулятори мали змогу оцінювати ефект. Вказано, що без чіткого вимірювання (скільки активів заморожено, скільки сервісів відмовлено, на скільки знизився обсяг операцій) важко довести ефективність чи скоригувати політику.

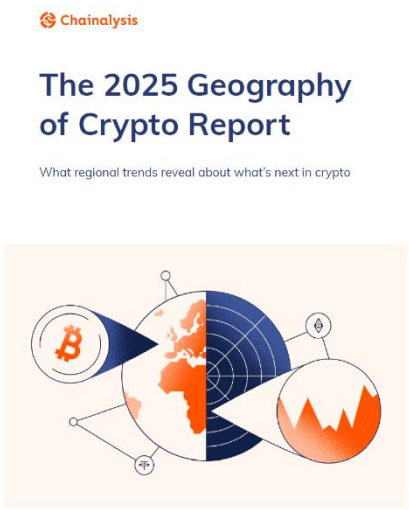
Загалом, висновком є те, що санкції вже стали усталеним елементом стратегії кіберстримування у США, ЄС і Великій Британії. Однак вони не є панацеєю — самі по собі не «припиняють» кіберзагрозу, але можуть значно підвищити вартість і ризики для держав-акторів чи їхніх проксі. Майбутнім завданням стає зробити санкції менш символічними і більш результативними

Висновки:

- **Чітко формулюйте «поведінкову мету» для кожного лістингу:** яку саме діяльність має бути ускладнено або зупинено, і вимірюйте відповідні показники — наприклад, зниження доступу до сервісів, зростання витрат зловмисників.
- **Використовуйте санкції в складі комплексної кампанії:** поєднуйте лістинги з дипломатичними демаршами, технічними попередженнями, кримінальними обвинуваченнями, акціями із заморожування активів.
- **Орієнтуйтеся на посередників кібероперацій - інфраструктуру**, технологічних та фінансових посередників - оскільки саме через них супротивник масштабує операції; знищення або ускладнення їхньої роботи дає мультиплікативний ефект.
- **Забезпечуйте високу прозорість та міжнародну координацію:** публікуйте технічні/доказові довідки до санкційних рішень; узгоджуйте дії із союзниками; впровадьте механізми моніторингу й оцінки ефекту — скільки сервісів було припинено, скільки коштів/активів заморожено, чи знизився обсяг злочинної діяльності.

через точніше таргетування, кращу доказову базу, більш тісну координацію між юрисдикціями та прозоре замірювання впливу.

Глобальна карта криптоекономіки 2025: як світ переходить від спекуляцій до інституційного прийняття цифрових активів [10]



Документ є одним із найповніших аналітичних звітів про сучасну географію прийняття криптовалют у світі. Він відображає фундаментальні зміни у глобальній структурі криптоекономіки, вказує на домінуючі регіони, економічні рушії, соціально-політичні фактори та трансформацію ролі криптовалют у фінансових системах. На основі даних, зібраних з понад 13 мільярдів вебвідвідувань і сотень мільйонів транзакцій, аналітики Chainalysis побудували Глобальний індекс прийняття криптовалют (2025), який охоплює 151 країну та оцінює ступінь «вкоріненості» криптовалют у різних типах економік. Методологія індексу передбачає чотири основні субіндекси: обсяг отриманих на централізовані сервіси криптоактивів, роздрібні транзакції, обсяг операцій у DeFi-протоколах та інституційні перекази, усі скориговані на показник ВВП за паритетом купівельної спроможності. У 2025 році аналітична модель зазнала суттєвих змін — з неї вилучили «роздрібний DeFi-субіндекс», який виявився статистично надмірним, і натомість додали показник інституційної активності, що дозволило краще відобразити нову хвилю проникнення криптовалют у традиційні фінансові ринки.

Звіт фіксує, що Індія та США очолили рейтинг глобального прийняття криптовалют, проте характер лідерства цих країн має принципово різну природу: Індія демонструє переважно содель адаптації «згори до низу», тобто масове залучення населення через мобільні додатки, торгові платформи й перекази, тоді як США формують процес прийняття «згори до низу» через ETF, банки, регульовані кастодіальні сервіси й токенізацію активів. Особливо примітним є те, що серед перших десяти країн опинилися переважно держави Глобального Півдня (країни, що розвиваються) — Пакистан, В'єтнам, Бразилія, Нігерія, Індонезія, Філіппіни — що свідчить про те, що криптовалюта перестала бути лише інструментом спекуляції, а стала реальним фінансовим засобом для збереження вартості, доступу до долара, переказів і розрахунків у нестабільних економіках.

Вперше в історії Україна досягла рекордного результату — 8 місця у світі в загальному рейтингу та 1 місця у світі після коригування на чисельність населення, що демонструє унікальний рівень проникнення криптовалют у повсякденну економічну активність українців. Chainalysis пояснює цей феномен поєднанням трьох факторів: високою технічною грамотністю населення, недовірою до традиційних банківських інститутів через воєнні та економічні ризики, а також активним використанням криптовалют для міжнародних транзакцій, донатів і збереження вартості на тлі валютних обмежень. Таким чином, Україна розглядається як один із провідних прикладів «східноєвропейського криптопіднесення», разом із Молдовою та Грузією, де криптовалюта поступово інтегрується у національні фінансові процеси, створюючи нову культуру цифрових фінансів.

Глобальні дані свідчать про те, що в період з липня 2024 до червня 2025 року наступила ера масової інституціоналізації крипторинку. Серед найбільш визначних процесів — стрімке

[10] https://go.chainalysis.com/2025-geography-of-cryptocurrency-report.html

зростання обсягів торгівлі токенізованими державними облігаціями США, що майже вчетверо збільшили активи під управлінням за рік (до понад $7 млрд), а також запуск і швидка експансія біткоїн-ETF з активами понад $179 млрд, більшість із яких припадає на американські фонди. Це означає, що криптовалюти фактично перетворилися на регульований клас активів у традиційній фінансовій системі. У США ключовим каталізатором цього процесу стало ухвалення GENIUS Act у липні 2025 року, який установив дворівневу систему регулювання стейблкоїнів і фактично визнав їх фінансовими інструментами під федеральним і штатним наглядом.

Водночас у Європейському Союзі запровадження Регламенту MiCA радикально змінило структуру ринку — обмеживши використання нерегульованих стейблкоїнів і створивши умови для розвитку локальних токенів, прив'язаних до євро. Стейблкоїн EURC, випущений Circle у відповідності до MiCA, зріс на 2727 % за рік, витісняючи USDC і USDT з європейських ринків. Такі процеси не лише посилюють європейську фінансову автономію, а й створюють модель прозорого регулювання для решти світу. На противагу, у США ринок стейблкоїнів залишився домінантно доларовим, і загальний обсяг транзакцій із ними у першому півріччі 2025 року сягнув $12,7 трлн, що свідчить про закріплення «глобальної доларового цифрового домінування».

Регіональний аналіз підкреслює, що Азійсько-Тихоокеанський регіон (APAC) став найдинамічнішим осередком криптоактивності у світі, збільшивши транзакційний обсяг на 69 %. Індія залишається найбільшим ринком із понад $338 млрд обігу, де криптовалюта інтегрована у цифрову фінансову екосистему поряд із системами UPI та eRupi. Південна Корея характеризується високою часткою «професійної торгівлі», а Японія — найшвидшими темпами зростання завдяки лібералізації податкової політики та появі ліцензованих стейблкоїнів, забезпечених єною. В'єтнам і Пакистан і надалі демонструють змішану модель використання — одночасно для переказів, заощаджень і малого бізнесу.

Північна Америка, за підрахунками, охоплює 26 % світової криптоактивності. США забезпечили собі лідерство не лише через обсяги транзакцій ($2,3 трлн за рік), а й через найрозвиненішу регуляторну інфраструктуру. Скасування «регулювання через покарання» з боку SEC і запровадження єдиних принципів для банків та інвестиційних компаній перетворили крипторинок на інституційний сегмент фінансової системи. Цікаво, що в 2024–2025 роках біткоїн зберіг стабільну частку — 42 % усіх фіатних придбань, що підтверджує його статус базового цифрового активу.

Латинська Америка представлена бурхливим, хоча й волатильним ростом: з 2022 по 2025 рік регіон зафіксував сукупний обсяг транзакцій у $1,5 трлн, а Бразилія стала беззаперечним лідером із $318,8 млрд обігу. Висока інфляція та валютні обмеження стимулюють використання стейблкоїнів, які становлять понад 90 % криптопотоків у країні. Аргентина, Мексика, Венесуела й Колумбія також демонструють високу адаптацію криптовалюти як «паралельної фінансової системи», що забезпечує стабільність там, де місцеві валюти стрімко знецінюються.

Субсахарська Африка продовжує підтверджувати статус «лабораторії реальної корисності криптовалют». Регіон зріс на 52 % і досяг $205 млрд річного обігу, з чого найбільша частка припадає на Нігерію ($92 млрд) і Південну Африку. Тут криптовалюта стала не стільки інвестиційним інструментом, скільки елементом базової фінансової інфраструктури для населення без банківського доступу. Нігерія використовує стейблкоїни як заміну долару на тлі інфляції та валютних обмежень, тоді як Південна Африка виділяється розвиненим регулюванням і ліцензуванням постачальників віртуальних активів.

Європа у 2025 році постає як ринок зрілого типу з мережевими ефектами: зростання відбувається навіть у великих економіках, що вже насичені криптосервісами. Загальний обсяг транзакцій перевищив $2,6 трлн, причому 54 % приросту продемонструвала Німеччина, 52 % — Україна, 51 % — Польща. Впровадження MiCA гармонізувало ринок, сприяло входженню банків

і платіжних компаній у сферу цифрових активів і спричинило бум локальних єврових стейблкоїнів. Водночас зростає частка DeFi-операцій, особливо у Великій Британії та росії, що свідчить про структурну трансформацію європейського ринку від централізованих бірж до децентралізованих платформ.

Регіон Близького Сходу і Північної Африки показує складну картину. Туреччина утримує домінування, незважаючи на інфляцію та валютну кризу, з кумулятивним обсягом операцій понад $878 млрд. Проте звіт відзначає спад роздрібної активності, що пояснюється зростанням бідності населення і посиленням регуляцій відповідно до стандартів FATF. Паралельно спостерігається сплеск спекулятивних операцій з альткоїнами, що створює ризики для фінансової стабільності. Об'єднані Арабські Емірати і далі розвивають модель «регульованої інноваційної юрисдикції», тоді як Ізраїль використовував криптовалюти як механізм фінансової гнучкості під час військової кризи.

Висновки:

- **Україна — глобальний лідер за рівнем криптоактивності на душу населення,** що свідчить про високий рівень цифрової грамотності та довіри до криптовалют як альтернативного фінансового інструменту.
- **Інституціоналізація крипторинку** (через ETF, токенізовані активи та регульовані стейблкоїни) перетворює криптовалюти на повноцінний клас активів у світовій фінансовій системі.
- **Регуляторна гармонізація — ключовий чинник розвитку:** MiCA в ЄС і GENIUS Act у США створюють нову парадигму легального крипторинку, зміцнюючи роль долара й євро у цифрових розрахунках.
- **Глобальний тренд зміщується на Південь і Схід,** де криптовалюта виконує прикладні функції — від захисту від інфляції до фінансової доступності, формуючи «нову фінансову географію» світу.

У ширшому контексті звіт робить висновок, що глобальна криптоадаптація більше не обмежується країнами з високим доходом. Тенденція «синхронізації темпів зростання» означає, що країни з високим, середнім і низьким рівнем доходу нині демонструють схожі темпи росту. У багатьох з них криптовалюта стала засобом фінансової інклюзії, компенсації банківських прогалин і захисту від валютної волатильності. Водночас у державах із низьким доходом прогрес залишається нестійким через інфраструктурні й політичні обмеження.

Загальний висновок Chainalysis полягає в тому, що 2025 рік став точкою переходу від «крипторинку» до «криптоекономіки». Криптовалюти перестали бути маргінальним або спекулятивним феноменом — вони стали системним інструментом у міжнародних фінансах, елементом макроекономічних політик і фактором валютної геополітики. Нові регуляторні режими у США та ЄС, інституційні інвестиції через ETF і токенізовані облігації, а також стрімке зростання APAC та Латинської Америки формують нову багатополярну архітектуру цифрових фінансів. Україна, відповідно до цього звіту, виступає унікальним прикладом держави, де криптовалюта стала одночасно інструментом стійкості, мобілізації ресурсів і цифрової трансформації фінансової системи, що поєднує практичне використання, технологічний розвиток і високу адаптивність суспільства.

Рекомендовані матеріали та події

Вебінар щодо сприяння фінансовій інклюзії за допомогою ризик-орієнтованого підходу до ПВК/ФТ[11]

FATF повідомив про проведення важливого вебінару, присвяченого ключовим змінам у сфері ПВК/ФТ у контексті забезпечення фінансової інклюзії. Вебінар має на меті сприяти впровадженню ризик-орієнтованого підходу з метою розвитку фінансової інклюзії.

Обговорення буде зосереджено на поясненні ключових змін в оновлених Стандартах та оновленому Керівництві FATF щодо фінансової інклюзії та заходів ПВК/ФТ. Учасники зможуть ознайомитися з практичними методами та конкретними прикладами впровадження (case studies). Крім того, на вебінарі будуть висвітлені виклики, з якими стикаються як наглядові органи, так і фінансові установи.

Вебінар відбудеться 19 листопада 2025 року. Час проведення: 13:00–14:30 за центральноєвропейським часом (CET). Робоча мова вебінару – англійська з можливістю перекладу французькою мовою.

У заході візьмуть участь висококваліфіковані фахівці:

• Модератор: Такахіде Хабучі (Takahide Habuchi), співголова PDG.

• Спікери:

◦ Катрін Діон (Catherine Dion) – співкерівниця проектної групи / Директор Департаменту ПВК/ФТ у Міністерстві юстиції Люксембургу.

◦ Робін Ньюнхем (Robin Newnham) – керівник відділу аналізу політики та розбудови потенціалу в Альянсі за фінансову інклюзію (Alliance for Financial Inclusion).

◦ Елен Ерфтемеєр (Helène Erftemeijer) – галузевий координатор ПВК/ФТ та санкцій у Нідерландській банківській асоціації (Dutch Banking Association).

Вебінар буде корисним для представників наглядових органів та фінансових установ, які прагнуть впровадити ефективний ризик-орієнтований підхід та сприяти фінансовій інклюзії, дотримуючись при цьому стандартів ПВК/ФТ.

Як взяти участь та реєстрація:

Для участі необхідно пройти реєстрацію. Реєстрація здійснюється через платформу Zoom за посиланням. Крайній термін реєстрації: 17 листопада 2025 року.

Інша важлива інформація:

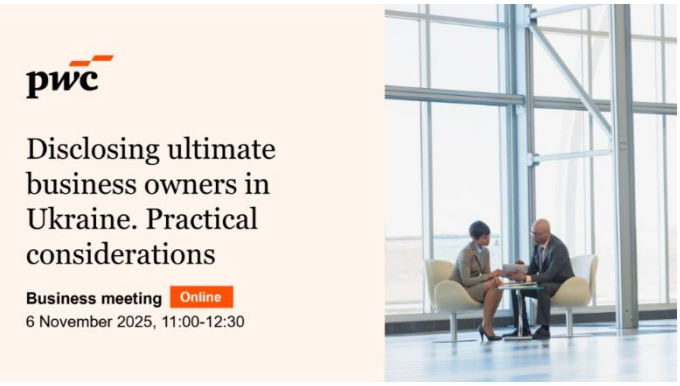
1. Запитання та опитування: Учасникам пропонується заповнити коротке опитування, щоб поділитися своїм досвідом та поглядами щодо впровадження ризик-орієнтованого підходу. Питання до спікерів можна надіслати заздалегідь під час реєстрації через Zoom або електронною поштою до Секретаріату.

[11] https://us02web.zoom.us/webinar/register/WN_IPMM4HqVSSaO4K6zvD4hSw#/registration

2. Запис вебінару: Запис вебінару буде доступний після заходу та опублікований у Спільноті PDG, а також на YouTube-каналі FATF.

3. Контактна інформація: У разі виникнення будь-яких питань, будь ласка, звертайтеся за адресою: pdg@fatf-gafi.org.

Розкриття кінцевих бенефіціарних власників в Україні. Практичні аспекти [12]



6 листопада відбудеться онлайн-зустріч на тему «Розкриття кінцевих бенефіціарних власників в Україні. Практичні аспекти», яку організовує компанія PwC. Захід проходитиме з 11:00 до 12:30.

Під час вебінару експерти зосередяться на актуальних регуляторних вимогах щодо розкриття структури власності та кінцевих бенефіціарних власників (КБВ) в умовах воєнного стану. Буде розглянуто чинну законодавчу базу, практичні аспекти застосування її положень, а також типові випадки невідповідності структури власності та наслідки нерозкриття інформації.

Спікерами виступлять фахівці практики банківського, фінансового та корпоративного права:

- Вадим Романюк - Старший менеджер, керівник практики Банківського, фінансового та корпоративного права АО PwC Legal в Україні;
- Ольга Бутник - Менеджерка практики Банківського, фінансового та корпоративного права АО PwC Legal в Україні; та
- Михайло Франчук - Старший консультант практики Банківського, фінансового та корпоративного права АО PwC Legal в Україні.

Захід розрахований на керівників компаній, юристів та інших фахівців, відповідальних за корпоративне управління та дотримання нормативних вимоG.

Участь у вебінарі безкоштовна, мова проведення — українська. Для участі необхідна попередня реєстрація за посиланням.

Інші новини

Юрисдикції під посиленим моніторингом [13]

На своєму пленарному засіданні FATF оновила перелік країн, які входять до так званого сірого списку. За визначенням FATF, «юрисдикції під посиленим моніторингом» — це країни, які визнали наявність стратегічних прогалин у режимах ПВК/ФТ/ФР, взяли політичні зобов'язання їх швидко усунути та звітують про прогрес, але щодо них FATF не закликає застосовувати заходи посиленої обачності як до «високоризикових»; натомість очікується ризик-орієнтований підхід і недопущення переривання легітимних потоків (гуманітарна допомога, діяльність НПО, грошові перекази) з урахуванням гуманітарних винятків Ради Безпеки ООН. Саме така логіка пояснює,

[12] https://contents.pwc.com/LP=6913
[13] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2025.html

чому «сірий список» — це не «санкційний вирок», а дорожня карта виправлення недоліків під наглядом FATF і Регіональних органів типу FATF (FSRBs).

Станом на жовтень 2025 року до «сірого списку» належать Алжир, Ангола, Болівія, Болгарія, Камерун, Кот-д'Івуар, Демократична Республіка Конго, Гаїті, Кенія, Лаоська НДР, Ліван, Монако, Намібія, Непал, Південний Судан, Сирія, Венесуела, В'єтнам, Британські Віргінські Острови та Ємен. Разом ці 20 юрисдикцій репрезентують широкий спектр прогалин: від недостатнього ризик-орієнтованого нагляду за фінансовими установами та ВНУП (DNFBPs), доступу до бенефіціарної власності і санкцій за порушення прозорості — до неналежного використання фінансової розвідки, відсутності розслідування/переслідування ВК/ФТ відповідно до ризик-профілю, конфіскації активів, а також невчасного запровадження цільових фінансових санкцій з ФТ і ФР. Окремі країни мають специфічні статуси: наприклад, Сирія та Ємен технічно закрили більшість дій Плану, але чекають на виїзну перевірку FATF через безпекові умови; Британські Віргінські Острови зобов'язалися підвищити якість SAR, ризик-орієнтований нагляд за VASP/TCSP та забезпечити повноцінний доступ до даних про КБВ; Кенія ще має підсилити нагляд за високоризиковими секторами; Алжир і Ангола у блоці країн, яким потрібно довести дієвість нових процедур нагляду і санкцій за порушення норм щодо КБВ, покращення STR, аналітичних спроможностей ПФР та вбудовування ризик-орієнтованого підходу до НПО. Болівія та Болгарія звітують про законодавчі реформи і посилення санкційного режиму, але ключовим маркером виходу з процесу лишається відповідність переслідувань і конфіскацій їх реальним ризикам, а не лише нормотворчий прогрес. Ці акценти добре видно у поточних заявах FATF, де кожна юрисдикція має свій план дій.

В той же час Буркіна-Фасо, Мозамбік, Нігерія та ПАР були вилучені із «сірого списку» після підтвердження суттєвого прогресу — від посилення координації, ризик-орієнтованого нагляду та прозорості КБВ до приросту використання фінансової розвідки, розслідувань і конфіскацій. Ці рішення підкреслюють, що критерієм є не декларації, а результативність (синхронізація національних стратегій із ризиками, міжвідомча практика, якісні STR/SAR, приріст справ по ВК/ФТ).

Ваша думка важлива!

1. Як держави можуть ефективно виявляти та запобігати залученню власних громадян у схеми, що сприяють обходу санкцій?
2. Як міжнародна координація між OFSI, OFAC, ЄС та G7 може посилити спроможність України протидіяти обходу санкцій через треті країни, особливо у сфері криптоактивів та експорту високоризикових товарів?
3. Який підхід до регулювання CASPs (криптосервіс-провайдерів) є найбільш ефективним — європейський (MiCA) чи американський (CLARITY/GENIUS Acts)?
4. Як впровадження глобальних регуляторних рамок — таких як MiCA в ЄС чи GENIUS Act у США — може вплинути на національне законодавство України у сфері ПВК/ФТ та регулювання віртуальних активів?
5. Як Україна може використати свій досвід роботи АРМА для формування власної моделі соціального повторного використання активів, яка відповідала б стандартам ЄС і водночас враховувала специфіку післявоєнного відновлення?
6. Які соціально-економічні групи в Україні потенційно «виграють», а які можуть зазнати ризиків у разі переведення державних виплат у формат цифрової гривні (CBDC), і як це вплине на рівень фінансової інклюзії?
7. Які ризики і переваги матиме для банківського сектору України впровадження подібного до цифрового євро підходу з урахуванням спільного використання інфраструктури та синергій між державними і приватними учасниками платіжного ринку?

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-2025-44

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

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