Методологічний бюлетень

Серійний номер: МінФін-AML-2025-22

Травень 2025

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

Пітер Маршалл

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Найкращі практики щодо належної перевірки джерел багатства [1]

Документ, розроблений у рамках галузевого партнерства з питань протидії відмиванню коштів і фінансуванню тероризму (AML/CFT Industry Partnership, ACIP) за сприяння Валютного управління Сінгапуру (MAS), містить детальні рекомендації щодо найкращих практик належної перевірки джерела статків (Source of Wealth, SoW) клієнтів фінансових установ. Основна мета документа — надати фінансовим установам практичні інструменти й методологію для ефективного здійснення оцінки та підтвердження легітимності походження активів клієнтів, які становлять підвищений ризик відмивання коштів або фінансування тероризму.

[1] https://www.mas.gov.sg/regulation/external-publications/industry-perspectives-on-best-practices-for-source-of-wealth-due-diligence

Документ побудований на ризик-орієнтованому підході та передбачає застосування принципу «однаковий ризик — однаковий контроль» (same risk, same control). Він визначає основні принципи оцінки джерел статків: матеріальність (визначення найбільш значущих джерел статків), актуальність (отримання релевантних документів для підтвердження), та обачність (проведення ретельної перевірки й оцінки достовірності документів). Особлива увага приділяється складним випадкам, зокрема коли інформація щодо джерела статків походить з давніх часів або коли вона не може бути легко перевірена.

У документі запропоновано трирівневий підхід до визначення та підтвердження SoW, що залежить від сегменту клієнтів — приватний банкінг та управління активами, роздрібний банкінг і корпоративний банкінг. Для приватного банкінгу й управління активами рекомендується максимально суворий підхід з обов'язковим підтвердженням інформації, враховуючи складність транзакцій та розміри активів. Для роздрібного банкінгу пропонується застосовувати дворівневий підхід: базовий та розширений, де розширений передбачає поглиблене підтвердження інформації у разі виявлення специфічних факторів ризику (наприклад, іноземні політично значущі особи, негативні новини щодо клієнта, активи понад певні пороги). У корпоративному сегменті також рекомендовано дворівневий підхід, де важливо враховувати структуру компанії, її зв'язки з високоризиковими юрисдикціями, політично значущими особами, та обсяги активів.

Окрема увага приділена практичним аспектам підтвердження походження статків із різних джерел: спадок і дарування, доходи від бізнесу, інвестиційні прибутки, доходи від продажу товарів, які важко оцінити (твори мистецтва, цифрові активи), та доходи від трудової діяльності. Для кожної категорії надаються детальні рекомендації щодо типів документів, способів оцінки ризиків та додаткових заходів контролю.

Важливим елементом документа є рекомендації щодо постійного моніторингу клієнтів, який має охоплювати не лише автоматизовані транзакційні перевірки, а й регулярне оновлення інформації щодо джерела статків, особливо при зміні профілів ризику клієнтів. Пропонується активно використовувати аналітику та технологічні рішення (наприклад, штучний інтелект і машинне навчання) для своєчасного виявлення ознак підвищення ризику.

Окремий блок присвячено ролі керівництва фінансових установ. Установам рекомендується чітко визначати межі допустимого ризику, забезпечувати ефективні механізми ескалації складних кейсів і встановлювати чіткі критерії прийняття рішень щодо продовження співпраці з клієнтами з невизначеним або непідтвердженим джерелом статків.

Висновки:

- **Запровадити трирівневий ризик-орієнтований підхід до перевірки джерела статків**, диференціюючи клієнтів залежно від сегмента бізнесу (приватний, роздрібний і корпоративний банкінг), та застосовувати відповідний рівень підтвердження SoW залежно від виявлених факторів ризику.
- **Активно використовувати аналітичні інструменти та технологічні рішення** для покращення моніторингу ризиків, зокрема штучний інтелект для виявлення потенційних ознак шахрайства або підробки документів щодо джерел статків.
- **Створити ефективні механізми ескалації складних кейсів до вищого керівництва** у разі неможливості підтвердження або встановлення повної прозорості походження коштів, що дозволить ухвалювати обґрунтовані рішення щодо подальшого співробітництва з клієнтами.
- **Регулярно переглядати і оновлювати інформацію про джерело статків клієнтів**, особливо після зміни їхнього профілю ризику або виявлення невідповідностей між заявленими й фактичними активами, що дозволяє фінансовим установам оперативно реагувати на нові ризики.

Таким чином, документ є комплексним керівництвом, яке дозволяє фінансовим установам системно підходити до належної перевірки джерел статків клієнтів, зменшуючи ризики відмивання коштів та фінансування тероризму, забезпечуючи відповідність міжнародним стандартам і національним регуляторним вимогам.

Трасти у тіні: Розкриття таємниць прихованого володіння нерухомістю у Сполученому Королівстві [2]

Звіт, опублікований Transparency International UK, детально аналізує проблему використання трастових структур для приховування власності на нерухомість у Сполученому Королівстві, що сприяє відмиванню грошей, ухилянню від санкцій та іншим економічним злочинам. Документ підкреслює, що, незважаючи на прогрес у підвищенні прозорості власності через компанії, трасти залишаються ключовим інструментом для забезпечення анонімності заможних осіб, зокрема тих, чиї статки мають сумнівне походження. Звіт ґрунтується на даних відкритих джерел, витоках інформації, судових справах, а також розслідуваннях журналістів і громадських організацій, і пропонує конкретні рекомендації для реформування законодавства Сполученого Королівства, щоб усунути прогалини, які дозволяють зловмисникам уникати прозорості.

Автори звіту, Стів Гудріч та Марго Моллат, розкривають масштаби використання трастів, зазначаючи, що ці юридичні механізми, які беруть свій початок ще з часів хрестових походів, коли нормандські лицарі передавали свої землі довіреним особам, залишаються актуальними й сьогодні. Трасти дозволяють відокремити юридичне управління активами від їхньої фактичної вигоди: довірена особа (трасті) контролює майно, але бенефіціар отримує від нього прибуток. Це створює можливості для анонімності, оскільки в земельних реєстрах зазвичай вказується лише ім’я трасті, а не бенефіціара чи засновника трасту.

Дослідження Transparency International UK виявило, що в Англії та Уельсі щонайменше 236,500 об’єктів нерухомості, вартістю приблизно £64 мільярди, належать трастовим структурам. З них 170 об’єктів, вартістю £2.5 мільярда, пов’язані з підозрілим багатством, включаючи активи, що належать санкціонованим особам, політично значущим особам (PEP) із країн із високим ризиком корупції та особам, обвинуваченим у корупційних злочинах. Зокрема, 138 із цих об’єктів, вартістю £2.1 мільярда, були придбані за останні 15 років, що вказує на сучасність цієї проблеми.

Звіт наводить конкретні приклади використання трастів для приховування сумнівного багатства. Наприклад, квартира в Лондоні вартістю £61 мільйон, що належить партнеру російського олігарха Олександра Пономаренка, пов’язаного з так званим «палацом Путіна», була придбана через трастову структуру і не потрапила під заморожування активів у Сполученому Королівстві, хоча подібні активи у Франції були заморожені. Інший приклад — особняк у Лондоні вартістю £8.3 мільйона, пов’язаний із санкціонованим союзником Путіна Ігорем Комаровим, який також не був заморожений. Крім того, звіт згадує £130 мільйонів нерухомості, що належить першій родині Азербайджану (Алієвим) та їхнім соратникам, £40 мільйонів комерційної нерухомості в центрі Лондона, контрольованої членом сінгапурської організації з відмивання коштів, який відбуває покарання, та £55 мільйонів комерційної нерухомості, що належала колишньому міністру фінансів Малайзії через трасти. Ці випадки ілюструють, як трасти дозволяють особам із сумнівними статками інвестувати в британську нерухомість без належного контролю.

[2] https://www.transparency.org.uk/news/trust-issues-tackling-final-frontier-secret-property-ownership

У Сполученому Королівстві за останні роки було досягнуто певного прогресу в підвищенні прозорості власності на нерухомість. У 2016 році було запроваджено реєстр осіб із значним контролем (PSC), який розкриває інформацію про тих, хто контролює британські компанії. У 2022 році, після вторгнення Росії в Україну та зростання тиску на російських еліт, було створено Реєстр закордонних суб'єктів (ROE), який зобов'язує офшорні компанії, що володіють нерухомістю у Сполученому Королівстві, розкривати своїх кінцевих власників. Ці реформи принесли певні результати, виявивши власників, пов'язаних із політикою чи санкціями.

Проте звіт підкреслює, що трасти дозволяють обходити ці вимоги. Наприклад, офшорні компанії, контрольовані трастами, зобов'язані подавати інформацію про трасти до Companies House, але ця інформація не публікується. Британські компанії, контрольовані трастами, мають ще менші вимоги: вони повідомляють лише про довірених осіб, а не про бенефіціарів чи засновників. Це створює парадоксальну ситуацію, коли британські компанії можуть бути менш прозорими, ніж офшорні. За даними звіту, 23,000 об'єктів нерухомості вартістю £17.5 мільярда належать офшорним компаніям із трастами в структурі власності, а 49,000 об'єктів вартістю £9 мільярдів належать британським компаніям, контрольованим трастами.

Ще однією проблемою є Реєстр трастів (Trust Registration Service, TRS), який охоплює лише трасти, створені після 6 жовтня 2020 року, залишаючи значну частину старих трастів поза обліком. Доступ до інформації з TRS обмежений: заявники, такі як журналісти чи громадські організації, повинні знати назву трасту, що часто є неможливим, а обробка запитів може тривати до восьми тижнів. Навіть у разі успішного запиту отримана інформація часто є недостатньою для розслідування фінансових злочинів. Звіт зазначає, що Companies House може відхиляти до 99% заявок через надмірно обережне тлумачення законодавства, а вимога доводити «легітимний інтерес» (наприклад, розслідування відмивання грошей чи ухилення від санкцій) ускладнює доступ для журналістів і громадських організацій.

Висновки:

- **Зобов'язати трасти до розкриття інформації:** Уряд Сполученого Королівства має законодавчо вимагати від трастів, що володіють нерухомістю, повідомляти про бенефіціарів і засновників до земельних реєстрів і Companies House, із публікацією цих даних для громадськості.
- **Покращити доступ до Реєстру трастів:** Спростити процедуру доступу до інформації про трасти, усунувши вимогу вказувати назву трасту та скоротивши час обробки запитів до двох тижнів, щоб полегшити розслідування журналістів і громадських організацій.
- **Інтегрувати дані земельних реєстрів:** Зобов'язати земельні реєстри Сполученого Королівства чітко класифікувати типи власників (трасти, компанії, фізичні особи) та надавати безкоштовні масові дані про власність щомісяця.
- **Розширити охоплення Реєстру трастів:** Включити до TRS трасти, створені до жовтня 2020 року, та забезпечити громадський доступ до інформації про закордонні трасти, що володіють нерухомістю у Сполученому Королівстві, для підвищення прозорості.

Звіт також вказує на тенденцію переходу активів до трастів у відповідь на посилення прозорості компаній. Прикладом є випадок Максима Бакієва, сина колишнього президента Киргизстану, який, за даними розслідування Global Witness, був причетний до розкрадання державних коштів і відмивання грошей. У 2022 році, коли набули чинності нові вимоги ROE, Бакієв перевів свій £3.5-мільйонний заміський будинок у Сурреї з белізької компанії на траст, керований британськими юристами. У рідкісному випадку успішного запиту до TRS, було підтверджено, що Бакієв є бенефіціаром цього трасту, що демонструє, як зловмисники адаптуються до нових правил.

Для вирішення цих проблем звіт пропонує низку реформ. По-перше, Companies House має

уникати надмірно обмежувального підходу до надання доступу до інформації про трасти, що контролюють закордонні суб'єкти, і отримати повноваження публікувати дані про трасти, які контролюють як британські, так і офшорні компанії. По-друге, земельні реєстри Сполученого Королівства повинні зобов'язати трасти повідомляти про пряму власність на землю, чітко класифікувати типи власників (трасти, компанії, фізичні особи) та надавати унікальні реєстраційні номери й інформацію про юрисдикцію походження. Крім того, земельні реєстри мають надавати безкоштовні дані про власність щомісяця. По-третє, TRS слід розширити, щоб охопити трасти, створені до жовтня 2020 року, і надати громадський доступ до інформації про закордонні трасти, що володіють нерухомістю у Сполученому Королівстві. Ці реформи спрямовані на створення інтегрованої системи, яка забезпечить прозорість власності та ускладнить використання трастів для приховування сумнівного багатства.

EBA 2024: Регуляторна трансформація, цифрова стійкість та нова ера нагляду в ЄС [3]

Щорічний звіт Європейського банківського органу (EBA) за 2024 рік є комплексним аналітичним документом, що системно узагальнює ключові здобутки регулятора в межах реалізації його мандату в контексті глибоких трансформацій на фінансовому, регуляторному та геополітичному рівнях. У звіті висвітлено, що EBA досягла 93% завдань, визначених у Робочій програмі на 2024 рік, при цьому зосередившись на реалізації п'яти ключових пріоритетів: імплементації рамки Basel III в ЄС та зміцненні Єдиного зводу правил, моніторингу фінансової стабільності в умовах високих процентних ставок і геополітичної напруги, розбудові цифрової інфраструктури даних, посиленні нагляду за DORA і MiCA, а також підтримці інновацій та захисту прав споживачів у контексті переходу до нової архітектури ПВК/ФТ.

У сфері імплементації Basel III EBA опрацювала понад 140 мандатів у межах пакету CRR III/CRD VI, зокрема через публікацію консультаційних документів, технічних стандартів і звітів, що охоплюють кредитний, ринковий та операційний ризики. Значну увагу було приділено розбудові Єдиного зводу правил у сфері капіталу (CET1, TLAC/MREL), ліквідності (NSFR, LCR), оцінки відповідності, структури винагород (у т.ч. високооплачувальні працівники, гендерна нейтральність), а також створенню єдиного підходу до нагляду за установами третіх країн, що діють у ЄС. Водночас EBA продовжила інтеграцію принципу пропорційності, зокрема щодо малого та середнього банкінгу, шляхом спрощення підходів до регулювання без втрати наглядувальної якості.

Фінансову стабільність у 2024 році EBA моніторила в умовах підвищеної волатильності, викликаної інфляційним тиском, геополітичними конфліктами (насамперед війною Росії проти України), уповільненням глобального зростання та фрагментацією ланцюгів постачання. Сектор банків ЄС демонстрував високу прибутковість, капіталізацію (CET1 ~16%) та ліквідність, що дало змогу пом'якшити вплив імовірних шоків. Водночас посилювались операційні та кіберризики, а також ризики, пов'язані з комерційною нерухомістю. EBA провела Звіт про оцінку ризиків у два етапи(весна та осінь), оновила методологію стрес-тестування і вперше включила до неї компоненти кліматичних ризиків через спеціальне сценарне тестування (Fit-for-55), результати

[3] https://www.eba.europa.eu/sites/default/files/2025-05/c0d3817e-da24-42fc-b991-b7d446b2e941/2024%20Annual%20Report_Part%201.pdf

якого засвідчили обмежений прямий вплив «Run-on-Brown» шоків, але потенційно значну втрату капіталу в разі поєднання з макроекономічними потрясіннями.

Розвиток інфраструктури даних став ще одним стратегічним вектором. Через платформу EUCLID, що охоплює понад 9500 показників для 123 банків, EBA забезпечила прозорість, дисципліну ринку та можливість візуалізації даних. Установа також підготувала хаб для Pillar 3 disclosures, реалізувала пілотний проєкт з інтеграції звітності, впровадила нову модель DPM 2.0, розпочала адаптацію до даних від учасників MiCA/DORA, запустила DPM Studio та підготувала інтеграційний словник. Усі ці заходи мають забезпечити сумісність звітності, зменшити навантаження на установи та підвищити якість даних у єдиному цифровому екосередовищі.

У сфері цифрового регулювання EBA, у співпраці з іншими Європейськими наглядовими органами (ESA), продовжила підготовку до впровадження DORA, зокрема шляхом створення спільної директоратної структури нагляду, запуску тренінгів, формування Європейської координаційної рамки реагування на кіберінциденти (EU-SCICF), а також затвердження операційної моделі нагляду за критичними ІКТ-провайдерами. У межах MiCA, EBA затвердила 20 технічних стандартів і керівництв, створила наглядову рамку для значимих токенів (ARTs, EMTs), запровадила шаблони звітності, утворила тимчасову структуру «Crypto-Assets Standing Committee» для сприяння конвергенції нагляду.

Інновації та захист споживачів були в центрі уваги EBA, яка аналізувала ризики штучного інтелекту, DeFi, токенізованих депозитів, моніторила практики небанківських кредиторів, скарги споживачів і доступ до фінансових послуг. У сфері ПВК/ФТ регулятор провів оцінку нових фінансових ризиків, гармонізував підходи до нагляду за ПВК, сприяв координації на рівні держав-учасниць та підготувався до передачі повноважень новому європейському органу – AMLA – що має запрацювати у 2025 році.

Організаційно-змістовні трансформації EBA у 2024 році охоплюють стратегічні кадрові ініціативи – запуск HR-стратегії Horizon 2029, розвиток інституту внутрішньої мобільності, нову візуальну ідентичність, підвищення гнучкості, цифровізації та рівня задоволеності персоналу. Завдяки цим змінам EBA змогла не лише утримати рівень ефективності у відповідь на численні виклики (COVID, війна, інфляція), але й закласти системний фундамент для переходу до нової регуляторної епохи в 2025 році.

Загалом звіт демонструє послідовність, системність і стратегічну орієнтацію EBA на забезпечення стійкості фінансової системи ЄС, ефективного

Висновки:

- **EBA завершила 93% завдань 2024 року, зокрема почала реалізацію 140 мандатів в рамках CRR III/CRD VI –** установам слід готуватись до значних змін у регуляторному середовищі, включно з оновленими вимогами до кредитного та операційного ризику, ESG-розкриття та вимог до структур капіталу.
- **Початок практичного нагляду за криптоактивами через MiCA** – EBA вже надала 20 технічних стандартів і керівництв; установам та регуляторам слід адаптувати політики до нових вимог щодо стабільності, захисту споживачів і нагляду за ART та EMT.
- **Кліматичні ризики інтегруються у загальноєвропейське стрес-тестування з 2027 року через «комбінований підхід»** – фінансовим установам рекомендовано готувати бізнес-моделі до довгострокових кліматичних сценаріїв (Run-on-Brown, макро-фінансові потрясіння).
- **EBA підтримує цифрову трансформацію через платформу EUCLID, інтегровану звітність та DPM 2.0 –** фінансовим установам важливо переглянути внутрішні IT-стратегії і забезпечити сумісність своїх звітних систем із новими вимогами.

впровадження регуляторних реформ і проактивного реагування на виклики трансформації банківської екосистеми в умовах цифрової, кліматичної й геополітичної турбулентності.

Санкції

ЄС погодив 17-й пакет санкцій [4]

20 травня 2025 року Європейський Союз ухвалив 17-й пакет санкцій проти Російської Федерації у відповідь на її триваючу агресію проти України. Цей пакет став одним із наймасштабніших з початку війни, спрямованим на посилення економічного тиску на Росію та обмеження її здатності фінансувати військові дії.

Основні елементи 17-го пакету санкцій:

1. Боротьба з «тіньовим флотом» Росії. ЄС запровадив санкції проти 189 додаткових суден, які входять до так званого «тіньового флоту» Росії — мережі танкерів, що використовуються для обходу санкцій та транспортування нафти за допомогою непрозорих схем. Загальна кількість таких суден, що підпадають під санкції, досягла 342. Ці заходи включають заборону на доступ до портів ЄС та обмеження на надання послуг, таких як страхування та технічне обслуговування.
2. Обмеження в енергетичному секторі. Санкції були накладені на російську нафтову компанію «Сургутнафтогаз», яка є одним із головних джерел доходів для російського бюджету. Також під санкції потрапила велика російська компанія з транспортування нафти. Ці заходи спрямовані на зменшення енергетичних доходів Росії, які використовуються для фінансування війни.
3. Розширення списку осіб та організацій під санкціями. До списку санкцій додано 66 фізичних осіб та 67 юридичних осіб, включаючи компанії з Росії, Китаю, Туреччини, В'єтнаму, ОАЕ, Сербії та Узбекистану, які підтримують російський військово-промисловий комплекс. Ці санкції включають заморожування активів та заборону на надання фінансових послуг.
4. Обмеження на експорт технологій подвійного призначення. ЄС розширив обмеження на експорт товарів та технологій подвійного призначення, включаючи хімічні прекурсори для енергетичних матеріалів та компоненти для верстатів з числовим програмним управлінням (ЧПУ). Ці заходи спрямовані на обмеження доступу Росії до критично важливих технологій для її військово-промислового комплексу.
5. Продовження винятку для проєкту «Сахалін-2». З огляду на енергетичну безпеку Японії, ЄС продовжив до 28 червня 2026 року виняток з обмежень на транспортування нафти з проєкту «Сахалін-2» до Японії.

Ефективність санкцій

Згідно з даними ЄС, з моменту запровадження обмежень на «тіньовий флот» доходи Росії від експорту нафти зменшилися на 38 мільярдів євро. У березні 2025 року ці доходи були на 13,7% нижчими порівняно з березнем 2023 року та на 20,3% нижчими порівняно з березнем 2022 року.

Висновки та подальші кроки

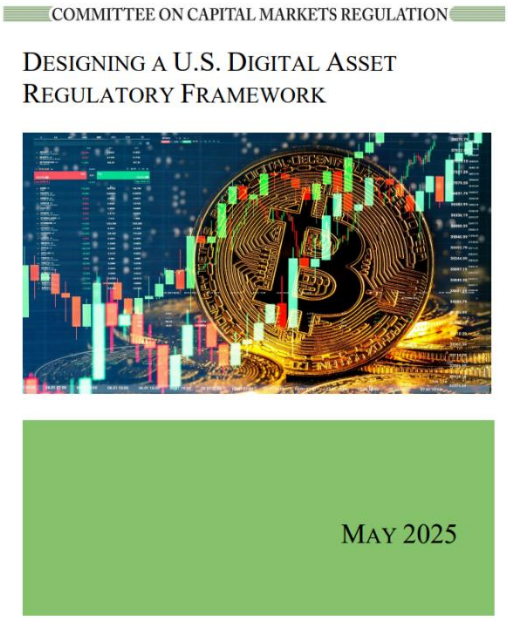
[4] https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russia-s-war-of-aggression-against-ukraine-eu-agrees-17th-package-of-sanctions/

17-й пакет санкцій ЄС демонструє рішучість Європейського Союзу посилювати економічний тиск на Росію з метою припинення її агресії проти України. Очікується, що в разі відсутності прогресу в мирних переговорах, ЄС продовжить розширювати санкції, зокрема в енергетичному та фінансовому секторах.

Для України та її партнерів важливо забезпечити ефективне впровадження та моніторинг цих санкцій, а також продовжувати дипломатичні зусилля для досягнення справедливого миру.

Звіти окремих інституцій та експертів

Розробка регуляторної бази цифрових активів у США [5]



Документ, підготовлений авторитетною дослідницькою організацією Committee on Capital Markets Regulation (CCMR), детально розглядає ключові аспекти та принципи побудови національної регуляторної бази США для цифрових активів. Автори наголошують, що відсутність чіткого федерального регулювання цифрових активів знижує конкурентоспроможність США на міжнародному рівні порівняно з ЄС, Сполученим Королівством, Японією, ОАЕ та Гонконгом, де вже впроваджені або впроваджуються відповідні нормативні режими.

У звіті докладно описані три основні категорії цифрових активів: цифрові активи-товари (digital asset commodities), цифрові активи-цінні папери (digital asset securities) та стейблкоїни. Прикладом цифрових активів-товарів виступають Bitcoin та Ethereum, а до цифрових активів-цінних паперів належать токени, які представляють собою інвестиційні контракти відповідно до тесту Howey або ж є токенізованими версіями традиційних цінних паперів. Стейблкоїни визначаються як цифрові активи, прив'язані до певного активу, найчастіше фіатної валюти.

У рамках створення ефективного регуляторного середовища, документ пропонує 10 базових принципів:

- Створення спеціалізованих режимів реєстрації торгових платформ та брокер-дилерів, які будуть враховувати специфіку цифрових активів.
- Впровадження чітких вимог щодо зберігання (custody) цифрових активів, які гарантують захист активів клієнтів і забезпечують вибір способу зберігання.
- Формування чітких критеріїв для розмежування цифрових активів-товарів та цифрових активів-цінних паперів.
- Надання повноважень щодо регулювання цифрових активів-товарів Комісії з торгівлі товарними ф'ючерсами (CFTC), а цифрових активів-цінних паперів — Комісії з цінних паперів і бірж (SEC).
- Адаптація правил розкриття інформації для цифрових активів з урахуванням їх специфіки.
- Дозвіл надання спільних послуг для традиційних фінансових активів та цифрових активів.

[5] https://capmktsreg.org/wp-content/uploads/2025/05/CCMR-Designing-a-U.S.-Digital-Asset-Regulatory-Framework-05.14.25-Final.pdf

- Збереження ролі брокер-дилерів із одночасним дозволом на пряму торгівлю цифровими активами без посередництва, але з відповідними захисними заходами.
- Визнання статусу реєстрації за вже існуючими регуляторними режимами та забезпечення перехідного періоду для досягнення відповідності.
- Чітке визначення федеративного пріоритету над законами штатів щодо цифрових активів.
- Обмеження екстериторіального впливу регулювання та розвиток міжнародних стандартів взаємного визнання (substituted compliance).

Документ детально аналізує необхідність створення нового регуляторного середовища через невідповідність існуючих правил, особливо через судові конфлікти між SEC та платформами цифрових активів. Значна увага приділена можливості зберігання цифрових активів безпосередньо платформами, що забезпечує швидкість та ефективність торгівлі, проте потребує додаткових механізмів захисту активів клієнтів (наприклад, юридичного відокремлення активів клієнтів від активів платформ).

Також документ пропонує чітку таксономію цифрових активів, що дозволить зменшити регуляторну невизначеність та покращити правову визначеність для учасників ринку. Важливим є визнання, що категорія цифрового активу може змінюватися з часом, тому регуляторні рамки повинні передбачати механізм переходу активу з категорії цінних паперів у категорію товарів (наприклад, після досягнення децентралізації мережі).

Документ пропонує рекомендації щодо міжнародної співпраці та встановлення рамок для міжнародного взаємного визнання регулювання цифрових активів, що допоможе уникнути дублювання регуляторних вимог та сприятиме глобальній інтеграції цифрових ринків.

Висновки:

- **Створити чіткі, спеціалізовані режими реєстрації торгових платформ та брокер-дилерів цифрових активів**, що відповідають міжнародним стандартам та дозволяють США залишатися конкурентоспроможними на світовому ринку.
- **Впровадити суворі, але гнучкі правила зберігання цифрових активів** із забезпеченням додаткових механізмів захисту (відокремлення активів клієнтів, регулярні перевірки), з можливістю зберігання активів безпосередньо платформами.
- **Розробити та впровадити чітку юридичну таксономію для класифікації цифрових активів**, що дозволить зменшити невизначеність для інвесторів та ринку, а також чітко визначити відповідні органи регулювання.
- **Забезпечити федеральний пріоритет регулювання цифрових активів**, що дозволить уніфікувати правові підходи та уникнути конфліктів із законодавством штатів, посилюючи стабільність і передбачуваність правового середовища для учасників ринку.

Гроші з диму: що втрачає Україна через нелегальний ринок тютюну [6]

Спеціальний проєкт Економічної правди «Тіньовий продаж цигарок: ознаки нелегальної продукції» глибоко аналізує масштаби та механізми функціонування нелегального ринку тютюнових виробів в Україні. Дослідження розкриває критичну ситуацію, що склалася у зв'язку зі зростанням нелегального обігу сигарет після тимчасового спаду. За даними компанії Kantar Ukraine, у лютому 2025 року частка нелегального ринку досягла 14,1%, що еквівалентно 5 млрд сигарет. Внаслідок цього бюджет України втрачає понад 24 млрд грн на рік. Для порівняння, цих

[6] https://epravda.com.ua/projects/groshi-z-dimu-806664/

коштів було б достатньо для закупівлі понад 400 тисяч FPV-дронів для української армії, 120 бойових безпілотників типу «Байрактар», будівництва понад 12 тисяч квартир для постраждалих від війни родин або утримання десятків тисяч військовослужбовців.

Автори детально описують основні схеми, які використовують нелегальні виробники та продавці цигарок. Основними формами нелегального обігу є контрафактна продукція, цигарки, призначені для Duty Free або експорту, які залишаються в Україні, та використання псевдоекспортних схем через Одеський порт. Понад половину нелегальної продукції з маркуванням Duty Free виробляє «Винниківська тютюнова фабрика». Іншими значними гравцями на нелегальному ринку є компанії «Маршалл Файнест Тобакко», «Юнайтед Табако», VK Tobacco FZE, а також «Українське тютюнове виробництво». Часто виявляються факти підробки акцизних марок та порушення правил маркування. В результаті цього, ринок переповнюється контрафактною продукцією, яка реалізується за заниженими цінами, створюючи умови для несправедливої конкуренції та завдаючи значних фінансових втрат державі.

У дослідженні також акцентується увага на тому, як легальні заходи, спрямовані на підвищення доходів державного бюджету, зокрема підвищення акцизних зборів на тютюнові вироби, можуть сприяти подальшому розвитку тіньового ринку. Так, у 2025 році було прийнято рішення про підвищення акцизів на сигарети, що призведе до суттєвого зростання роздрібних цін і, відповідно, збільшення привабливості нелегальної продукції для споживачів.

Автори наголошують, що в умовах війни несплата податків фактично дорівнює зраді, оскільки недоотримані бюджетом кошти могли б спрямовуватися на оборону, закупівлю зброї та зміцнення економічної безпеки держави. Вони також акцентують увагу на відповідальності споживачів, які,

Висновки:

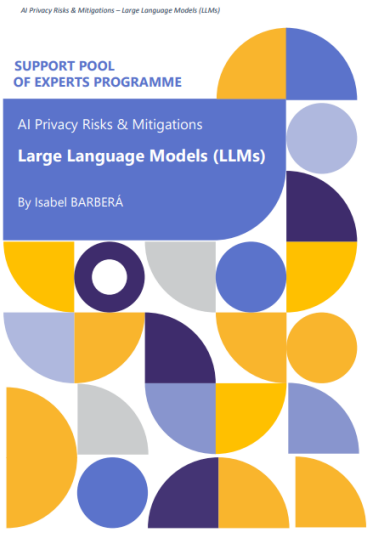
- **Створити ефективну систему моніторингу та контролю за виробництвом і обігом тютюнових виробів**, включаючи запровадження «бібліотеки зразків» продукції та застосування сучасних технологій трасологічних експертиз, що дозволить правоохоронним органам оперативно виявляти й ліквідувати канали нелегального постачання.
- **Посилити митний контроль, особливо в портах та на кордонах**, де часто реалізуються псевдоекспортні та контрабандні схеми, і посилити відповідальність посадовців, які допускають ввезення або вивезення нелегальної продукції.
- **Застосовувати поступовий і прогнозований підхід до підвищення акцизних ставок**, щоб уникнути різких стрибків цін на легальну продукцію, що може спровокувати перехід споживачів на нелегальний ринок.
- **Провести масштабні просвітницькі кампанії серед населення**, спрямовані на роз'яснення ризиків та негативних наслідків придбання нелегальної тютюнової продукції, підкреслюючи відповідальність кожного споживача перед державою в умовах війни.

купуючи дешевшу нелегальну продукцію, не лише завдають шкоди бюджету, але й стають учасниками злочинних схем.

Документ також детально аналізує міжнародний досвід боротьби з нелегальним тютюновим ринком, вказуючи на успішні кейси Польщі та Румунії. Польський досвід демонструє важливість диференційованого оподаткування та прогнозованості підвищення цін, які допомогли знизити рівень нелегальної торгівлі. Румунія впоралась зі зростанням нелегальної продукції завдяки поступовості оподаткування та паралельним заходам посилення контролю та правоохоронної діяльності.

Для подолання тіньового ринку в Україні експерти пропонують впровадження інтегрованого підходу, який включає посилений митний та правоохоронний контроль, активну співпрацю з легальними виробниками, використання сучасних аналітичних систем моніторингу продукції та створення «бібліотеки зразків» готових виробів для оперативної ідентифікації нелегальної продукції.

Ризики конфіденційності штучного інтелекту [7]



Документ являє собою детальний та комплексний звіт, присвячений питанням приватності та захисту персональних даних при використанні великих мовних моделей (LLMs). Він охоплює увесь життєвий цикл штучного інтелекту, детально описуючи технологічні аспекти, особливості обробки даних, можливі ризики на різних стадіях розробки, впровадження і використання таких моделей, а також пропонує широкий спектр рекомендацій для мінімізації цих ризиків.

Автори документа звертають увагу на зростаюче значення LLM у різних секторах економіки та їхні потенційні загрози для конфіденційності даних. Документ охоплює фундаментальні технологічні основи LLM, такі як архітектури трансформерів, алгоритми тонкого налаштування (fine-tuning), методи навчання з підкріпленням з використанням людського зворотного зв'язку (RLHF), а також нові тенденції, такі як автономні агентні системи штучного інтелекту (agentic AI). Ці технології підвищують ризики несанкціонованого доступу, неконтрольованого використання особистих даних та створюють можливості для випадкових або навмисних витоків інформації.

У документі акцентується увага на необхідності впровадження принципів Privacy by Design, інтегрованого підходу до управління ризиками, який передбачає раннє виявлення й активне усунення потенційних загроз ще на етапах проектування та збору даних. Розглядається повний життєвий цикл моделі LLM відповідно до стандартів ISO/IEC 22989 та ISO/IEC 5338, включаючи такі фази, як збір та підготовка даних, тренування моделей, перевірка та валідація, розгортання, експлуатація, моніторинг, технічне обслуговування, оновлення та виведення з експлуатації. На кожній з цих стадій виникають специфічні ризики, що вимагають особливих методів захисту, які детально описані в документі.

Серед ключових ризиків, які розглядаються у звіті, автори виокремлюють потенційну компрометацію конфіденційних даних через включення їх до навчальних наборів даних без належної анонімізації, ненавмисне запам'ятовування моделлю чутливої інформації (overfitting), ризики атак з боку зловмисників, які можуть спрямовуватися на саму модель чи на

[7] https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf

інфраструктуру, що її підтримує, а також ризики, пов'язані з неправильною інтерпретацією вихідних даних моделей через упередженість або недостатню прозорість.

Для кожного з цих ризиків пропонуються конкретні заходи щодо їх зменшення. Наприклад, застосування технологій анонімізації та псевдоанонімізації, впровадження методик диференційної приватності (differential privacy), посилення заходів кібербезпеки, таких як багаторівнева аутентифікація, управління привілейованим доступом (PAM) [8] , контроль доступу на основі ролей (RBAC)[9] та використання захищених обчислювальних середовищ з надійним шифруванням даних. Також автори наголошують на важливості регулярних аудитів і тестувань моделей на предмет витоків або запам'ятовування чутливої інформації, включаючи спеціалізовані атаки на кшталт model inversion [10] або membership inference attacks[11].

Окрему увагу автори приділяють важливості прозорості та підзвітності, зокрема через чітке документування процедур збору, обробки даних, ризиків та застосованих заходів з їх мінімізації. У документі наголошується, що ефективне управління приватністю даних має бути неперервним процесом, з регулярною переоцінкою ризиків, постійним моніторингом ефективності захисних заходів і, за необхідності, адаптацією до нових загроз та умов використання моделей.

Висновки:

- **Інтегрувати Privacy by Design у всі стадії життєвого циклу LLM**, забезпечивши попередню оцінку ризиків та впровадження захисних заходів на етапах проектування, розробки, розгортання та експлуатації моделей.
- **Застосовувати диференційну приватність та псевдоанонімізацію**, щоб запобігти витокам і компрометації персональних даних при тренуванні та використанні моделей, і регулярно проводити аудит моделей на предмет небажаного запам’ятовування чутливої інформації.
- **Посилити кібербезпеку інфраструктури LLM** через використання захищених середовищ з багаторівневою аутентифікацією, ролевим контролем доступу та постійним моніторингом аномалій для швидкого виявлення та реагування на потенційні інциденти.
- **Регулярно переглядати та оновлювати оцінку ризиків**, проводити внутрішні та зовнішні аудити, документувати процеси та забезпечувати прозорість у комунікації з кінцевими користувачами щодо використання їхніх даних, тим самим зміцнюючи довіру та підзвітність.

Документ містить також практичні кейси, які демонструють застосування наведених методологій управління ризиками у реальних сценаріях, що дозволяє більш предметно зрозуміти специфіку впровадження рекомендацій. У заключних розділах наведено

[8] Набір технологій, процесів і політик, спрямованих на контроль та моніторинг доступу до критично важливих інформаційних ресурсів організації, зокрема облікових записів з підвищеними правами. PAM допомагає мінімізувати ризики несанкціонованого доступу, витоків інформації та кіберзагроз, забезпечуючи належний рівень захисту конфіденційних даних та відповідність нормативно-правовим вимогам.

[9] Модель управління доступом, за якої права користувача визначаються не індивідуально, а на основі ролі, яку він виконує в межах організації. Кожна роль пов’язана з певним набором дозволів до ресурсів або дій у системі, і користувачі отримують доступ лише до того, що необхідно для виконання їхніх службових обов’язків.

[10] тип атаки на штучний інтелект, за якого зловмисник, маючи доступ до моделі (наприклад, через API), намагається відтворити або реконструювати вихідні дані, на яких модель навчалася. У контексті конфіденційності така атака може призвести до витоку персональних або чутливих даних

[11] тип атаки на модель машинного навчання, за якої зловмисник намагається визначити, чи входили конкретні дані (наприклад, особисті відомості користувача) до навчального набору цієї моделі. Така атака дозволяє отримати інформацію про участь особи в процесі навчання, що може порушити її право на конфіденційність і суперечити принципам захисту персональних даних, зокрема вимогам GDPR.

інструментарій, стандарти та методології, що допомагають організаціям систематизувати підхід до захисту даних при використанні великих мовних моделей.

Як машинне навчання виявляє незаконні криптовалютні потоки [12]

Документ представляє ґрунтовне дослідження, присвячене застосуванню машинного навчання для виявлення незаконної активності в криптовалютних транзакціях, з особливим акцентом на біткоїн, де псевдонімність ускладнює ідентифікацію реальних осіб за адресами. Дослідження спрямоване на вирішення ключового питання: чи може модель машинного навчання ефективно ідентифікувати підозрілі поведінкові патерни на блокчейні ще до того, як пов'язані адреси потраплять до чорних списків або викличуть необхідність ручного аналізу.

Традиційні методи протидії відмиванню грошей (AML), що спираються на статичні чорні списки адрес, пов'язаних із відомими злочинами, виявляються неефективними через швидку еволюцію технік відмивання. Зловмисники активно використовують криптовалютні міксери, децентралізовані фінансові протоколи (DeFi), крос-чейн мости, стейблкойни та скоординовані мережі, щоб розірвати зв'язки між джерелами та одержувачами коштів. Такі методи дозволяють генерувати нові адреси, змінювати інфраструктуру та адаптувати поведінку, роблячи чорні списки застарілими незабаром після їх створення. Це підкреслює потребу в інноваційному, поведінково-орієнтованому підході, який здатен виявляти ризики на основі динамічних патернів, а не статичних ідентифікаторів.

У центрі дослідження — модель машинного навчання, побудована на основі градієнтного бустингу дерев рішень (XGBoost), обраного після порівняння з іншими методами, такими як графові нейронні мережі, завдяки його високій точності та ефективності на структурованих даних блокчейну. Модель аналізує кластери біткоїн-адрес, ймовірно контрольованих однією особою чи організацією, і видає два основні результати: ймовірнісну ризик-оцінку, яка вказує на рівень підозрілості кластера, та функціональну класифікацію, що визначає тип сутності, наприклад, біржа, міксер, даркнет-маркет, майнер чи санкціонована організація.

Замість фокусу на окремих адресах модель досліджує поведінкові характеристики кластерів, обробляючи високовимірний вектор із понад 1000 ознак, які охоплюють широкий спектр аспектів діяльності, від базових метрик, таких як кількість транзакцій чи баланс, до складних графових патернів, що відображають взаємодію в мережі блокчейну. Навчальний набір даних включає мільйони позначених кластерів, створених на основі відкритих джерел інформації та блокчейн-аналітики, що дозволяє моделі не лише розпізнавати відомі ризиковані сутності, а й узагальнювати патерни для виявлення нових, раніше не позначених кластерів.

Ознаки моделі згруповані в 11 категорій, кожна з яких детально описує певний аспект поведінки кластера.

[12] https://20255707.fs1.hubspotusercontent-na1.net/hubfs/20255707/Inside%20AMLBot%E2%80%99s%20Machine%20Learning%20Engine.pdf?utm_medium=email&_hsenc=p2ANqtz-8TWlRwuTeeJd2mf40cptHwMSNT9PVpSeInfvZT6ZLguvIOlspa-_238rSPFVnMGdFugLyw2pnbeyivzA11vYoLrccpVQ&_hsmi=362808630&utm_content=362808630&utm_source=hs_automation

- Перша категорія охоплює загальний профіль кластера, включаючи кількість адрес, загальний обсяг транзакцій, баланс, кількість депозитів і виведень, що дає уявлення про масштаб і активність сутності.
- Друга категорія аналізує темпоральну динаміку, наприклад, частоту транзакцій за останній квартал чи співвідношення недавньої активності до пікової, що може вказувати на сплески, характерні для незаконних операцій.
- Третя категорія досліджує потоки та напрямки транзакцій, аналізуючи співвідношення вхідних і вихідних операцій та складність транзакцій, таких як операції з багатьма входами та виходами, які часто асоціюються з міксерами.
- Четверта та п'ята категорії зосереджені на входах і виходах транзакцій, оцінюючи їхню кількість, розмір, розподіл і відсоток повторюваних сум, що може сигналізувати про автоматизовані патерни чи «дастинг-атаки».
- Шоста категорія аналізує типи скриптів і адрес (P2PKH, SegWit, Taproot, мультисиг), що дозволяє визначити технологію гаманця чи тип сервісу, наприклад, біржу чи міксер.
- Сьома категорія включає метадані блокчейну, такі як розмір транзакції, комісії чи використання полів lock_time, які можуть вказувати на термінові чи спам-транзакції.
- Восьма категорія агрегує статистичні метрики, як-от середнє, медіану чи перцентилі розмірів транзакцій, для оцінки варіабельності поведінки.
- Дев'ята категорія досліджує часові патерни, наприклад, транзакції вночі чи у вихідні, що може відображати автоматизовані процеси.
- Десята категорія аналізує джерела та напрямки коштів, визначаючи типи контрагентів, таких як біржі чи міксери.
- Одинадцята категорія фіксує перші відомі сутності, що взаємодіють із кластером, наприклад, біржу, що надіслала перші кошти, чи міксер, що їх отримав, що може вказувати на початкову мету кластера.

Продуктивність моделі оцінюється за допомогою стандартних метрик, зокрема площі під кривою операторської характеристики приймача (AUC-ROC), яка вимірює здатність моделі розрізняти ризиковані та безпечні кластери. Тестування показало вражаючі результати: AUC-ROC перевищує 0.9 для більшості категорій, досягаючи значень, близьких до 1.0 для майнерів (1.00), міксерів (0.96) і санкціонованих сутностей (0.92). Загальна точність класифікації перевищує 90%, що значно перевершує традиційні системи на основі чорних списків. Модель демонструє низький рівень хибнопозитивних результатів при високій чутливості, що є критично важливим для зменшення шуму в реальних AML-системах.

Для забезпечення довіри та відповідності регуляторним вимогам модель використовує SHAP (Shapley Additive exPlanations), який пояснює внесок кожної ознаки в передбачення. На індивідуальному рівні SHAP-значення показують, які ознаки найбільше вплинули на ризик-оцінку конкретного кластера, наприклад, високий відсоток вхідних коштів від міксерів чи повторювані суми виходів, що характерно для технік відмивання. На глобальному рівні SHAP Summary Plots ілюструють, які ознаки є найвпливовішими для всієї моделі, наприклад, складні структури транзакцій для міксерів чи вхідні кошти від даркнет-адрес для даркнет-маркетів. Ця прозорість дозволяє командам із комплаєнсу та аудиторам зрозуміти логіку моделі, що є ключовим для відповідності стандартам модельного ризику та регуляторним вимогам, таким як MICA (ЄС), Travel Rule (FATF) і настанови FinCEN.

Модель має широкий спектр потенційних застосувань у сфері комплаєнсу блокчейну. Вона може використовуватися біржами для скринінгу вхідних депозитів, дозволяючи виявляти ризики, пов'язані з типологіями, такими як ransomware чи міксери, ще до їхньої офіційної атрибуції. У розслідуваннях модель допомагає ідентифікувати підозрілих посередників у складних ланцюжках відмивання, полегшуючи аналіз хакерських атак, шахрайства чи ухилення від санкцій. Крім того, модель здатна прогнозувати нові форми незаконної активності, аналізуючи схожість із відомими патернами, що дозволяє проактивно адаптувати стратегії виявлення. Для фінансових установ і криптобізнесів модель підтримує оцінку ризиків контрагентів, допомагаючи в прийнятті рішень щодо онбордингу чи маршрутизації транзакцій. Ці можливості роблять модель цінним інструментом для модернізації AML-стратегій у криптовалютному просторі.

Висновки:

- **Раннє виявлення ризиків через поведінковий аналіз:** Впроваджуйте ML-моделі, що аналізують поведінкові патерни, для виявлення підозрілої активності до внесення адрес у чорні списки, замінюючи або доповнюючи традиційні методи.
- **Прозорість передбачень:** Використовуйте SHAP для пояснення рішень моделі, щоб забезпечити відповідність регуляторним стандартам і підвищити довіру комплаєнс-команд.
- **Інтеграція в операційні процеси:** Застосовуйте модель для скринінгу вхідних транзакцій на біржах і пріоритизації цілей у розслідуваннях, оптимізуючи ресурси та знижуючи ризики.
- **Проактивна адаптація до нових загроз:** Використовуйте здатність моделі узагальнювати патерни для виявлення нових методів відмивання, таких як DeFi чи крос-чейн мости, для своєчасного реагування на еволюцію загроз.

Модель відповідає сучасним регуляторним стандартам, включаючи MICA, Travel Rule і настанови FinCEN, які вимагають прозорих і масштабованих систем для виявлення фінансових злочинів. Незважаючи на те, що модель наразі перебуває в контрольованому тестовому середовищі AMLBot, і її масштабне впровадження потребує додаткової технічної інфраструктури та організаційної готовності, дослідження демонструє, що поведінково-орієнтовані моделі можуть революціонізувати AML, пропонуючи проактивний, прозорий і адаптивний інструмент для боротьби з фінансовими злочинами в децентралізованих мережах.

Цифрові активи в епоху ставок і спредів: взаємодія крипторинку і ринку облігацій [13]

Аналітичний звіт досліджує взаємозв'язок між коливаннями на ринку державних і корпоративних облігацій США та поведінкою криптовалют, передусім біткоїна, в умовах змін глобального макроекономічного середовища. Основна ідея документа полягає в тому, що від 2020 року криптовалютний ринок дедалі тісніше корелює з традиційними фінансовими ринками, особливо з ринком боргових інструментів, через зростання інституційної участі, збільшення ліквідності та посилення чутливості до монетарної політики, інфляції, процентних ставок і загального ризик-апетиту.

У першому розділі звіту зазначається, що в першій половині 2025 року ринок облігацій США зазнав різкої волатильності: дохідність 10-річних казначейських облігацій піднялась із 3.8% до

[13] https://public.bnbstatic.com/static/files/research/impact-of-bond-market-volatility-on-the-cryptocurrency-market.pdf

4.6%, а індекс MOVE, який відображає очікування волатильності на ринку державних облігацій США, сягнув 139 — максимуму з 2022 року. Ці зміни супроводжувалися стрімким розширенням кредитних спредів (особливо HY OAS), що свідчило про зростання інвесторської настороженості та підвищення ризику дефолтів у корпоративному секторі. При цьому зафіксовано синхронні просадки як традиційних ризикових активів, так і біткоїна, що свідчить про уразливість крипторинку до системних макрошоків.

Далі автори розглядають механізми поширення фінансової напруги з ринку облігацій на ринок криптовалют. Виділяються чотири канали: зміна апетиту до ризику та ліквідності (особливо внаслідок волатильності та розширення кредитних спредів), зміна альтернативної вартості інвестування (реальні процентні ставки впливають на дохідність безризикових активів і пригнічують попит на безпроцентні активи, як-от біткоїн), загальноекономічні макрофактори (через вплив на економічне зростання, споживчу впевненість, попит на капітал) та внутрішня ампліфікація ризиків усередині крипторинку (леверидж, стабількоїни, платформи DeFi, які нестійкі до зовнішніх шоків). Показано, що у періоди посилення кредитних ризиків або підвищення облігаційної волатильності спостерігається зниження ціни біткоїна — і навпаки, періоди зниження дохідностей та кредитних премій, як правило, сприяють його зростанню.

Особливу увагу в документі приділено аналізу історичних епізодів (наприклад, криза 2020 року, агресивний цикл підвищення ставок у 2022 році, банківська криза в США у березні 2023 року), які дозволяють виявити різну поведінку біткоїна залежно від природи макрошоку. Підкреслено, що у періоди системного дефіциту ліквідності біткоїн поводиться як високоризиковий актив і падає разом із ринком, тоді як за специфічних фінансових стресів (як-от крах регіональних банків) може виступати у ролі «цифрового безпечного притулку».

У розділі про сценарний аналіз запропоновано три можливі сценарії розвитку подій: 1) продовження макроневизначеності, 2) поступове стабілізування макроекономічної ситуації та повернення до «м'якої посадки», 3) загострення боргової кризи з системними ризиками. У кожному випадку надано прогноз можливого впливу на крипторинок, динаміку BTC, поведінку інституцій та стан інфраструктури DeFi. Вказано, що у базовому сценарії очікується флетація ринку з низькою волатильністю і відсутністю чітких

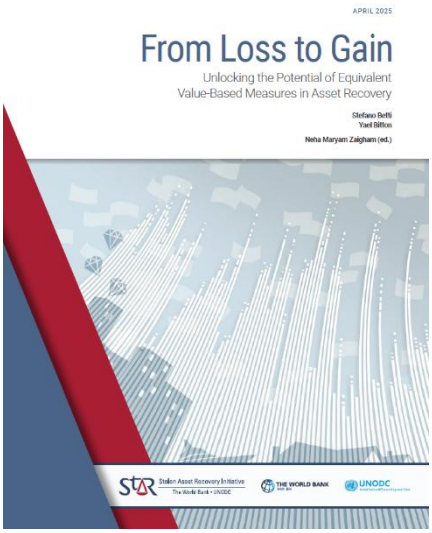
Висновки:

- **Кореляція між облігаціями та BTC зросла.** Після 2020 року BTC дедалі більше поводиться як ризиковий актив, чутливий до змін у дохідностях облігацій і макрофакторах. Це посилює потребу враховувати облігаційні індикатори в криптоаналізі.
- **Висока дохідність та реальні ставки пригнічують крипторинок.** Зростання реальних процентних ставок (особливо за 2-річними облігаціями) створює «альтернативну вартість» для інвесторів, що сприяє відтоку капіталу з криптоактивів у безризикові облігації.
- **Індикатори волатильності та кредитних ризиків є ранніми тригерами для крипторинку.** Стрибки індексу MOVE та HY OAS часто передують падінням на крипторинку, тому їх варто використовувати для побудови моделей раннього попередження.
- **Реакція криптовалют на макрошоки залежить від типу стресу.** У разі ліквідності (наприклад, 2020) крипто падає разом із усім ринком. У разі системного банківського ризику (2023) — можливе часткове відокремлення BTC від традиційних активів.

трендів, у позитивному — нова фаза бичачого ринку (до $110 тис. за BTC), а у кризовому — черговий глибокий спад криптовалют із посиленням регуляторного тиску, проблемами стабількоїнів і платформ DeFi.

Завершуючи, автори підкреслюють, що кореляція між криптоактивами та макроринками не є постійною, а динамічно змінюється залежно від макроекономічного контексту, змін у структурі ринку, регуляторного фону та домінуючих наративів. Попри окремі епізоди «від'єднання» (наприклад, у березні 2023), загалом біткоїн дедалі більше поводиться як актив, чутливий до глобального фінансового циклу, і це потрібно враховувати як трейдерам, так і аналітикам при побудові моделей оцінки ризику.

Конфіскація за еквівалентною вартістю: недооцінений інструмент у глобальному поверненні активів [14]



Документ, підготовлений у рамках Ініціативи з повернення вкрадених активів (StAR) спільно зі Світовим банком і Управлінням ООН з наркотиків і злочинності (УНЗ ООН), є фундаментальним аналітичним звітом, присвяченим потенціалу застосування заходів конфіскації за еквівалентною вартістю (EVB) як ефективного інструменту у справі повернення активів, здобутих злочинним шляхом. У цьому звіті робиться спроба подолати одну з найбільш критичних прогалин у глобальній антикорупційній архітектурі — невідповідність між обсягами і масштабами корупційних правопорушень та реально поверненими активами. Автори вказують, що за оцінками ООН, щороку через корупцію втрачається до 5% світового ВВП, однак лише незначна частка цих коштів повертається до законного власника — держави чи потерпілої сторони. Однією з основних причин неефективності повернення активів визначено сувору вимогу більшості юрисдикцій наявності прямого зв'язку між активами і конкретним злочином, що значно ускладнює конфіскацію в умовах складних фінансових схем, офшорних структур, використання підставних осіб або готівкових операцій. Саме тому EVB-заходи, які дозволяють конфісковувати майно, що є рівнозначним за вартістю до кримінального доходу, незалежно від його безпосереднього зв'язку з правопорушенням, пропонуються як стратегічне розширення юридичних можливостей правоохоронних органів і судів.

Документ детально аналізує, як EVB-заходи закріплені в основних міжнародних конвенціях, таких як Конвенція ООН проти корупції (UNCAC), Конвенція Ради Європи про відмивання, виявлення, арешт і конфіскацію доходів від злочинної діяльності (Варшавська конвенція), директиви Європейського Союзу (зокрема Директива 2014/42/EU та нова Директива 2024 року), Конвенція OECP про боротьбу з підкупом іноземних посадовців, Африканська антикорупційна конвенція та нормативні акти CEMAC. У цих документах визнається як можливість, так і необхідність для держав-учасниць приймати внутрішнє законодавство, яке дозволяє конфіскацію не лише безпосередньо отриманих злочинних доходів, але й майна, еквівалентного за вартістю до таких доходів. Окрема увага приділяється питанню, що навіть у «моністичних» правових системах, де міжнародні договори формально мають пряму дію,

[14] https://star.worldbank.org/publications/loss-gain-unlocking-potential-equivalent-value-based-measures-asset-recovery

положення UNCAC щодо EVB не є самовиконуваними — вони потребують спеціального імплементаційного закону, який би деталізував умови застосування таких заходів.

Звіт також містить порівняльний огляд національного досвіду 22 країн з різних регіонів і правових традицій, зокрема Франції, Сполученого Королівства, Ізраїлю, Південної Африки, Бразилії, Сполучених Штатів, Італії, Пакистану, Лівану, Боснії і Герцеговини, Іспанії, Індії, Кореї, Швейцарії, Нігерії та інших. Усі ці юрисдикції так чи інакше мають у своєму законодавстві положення, що дозволяють застосовувати EVB-заходи, однак їх реальне використання варіюється від рутинної практики до майже повної відсутності застосування. Основними перешкодами на практиці виявлено: правову невизначеність у формулюваннях норм, відсутність термінологічної єдності (EVB може називатися «ордер про грошове стягнення», «вимога про сягнення еквівалентної вартості», «судове рішення про грошове стягнення» тощо), обмежене застосування до лише окремих злочинів (наприклад, виключно відмивання доходів), нестачу навичок у суддів і прокурорів, а також недостатнє нормативне забезпечення тимчасових заходів — таких як арешт або замороження майна на підставі еквівалентної вартості.

Окремий блок звіту присвячено дискусії щодо того, чи слід EVB-заходи вважати вторинним або первинним інструментом конфіскації. У більшості юрисдикцій EVB використовується лише як резервний варіант, коли неможливо знайти безпосередньо «злочинне» майно. Проте інші країни, зокрема Південно-Африканська Республіка, Сполучене Королівство чи Франція, надають EVB-заходам статус повноцінного інструменту, що дозволяє значно оперативніше реагувати на корупційні та економічні злочини. При цьому показано, що застосування EVB у форматі тимчасових заходів (наприклад, арешт коштів до вироку) є критично необхідним, адже інакше до моменту винесення рішення активи можуть бути розпорошені або виведені за межі юрисдикції.

Важливою складовою є аналіз способів розрахунку так званої «вигоди», яку отримав злочинець і яка є базою для визначення розміру конфіскації. У звіті порівнюються два підходи: «чистий прибуток із вирахуванням витрат» і «загальний дохід без вирахування», а також проблематика оцінки активів у юрисдикціях з низьким рівнем прозорості або в умовах обмеженого доступу до бухгалтерської експертизи. Звіт також проводить порівняння EVB-заходів з іншими близькими

Висновки:

- **EVB-заходи є ефективним способом подолати труднощі доказування походження активів** — вони дозволяють конфісковувати майно правопорушника, еквівалентне за вартістю до незаконно одержаного, навіть без прямого зв'язку з конкретним злочином.
- **Незважаючи на міжнародні зобов'язання (UNCAC, FATF, EU Directives), EVB-підхід залишається недостатньо імплементованим та використаним** — часто через брак національного законодавства, термінологічну неузгодженість або недостатню кваліфікацію практиків.
- **Наявність EVB-положень у законодавстві не гарантує їх ефективного застосування** — необхідне активне підвищення обізнаності, навчання прокурорів і суддів, створення «культури конфіскації» та звітності щодо практики застосування EVB.
- **Псевдо-децентралізовані проєкти (on-chain CeFi) повинні готуватись до правових наслідків,** оскільки юридична відповідальність може бути встановлена навіть за наявності формальної децентралізації, якщо зберігається реальний контроль.
- **Для покращення міжнародного співробітництва необхідна уніфікація термінології EVB-заходів —** адже відмінності в термінах призводять до відмов або затримок у виконанні запитів про правову допомогу (MLA).

механізмами — такими як судовий припис про пояснення походження активів, розширена конфіскація, незаконне збагачення, грошові штрафи та компенсація шкоди потерпілим. Попри певні схожості, EVB має свою окрему логіку: тут мова не про покарання чи репарації, а про вилучення вигоди, яка не повинна залишатися у злочинця, незалежно від того, у якому саме майні вона реалізувалася.

Фінальний розділ звіту містить чітко сформульовані рекомендації для законодавців, суддів, слідчих і міжнародних експертів. Зокрема, пропонується імплементувати положення UNCAC щодо EVB у національне законодавство із чітким розмежуванням між видимими доходами та активами, що можуть бути об'єктом конфіскації за вартістю. Також пропонується визнати EVB не лише як допоміжний, а й як самостійний інструмент конфіскації, запровадити EVB-тимчасові заходи для замороження майна, розробити внутрішні керівництва і процедури, організувати тренінги для практиків, гармонізувати термінологію з іншими юрисдикціями, і створити інституційну звітність щодо кількості та результативності EVB-рішень. Документ супроводжується додатками, у яких подано чек-листи для політиків і практиків, витяги з UNCAC, а також стандартизований опитувальник для національних експертів. У підсумку звіт не лише узагальнює міжнародну практику, а й створює концептуальну та методичну основу для того, щоб заходи конфіскації за еквівалентною вартістю стали повноцінною частиною глобальної інфраструктури боротьби з корупцією, що особливо актуально для країн з високим рівнем складної фінансової злочинності, як-от Україна.

Наднаціональні запобіжники: як убезпечити фінансування, призначене для кліматичних цілей від корупції у глобальному масштабі [15]

Документ є ґрунтовним аналітичним оглядом ключових викликів, які постають перед міжнародною спільнотою у сфері забезпечення доброчесності в фінансуванні, що призначене для кліматичних цілей. Звіт був підготовлений за підсумками Другого симпозіуму з наднаціональних відповідей на корупцію, що відбувся у травні 2024 року під егідою Світового банку, Green Climate Fund, Transparency International та низки інших впливових організацій. Основна мета документа — проаналізувати, наскільки нинішня архітектура фінансування кліматичних дій відповідає викликам, пов'язаним із корупційними ризиками, системними прогалинами у підзвітності, фрагментацією механізмів нагляду та відсутністю обов'язкових стандартів доброчесності для державних і недержавних учасників, залучених до кліматичних ініціатив. У центрі уваги опиняється нове глобальне середовище, де кліматичні ресурси обчислюються трильйонами доларів США, і навіть втрата одного відсотка таких коштів через зловживання або корупцію означає мільярдні втрати, які можуть унеможливити адаптацію найбільш вразливих спільнот до кліматичних катастроф.

Звіт фіксує, що на тлі дедалі серйознішої зміни клімату та зростання очікувань від фінансових зобов'язань розвинених країн, механізми фінансування залишаються надзвичайно уразливими. Йдеться не лише про класичні корупційні злочини, як-от хабарництво, змови в публічних закупівлях, відмивання коштів і привласнення грантових ресурсів, але й про більш розмиті, але не менш небезпечні ризики: greenwashing (маніпулятивна стратегія, коли компанії, уряди або

[15] https://www.lse.ac.uk/granthaminstitute/wp-content/uploads/2025/05/Integrity-in-Climate-Finance-and-Action-Knowledge-Report.pdf

організації стверджують, що діють екологічно відповідально, аленасправді перебільшують, викривляють або вигадують свій внесок у захист довкілля чи боротьбу зі зміною клімату), конфлікти інтересів, закритість інформації, слабку незалежну оцінку ефективності, формальність у залученні громадськості та відсутність дієвих механізмів захисту викривачів. Підкреслюється, що найбільш ризиконебезпечними є ті сектори, які традиційно мають високу концентрацію державних інвестицій і слабкий нагляд — зокрема, енергетика, лісове господарство, інфраструктурні проєкти, гірничодобувна промисловість. Особливо загрозливою виглядає ситуація у добровільному вуглецевому ринку, де недостатній регуляторний нагляд, відсутність єдиних стандартів обліку, недостатня перевірка додатковості проєктів та уразливість до шахрайства створюють середовище, що активно експлуатується недоброчесними учасниками. Масові закупівлі вуглецевих кредитів з сумнівною верифікацією стають приводом для судових позовів, втрати довіри до кліматичних ініціатив загалом, а також інструментом легалізації доходів сумнівного походження.

Водночас автори звертають увагу на те, що національні юрисдикції часто неспроможні забезпечити належний антикорупційний контроль — через обмеженість ресурсів, політичну залежність інституцій, корумпованість місцевої влади або системні викривлення. Тому ключову роль у побудові ефективної системи доброчесності відіграють саме наднаціональні учасники: багатосторонні банки розвитку, міжурядові організації, глобальні фонди, приватні донори та транснаціональні корпорації. Звіт підкреслює необхідність зміцнення їхньої ролі, причому не лише шляхом впровадження внутрішніх кодексів і процедур, а через створення наднаціональних механізмів, що можуть діяти незалежно від політичної волі конкретних країн. Важливими прикладами таких механізмів названі санкційна система Світового банку, механізм взаємного визначення рішень про відсторонення між МФІ, незалежні підрозділи доброчесності (на кшталт IIU GCF), а також ініціативи щодо розкриття бенефіціарної власності та конфліктів інтересів.

У документі представлено також стратегічні пропозиції щодо координації між трьома основними конвенціями ООН — UNFCCC, UNCAC і UNTOC, оскільки всі вони, хоч і фокусуються на різних аспектах (клімат, корупція, організована злочинність), фактично мають перетин у сферах ризику, зокрема щодо управління природними ресурсами, вуглецевого ринку, ліцензування,

Висновки:

- **Фрагментація фінансування, яке призначено для кліматичних цілей створює системні прогалини в підзвітності,** що збільшує ризики корупції в таких секторах, як лісозаготівля, відновлювана енергетика, управління відходами та видобуток ресурсів. Необхідно запровадити єдині наднаціональні стандарти прозорості та моніторингу.
- **Добровільний вуглецевий ринок (VCM) є високоризиковим середовищем,** в якому часто трапляється greenwashing, подвійний облік і корупційне привласнення вигоди. Рекомендується створити національні реєстри вуглецевих кредитів, запровадити сертифікаційні вимоги та механізми відшкодування шкоди.
- **Поточна архітектура доброчесності в міжнародних фінансових інституціях не адаптована до кліматичних викликів.** Пропонується інтеграція функцій доброчесності й підзвітності в межах МФІ та впровадження кліматично орієнтованої процедури санкцій і перевірки доброчесності.
- **Наднаціональні відповіді мають стати ключовим інструментом,** особливо у випадках, коли національні юрисдикції неспроможні забезпечити антикорупційний нагляд. Ініціативи на кшталт IFI Task Force, FATF, UNCAC і UNTOC мають бути інтегровані з кліматичними цілями через спеціалізовані мандати й координаційні механізми.

держзакупівель, тощо. Ключовою точкою впливу в межах кліматичної політики визначається Конференція Сторін (COP), яка має потенціал інтегрувати доброчесність у всі ключові інструменти реалізації Паризької угоди — зокрема у Національно визначені внески (NDC), Звіти про прозорість (BTRs), Стратегії довгострокового розвитку (LTSs). Звіт пропонує розширити мандат COP з метою включення ризиків порушення доброчесності у глобальні кліматичні огляди, зокрема в процес Global Stocktake, та формалізувати вимоги щодо звітування про впровадження антикорупційних заходів у фінансованих проєктах.

Увагу також приділено питанням зміцнення внутрішніх інституційних спроможностей, включаючи подолання «силосності» всередині багатосторонніх банків розвитку, де підрозділи доброчесності, екологічного моніторингу та управління скаргами працюють ізольовано. Документ пропонує створення спільних робочих груп, впровадження законодавчої рамки перевірки доброчесності (IDD) з кліматичним компонентом, інтеграцію кліматичних індикаторів у санкційні системи, запровадження процедур співпраці з громадянським суспільством для незалежного моніторингу. Особливе місце займає розгляд ролі реєстрів бенефіціарної власності як інструменту запобігання відмиванню коштів коштів, призначених для кліматичного фінансування а також необхідність створення механізмів відшкодування шкоди від випадків порушення доброчесності.

У підсумку, Knowledge Report є комплексним закликом до переосмислення архітектури кліматичного фінансування не лише через призму обсягів і швидкості виділення коштів, а насамперед через призму якості, цільового спрямування, прозорості та відповідальності. У ньому закладено чітке розуміння, що жодна кліматична стратегія не буде успішною без вбудованої системи доброчесності, а самі гарантії доброчесності мають бути не супутнім інструментом, а фундаментом для ефективної, етичної та довготривалої кліматичної дії.

Майбутнє грошей вже тут: як стейблкоїни змінюють глобальну фінансову архітектуру[16]

Документ є однією з найбільш комплексних і глибоких спроб системно осмислити роль стейблкоїнів у трансформації глобальної фінансової архітектури. Автори пропонують структурований підхід до оцінки потенціалу стейблкоїнів через п’ять ключових випробувань (killer tests), які охоплюють не лише технологічні й економічні аспекти, а й системну інтеграцію в монетарне регулювання, геополітичну конфігурацію та майбутнє інституційної конкуренції між державними та приватними емітентами цифрових грошей. Звіт відкривається контекстуалізацією: стейблкоїни вийшли за межі нішевих інструментів крипторинку, і тепер із ринковою капіталізацією понад $210 млрд і річним обсягом транзакцій у $26,1 трлн претендують на статус альтернативного шару глобальної фінансової інфраструктури. Хоча майже 90% транзакцій 2024 року припадають на трейдинг у централізованих і децентралізованих біржах, близько 5–10% — це реальні платежі у B2B, P2P, корпоративному казначействі, трансграничних трансферах і роздрібній торгівлі. Саме ці нові юзкейси розглядаються як джерело потенційного зростання й об’єкт детального аналізу.

Перше випробування стосується перевірки, чи дійсно стейблкоїни створюють інкрементальну вартість у порівнянні з традиційними платіжними механізмами, такими як платежі в реальному

[16] https://richturrin.substack.com/p/five-killer-tests-for-stablecoins

часі (RTP), відкритий банкінг, банківські перекази або карткові системи. BCG оцінює чотири виміри: швидкість, вартість, трасованість і автоматизацію. Виявлено, що хоч блокчейн-перекази можуть бути майже миттєвими, введення та виведення коштів до фіатних валют часто повільний і залежить від локальних провайдерів. Вартість переказів може бути вкрай низькою (від $0.0001) на деяких мережах, але ціни gas fees можуть варіюватися до $3–6 на Ethereum або Tron. У галузі трасованості блокчейн переважає завдяки прозорості транзакцій, хоча інституційні платіжні системи мають кращу структурованість даних. Найбільший потенціал стейблкоїнів — у програмованості: за допомогою смарт-контрактів можливе створення умовних, ескроу- та автоматизованих платежів, які особливо релевантні для агентної торгівлі, AI-комерції та токенізованих активів. Тим не менш, рівень інтеграції в регульовану інфраструктуру все ще обмежений.

Друге випробування фокусується на реальному попиті поза криптоспекулятивними ринками. За даними Visa Onchain Dashboard, лише близько $2,1 трлн транзакцій 2024 року можна класифікувати як «реальні» — це платежі, розрахунки з реальними активами (RWA), транкордонні перекази, роздрібні покупки, фінансування рахунків і B2B-розрахунки. У звіті наводяться приклади кейсів Circle (мережа CPN, яка стає конкурентом SWIFT), Coinbase (протокол x402 для інтеграції AI-агентів з платіжною інфраструктурою), Bridge (банківські транскордонні сервіси з введенням або виведенням коштів) і Bitso (10% трансферів між США та Мексикою через стейблкоїни). Також розглянуто зростання ринку токенізованих фондів і money market funds, у яких стабільні монети використовуються як платіжна й розрахункова інфраструктура. Проте підкреслено, що відчутні бар'єри залишаються: фрагментація мереж, слабка інтероперабельність, висока вартість фіат-конверсій, обмежена технічна обізнаність кінцевих користувачів.

Висновки:

- **Стейблкоїни – не замінник, а доповнення до CBDC/TD.** Вони відіграватимуть незалежну роль в інфраструктурі майбутніх платежів, особливо в трансграничних розрахунках і B2B-скарбниці, але не замінять банківські депозити чи цифрові валюти центробанків.
- **Основна додана вартість — у міжнародних та автоматизованих сценаріях**. Стейблкоїни дають перевагу в швидкості, вартості та програмованості лише у вузьких сферах застосування: трансграничні P2P, AI-агенти, DeFi, RWA. У традиційних випадках користі менше через фрагментацію, ончейн/оффчейн бар'єри та високі витрати на введення або виведення коштів.
- **Висока рентабельність бізнесу – але вразлива модель.** Нинішня прибутковість емітентів базується на високих ставках і обсягах резервів. Для стабільності потрібен перехід до транзакційних моделей, партнерств із банками та інтеграції в традиційну інфраструктуру.
- **Регуляторна підтримка зростає, але ризики залишаються.** Регулювання стає більш сприятливим, але зберігаються ризики доларизації, системних потрясінь через масові викупи резервів та неузгодженості у правових і KYC-процедурах. Необхідна скоординована глобальна рамка з прозорістю резервів, механізмами обміну та фінансової стабільності.

Третій тест присвячений оцінці життєздатності бізнес-моделей. Емітенти, такі як Tether і Circle, генерують мільярдні доходи через процентні прибутки від резервів, що зберігаються у держоблігаціях США. Наприклад, Tether у 2024 році мав прибуток $53,5 млрд із командою близько 100 осіб. Проте така модель є вразливою до монетарної політики, тож компанії дедалі більше фокусуються на транзакційній монетизації — через запуск власних платіжних мереж, інфраструктурних альянсів із банками та стратегічні M&A (зокрема, придбання Bridge компанією Stripe). Банки, у свою чергу, також можуть отримувати вигоду, виступаючи як кастодіани

резервів, провідники FX-операцій і структурованих фінансових послуг для емітентів монет.

Четверте випробування стосується регуляторного контексту. У США адміністрація Трампа відмовилася від розробки CBDC, натомість просуває закони, які визнають платіжні стейблкоїни легітимними інструментами, за умови 100% резервного забезпечення та прозорості. В ЄС набрав чинності регламент MiCA, який також інтегрує стейблкоїни у фінансову архітектуру. Водночас у звіті ідентифіковано критичні макрофінансові ризики: потенційна доларизація економік країн з нестабільною валютою, витіснення банківської інтермедіації, системні ризики у разі масового викупу активів із резервів емітентів, а також нормативна невизначеність у сфері ПВК/ФТ. Автори наголошують, що потреба в глобальній скоординованій рамці — з прозорими резервами, єдиними вимогами до ліквідності, інтегрованими KYC/ПВК — є критичною для безпечного зростання ринку.

П’яте випробування аналізує питання співіснування трьох цифрових форматів грошей: стейблкоїнів, CBDC і токенізованих банківських депозитів. BCG пропонує бачення доповнюючої триархії, в якій кожен тип виконує унікальну функцію: CBDC — як безризиковий інструмент центробанку та системна опора, TD — як капіталоефективна форма банківських грошей, що зберігає кредитну функцію, а стейблкоїни — як вектор інновацій, інструмент для не-банківських суб’єктів і платформа для інтеграції з DeFi, Web3, агентною AI-економікою. Проте наголошено на важливості забезпечення взаємної конвертованості, збереження принципу єдиної вартості грошей, захисту споживача, чіткого визначення зобов’язань емітентів і механізмів управління ризиками.

У підсумку документ формулює стратегічні висновки для екосистемних учасників — банків, платіжних провайдерів, технологічних платформ, криптобірж і регуляторів. Основне послання полягає в тому, що вікно можливостей ще відкрите, але невблаганно закривається. Успішні учасники — це ті, хто вже зараз визначить свою роль у ланцюгу вартості (емісія, кастодіальна підтримка, введення або виведення коштів, транскордонна платіжна інфраструктура, скарбничі сервіси), встановить партнерство з державними структурами й інвестує у прозору, надійну й масштабовану платіжну архітектуру майбутнього. Технологія більше не є обмеженням — головною загрозою є втрата релевантності.

Майнінг біткойнів у 2025 році: економіка після халвінгу, еволюція обладнання та глобальні зрушення [17]

Аналітичний звіт “Bitcoin Mining 2025” глибоко досліджує поточний стан, економіку, технологічні зміни та геополітичні зрушення в галузі майнінгу біткоїнів після чергового халвінгу у квітні 2024 року. Документ охоплює ряд даних, оцінок, прогнозів і графіків, зосереджуючись на тому, як скорочення винагороди за блок з 6,25 до 3,125 BTC змінило фінансову модель видобутку, розстановку гравців у глобальному просторі та вимоги до майнінгового обладнання. Автори дослідження використовують багаторівневий підхід: поєднують ончейн-аналітику, енергетичні моделі, фінансову статистику, аналіз ринку ASIC-пристроїв, а також політичні та регуляторні тенденції, які формують доступ до інфраструктури.

[17] https://s3.cointelegraph.com/Bitcoin-Mining-2025-Post-Halving%20Economics-Hardware-Evolution-and-Global-Shifts-Report.pdf

Одним з основних висновків звіту є зниження маржинальності майнінгу після халвінгу: середній прибуток з одного терахешу за секунду (TH/s) зменшився на 45–50%, тоді як витрати на електроенергію залишаються ключовим визначальним фактором життєздатності майнінгових ферм. Через це майнери з низькоефективним обладнанням були змушені вийти з ринку, поступаючись місцем найбільш енергоефективним пристроям на кшталт Antminer S21, WhatsMiner M60 та інших моделей із показником енергоефективності менше ніж 20 J/TH. Звіт також констатує зростання централізації майнінгу: 5 найбільших публічних компаній зосередили понад 23% хешрейту мережі, що є рекордним показником за останні роки. У цьому контексті наголошується на важливості прозорості операцій цих компаній, оскільки вони є емітентами акцій на публічних ринках і підзвітні фінансовим регуляторам.

Особливу увагу приділено регіональним змінам. США залишаються провідною юрисдикцією, однак зростає тиск на сектор з боку регуляторів (наприклад, податкові ініціативи щодо енергоспоживання, проєкт Digital Asset Mining Energy excise tax). Натомість спостерігається активний розвиток майнінгових кластерів у Латинській Америці (Парагвай, Аргентина), Близькому Сході (ОАЕ, Оман), Африці (Західна та Центральна частини континенту), а також Китаї — незважаючи на офіційну заборону, "зелені" майнери, які використовують гідроелектростанції в сезон дощів, зберігають значну активність. Ці нові центри зосереджуються на використанні надлишкової енергії, інтеграції з відновлюваними джерелами та кооперації з урядами в межах пілотних енергетичних ініціатив.

У технічному вимірі звіт аналізує еволюцію ASIC-пристроїв: нове покоління чіпів базується на 3-нм і навіть експериментальних 2-нм технологіях. Порівняння вказує, що між поколіннями пристроїв спостерігається приріст продуктивності на 15–20%, водночас із зменшенням споживання енергії. Також документ розглядає альтернативні моделі оптимізації доходів — наприклад, терміновий хеджинг доходів через BTC derivatives або «підключення» майнінгу до централізованих енергетичних ринків як інструмент балансування (demand response).

Окремий розділ присвячений темі ESG (Environmental, Social, Governance): автори зазначають, що майнінг стикається зі зростаючою критикою з боку екологічних організацій, і великі компанії змушені впроваджувати звітність про вуглецевий слід, купувати "зелені сертифікати" або інвестувати в проєкти на основі відновлюваної енергії, щоб зберегти доступ до банківського фінансування та легальну присутність на публічних ринках.

Висновки:

- **Після халвінгу 2024 року майнінг біткоїнів став економічно життєздатним лише для високоефективного обладнання** з показниками нижчими за 20 J/TH, що вимагає від учасників ринку оперативного оновлення парку пристроїв та оптимізації споживання енергії.
- **Глобальний зсув у географії майнінгу вказує на зростання ролі країн Глобального Півдня**, які пропонують дешеву або надлишкову енергію, отже, компаніям слід розглядати стратегічну релокацію або міжнародне партнерство.
- **Концентрація хешрейту в руках публічних компаній вимагає посилення прозорості та ризик-менеджменту** для уникнення звинувачень у централізації й втрати децентралізованої природи мережі Bitcoin.
- **Екологічний тиск та очікування ESG-звітності вимагають від гравців ринку залучення інструментів сталого розвитку** — від впровадження моніторингу викидів CO_2 до інтеграції у відновлювану енергетику або програми карбонової компенсації.

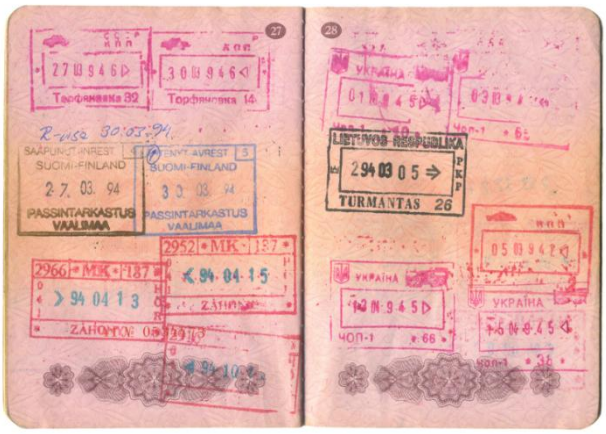
У фінансовому аспекті також зроблено важливі висновки: зниження доходу змусило частину майнерів шукати партнерства з центрами обробки даних (Data Centers) або перетворювати

майнінгову інфраструктуру на хмарні сервіси (Cloud Hashrate). Це відкриває нову гібридну бізнес-модель, де майнінг стає частиною ширшої енергетично-обчислювальної екосистеми.

Загалом, документ формує цілісну картину пост-халвінгової реальності в секторі майнінгу, де виживання та прибутковість дедалі більше залежать не лише від обладнання та вартості енергії, а й від здатності адаптуватися до регуляторних викликів, технологічного прогресу та геоекономічних трансформацій.

Інші новини

Від хаосу до ясності: Роль машинного навчання для пошуку паспортів [18]



Стаття Global Investigative Journalism Network (GIJN) за авторством Клемана Думуро, описує інноваційний підхід до виявлення паспортів у великих масивах документів за допомогою машинного навчання, розроблений у співпраці Міжнародного консорціуму журналістів-розслідувачів (ICIJ) з ученими з Центру ресурсів штучного інтелекту в журналістиці Осло-Метського університету та Норвезькою громадською телерадіокомпанією (NRK).

Стаття фокусується на полегшенні розслідувань офшорних компаній і трастів шляхом автоматизації пошуку паспортів у витоках даних, таких як Pandora Papers, Panama Papers і Paradise Papers. Паспорти є критично важливими для журналістів-розслідувачів, оскільки містять ключову інформацію, зокрема ім'я власника, громадянство, дату народження, номер паспорта та дату видачі, що зберігаються в машиночитній зоні (MRZ) — двох рядках тексту внизу сторінки з фотографією паспорта. Ці дані допомагають ідентифікувати кінцевих бенефіціарів офшорних структур у юрисдикціях із високим рівнем секретності, що є важливим для викриття прихованих фінансових схем.

Традиційні методи пошуку паспортів, які використовувала ICIJ, базувалися на застосуванні пошукової системи Datashare, де журналісти шукали документи за ключовими словами, такими як назви країн, «дата закінчення», «місце народження», «номер паспорта», або типовими назвами файлів, як-от «passport.pdf» чи «passport.jpg». Ці методи були неефективними через низьку точність, пропуски документів і численні помилкові збіги, спричинені поганою якістю сканів або обмеженнями оптичного розпізнавання символів (OCR). Наприклад, багато паспортів не мали явних назв файлів, а ключові слова могли зустрічатися в інших документах, що призводило до тривалого ручного аналізу тисяч сторінок.

Щоб подолати ці виклики, ICIJ у співпраці з NRK розробила інструмент на основі машинного навчання, який використовує алгоритми комп'ютерного зору, зокрема модель YOLO (You Only Look Once), адаптовану для виявлення паспортів. Ця модель, навчена на великому наборі різноманітних зображень паспортів, досягла 100% виявлення паспортних сторінок із точністю 86%, що означає лише 14% помилкових позитивних результатів. Інструмент спочатку конвертує документи в зображення, виявляє паспорти, а потім зчитує дані з MRZ за допомогою спеціалізованого OCR.

[18] https://gijn.org/stories/passports-machine-learning-icij/

Інтеграція інструменту в робочий процес ICIJ дозволила обробляти до 500 сторінок за хвилину на сервері з графічним процесором на 16 ГБ пам'яті. Після виявлення паспортів передбачення моделі передаються на платформу Prophecies для перевірки журналістами, що значно скорочує час на аналіз завдяки високій точності моделі. Перевірені документи позначаються в Datashare для негайного використання репортерами. Наприклад, під час одного розслідування інструмент звузив аналіз 110 000 документів до 3000 цільових перевірок, виявивши 500 унікальних паспортів після видалення дублікатів і перевірки додаткової інформації, що заощадило значний час для журналістів. Інструмент також відкриває можливості для автоматизованого зіставлення документів із реальними особами, що може ще більше оптимізувати розслідування.

Особлива увага приділяється безпеці та конфіденційності, оскільки паспортні дані є чутливими. ICIJ забезпечує захист інформації, обробляючи дані виключно в межах власної інфраструктури, без залучення сторонніх сторін. Співробітники та партнери підписують угоди про нерозголошення, а ваги моделі не публікуються, щоб уникнути атак типу Membership Inference Attacks, які могли б розкрити, на яких паспортах модель навчалася.

ICIJ планує поділитися методологією навчання моделі, щоб інші журналістські організації могли створювати власні інструменти, що може мати значний вплив на розслідувальну журналістику. Співпраця з академічними партнерами виявилася плідною, і ICIJ уже працює над новими проєктами, поєднуючи експертизу журналістів із новітніми технологіями.

Шахрайські схеми у рекрутингу: як обманюють шукачів роботи [19]

Стаття BBC детально висвітлює тривожне зростання шахрайських схем, спрямованих на шукачів роботи у Сполученому Королівстві, спираючись на дані Action Fraud, свідчення жертв, коментарі експертів та офіційних осіб.

За даними Action Fraud, у 2024 році було зареєстровано 4876 скарг на шахрайства, пов'язані з працевлаштуванням, що становить удвічі більше ніж порівняно з 2094 скаргами у 2022 році, а середня сума втрат на одну жертву склала £4707, що підкреслює значний фінансовий і психологічний вплив на постраждалих. Шахраї використовують витончені методи, створюючи переконливі фіктивні оголошення про роботу, які розміщують на легітимних платформах для пошуку роботи, а також надсилають пропозиції через WhatsApp, текстові повідомлення чи електронну пошту. Ці оголошення часто містять привабливі, але нереалістичні пропозиції зарплат, розмиті описи вакансій або непрофесійну комунікацію, що ускладнює їх розпізнавання для необережних кандидатів.

Одна з жертв, яка побажала залишитися анонімною, поділилася своїм досвідом: вона заплатила £280 за так званий «HR-курс» після відгуку на вакансію, розміщену на легітимному сайті. Згодом її змусили розміщувати шахрайські оголошення на власних сторінках у соціальних мережах, виступаючи в ролі «рекрутера», і передавати персональні дані інших кандидатів, яких також просили сплатити подібні внески. Анна розповіла, що шахраї вимагали від неї щодня надавати дані 16 нових кандидатів, або 80 на тиждень, і лише через тиждень вона зрозуміла, що її використовують для збору особистих даних, які потім продаються іншим злочинцям. Вона зазначила, що шахраї здавалися переконливими, проводячи «інтерв'ю» та «тренінги», а їхні пояснення щодо обмеженої інформації на вебсайті — нібито через статус стартапу — спочатку виглядали правдоподібними.

[19] https://www.bbc.com/news/articles/cg5qd3ve168o

Окрім шукачів роботи, шахрайства зачіпають і легітимні компанії. Шон Нірі, власник рекрутингової агенції з інженерії в Кнатсфорді, Чешир, розповів, що його компанію намагаються використати шахраї вже майже три роки, що завдає шкоди репутації, яку він будував дев'ять років. Він отримує щоденні дзвінки від жертв, які повірили фіктивним пропозиціям, виданим від імені його фірми, і зазначив, що хоча є ознаки шахрайських підходів, їх не завжди легко розпізнати кандидатам. Аналогічно, Стівен Тейлор, директор фірми Winterwood Farms у Мейдстоуні, Кент, повідомив, що приблизно 18 місяців тому шахраї почали рекламувати фіктивні посади від імені його компанії. Жертви зверталися, щоб перевірити легітимність пропозицій, коли шахраї вимагали оплату або коли кандидати починали підозрювати обман.

Експерти наголошують на складності проблеми. Клайв Філліпс, менеджер Trading Standards у Кенті, пояснив, що шахраї імітують легітимних рекрутерів, використовуючи переконливі методи для отримання грошей або особистих даних, які потім продаються на чорному ринку. Він вказав на ключові ознаки шахрайських оголошень: нереалістичні зарплати, розмиті описи, вимоги авансових платежів або надання конфіденційної інформації. Кіт Россер, голова JobsAware, зазначив, що Закон про безпеку в Інтернеті (Online Safety Act) зобов'язує платформи проводити ретельну перевірку та видаляти шахрайські оголошення, але впровадження цього закону залишається нерівномірним, що ускладнює боротьбу з проблемою. Лоррейн Ларія, головний офіцер зі стандартів Recruitment and Employment Confederation, підкреслила, що справжні рекрутери ніколи не вимагають оплати за пошук роботи, оскільки це незаконно, і закликала шукачів роботи чинити опір будь-яким таким вимогам.

Action Fraud і Міністерство внутрішніх справ Сполученого Королівства також відреагували на проблему. Представник Action Fraud порадив уникати сплати авансових внесків, перевіряти легітимність пропозицій і використовувати надійні паролі та двофакторну автентифікацію для захисту онлайн-акаунтів. Представник МВС назвав ці злочини «абсолютно ганебними» і повідомив, що уряд працює над новою розширеною стратегією боротьби з шахрайством, співпрацюючи з правоохоронними органами, приватним сектором і технологічними компаніями. Для захисту шукачам роботи рекомендують перевіряти існування компаній через офіційні джерела, уникати будь-яких платежів за працевлаштування, звертати увагу на підозрілі ознаки в оголошеннях і повідомляти про шахрайські повідомлення. Стаття підкреслює системний характер проблеми, необхідність пильності та посилення заходів безпеки як на індивідуальному, так і на державному рівні.

Винне шахрайство у Швейцарії: Розкриття обману у Вале [20]

Стаття від Wine-Searcher розкриває масштабне винне шахрайство в Швейцарії, зосереджуючись на регіоні Вале, найбільшому виноробному регіоні країни, та двох ключових постатях – Седріку Флактіону та Домініку Жиру, які опинилися в центрі скандалів через фальсифікацію вин і пов'язані з цим злочини.

Седрік Флактіон, винороб і власник виноробні Cave des Cailles (тепер Maison Rouge) у селі Сен-П'єр-де-Клаж, був засуджений 2 вересня 2024 року судом у Сьйоні до трьох з половиною років ув'язнення та виплати компенсації у розмірі 1,94 мільйона швейцарських франків (приблизно 2,34 мільйона доларів США). Його звинуватили у купівлі 750 000 літрів дешевого іспанського наливного вина та 105 000 літрів піно нуару з менш престижного швейцарського апеласьйону

[20] https://www.wine-searcher.com/m/2025/05/wine-fraud-rocks-switzerland

Шаффхаузен у період з 2009 по 2016 рік, які він видавав за вино апеласьйону Вале, що має вищий статус і ціну. Флактіон продавав фальсифіковане вино за 9–13 франків за літр, купуючи іспанське вино за 1,5 франка, а піно нуар із Шаффхаузена – за 3 франки за літр, отримавши прибуток у розмірі близько 1 мільйона франків при обороті в 12 мільйонів франків. Суд встановив, що він створив 52 фальшиві інвойси та використовував письмові інструкції для змішування вин, щоб приховати їх походження.

Хоча Флактіон частково визнав провину, зокрема у створенні фальшивих інвойсів і перевищенні дозволених обсягів виробництва, він заперечував продаж іспанського чи шаффхаузенського вина як продукцію Вале, стверджуючи через адвоката, що піно нуар продавався як вино нижчої категорії. Суддя Софія Бартольді Метрайє зазначила, що шахрайство стало для нього «звичною практикою», і він не взяв на себе повну відповідальність. Перед судом поліція конфіскувала 13 його автомобілів, включаючи два Aston Martin, два Ferrari, два Porsche, Audi та BMW, заблокувала 15 банківських рахунків і заморозила активи. Флактіон подав апеляцію, розгляд якої заплановано на липень 2025 року, але його активи залишаються під арештом.

Домінік Жиру, ще одна суперечлива постать, також перебуває під слідством за подібні звинувачення. Раніше відомий як власник Giroud Vins (перейменованої на Château Constellation у 2014 році після звинувачень у шахрайстві), Жиру має історію кримінальних порушень, включаючи ухилення від сплати податків і шпигунство. У 2023 році Федеральний суд Швейцарії підтвердив його засудження за найм детектива та хакера для стеження за журналістами, а також за зв’язки з екстремістськими організаціями. У справі Флактіона Жиру згадується як особа, якій постачалося іспанське вино, причому 43 із 52 фальшивих інвойсів Флактіона були оформлені на компанії, пов’язані з Жиру, на суму близько 3 мільйонів франків.

Жиру, у свою чергу, звинувачується у створенні фальшивих інвойсів на ім’я Флактіона. У 2015 році Професійна асоціація виноградарства та виноробства Вале (IVV) подала проти нього позов на основі його зізнання про використання неапеляційних сортів винограду для виробництва вина Вале, а в травні 2022 року кантон Вале звинуватив Château Constellation у продажу 30 000 літрів фальсифікованого вина. У червні 2024 року для розслідування справи призначили спеціального прокурора Шарля Наварро, що підкреслює її серйозність.

Стаття підкреслює, що винне шахрайство не обмежується Швейцарією: схожі випадки зафіксовано у Франції (справа в Бордо з 34 000 гектолітрами іспанського вина, проданого як вино Бордо) та Іспанії (справа Reserva de la Tierra з 10 мільйонами пляшок фальсифікованого вина). Такі схеми зазвичай передбачають змішування дешевого наливного вина з якіснішим або видачу його за престижний апеласьйон, а розслідування тривають роками через складність.

У Швейцарії, зокрема в Вале, вживаються заходи для боротьби з шахрайством. Голова IVV Іван Аймон зазначає, що чесні винороби страждають від конкуренції з шахраями, які продають дешевше фальсифіковане вино, тоді як виробництво у високогірному Вале є дорогим. Нові правила передбачають обмеження обсягів виробництва для кожного сорту винограду, створення єдиного органу контролю та посилення ізотопного тестування вин для перевірки їх походження. Аймон наголошує, що ізотопне тестування є найефективнішим методом, але потребує ширшої бази даних і юридичного визнання в судах. Шахрайство завдає шкоди репутації апеласьйонів і економічним інтересам чесних виноробів, тому посилення контролю та прозорості в ланцюжку постачання є критично важливими.

Ваша думка важлива!

1. Яким чином слід розширити або доповнити наглядову рамку MiCA для подолання викликів, пов'язаних з анонімністю DeFi-протоколів, і як елементи такого підходу можуть бути адаптовані для впровадження в Україні?
2. Як Україна може адаптувати підходи до регулювання ринку криптоактивів з урахуванням досвіду впровадження MiCA в ЄС?
3. Чи варто Україні адаптувати підхід США до регулювання цифрових активів, з розмежуванням повноважень за типами активів? Які елементи моделі США можуть бути релевантними для українського ринку під час формування національного режиму?
4. Як може виглядати модель регулювання крипторинку в Україні, яка водночас захищатиме інвесторів від глобальних макрошоків та не гальмуватиме розвиток Web3-екосистеми на тлі посилення фінансових ризиків у світі?
5. Якими мають бути законодавчі рамки для стейблкоїнів в Україні, щоб забезпечити інновації у платіжній інфраструктурі без створення ризиків для монетарного суверенітету та фінансової стабільності?
6. Як Україні розбудувати інституційну «культуру конфіскації», яка поєднувала б агресивні антикорупційні підходи із гарантіями справедливого судочинства та ефективним менеджментом арештованих активів?
7. Чи може трирівнева система перевірки джерела статків стати новим стандартом для всіх СПФМ в Україні? Які труднощі можуть виникнути при впровадженні такого підходу в умовах обмежених ресурсів чи невизначеності профілю клієнта?

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-2025-22

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

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