Методологічний бюлетень

Серійний номер: МінФін-AML-2025-20

Травень 2025

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

Пітер Маршалл

Мета

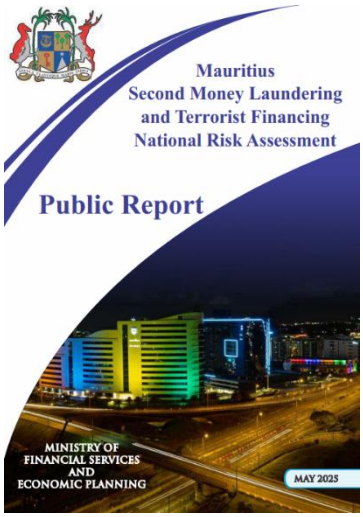
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено 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

Звіт НОР Республіки Маврикій [1]



Другий звіт про Національну оцінку ризиків Маврикію (НОР) є масштабним стратегічним документом, що охоплює широкий спектр внутрішніх і транскордонних загроз у фінансовій системі країни. У звіті відображено еволюцію національної системи ПВК/ФТ з моменту першої оцінки, адаптацію до нових викликів — зокрема, цифровізації, транснаціональної злочинності, а також — підвищення рівня ризиків, пов’язаних із використанням складних корпоративних структур, віртуальних активів і міжнародного фінансового посередництва.

Звіт охоплює оцінку як національний, так і секторіальний рівень. Методологія, використана для оцінки, базується на вимогах FATF, з використанням якісного та кількісного аналізу, фокус-груп, даних від правоохоронних органів, ПФР, регуляторів, підзвітних установ і

[1] https://www.fiumauritius.org/fiu/?p=5147

зовнішніх експертів. Враховувалися як кількісні показники підозрілих транзакцій, розслідувань, судових справ, так і якісні характеристики, включаючи спроможність установ до виявлення ризиків, рівень впровадження ризик-орієнтованого підходу, та ефективність нагляду.

Основними ідентифікованими загрозами у сфері ВК стали: податкові правопорушення (включаючи ухилення від податків та фальсифікацію рахунків), корупція (в т.ч. у транскордонних угодах), наркотрафік, шахрайство (особливо в галузі онлайн-трейдингу та інвестицій), а також незаконне використання юридичних осіб для приховування активів. Особливо наголошено на високому ризику, пов'язаному з офшорними структурами та фондами, що адмініструються юридичними або фідуціарними компаніями, а також на високій уразливості секторів, що обслуговують таких клієнтів — включаючи трастові компанії, юридичні фірми, бухгалтерів та номінальних директорів.

Серед найбільш вразливих секторів було визнано:

- Небанківські фінансові установи, особливо ті, що надають послуги з управління активами, трастів і фондів.
- Юридичні особи та правові утворення, через низький рівень прозорості бенефіціарної власності.
- Професійні посередники, які виступають як формальні засоби входу до фінансової системи Маврикію для іноземних осіб.
- Сектор азартних ігор, що має високий потенціал для інтеграції готівки до легальної економіки.
- Нерухомість, як один із найпоширеніших засобів розміщення нелегальних доходів.

У сфері фінансування тероризму (ФТ) ризик класифіковано як низький, однак із обережністю вказано на потенційні вразливості, пов'язані з:

- Відсутністю достатньої прозорості в секторі неприбуткових організацій (НПО).
- Ризиком використання нових платіжних технологій (цифрові гаманці, криптовалюти) для мікротранзакцій у рамках підтримки екстремістських організацій.
- Можливими зовнішніми впливами з боку радикальних осередків, що діють у суміжних регіонах Африки.

Важливе місце у звіті займає аналіз новітніх ризиків, пов'язаних із:

- Віртуальними активами (ВА): хоча обсяг операцій із ВА у Маврикії наразі невеликий, потенціал їх використання для ВК/ФТ визнаний як високий. Регулятор розробляє правову рамку для контролю таких активів.

Висновки:

- **Високий ризик ВК через використання офшорних структур і складних юридичних осіб**: Рекомендується законодавчо обмежити можливість створення анонімних корпоративних структур та забезпечити обов'язкову ідентифікацію кінцевих бенефіціарних власників.
- **Недостатня імплементація РОП серед малих підзвітних суб'єктів**: Потрібна системна просвітницька робота та диференційований нагляд за юристами, бухгалтерами, агентами з нерухомості та НПО.
- **Недосконаліть ІТ-систем ПФР та слабкий обмін інформацією**: Пріоритет - автоматизація обміну даними між установами та модернізація механізмів виявлення підозрілих транзакцій.
- **Загроза з боку цифрових активів і платіжних платформ**: Слід впровадити регулювання діяльності провайдерів послуг з віртуальними активами та контролювати їх участь у фінансовому ринку.

- Фінтех-компаніями, які можуть діяти поза межами традиційного банківського нагляду.
- Платформами електронних грошей, які дедалі частіше використовуються для переказу коштів між юрисдикціями.

У звіті зазначено покращення в роботі підрозділу фінансової розвідки (ПФР), включаючи зростання кількості повідомлень про підозрілі операції, особливо з боку банківського сектора, однак вказано на низький рівень залученості нефінансових установ. Визначено потребу у зміцненні аналітичної спроможності ПФР, зокрема у сфері аналізу цифрових транзакцій та транскордонного обміну інформацією.

Документ завершується комплексним планом дій, який охоплює:

- Гармонізацію законодавства з міжнародними стандартами;
- Вдосконалення процедур верифікації бенефіціарної власності;
- Розвиток механізмів обміну інформацією між регуляторами;
- Цільове навчання для підзвітних суб'єктів (особливо у вразливих секторах);
- Побудову національної IT-платформи для збору, аналізу і поширення даних з ВК/ФТ.

Звіт також підкреслює важливість координації між ПФР, правоохоронними органами та регуляторами, а також подальше укріплення міжнародного співробітництва, зокрема через Egmont Group, ESAAMLG і співпрацю з ЄС.

Керівництво SFO 2025: як уникнути кримінального переслідування [2]

Документ, є офіційним керівництвом Управління з розслідування шахрайства Сполученого Королівства (Serious Fraud Office – SFO), яке описує підхід відомства до корпоративного кримінального переслідування, зокрема в контексті самостійного повідомлення про правопорушення (self-reporting), співпраці та укладення «угод про відкладене кримінальне переслідування» (Deferred Prosecution Agreements – DPA). Керівництво визначає умови, за яких компанії можуть уникнути кримінального переслідування через конструктивну взаємодію з SFO, акцентуючи увагу на важливості відповідального та своєчасного повідомлення як ознаки належного корпоративного управління.

SFO заявляє, що надання компанією швидкого повідомлення та подальша повноцінна співпраця з відомством є основними факторами, які суттєво підвищують імовірність отримання запрошення до переговорів щодо DPA замість формального обвинувачення. Навіть якщо компанія не ініціювала повідомлення, але надала виняткову підтримку під час розслідування (наприклад, зібрала докази, зберегла матеріали, надала доступ до співробітників), вона також може розраховувати на розгляд DPA як альтернативи обвинуваченню. Однак, якщо компанія свідомо не повідомила SFO про злочин у розумний строк після його виявлення, це розглядається як публічний інтерес на користь кримінального переслідування.

Процедура повідомлення детально регламентована. Повідомлення має надсилатися до розвідувального підрозділу SFO (Intelligence Division) через захищену форму. У першому зверненні необхідно надати всі відомі факти, включаючи опис підозрюваних правопорушень, причетних осіб, відповідні юрисдикції, наявні докази, ризики знищення інформації або

[2] https://www.gov.uk/government/publications/sfo-corporate-guidance/sfo-corporate-guidance

розпорошення активів. До того як надаються цифрові матеріали, необхідно погодити формат передачі. Водночас повідомлення, подане до іншого регулятора або в межах Звіту про підозрілу активність (SAR), не визнається повідомленням, якщо не відбувається одночасне або негайне повідомлення SFO. Підрозділ зобов'язується зв'язатися з компанією упродовж 48 робочих годин, оновлювати статус розгляду справи, ухвалити рішення про початок розслідування протягом 6 місяців та за можливості завершити переговори щодо DPA також у цей термін.

Ключовою складовою в оцінці SFO є характер та повнота співпраці компанії. Співпраця передбачає активну та добровільну допомогу, яка перевищує мінімальні законодавчі вимоги, як-от надання матеріалів у відповідь на запити за статтею 2 Закону про кримінальну юстицію. Як приклад зразкової співпраці, SFO наводить перелік конкретних дій: оперативне збереження матеріалів, структурована передача документів, розкриття інформації про підозрюваних осіб, участь в обговоренні параметрів внутрішнього розслідування, надання результатів цих розслідувань, у тому числі записів інтерв'ю (з відмовою від юридичної привілеї, якщо можливо), інформування про дії інших правоохоронців, надання фінансової інформації щодо шкоди та прибутку, що виникли внаслідок правопорушення, а також демонстрація кроків із виправлення внутрішніх комплаєнс-процедур. SFO визнає право компаній зберігати юридичну привілегію (LPP), проте вважає добровільну відмову від неї проявом високої доброчесності.

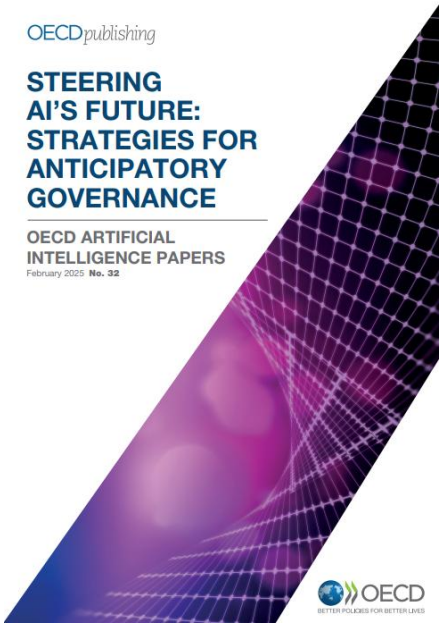
Разом із тим документ також чітко окреслює, що вважатиметься ознаками недобросовісної поведінки: «форум-шопінг» (спроби спрямовано звернутися до іншої юрисдикції задля уникнення переслідування у Британії), спроби замовчування або применшення правопорушень, затягування з передачею інформації, навмисне перевантаження розслідування надмірною кількістю несуттєвих матеріалів. Така поведінка серйозно ускладнює можливість розгляду справи через DPA і свідчить про відсутність справжньої співпраці.

Документ узгоджується з нормами Кодексу прокурорів суду Корони, офіційним Керівництвом щодо переслідування компаній, а також Кодексом DPA. У підсумку, SFO заявляє, що лише в «виняткових випадках» буде розглядатися можливість кримінального переслідування щодо компанії, яка вчасно самостійно повідомила про правопорушення та в повному обсязі співпрацює. Це створює сприятливе регуляторне середовище для компаній, що прагнуть демонструвати прозорість, відповідальність і корпоративну доброчесність.

Висновки:

- **Швидке повідомлення – критично важливе для уникнення обвинувачення.** Якщо компанія добровільно та без зволікань повідомляє SFO про підозру на правопорушення, це значно підвищує шанси на розгляд справи через угоду (DPA), а не шляхом кримінального переслідування.
- **Лише реальна, активна співпраця дає право на DPA.** Навіть після повідомлення компанія повинна активно сприяти розслідуванню: передавати документи, надавати доступ до персоналу, ділитися результатами внутрішнього розслідування, демонструвати прозорість і відкритість.
- **Несумлінна або тактична поведінка підриває довіру та призводить до обвинувачення.** Якщо компанія затягує передачу інформації, применшує масштаби порушення або намагається уникнути юрисдикції SFO, це буде розцінено як відсутність співпраці та привід до відкриття кримінальної справи.
- **SFO забезпечує прозорі строки та процедурну визначеність.** Відомство гарантує швидкий контакт (до 48 годин), рішення про розслідування протягом 6 місяців та оперативне завершення переговорів щодо DPA – це створює передбачуване середовище для бізнесу.

AI: Стратегії передбачувального врядування [3]



Документ представляє собою стратегічний план дій щодо впровадження адаптивного та проактивного врядування штучного інтелекту (AI), побудованого на основі Рамкової системи передбачувального врядування для новітніх технологій OECD. Його основна мета — підтримка урядів у формуванні політик, здатних передбачати виклики, пов'язані зі стрімким розвитком AI, та керувати ними, одночасно забезпечуючи інноваційність, етичність і безпечність таких технологій.

Центральною ідеєю звіту є п'ять елементів ефективного передбачувального врядування: цінності, стратегічна аналітика, залучення заінтересованих сторін, гнучке регулювання та міжнародна співпраця. У кожному з цих напрямів запропоновано приклади інституційних підходів, інструментів та платформ, які вже реалізуються, зокрема через OECD.AI Observatory, систему моніторингу інцидентів AIM, мережу ONE AI, а також співпрацю в межах Глобального партнерства з питань AI (GPAI).

Особливу увагу приділено концепції вбудовування етичних цінностей у життєвий цикл систем AI. Це передбачає не лише декларативне проголошення принципів (зокрема оновлених Принципів OECD щодо AI), а й їх інституціоналізацію через інструменти, такі як Каталог інструментів і метрик для надійного AI. Таке втілення має враховувати права людини, приватність, відсутність дискримінації, прозорість і підзвітність систем AI.

Другий напрям — стратегічна аналітика — охоплює як реальний моніторинг інцидентів, так і форсайт-дослідження, що дозволяє прогнозувати майбутні ризики, можливості та пріоритети. Звіт детально описує роль групи експертів OECD.AI щодо майбутнього AI, яка ідентифікувала десятки потенційних переваг, загроз та політичних рішень для майбутнього використання AI. Визначено приклади "слабких сигналів", що вимагають уваги — від концентрації влади в обмеженому колі компаній до ризиків втрати контролю над критичними системами.

Слабкі сигнали — це ранні, малопомітні ознаки або індикатори майбутніх змін, тенденцій або загроз, які на момент виявлення можуть виглядати несуттєвими, випадковими або ізольованими, але згодом можуть мати значний вплив на систему, сферу чи політику. У контексті управління штучним інтелектом, слабкі сигнали допомагають виявляти нові ризики або можливості, які ще не стали домінантними або загальновизнаними, але можуть істотно вплинути на розвиток AI у майбутньому.

У звіті OECD до слабких сигналів, які відстежуються через систему AIM, належать повідомлення про інциденти, пов'язані з використанням ШІ, що можуть вказувати на:

- нові типи зловживань або кіберзагроз (наприклад, дезінформація за допомогою генеративного AI);
- несподівані соціальні чи етичні наслідки (наприклад, дискримінація через алгоритми);
- концентрацію влади в окремих корпораціях або країнах (що може підірвати конкуренцію й демократичні процеси);
- випадки порушення прав людини, які ще не мають масштабного резонансу, але сигналізують про потенційно системні ризики.

[3] https://www.oecd.org/en/publications/steering-ai-s-future_5480ff0a-en.html

Виявлення та аналіз слабких сигналів є частиною стратегічного передбачення і служить основою для проактивного (а не реактивного) врядування. Замість того, щоб чекати, поки проблема стане очевидною і поширеною, аналіз слабких сигналів дозволяє заздалегідь готувати політичні, етичні чи технологічні відповіді.

Наприклад, через залучення стейкхолдерів, яке описується як багаторівнева система — від інформування до співтворення рішень. Зокрема, описано практики громадського обговорення, відкритих консультацій, колективних платформ (ONE AI, GPAI) та використання самих систем AI для модерації або аналізу громадської думки.

Гнучке врядування передбачає використання інструментів регуляторного експериментування, таких як "пісочниці", впровадження стандартів, підходів із вбудованими цінностями (наприклад, етика або захист даних, передбачені ще на етапі проєктування системи), а також управління ризиками на основі взаємно узгоджених (інтероперабельних) рамкових моделей. Особливий акцент зроблено на відповідальності бізнесу через застосування оновлених Керівних принципів OECD для міжнародних підприємств (MNE Guidelines), які зобов’язують проводити комплексну належну перевірку на всіх етапах розробки та застосування AI. Це має особливе значення в умовах транснаціонального характеру фінансування та застосування систем ШІ.

Висновки:

- Передбачувальне врядування AI має будуватися на динамічному поєднанні етичних принципів, технологічного аналізу та відкритої взаємодії всіх учасників інноваційного процесу.
- Системне управління ризиками, засноване на глобально узгоджених стандартах, є критично важливим для довіри до AI.
- Бізнес має відігравати активну роль у забезпеченні відповідального використання AI через інструменти належної перевірки та етики, передбаченої ще на етапі проєктування системи.
- Міжнародна координація, інтероперабельність політик та стандартизація звітності щодо інцидентів - запорука ефективного глобального врядування AI.

Міжнародна співпраця висвітлюється як невід'ємна частина ефективного врядування AI, що охоплює як глобальні ініціативи (ООН, ЮНЕСКО, G7, G20), так і регіональні стратегії (наприклад, Закон ЄС про AI, стратегія Африканського Союзу) та багатосторонні формати (OECD, GPAI, Globalpolicy.AI). Акцентовано важливість взаємосумісності, узгодженості та спільного визначення термінів, підходів до моніторингу інцидентів та оцінки ризиків.

Санкції

Тренди санкцій, на які варто звернути увагу у 2025 році [4]

Поточний 2025 рік ознаменувався зростаючим тиском міжнародної санкційної політики — як у широті охоплення юрисдикцій, так і в складності динаміки її реалізації. Після серії глобальних зрушень, включаючи посилення геополітичної напруги, повернення на посаду президента США Дональда Трампа, продовження війни Росії проти України, а також ескалації конфліктів на Близькому Сході та навколо Північної Кореї, санкційна інфраструктура перестає бути просто

[4] https://complyadvantage.com/insights/sanctions-trends-2025/?utm_campaign=CA0002.4%20%7C%20PEPs%2FSanctions%20%7C%20NTR%20%7C%20EMEA%20%7C%20AMER%20%7C%20APAC&utm_medium=email&_hsenc=p2ANqtz--gisFky5gvuEk8iwwVO9pyw7VX1L9dbVz8lraO4qtCa7JTnc3vYw0CxFwmVWwC02er6fP9b6piSchKCWEbKoz8psUhoQ&_hsmi=344920734&utm_content=344920734&utm_source=hs_automation

інструментом міжнародної політики — вона стає самостійною ареною впливу та боротьби за економічну перевагу.

Аналітики Comply Advantage фіксують чотири взаємопов'язані тренди, які будуть формувати цей простір у найближчі місяці та роки. По-перше, відчутне посилення політики Сполучених Штатів щодо Китаю не залишає сумнівів, що нова адміністрація США буде безкомпромісною в питаннях економічної безпеки. Санкції, які раніше мали точковий характер — наприклад, проти компаній, що співпрацювали з російськими чи іранськими суб'єктами, — тепер можуть еволюціонувати в повноцінну систему вторинних санкцій проти великих китайських банків або промислових конгломератів. Для фінансових установ це означає зростання регуляторної невизначеності, особливо якщо вони одночасно працюють у юрисдикціях з протилежними стратегічними інтересами.

По-друге, незважаючи на певну втомленість медіа та інституцій від тривалої російсько-української війни, питання санкцій проти РФ залишається центральним у європейському і трансатлантичному порядку денному. Попри гучні пакети обмежень, досі залишається величезний простір для обходу санкцій — через треті країни, підставних осіб, схеми з подвійним призначенням та навіть через криптовалютні канали. Пріоритетом для західних урядів на 2025 рік є закриття цих лазівок. Йдеться не лише про подальше розширення чорних списків, а й про удосконалення механізмів контролю за експортом, посилення міждержавного обміну даними, а головне — про підвищення відповідальності третіх країн, які фактично дозволяють обхід санкцій.

У цьому контексті все частіше лунає дискусія про запровадження повноцінного режиму вторинних санкцій для посередників у Центральній Азії, Кавказі, Туреччині, ОАЕ та навіть окремих гравців у Східній Європі. Такі заходи створюють особливий тиск на платіжні системи, банки, логістичні оператори, верифікаційні служби та компанії, що надають послуги з цифрової інфраструктури. Це, в свою чергу, означає необхідність більш тонкого і структурного ризик-менеджменту з боку комплаєнс-відділів.

У випадку Близького Сходу фокус санкційної політики залишається на Ірані. Санкції проти Тегерану дедалі частіше накладаються не стільки за ядерну програму, скільки через його проксі-активність у регіоні — фінансування ХАМАС, Хезболли, хуситів та інших структур, які Захід розглядає як терористичні організації. Неформальні мережі фінансування, обхід через гуманітарні фонди, використання криптоактивів і псевдоблагодійних платформ — усе це стає частиною нової парадигми, до якої фінансові установи мусять бути готові. В умовах швидкої ескалації, ризик випадкового порушення санкцій зростає. Саме тому ключовим ресурсом стає якісний моніторинг клієнтської бази, виявлення регіонального ланцюга контрагентів, а також запровадження гнучких, швидко оновлюваних сценаріїв скринінгу.

Північна Корея — ще один стратегічний напрям для санкційного тиску. На тлі зростаючої воєнно-промислової співпраці між КНДР і РФ, Захід готується до введення нових санкційних режимів, спрямованих не лише на Пхеньян, а й на його міжнародних "фасилітаторів" — компанії, посередників, криптобіржі, які допомагають організовувати схеми "зброя в обмін на паливо". Тут особливу увагу приділяють компаніям з реєстрацією у Гонконгу, Південно-Східній Азії та ОАЕ — через них КНДР роками обходила обмеження РБ ООН.

У підсумку — 2025 рік демонструє, що санкції дедалі більше функціонують не як реакція, а як проактивний геоекономічний інструмент, який впливає на фінансові ринки, змінює логіку побудови ланцюгів поставок, структуру кореспондентських відносин і архітектуру ризиків.

Сучасний комплаєнс не може бути реактивним: очікується перехід до динамічних систем управління ризиками, з глибокою інтеграцією даних у реальному часі, автоматизованим скринінгом на рівні транзакцій, передбачувальним сценарним аналізом та стратегічним плануванням дій у разі потрапляння клієнтів або партнерів до списків.

Звіти окремих інституцій та експертів

Цифрові долари: банки та державний сектор стимулюють впровадження блокчейну [5]

Документ є всеохоплюючим стратегічним аналізом сучасного стану та перспектив впровадження блокчейн-технологій у фінансовому секторі та державному управлінні. Він зосереджений на двох ключових напрямах: по-перше, на зростаючому значенні стейблкоїнів як нового фінансового інструменту в умовах зміни регуляторного ландшафту, і по-друге — на застосуванні блокчейну для модернізації державних систем управління, фінансування, надання послуг та посилення прозорості. Центральною темою документа є теза, що 2025 рік потенційно може стати "моментом ChatGPT" для блокчейн-індустрії — переломним моментом масового прийняття технології на тлі регуляторної визначеності, економічної доцільності та політичної волі.

Стейблкоїни, як новий клас цифрових активів, займають провідне місце у звіті. Зазначено, що їхній загальний обсяг у обігу на квітень 2025 року перевищив $230 млрд, при цьому дві основні монети — USDT і USDC — домінують на ринку. Аналітики Citi прогнозують, що у базовому сценарії до 2030 року ринок стейблкоїнів може сягнути $1.6 трлн, а в оптимістичному — $3.7 трлн. Очікується, що 90% ринку залишатиметься деномінованим у доларах США, що водночас створює ризики “цифрової доларизації” для інших країн і загрозу стратегічній автономії у сфері фінансової політики.

Звіт аналізує моделі функціонування стейблкоїнів (передусім — забезпечених фіатними активами), механізми підтримки їх прив'язки до базових валют, схеми розміщення резервів (у т.ч. US Treasuries), а також основні напрями їхнього використання: криптотрейдинг (90–95% обсягу), B2B-платежі, міжнародні перекази, операції на ринку капіталу. У документі підкреслено, що за умов сприятливого регулювання, банки можуть зіграти ключову роль у розвитку екосистеми стейблкоїнів — через надання послуг зі зберігання, управління ліквідністю, біржової торгівлі, обробки платежів, інтеграції карткових рішень і навіть емісії власних стейблкоїнів.

Водночас автори звіту не ігнорують системні ризики. Вказано на численні випадки втрати прив'язки (de-pegging), особливо серед великих стейблкоїнів у 2023 році, що може призводити до втрати довіри, “банківських набігів” на емітентів, ліквідності, колапсу бірж і навіть системного ефекту доміно. Залишається актуальним питання резервної забезпеченості, прозорості аудиту та правового статусу таких активів. Невизначеність регулювання називається головним бар’єром до масштабної інтеграції стейблкоїнів у традиційну фінансову систему, однак ситуація змінюється: приклади MICA (ЄС), ініціатив у США (Stablecoin Act, GENIUS Bill) та Гонконгу дають підстави очікувати на нову хвилю прийняття.

[5] https://www.citigroup.com/global/insights/digital-dollars

Окрема частина документа присвячена потенціалу блокчейну у державному секторі. Тут блокчейн позиціонується не як альтернатива базам даних, а як довірчий протокол — інфраструктура для прозорості, цілісності й контрольованого доступу до чутливих даних. Наведено приклади використання у таких сферах:

- Публічні фінанси і бюджетні витрати: реальний час, простежуваність, аудит без змін у записах.
- Розподіл соціальних виплат і грантів: смарт-контракти, адресність допомоги, зменшення шахрайства.
- Реєстри та документообіг: забезпечення достовірності записів (наприклад, земельний кадастр, освіта, медичні дані).
- Гуманітарна допомога: UNHCR вже використовує Stellar для надання допомоги в Україні, Аргентині та інших регіонах.
- Токенізація активів: емісія державних облігацій (EIB, Lugano), цифрові боргові зобов'язання (Project Promissa).
- Цифрова ідентичність: приклади зі Швейцарії та Бразилії, використання Zero-Knowledge Proofs.

Висновки:

- **До 2030 року стейблкоїн-емітенти можуть стати одними з найбільших власників державних облігацій США,** що потенційно призведе до макроекономічних наслідків — зокрема, дефіциту "безпечних" активів на ринку та зниження можливостей банківської системи надавати кредити.
- **Блокчейн дозволяє модернізувати державні сервіси, знижуючи корупцію, підвищуючи прозорість та точність розподілу коштів** — наприклад, через смарт-контракти у грантах або токенізацію публічних активів.
- **Впровадження державної цифрової ідентифікації на основі блокчейну дає змогу надавати послуги навіть тим громадянам, які не мають офіційних документів**, при цьому гарантуючи конфіденційність і захист їхніх персональних даних.
- **Ключовим драйвером масового впровадження блокчейну є чітке, погоджене регулювання**, особливо щодо прозорості резервів, режиму ліцензування стейблкоїнів і правового визнання смарт-контрактів у державних системах.

Зазначено, що реальне розгортання блокчейну у державному секторі стикається з такими викликами: відсутність нормативної визначеності, обмежена масштабованість, інерція старих систем, невизначеність економічного ефекту, ризики зловживання (незаконні транзакції через DeFi — понад $51 млрд у 2024 році). Тим не менш, глобальні фінансові установи (як-от Світовий банк із FundsChain, BIS з Project Promissa) вже активно реалізують пілотні блокчейн-проєкти, що свідчить про перехід від експериментів до масштабного розгортання.

Загалом документ містить комплексну дорожню карту як для держав, так і фінансових установ щодо того, як впроваджувати блокчейн з урахуванням національного суверенітету, регуляторних вимог, стратегічної автономії та прагматичних ринкових потреб.

Санкції США викривають роль М'янми у кібершахрайстві та торгівлі людьми [6]

Міністерство фінансів США через своє Управління з контролю за іноземними активами (OFAC), 5 травня 2025 року, оголосило про санкції проти каренської національної армії (Karen National

[6] https://www.occrp.org/en/news/us-sanctions-myanmar-militia-tied-to-global-scam-empire-human-trafficking

Army, KNA) у М'янмі, її лідера Со Чіт Тху (Saw Chit Thu) та його синів, визнавши KNA транснаціональною злочинною організацією.

Санкції охоплюють не лише KNA, а й Со Чіт Тху, який є центральною фігурою в шахрайській економіці регіону, та його синів, які займають офіцерські посади в організації та мають частки в пов'язаних бізнесах. Ці заходи блокують усі активи підсанкційних осіб у США або під контролем американських громадян, а також забороняють американським особам проводити будь-які транзакції з ними. Іноземні особи, які сприяють порушенню санкцій, також ризикують потрапити під обмеження чи переслідування.

У центрі уваги – діяльність KNA у Шве Кокко, штат Карен, на кордоні з Таїландом, де організація створила кримінальний анклав, що є осередком численних злочинних синдикатів. KNA, раніше відома як Karen Border Guard Force, використовує свою співпрацю з військовим режимом М'янми для захисту та розширення незаконних операцій, навіть після зміни назви в березні 2024 року, що було спробою дистанціюватися від режиму. Організація отримує значні прибутки від оренди землі іншим злочинним групам, надання комунальних послуг, таких як електроенергія, для шахрайських центрів, забезпечення збройної охорони в цих комплексах і сприяння торгівлі людьми та контрабанді. Зокрема, KNA охороняє сумнозвісний комплекс KK Park, де жертв змушують до шахрайства, а також пов'язана з Yatai New City – проєктом, який позиціонується як мегапроект вартістю 15 мільярдів доларів, але насправді є прикриттям для шахрайських центрів і нелегальних казино, очолюваним Ше Чжицзяном, що перебуває у в'язниці в Таїланді.

Висновки:

- **Посилення тиску на Таїланд:** США мають співпрацювати з тайською владою для прискорення арешту Со Чіт Тху та його синів, використовуючи санкції як важіль.
- **Блокування фінансів:** Криптовалютні платформи повинні посилити моніторинг транзакцій із Південно-Східної Азії для припинення відмивання доходів KNA.
- **Порятунок жертв:** Міжнародні організації мають створити програми визволення та реабілітації жертв торгівлі людьми з шахрайських центрів, як KK Park.
- **Міжнародна співпраця:** США, ЄС і Сполучене Королівство повинні об'єднати зусилля для обміну розвідданими та ізоляції злочинних груп, подібних до KNA.

Кібершахрайство базується на складних схемах, відомих як "pig butchering", які експлуатують вразливості жертв, таких як розлучення, втрата близьких чи фінансові труднощі. Шахраї, часто самі будучи жертвами торгівлі людьми, працюють у тюремних умовах у call-центрах або переобладнаних готелях і казино, де їх змушують під загрозою насильства встановлювати довірливі стосунки з жертвами та обманом залучати їх до інвестування в фальшиві криптовалютні платформи. Жертви бачать фіктивні прибутки, але втрачають усі кошти, коли шахраї зникають.

Збитки американців від таких схем, за даними Міністерства фінансів США, склали приблизно 2 мільярди доларів у 2022 році та 3,5 мільярда доларів у 2023 році, тоді як OCCRP оцінює загальні втрати з 2022 року в 5,5 мільярда доларів, що свідчить про зростання масштабів проблеми. Ці угрупування є частиною ширшої транснаціональної злочинної мережі в Південно-Східній Азії, яка проводить відмивання коштів через такі установи,

як камбоджійська Huione Group, визнана FinCEN у травні 2025 року ключовим вузлом для відмивання доходів від кіберзлочинів.

Торгівля людьми є основою цих шахрайських операцій. Жертв, переважно з Азії, але також з інших регіонів, запрошують до М'янми під виглядом легальних пропозицій роботи, після чого їх перевозять через кордон із Таїланду та утримують у жорстоких умовах. Ці люди змушені працювати в шахрайських центрах, де зазнають фізичного насильства та приниження.

Документи підкреслюють роль KNA у сприянні цій торгівлі, зокрема через надання логістичної підтримки та безпеки для таких комплексів. Со Чіт Тху, якого також називають Сан М'їнт, разом зі своєю сім'єю контролює щонайменше дев'ять компаній у штаті Карен, які фінансують його розкішний спосіб життя за рахунок злочинних доходів.

Міжнародний контекст також є важливим аспектом. Со Чіт Тху вже потрапив під санкції Сполученого Королівства у 2023 році та Європейського Союзу у 2024 році за причетність до шахрайських центрів і співпрацю з військовим режимом М'янми. Тайська поліція розслідує його діяльність, і в лютому 2025 року група активістів Justice For Myanmar повідомила про запит щодо ордеру на його арешт. Санкції США можуть посилити тиск на тайську владу для активізації дій проти Со Чіт Тху та його синів.

Розкриття Люксембурзького JBS: Глобальна схема уникнення податків [7]

Звіт, підготовлений організацією SOMO, є ґрунтовним дослідженням, що розкриває складні схеми уникнення оподаткування, які застосовує бразильська компанія JBS SA, найбільший у світі виробник м'яса, через використання Люксембургу як центрального хабу для податкової оптимізації. Документ охоплює широкий спектр тем, включаючи корпоративну структуру JBS, її глобальний вплив, звинувачення у неетичних практиках, а також детальний аналіз фінансових механізмів, які дозволили компанії уникнути сплати податків на суму від 221 до 442 мільйонів доларів США у період з 2019 по 2022 рік. Окрім цього, звіт висвітлює екологічні, соціальні та етичні проблеми, пов'язані з діяльністю JBS, підкреслюючи її роль у перешкоджанні переходу до сталого харчування та потенційні ризики для інвесторів у контексті схвалення лістингу компанії на Нью-Йоркській фондовій біржі (NYSE) у 2025 році.

JBS SA, з річним доходом у 73 мільярди доларів США, є не лише лідером м'ясної промисловості, але й компанією з розгалуженою мережею, що включає 375 дочірніх компаній у 37 країнах, 240 тисяч працівників і потужності для щоденного забою та переробки 75 000 корів, 14 мільйонів курей і 115 000 свиней. Проте репутація компанії затьмарена численними звинуваченнями, зокрема у причетності до незаконної вирубки лісів, захоплення земель корінних народів, значних викидів парникових газів, сучасного рабства, дитячої праці, жорстокого поводження з тваринами, корупції та небезпечних умов праці на м'ясопереробних підприємствах. Ці аспекти роблять JBS об'єктом пильної уваги, особливо в контексті її прагнення розширити вплив через лістинг на NYSE, що може забезпечити додаткові кошти для зростання, але також посилює потенційні негативні наслідки для довкілля та суспільства.

Центральною темою звіту є аналіз того, як JBS використовує Люксембург для уникнення податків, що має значний вплив на податкові бази країн, де компанія веде основну діяльність,

[7] https://www.somo.nl/jbss-global-tax-avoidance-hub-luxembourg/

зокрема США, які генерують 49% її глобального доходу. У 2022 році JBS мала 17 дочірніх компаній у Люксембурзі, які контролювали активи на суму 58 мільярдів доларів США в США, Канаді, Австралії та Європі. Ці компанії, більшість із яких є так званими "поштовими скриньками" без реальної економічної активності чи працівників (лише одна мала п'ять співробітників), відіграють ключову роль у двох основних схемах уникнення податків: зниження податку на дивіденди та корпоративного податку. За період 2019–2022 років 23 люксембурзькі дочірні компанії JBS задекларували прибуток у 3 мільярди доларів США, але сплатили лише 0,5 мільйона доларів корпоративного податку, що відповідає ефективній податковій ставці 0,02%. Деякі компанії навіть отримали податкові кредити, а загальна сума інших податків склала 45 мільйонів доларів США.

Перший механізм уникнення податків полягає у зниженні податку на дивіденди через використання сприятливих податкових угод Люксембургу з іншими країнами, відоме як "treaty shopping". Дивідендні потоки з глобальних операцій JBS спрямовуються через люксембурзькі компанії, що дозволяє зменшити або повністю уникнути податку на дивіденди. Наприклад, у США податок на дивіденди знижується з 30% до 5% завдяки угоді з Люксембургом. За оцінками, це дозволило JBS уникнути сплати 148 мільйонів доларів США податку на дивіденди в США за чотири роки, припускаючи, що дивідендні виплати пропорційні частці доходу компанії в цій країні.

Другий механізм передбачає зниження корпоративного податку через міжкорпоративні позики. Люксембурзькі компанії отримують позики з низькими відсотковими ставками (0,4–0,65%) від дочірніх компаній у юрисдикціях з низькими податками, таких як Мальта та штат Делавер (США), а потім надають позики іншим дочірнім компаніям у країнах із вищими податками, таких як Бразилія, США, Сполучене Королівство, Австралія та Мексика, за вищими ставками (в середньому 5%). У 2022 році люксембурзькі компанії отримали 333 мільйони доларів США відсоткового доходу, що дозволило знизити оподатковуваний прибуток у країнах із високими податками, заощадивши приблизно 73 мільйони доларів США корпоративного податку в 2022 році та 293 мільйони доларів США за 2019–2022 роки. Використання "умовних відсотків" через невідповідність податкових правил між Мальтою та Люксембургом додатково сприяло зниженню податкового навантаження.

Звіт також звертає увагу на зростаючий міжнародний тиск на боротьбу з ухиленням від сплати податків, зокрема з боку Європейської Комісії, яка розслідує випадки незаконної державної допомоги в Люксембурзі, подібні до справи JBS. Такі розслідування можуть призвести до значних штрафів і вимог повернення податків, як у випадку з

Висновки:

- **Необхідність розслідування схем JBS:** Європейська Комісія та податкові органи Люксембургу повинні терміново розслідувати схеми JBS, які дозволили уникнути податків на 221–442 мільйони доларів США у 2019–2022 роках, зокрема через "умовні відсотки" та міжкорпоративні позики.
- **Запровадження нових податкових правил:** Люксембург і Нідерланди мають ввести безумовні податки на дивіденди, відсотки та роялті, щоб унеможливити використання поштових компаній для зниження податкового навантаження.
- **Блокування реструктуризації JBS:** Акціонери JBS повинні відхилити пропозицію щодо створення нової холдингової компанії в Нідерландах через ризики, пов'язані з агресивним податковим плануванням та екологічними порушеннями.
- **Підвищення прозорості:** JBS зобов'язана розкрити у звітах для SEC повну інформацію про люксембурзькі податкові структури та їхні ризики, щоб захистити інвесторів від потенційних фінансових втрат.

Apple в Ірландії, де було стягнуто 13 мільярдів євро. Крім того, ліквідація п'яти люксембурзьких дочірніх компаній JBS у 2023 році може свідчити про реструктуризацію для зменшення регуляторного тиску, хоча звіт не аналізує вплив цих змін через брак даних за 2023 рік. JBS стверджує, що дотримується всіх податкових законів і співпрацює з податковими органами, але не надала конкретних спростувань звинувачень SOMO, назвавши звіт неточним.

На тлі схвалення лістингу JBS на NYSE 23 квітня 2025 року звіт підкреслює значні ризики для інвесторів через непрозорість компанії щодо її люксембурзьких структур і потенційні фінансові та репутаційні втрати. JBS не розкриває повною мірою ці ризики у своїх звітах для SEC, що становить загрозу для акціонерів. Звіт закликає Люксембург і Нідерланди запровадити безумовні податки на дивіденди, відсотки та роялті, а також усунути невідповідності в податкових режимах. Європейську Комісію та податкові органи Люксембургу закликають розслідувати законність схем JBS, а інвесторів і акціонерів – голосувати проти запропонованої реструктуризації, яка передбачає створення нової холдингової компанії в Нідерландах, через екологічні, соціальні та податкові ризики, пов'язані з діяльністю компанії.

Контрабанда Закарпаття: тіньова держава на західному кордоні України [8]

Аналітичний звіт від Global Initiative, є однією з найглибших спроб вивчення багаторівневої системи нелегальної торгівлі на західному прикордонні України — у Закарпатській області. У фокусі звіту – не лише структура й логістика контрабандних потоків, а й глибокі соціальні, політичні, історичні та економічні чинники, що сформували цю унікальну паралельну економіку на межі з Європейським Союзом. Автори дослідження наголошують, що контрабанда в Закарпатті є не просто економічною активністю, а самодостатньою системою влади, яка формує місцеву політику, визначає призначення у державних інституціях, контролює вибори, безпеку, медіа і навіть громадське сприйняття закону.

Головний акцент у дослідженні зроблено на тому, що Закарпаття, відокремлене від решти України Карпатами й інтегроване історично та демографічно у простір Центральної Європи, стало одним із найбільш вигідних транскордонних хабів для нелегального експорту сигарет, наркотиків, деревини, товарів широкого вжитку, а після 2022 року — й військовозобов'язаних чоловіків.

Впродовж десятиліть у регіоні сформувалась стабільна, жорстко ієрархізована кримінально-політична система, яка функціонує за принципом "телефонного права": рішення ухвалюються через неформальні зв'язки між митниками, СБУ, поліцією, політиками, суддями та кримінальними авторитетами. Одним із яскравих прикладів цієї взаємодії є "тріумвірат Мукачево" – політико-бізнесова коаліція, яка включає родину Балог, депутата Василя Петьовку та впливового фігуранта контрабандних розслідувань Михайла Ланя (відкрито названого у звіті кримінальним арбітром регіону). Всі вони роками утримували монополію на адміністративні й політичні рішення у регіоні та використовували цю владу для легітимізації і прикриття тіньових потоків.

[8] https://globalinitiative.net/analysis/illicit-trade-between-ukraines-transcarpathia-and-the-eu/

Повномасштабне вторгнення Росії в Україну 2022 року змусило переглянути логістику і пріоритети нелегальної торгівлі. Відбулося скорочення традиційної тютюнової контрабанди, натомість бурхливо зросли прибутки від "мобілізаційного трафіку" — нелегального переправлення чоловіків призовного віку через кордон.

Водночас активізувалися й нові напрями: створення кол-центрів шахрайського типу, виробництво синтетичних наркотиків та спроби локальних "еліт" повернутися до масштабної вирубки лісу під виглядом санітарних рубок чи будівництва туристичних об'єктів. Усе це стало можливо завдяки багаторічному поєднанню адміністративної вседозволеності, корумпованості митниці, браку прозорості у призначеннях та відсутності притягнення до відповідальності високопосадовців.

Висновки:

- **Закарпатська контрабанда є глибоко інтегрованою в регіональну політичну та економічну систему.** Вона є не маргінальним явищем, а сформованою паралельною структурою, яка охоплює місцеві еліти, правоохоронців, митників і навіть легальний бізнес, створюючи сталу мережу впливу і зиску.
- **Найбільші втрати бюджету України спричиняє сіра контрабанда, що існує завдяки державному покровительству.** Маніпуляції з митною вартістю, фіктивні документи та навмисне ігнорування перевірок здійснюються з відома і за участі посадових осіб, що робить такі схеми майже недоторканними.
- **Повномасштабна війна призвела до трансформації нелегального ринку: зростання контрабанди чоловіків, наркотиків та шахрайських схем.** У той час як тютюнова контрабанда дещо зменшилась, її місце зайняли ризиковіші, але більш прибуткові схеми, адаптовані до умов воєнного часу та мобілізації.
- **Без зміни законодавчої бази, реальної політичної волі та розвитку альтернатив для місцевого населення подолати контрабанду неможливо.** Поки кримінальна діяльність залишатиметься безкарною, а регіон не матиме конкурентних легальних джерел доходу, контрабанда залишатиметься основою економіки Закарпаття.

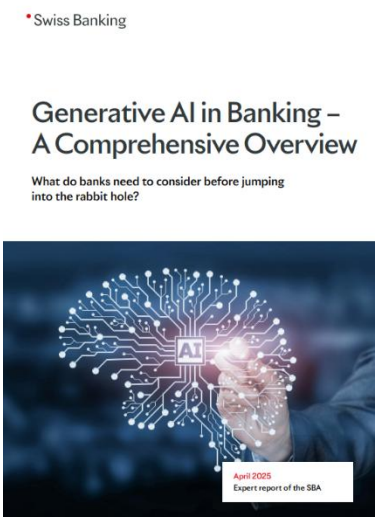
Звіт також містить критичну оцінку реформ, здійснених українською владою у 2021–2024 роках. Попри оголошення війни контрабанді, введення санкцій проти так званих "топ-10 контрабандистів" і кадрові чистки у митниці, вплив цих заходів виявився тимчасовим. У 2024 році багато санкцій було без пояснень скасовано, а нові механізми рекрутування корумпованих кадрів, на кшталт "продажу митниць", лише поглибили системну корупцію. Водночас за міжнародної підтримки (МВФ, Світовий банк, уряд США) у вересні 2024 року було ухвалено новий закон про реформу митниці, який включає міжнародний нагляд за призначеннями, підвищення зарплат і спробу інституційної декриміналізації митної служби. Втім, як зазначено в звіті, успіх реформ залежатиме не від закону, а від політичної волі Києва зламати глибоко вкорінену систему "інституційної змови".

Найгострішу критику отримало положення про "порогову" відповідальність: за новим законом кримінальним злочином вважається лише контрабанда товарів на суму понад 7,5 млн грн або підакцизної продукції на понад 1,1 млн грн. Це створює "коридор безкарності", в межах якого дрібні партії можуть транспортуватися масово без ризику. Звіт також застерігає, що без гармонізації Кримінального та Митного кодексів, без перетворення контрабанди на злочин незалежно від обсягу, усі інші антикорупційні ініціативи матимуть обмежений ефект.

Зрештою, звіт підкреслює: викорінити контрабанду без створення альтернатив економічного виживання у прикордонних громадах неможливо. За умов, коли контрабандний заробіток у рази перевищує легальні доходи, а держава не пропонує працюючих механізмів підтримки

малого бізнесу, логістики чи інфраструктури, стимул для правопорядку залишається мінімальним. Без одночасного демонтажу політико-кримінальних союзів, створення дієвих антикорупційних запобіжників та трансформації регіону у точку законного економічного зростання, Закарпаття залишатиметься серцем нелегальної торгівлі України з ЄС.

Генеративний AI у банківській сфері: стратегія впровадження, ризики та можливості для фінансових установ[9]



Аналітичний звіт Швейцарської банківської асоціації (SBA) є методологічним дороговказом для банківського сектору щодо інтеграції генеративного штучного інтелекту (GenAI) у банківські процеси, структури та стратегії. Документ охоплює ключові переваги, технологічні можливості, типові виклики, приклади застосування, а також регуляторні та етичні рамки, у межах яких має здійснюватися впровадження GenAI. У вступі звіту визначено унікальні характеристики GenAI як підкласу глибокого навчання, що відрізняється здатністю створювати новий контент – тексти, зображення, аудіо чи відео – на основі патернів, вивчених з великих масивів даних. У звіті надано порівняльний аналіз між генеративним та передбачуваним AI, із наголосом на творчі можливості, властиві першому, та його обмеження: ризик «галюцинацій», упередженість, кіберзагрози, ризики інтелектуальної власності та обмежена верифікація джерел. Зокрема, відзначено, що в контексті фінансового сектору GenAI здатен радикально змінити характер операцій, зокрема автоматизуючи повторювані завдання (підготовка звітів, транскрибування зустрічей), підвищуючи точність комплаєнс-діяльності, персоналізуючи обслуговування клієнтів, розширюючи можливості щодо аналітики та інноваційних фінансових продуктів. Конкретні кейси з банків Raiffeisen, Julius Bär, Pictet Group та інфраструктурного оператора SIX ілюструють реальне застосування GenAI у підвищенні продуктивності персоналу, забезпеченні пошуку в корпоративних базах знань, вдосконаленні внутрішніх перекладів або покращенні клієнтського досвіду. Центральне місце у звіті посідає запропонована чотирифазова модель впровадження GenAI у банківській установі, що передбачає фази дослідження, аналізу та розробки дорожньої карти, базової реалізації та масштабування з безперервним удосконаленням. У кожній з фаз розглянуто стратегічні, організаційні та технологічні завдання. Особливу увагу приділено ролі культури інновацій у банку, необхідності постійного навчання персоналу, формуванню governance framework, оцінці впливу на права суб'єктів персональних даних (зокрема через DPIA), а також вимогам до технічної інфраструктури — хмарної чи локальної. Значну частину звіту присвячено юридичним аспектам впровадження GenAI, зокрема дотриманню Федерального закону Швейцарії про захист даних (FADP), норм банківської таємниці (ст. 47 BA), законодавства про недобросовісну конкуренцію (UCA), а також рекомендаціям FINMA щодо управління ризиками, відповідальності, прозорості та недискримінації. Документ містить аналіз відповідності до міжнародних актів, зокрема європейського AI Act, наголошуючи на його екстериторіальності та важливості для швейцарських банків, які працюють у ЄС. Також розкрито технічні стратегії адаптації моделей LLM до внутрішніх потреб банків — через тонке налаштування моделей, збагачення генерації через пошук у крпоративних база знань (RAG) або предметну адаптацію моделей — що дозволяє зменшити ризики помилок, посилити

9 https://www.swissbanking.ch/_Resources/Persistent/2/0/3/b/203b937e175f25819ea271c883a095fe1dfa1ee0/SBA_Generative-AI-in-Banking_EN.pdf

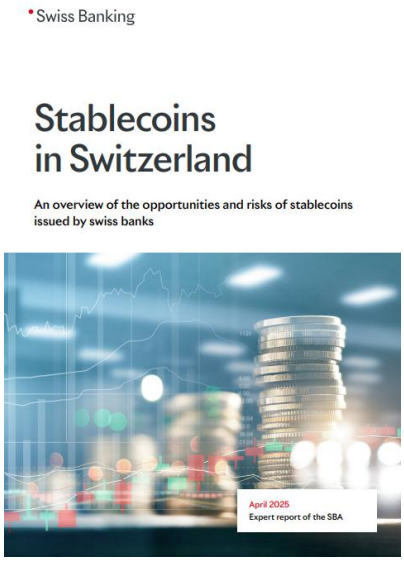
відповідність регуляторним вимогам і підвищити релевантність контенту. В останньому розділі автори описують перспективу переходу до Agentic AI — незалежних агентів, здатних самостійно керувати складними робочими процесами на основі цілей, контексту і змін навколишнього середовища, з урахуванням методів послідовної логіки запитів, паралельного виконання окремих етапів і контролю за якістю в реальному часі. Увесь документ побудовано як гнучкий і практикоорієнтований посібник, який, з одного боку, демонструє значний інноваційний потенціал GenAI для банківського сектора, а з іншого — чітко окреслює ризики, регуляторні вимоги та етичні межі, дотримання яких є критичним для безпечної та ефективної інтеграції нових технологій у високоризиковане середовище фінансових інституцій.

Висновки:

- **Інтеграція GenAI повинна бути стратегічно вмотивованою і поетапною.** Банкам рекомендується починати з пілотів у непрофільних зонах і розбудовувати внутрішню експертизу, з поступовим масштабуванням на основі досвіду та моніторингу ефективності.
- **Формування культури інновацій є критичним фактором успіху.** Забезпечення навчання персоналу, залучення «AI-чемпіонів», розробка політик і процедур щодо етичного використання GenAI — ключ до прийняття нових технологій усередині установ.
- **Дотримання вимог безпеки та нормативно-правового регулювання має бути вбудовано у процес розробки GenAI-застосунків.** Особливу увагу слід приділити захисту персональних даних, управлінню ризиками (упередженість, ризик «галюцинації», зловмисні запити), забезпеченню прозорості і можливості аудиту моделей.
- **Швейцарські банки повинні враховувати міжнародні регуляторні вимоги, зокрема EU AI Act.** Особливо це актуально для банків, які надають послуги на території ЄС або обробляють дані громадян ЄС, адже відповідність нормам GDPR і AI Act є обов'язковою.

Швейцарський франк у цифрову епоху: виклики та можливості впровадження банківських стейблкоїнів[10]

Документ, підготовлений Швейцарською банківською асоціацією (SBA), є ґрунтовним експертним аналізом перспектив, викликів і регуляторних передумов впровадження стейблкоїнів, емітованих швейцарськими банками. У ньому висвітлено потенціал таких цифрових платіжних інструментів для цифрової трансформації швейцарської економіки, а також ризики для монетарної політики, банківської системи та фінансового ринку. Автори позиціонують стейблкоїни як критичний інфраструктурний елемент нової епохи цифрових фінансів, здатний забезпечити безпечні, програмовані й дешеві платежі в реальному часі, особливо в умовах розвитку Web3, DeFi та цифрових активів. Оскільки Швейцарія наразі не має публічного стейблкоїна, прив'язаного до швейцарського франка (CHF), вона ризикує посилити свою стратегічну залежність від доларового сегменту цифрових валют, що потенційно може



10 https://www.swissbanking.ch/_Resources/Persistent/0/5/0/1/0501708bb8d749954729879c52024ab0cb65d2d7/SBA%20Expert%20report%20stablecoins.pdf

ускладнити реалізацію грошово-кредитної політики та знизити конкурентоспроможність на глобальному фінансовому ринку.

У документі надається систематизований огляд форм цифрових грошей, що включає як державні (готівка, депозитні гроші центрального банку, CBDC), так і приватні (депозитні токени, стейблкоїни, криптовалюти), з особливою увагою до їх правових статусів, платоспроможності, функціональної відповідності потребам користувачів і ролі у двошаровій банківській системі. Автори зазначають, що на відміну від криптовалют, які характеризуються високою волатильністю і обмеженим практичним застосуванням як засобу платежу, стейблкоїни — це цінні платіжні інструменти, що можуть забезпечити стабільність вартості завдяки механізмам забезпечення. У звіті класифіковано чотири основні моделі стейблкоїнів: забезпечені грошима (fiat-backed), товарами (commodity-backed), криптоактивами (crypto-backed) та алгоритмічні. Особливої уваги заслуговує концепція так званої трилеми стейблкоїна — неможливість одночасно досягти повної децентралізації, стабільності ціни й ефективності використання капіталу. На думку авторів, для широкого використання серед населення і бізнесу пріоритетними мають бути стабільність ціни та забезпечення довіри, що означає потребу у суворій регуляції, прозорому управлінні резервами та гарантіях обміну за номіналом.

Висновки:

- **Необхідність CHF-стейблкоїна:** Відсутність швейцарського франкового стейблкоїна може призвести до стратегічної залежності від USD-номінованих цифрових активів.
  Рекомендація: пришвидшити роботу над публічним CHF-стейблкоїном з повним або частковим забезпеченням через банки.
- **Пріоритет – довіра та стабільність:** Для широкого прийняття нових цифрових форм грошей критично важливо забезпечити їхню конвертованість «без запитань» та захист у разі банкрутства емітента.
  Рекомендація: розробити законодавчі основи гарантій для користувачів стейблкоїнів.
- **Баланс ризиків для фінансової системи:** Стейблкоїни з повним забезпеченням від SNB підвищують системну стабільність, але несуть ризик дезінтермедіації банків.
  Рекомендація: впровадити гнучкі обмеження обсягів випуску та правила доступу до забезпечення, зокрема у кризових умовах.
- **Формування прозорого регуляторного середовища:** Швейцарія має всі інституційні можливості для лідерства, але надмірні регуляції, як-от з боку FINMA щодо ПВК, можуть стримувати інновації.
  Рекомендація: забезпечити структурно нейтральний підхід до регулювання незалежно від типу емітента, запровадити ліцензії нового типу для провайдерів платіжних послуг.

У звіті глибоко проаналізовано дві перспективні моделі швейцарського стейблкоїна: повністю забезпеченого коштами центрального банку (SNB sight deposits) і комбіновано забезпеченого ліквідними держоблігаціями (HQLA), депозитами в банках і коштами в SNB. Повністю забезпечений стейблкоїн забезпечує максимальну стабільність і зменшує системні ризики, проте водночас він несе ризики дезінтермедіації — витоку депозитів з банківської системи, що потенційно може порушити трансмісію монетарної політики. Комбінована модель, хоча й містить певний ринковий ризик, є привабливою завдяки вищій прибутковості для банків-емітентів і меншому впливу на функціонування кредитної системи.

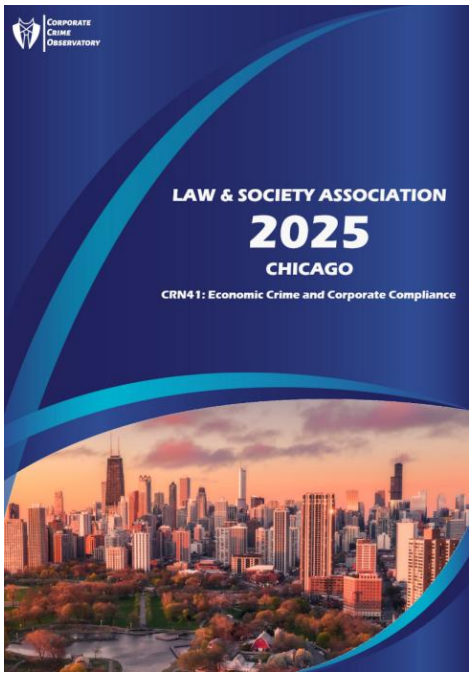
Автори окреслюють п’ять ключових сфер застосування стейблкоїнів у реальній економіці: P2P платежі, розрахунки в торгівлі цифровими активами, інтеграція в DeFi-протоколи, внутрішньогрупове управління ліквідністю у міжнародних компаніях, а також збереження вартості у періоди волатильності ринків криптоактивів. Окремо наголошується на потенційній стратегічній ролі CHF-стейблкоїна як інструменту, що здатен зміцнити позиції швейцарського франка як

резервної валюти, підтримати інноваційний розвиток та сприяти притоку капіталу до Швейцарії. Також описано міжнародний контекст, де домінують доларові стейблкоїни (USDT, USDC), які забезпечують понад 90% обсягів торгівлі. У зв'язку з цим Швейцарія повинна розглядати створення стейблкоїна не лише як внутрішній фінансовий інструмент, а як компонент глобальної валютної конкуренції.

Розділ ризиків у звіті подає критичний аналіз загроз, пов'язаних із випуском стейблкоїнів. Серед ключових — ризик втрати паритету через недосконале забезпечення або недовіру до емітента, дезінтермедіація банків, вплив на стабільність ринку капіталів через зміну попиту на HQLA, обмеження трансмісійної здатності монетарної політики, ризики монополізації інфраструктури платежів та концентрації даних у небанківських учасників (BigTech), а також значні виклики з боку ПВК/ФТ. Особливе занепокоєння викликає вимога FINMA щодо ідентифікації усіх користувачів стейблкоїнів, включаючи випадки, коли відсутні прямі договірні відносини з емітентом — така практика критикується як надмірна та невідповідна міжнародним стандартам.

У висновку підкреслюється, що стейблкоїни можуть зміцнити позиції Швейцарії як світового лідера у фінансових інноваціях лише за умови забезпечення правової визначеності, прозорості, довіри користувачів і чіткої взаємодії з грошово-кредитною системою. Важливим є створення нейтрального і конкурентного середовища, де банки матимуть не менше прав, ніж нові небанківські провайдери. SBA закликає до поступового, але цілеспрямованого формування законодавчого середовища, що забезпечить інклюзивний розвиток різних форм цифрових грошей із максимальним ефектом для добробуту країни.

Між правом, комплаєнсом і правдою: сучасні виклики економічної злочинності та корпоративної відповідальності у глобальному контексті[11]



Документ є розгорнутою програмою сесій Мережі спільних досліджень 41 (Collaborative Research Network 41 — CRN41), що функціонує в рамках щорічної конференції Law & Society Association. Основна увага CRN41 зосереджена на вивченні економічної злочинності, корпоративної відповідальності та нормативного регулювання у взаємозв'язку з правом, політикою, етикою та глобальним управлінням.

Документ містить деталізовану інформацію про низку сесій, у яких беруть участь провідні дослідники, юристи, соціологи, представники фінансового сектору та медіа, що досліджують як традиційні форми злочинності (відмивання коштів, корупція, ухилення від податків, фінансування тероризму, шахрайство), так і пов'язані із ними практики – корпоративні зловживання, екологічні злочини, токсичний лобізм, використання складних корпоративних структур для уникнення відповідальності, а також роль викривання та технологій у виявленні правопорушень.

Велику частину документу займає секція «Critical Perspectives on Anti-Corruption(ism)», де аналізується критичний погляд на глобальний антикорупційний рух. Дослідники стверджують, що сучасна протидія корупції часто використовується не лише для боротьби з реальними

[11] https://www.corporatecrime.co.uk/post/lsa-2025-chicago-crn41

злочинами, а як форма моральної регуляції, що слугує інституційному укріпленню капіталізму та легітимації міжнародних фінансових інституцій. Показовим є дослідження практик МВФ, Світового банку та ОЕСР, що просувають антикорупційні ініціативи, часто не з метою системного впливу на джерела корупції, а для нав'язування нормативних моделей, вигідних транснаціональним корпораціям.

У наступному блоці розглядається переосмислення корпоративної відповідальності в умовах глобалізації. Піднімається питання транснаціонального законодавства про сталий розвиток (Transnational Due Diligence Law), яке прагне охопити складну юрисдикційну реальність глобальних ланцюгів постачання та створити інструменти юридичної відповідальності компаній за порушення прав людини чи екологічні злочини. Паралельно розглядається феномен «нормалізації» прав — як у випадку механізму FPIC (Free, Prior and Informed Consent) у Колумбії, коли початково трансформативні права з часом інституціоналізуються і втрачають свій захисний потенціал. Особлива увага приділена ESG-інтеграції у корпоративне право, що все ще формально зосереджене на захисті акціонерів, хоча під тиском громадськості, судових позовів та нормативних зобов'язань починає зважати на екологічні та соціальні ризики. У сесіях, присвячених журналістиці та викривачам, дослідники аналізують роль розслідувальної журналістики як ключового інструменту викриття зловживань у разі неефективності або залежності офіційних інституцій. Наводиться кейс Carole Cadwalladr у Сполученому Королівстві як приклад застосування SLAPP-позовів проти журналістів, а також приклади розслідувань, що спонукали прокуратуру в Італії до відкриття гучних справ. Увага також приділяється криміналізації журналістики у Туреччині, використанню мови та символізму для уникнення переслідувань, а також рішенню ЄСПЛ та Суду ЄС як джерел формування стандартів захисту викривачів.

Висновки:

- **Інституційна антикорупція може бути політичним інструментом** — аналіз руху антикорупціонізму вказує на те, що він часто виконує функції морального контролю на користь глобальних економічних інтересів, а не протидії корупції як такої. Для України актуальним є аудит нормативних рамок на предмет їх «моралізуючої» або «репресивної» функції.
- **Транснаціональне право сталого розвитку (TDDL) формує нові зобов'язання** — корпоративні суб'єкти можуть нести відповідальність за дії у глобальних ланцюгах постачання, навіть у юрисдикціях із послабленим регулюванням. Україні варто врахувати ці механізми при гармонізації законодавства з директивами ЄС щодо сталого розвитку.
- **Викривачі та розслідувальна журналістика потребують посиленого правового захисту** — як показують кейси Сполученого Королівства, Італії та Туреччини, загроза SLAPP-позовів, кримінального переслідування та стеження чинить ефект стримування на свободу слова. Необхідно посилити законодавство про захист викривачів та обмежити зловживання цивільним і кримінальним переслідуванням у справах публічного інтересу.
- **Емпіричне дослідження діяльності підрозділів фінансової розвідки у США та країнах Латинської Америки** демонструє значну варіативність у підходах до санкціонування за недотримання ПВК-регулювання. Зокрема, порівнюються повноваження ПФР щодо накладення штрафів, прозорість оприлюднення рішень та вибірковість у ставленні до фінансового і нефінансового сектору. Ці дані підкреслюють потребу в уніфікації підходів до санкційної практики, зокрема щодо пропорційності та публічної звітності.

У сесії «Mandatory Regulation vs. Self-regulation» дослідники порівнюють різні моделі комплаєнсу — зокрема, як саморегуляція компаній без зовнішнього нагляду часто не забезпечує ефективної відповідальності, і навпаки — як наявність незалежного регулятора, як у випадку Банку Італії у контексті ПВК, забезпечує більш результативний нагляд. Розглядаються також питання регуляторного захоплення, коли державні структури втрачають незалежність через тиск бізнесу, приклади трансформації органів екологічного контролю, вплив стратегії легалізації (через ліцензування) на поведінку компаній. Дослідження ПФР як органів, що не тільки аналізують підозрілі транзакції, а й накладають санкції, відкриває перспективу вивчення практичної ефективності ПВК-регулювання у США, Аргентині, Бразилії та Чилі. Аналізується типова реакція суб'єктів ринку на вимоги ПВК, ступінь оприлюднення санкцій, диференціація підходів до фінансового і нефінансового сектору. У документі також висвітлюється роль штучного інтелекту у виявленні організаційного зловживання, а також інституціональна природа whistleblowing як елементу збереження демократичної легітимності.

Завершується програма круглим столом, присвяченим ролі викривачів у забезпеченні прозорості та справедливості, де беруть участь представники антикорупційних організацій, правники, колишні співробітники ФБР, академіки й адвокати, що працюють з викривачами.

Таким чином, документ є унікальним і глибоко міждисциплінарним джерелом для аналізу сучасних підходів до боротьби з економічною злочинністю, зокрема в контексті ПВК/ФТ, прав людини, корпоративного управління, регуляторної політики та захисту інформаторів. Він особливо актуальний для реформаторів та науковців, які працюють на перетині права, фінансів, етики й публічної політики.

ВНУП

Роль ВНУП у системі ПВК/ФТ: міжнародні стандарти, ризики та інструменти контролю[12]

Стаття розкриває ключову роль визначених нефінансових установ і професій (ВНУП) у глобальній архітектурі протидії відмиванню коштів (ПВК) і фінансуванню тероризму (ФТ). Автори підкреслюють, що хоча ВНУП формально не є учасниками фінансової системи, вони об'єктивно виступають важливими ланками в ланцюгах трансформації і легалізації злочинних активів. Зокрема, зазначається, що завдяки високій вартості активів, із якими вони працюють (наприклад, нерухомість, дорогоцінні метали, юридичні послуги щодо створення компаній або трастів), а також через можливість встановлення номінальних або анонімізованих правових структур, ВНУП часто використовуються зловмисниками для обхідного маневру регульованої фінансової системи.

У статті докладно пояснюється, що до переліку ВНУП, згідно з визначеннями FATF, відносяться казино, агенти з операцій з нерухомістю, постачальники бухгалтерських послуг, юристи та нотаріуси, які беруть участь у транзакціях від імені своїх клієнтів, торговці коштовностями та дорогоцінними металами, а також трастові компанії. Кожна з цих категорій є потенційною точкою входу для злочинного капіталу. Зокрема, адвокатські послуги часто залучаються при створенні складних корпоративних структур, а агенти з нерухомості можуть сприяти інтеграції коштів через купівлю активів на вторинному ринку.

[12] https://amlwatcher.com/blog/how-designated-non-financial-businesses-and-professions-dnfbps-contribute-to-aml-compliance/

У фокусі статті — впровадження міжнародних стандартів FATF щодо ВНУП. Автори висвітлюють, що Рекомендації FATF прямо зобов'язують ВНУП виконувати комплекс заходів з належної перевірки клієнтів (CDD), ідентифікації кінцевих бенефіціарних власників, застосування посиленої перевірки (EDD) для клієнтів із підвищеним ризиком, ведення обліку транзакцій, а також негайного повідомлення про підозрілі фінансові операції до національного підрозділу фінансової розвідки. Наголошується, що Рекомендації 12, 16, 17, 24 і 25 є основоположними у цьому контексті. Наприклад, Рекомендація 24 вимагає, щоб ВНУП перебували під наглядом або регулюванням з боку державних органів чи ефективних саморегулівних організацій, що особливо актуально для таких професій, як адвокати та аудитори.

Окрема увага в матеріалі приділяється обов'язкам ВНУП щодо впровадження внутрішніх політик та процедур із ПВК/ФТ, створення систем внутрішнього контролю, призначення відповідального за дотримання вимог комплаєнсу, а також навчання персоналу. Автори застерігають, що формальний підхід до дотримання вимог створює регуляторні прогалини, які можуть бути використані злочинцями. Тому критично важливою є інтеграція ризик-орієнтованого підходу, що вимагає від ВНУП не просто ідентифікувати клієнта, а й розуміти сутність його бізнесу, географічну зону ризику, зв'язки з політично значущими особами (PEP) та потенційними санкційними суб'єктами.

У практичному аспекті стаття містить докладний огляд інструментів, які можуть бути застосовані ВНУП для підтримки своїх зобов'язань. Зокрема, йдеться про використання систем автоматизованого скринінгу клієнтів за міжнародними санкційними списками, базами даних PEP, а також про впровадження транзакційного моніторингу з використанням штучного інтелекту або аналітики поведінкових моделей. Автори рекламують платформу AML Watcher як інноваційне рішення, яке дозволяє ВНУП не лише відповідати регуляторним вимогам, а й ефективно ідентифікувати нові загрози завдяки машинному навчанню, обробці великих даних і постійному моніторингу. Також наголошується на потребі інтеграції функціоналу з управління кейсами та централізованого документообігу, що полегшує доказову базу для регуляторів у разі перевірок.

Висновки:

- **ВНУП повинні впроваджувати повноцінні програми ПВК/ФТ:** Це включає проведення CDD/EDD, оцінку ризиків, моніторинг транзакцій та звітування про підозрілі дії.
- **Необхідно забезпечити належне регулювання та нагляд за ВНУП:** Включаючи ліцензування, реєстрацію та контроль з боку відповідних органів для запобігання використанню ВНУП у схемах відмивання коштів.
- **Використання технологічних рішень для підвищення ефективності заходів у сфері ПВК/ФТ:** Інструменти, такі як AML Watcher, можуть допомогти ВНУП у виявленні та запобіганні фінансовим злочинам.
- **Постійне навчання та підвищення обізнаності персоналу:** Регулярне навчання співробітників DNFBP щодо AML/CFT вимог та найкращих практик є критично важливим для ефективної боротьби з фінансовими злочинами.

У контексті глобальних трендів стаття підкреслює зростаюче значення ВНУП у структурі національних та транснаціональних режимів ПВК/ФТ. Автори наводять приклади випадків зловживання ВНУП у відмиванні коштів, зокрема через анонімні компанії, що створюються юридичними фірмами, або підставні купівлі дорогоцінностей. Це актуалізує вимогу до держав вживати заходів не лише до формального впровадження стандартів FATF, а й до їх реального дотримання через прозору систему звітності, нагляду, координації з Фінансовою розвідкою та міжнародними партнерами.

Загалом, стаття формує комплексне бачення того, як ВНУП можуть — і повинні — сприяти ефективному функціонуванню глобальної системи ПВК/ФТ. Вона пропонує системний підхід, що включає регуляторний нагляд, ризик-орієнтовану ідентифікацію клієнтів, цифрові інструменти аналізу та моніторингу, а також безперервне підвищення кваліфікації персоналу ВНУП. Такий підхід не лише мінімізує ризики для бізнесу, але й зміцнює фінансову безпеку держави та сприяє міжнародній співпраці у протидії глобальним фінансовим злочинам.

Рекомендовані матеріали та події

Тінь розкоші: Як предмети розкоші стали інструментом відмивання коштів у Європі[13]

Аналітичний бюлетень, підготовлений експертом у сфері фінансової злочинності Паоло Апріле, присвячений глибокому аналізу системного зв'язку між індустрією предметів розкоші та процесами відмивання коштів. У центрі уваги – сучасні схеми використання предметів розкоші і послуг для легалізації злочинних доходів, прогалини в регуляторному середовищі ЄС, нові законодавчі ініціативи, а також геоекономічний контекст, що формує сприятливі умови для зловживань. Автор починає з відтворення культурного і кримінального контексту, вказуючи, що вже десятиліттями предмети розкоші (авто, яхти, годинники, коштовності, твори мистецтва) використовуються злочинцями не лише як засіб демонстрації статусу, а і як інструмент відмивання доходів. Цей підхід історично укорінився у свідомості, зокрема під впливом попкультури, але й закріпився у практиці організованої злочинності — про що свідчать численні приклади вилучення майна на мільйони євро в Італії та Іспанії.

Суттєвим фактором поглиблення ризиків стала рецесія у секторі розкоші у 2024 році. Зниження продажів спричинене як економічною невизначеністю та інфляцією, так і глибшими структурними зсувами — зміною споживацьких уподобань, підвищеним попитом на сталість, цифровізацією торгівлі та політичними чинниками (зокрема — торговими тарифами адміністрації Трампа, які вдарили по європейських брендах). Ці зміни спонукають учасників ринку до ухвалення ризикованих рішень, включаючи свідоме ігнорування фінансового комплаєнсу в обмін на збереження прибутків. У цьому контексті постає питання: чи стане новий Регламент ЄС з ПВК бар'єром для нових злочинних потоків, чи, навпаки, запізнілою реакцією?

Автор окреслює еволюцію регулювання з боку ЄС: від Третьої Директиви (2005), яка вперше включила торгівців цінними товарами як суб'єктів фінмоніторингу, до П'ятої (2018), яка націлилася на обіг предметів мистецтва, коштовностей та нерухомості. Найновіший Регламент 2024 року йде ще далі — він передбачає створення єдиного переліку суб'єктів, які зобов'язані здійснювати ідентифікацію клієнтів, застосовувати посилену перевірку, обмежувати розрахунки готівкою (€10 000) та передавати інформацію про підозрілі транзакції до національних підрозділів фінансової розвідки (ПФР). Ці заходи покликані закрити численні прогалини, проте бюлетень детально вказує на зони, де злочинці досі мають простір для маневру.

13 https://www.canva.com/design/DAGSOxi89JQ/83pAB7N6CmuWdrpschhbew/view?utm_content=DAGSOxi89JQ&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=h54ab0b346d#1

Однією з найбільш вразливих зон залишаються бутики високої моди, які працюють з великими обсягами готівки без належного контролю. Інша — приватні клуби та VIP-сервіси, де обслуговуються надбагаті клієнти, що можуть здійснювати дорогі покупки без фіксації фінансових слідів. Також зазначено, що навіть коли формальні вимоги щодо CDD існують, їх обхід можливий через офшори, посередників, підставних осіб та транскордонні операції. Автор наголошує, що у випадках із такими транзакціями ключовою проблемою стає неможливість ефективної ідентифікації бенефіціарів, що ускладнює протидію ВК/ФТ.

Окрема частина присвячена «брудному» золотому та ювелірному ланцюгу постачання. Незаконний видобуток корисних копалин у Західній та Центральній Африці (Гана, Малі, ДРК, ПАР) генерує мільярдні доходи, які потім легалізуються через торгівлю прикрасами або продаж дорогоцінних металів за кордоном. Наводяться приклади шахрайств з класифікацією синтетичних діамантів як природних, використання аукціонних домів і неформальних посередників у Сінгапурі та Гонконгу. При цьому регулятори зосереджені на продавцях, але не на джерелі походження товару — шахтах, які часто перебувають поза правовим полем і експлуатуються організованими групами.

Ще одним викликом, що набуває загрозливих масштабів, є контрафакт. Автор описує схему, в якій мафіозні структури через фірми з утилізації отримують доступ до оригінальних залишків матеріалів — шкіри, тканин, фурнітури, — і виготовляють копії, практично не відмінні від оригіналів. Ці підробки продаються через онлайн-платформи або нелегальні канали, генеруючи прибутки, які потім інвестуються у наркотрафік, торгівлю людьми чи тероризм. Контрафактна продукція шкодить не тільки бізнесу, а й громадській безпеці, і вимагає консолідованої міждержавної відповіді.

Завершується документ важливим попередженням: дедлайн на імплементацію нових правил в ЄС – липень 2027 року. Проте досі незрозуміло, чи встигне сектор розкоші адаптуватися до вимог або ж, на тлі економічної нестабільності, свідомо обере шлях толерування фінансових порушень заради виживання. Документ прямо порушує питання, наскільки готові компанії до реалізації політик ПВК, і чи буде достатньо волі у держав та регуляторів, аби закріпити ці правила не лише на папері, а й у практиці.

Висновки:

- **Сектор розкоші залишається вразливим до відмивання коштів,** попри нормативні посилення — зокрема, ювелірні вироби, модні бутики та приватні клуби часто виходять за межі регулювання або ухиляються від належного контролю через складність ідентифікації бенефіціарів і складні схеми міжнародних транзакцій.
- **Новий Регламент ЄС з ПВК 2024 року створює якісно новий стандарт регулювання:** вводить обов’язкову перевірку клієнтів для торговців предметами розкоші, обмежує готівкові розрахунки та зобов’язує до подання звітів до ПФР. Проте ефективність залежить від здатності забезпечити реальне впровадження та міждержавну координацію.
- **Торгівля підробленими товарами — малодосліджене, але критично небезпечне джерело доходу ОЗГ,** що потребує залучення митних, правозахисних і технологічних рішень. Зокрема, необхідно переглянути практики поводження з виробничими відходами та укріпити контроль над інтернет-продажами.
- **Сировинна база (зокрема незаконний видобуток золота і діамантів) — джерело системної корупції та фінансових потоків з Африки до Європи.** Важливо посилити простежуваність походження сировини та посилити контроль за торговцями ювелірних виробів, у т.ч. через сертифікацію та розширення обов’язкових перевірок.

Інші новини

Регулятори ЄС заявляють, що всю історію блокчейну можна стерти для захисту персональних даних [14]

Європейські регулятори викликали хвилю дискусій у крипто-спільноті після заяв про потенційну можливість видалення історії блокчейнів, якщо цього вимагає виконання положень Загального регламенту про захист даних (GDPR). Така ініціатива, оприлюднена у публікації The Daily Hodl, демонструє дедалі глибший конфлікт між технічно незмінною природою блокчейну та юридичним правом на "забуття"[15].

Згідно з позицією ЄС, навіть реєстри розподіленої мережі, які побудовані на ідеї незворотності транзакцій, не повинні виводити себе з-під дії права на приватність. Ряд аналітиків розцінюють цю позицію як пряму загрозу основоположним принципам блокчейн-технології, зокрема — її прозорості та імунітету до ретроактивного втручання.

Як вказав експерт у сфері ПВК/ФТ та віртуальних активів Олексій Фещенко: Один із учасників нещодавнього тренінгу з криптовалют зазначив, що головна перешкода для правового прийняття блокчейну — це не відсутність технологій, а мислення політиків. Замість того, щоб адаптувати регулювання до реалій XXI століття, ми бачимо спроби ‘відшмагати море’ або стерти те, що за своєю природою не можна стерти.

У світлі цього зростає актуальність звіта Драґі (Draghi Report) — стратегічних документів, що закликають ЄС або ефективно інтегрувати блокчейн, або ризикувати бути залишеним позаду в історичному вимірі. Вибір між технологічною еволюцією і регуляторною інерцією стає питанням не лише політики, а й цифрового суверенітету.

Розслідування ЄВРОПОЛ

У травні 2025 року Європол повідомив про результати двох паралельних та масштабних операцій, що вразили одразу два критично важливих напрями транснаціональної злочинності: тіньовий банкінг та контрабанду мігрантів. Обидві справи розкривають складні, добре організовані структури, які використовували технологічну обізнаність, міжнародну логістику та зухвалість у побудові стійких схем обходу закону.

Справа №1: Знешкодження злочинної мережі тіньового банкінгу [16]. У січні 2025 року в рамках масштабної спільної операції між Іспанією, Австрією, Бельгією та Європолом, було затримано

[14] https://dailyhodl.com/2025/04/29/deleting-the-whole-blockchain-eu-regulators-say-entire-chain-histories-could-be-erased-for-personal-data-protection/

[15] Право на забуття - це стандартний термін, усталений у європейському праві, зокрема в межах GDPR (General Data Protection Regulation). Право на видалення конфіденційної інформації про особу з пошукових систем в Інтернеті та інших каталогів за певних обставин.

[16] https://www.europol.europa.eu/media-press/newsroom/news/17-providers-of-criminal-banking-services-arrested?mtm_campaign=press-releases-just-published-20250514&utm_term=press-releases-just-published&mtm_source=newsletter&mtm_medium=email&mtm_content=title&mtm_group=news

17 осіб, які діяли в рамках високоспеціалізованої структури, що надавала нелегальні банківські послуги злочинним групам по всьому Європейському Союзу. Злочинці створили паралельну фінансову інфраструктуру, що включала незаконні грошові перекази, обмін криптовалюти на готівку, конвертацію великих сум у матеріальні активи, а також повне "супровідне обслуговування" для уникнення нагляду з боку державних структур.

Головними підозрюваними стали особи з громадянством Китаю та Сирії. Під час проведених обшуків вилучено понад 4,5 мільйона євро готівкою, вогнепальну зброю (чотири рушниці), а також мобільні пристрої, носії інформації та ноутбуки, які, ймовірно, використовувались для організації операцій та контактів з клієнтами.

Операція була ініційована ще у 2023 році після серії підозрілих транзакцій і використання анонімних криптовалютних платформ для переказу коштів. Виявлено, що мережа діяла не лише на користь кримінальних угруповань, а й обслуговувала окремих осіб, які хотіли обійти фінансове регулювання, наприклад, пов'язане з податками чи валютним контролем. У центрі операції стояла діяльність групи в Мадриді, яка фактично виконувала функцію нелегального "банку", що працював цілодобово.

Європол надавав ключову аналітичну, оперативну та цифрову підтримку — зокрема в сфері обробки фінансових даних, аналізу вмісту пристроїв, відслідковування транзакцій у блокчейні та спільного управління базами підозрюваних осіб.

Справа №2: Розгром міжнародної мережі контрабанди мігрантів [17]. Друга операція, координація якої здійснювалася Європолом у травні 2025 року, була спрямована проти транснаціональної організації з незаконного переміщення мігрантів, що діяла між Балканським регіоном та країнами Західної Європи. В результаті масштабного багатоетапного рейду було заарештовано 15 осіб у Бельгії, Німеччині, Австрії та Польщі. Ці особи підозрюються у перевезенні щонайменше 300 осіб з країн Близького Сходу до ЄС, використовуючи легальні транспортні компанії як прикриття.

Розслідування було розпочато восени 2024 року після виявлення низки фальшивих документів під час імміграційної перевірки у Німеччині. У ході досудового розслідування з'ясувалося, що схема функціонувала завдяки чітко організованим логістичним маршрутам, з використанням вантажного транспорту, автобусів і навіть приватних перевезень. Мережа також включала пункти збору, конспіративні квартири, координаторів у третіх країнах, які займалися вербуванням осіб та підготовкою маршрутів переміщення.

Злочинці брали з кожного мігранта від 4 000 до 10 000 євро, гарантуючи безпечне прибуття до кінцевих країн — зазвичай Німеччини, Франції або Нідерландів. Багато з постраждалих осіб ставали жертвами експлуатації або торгівлі людьми вже після прибуття до ЄС.

Під час обшуків було вилучено грошові кошти, засоби комунікації, підроблені документи, а також документацію про маршрути та графіки транспортувань, що дозволяє говорити про чітко функціонуючу злочинну мережу. Європол також виявив зв'язки між цією групою та іншими кримінальними угрупованнями, зокрема в сфері підробки документів і легалізації доходів.

Обидві справи підкреслюють зростаючу складність організованої злочинності в Європі, де окремі канали — фінансові, міграційні, логістичні — починають перетинатися, утворюючи високоструктуровані, адаптивні кримінальні екосистеми. ЄВРОПОЛ діє не лише як координаційний центр, а як технологічно озброєний партнер національних поліцій, здатний

[17] https://www.europol.europa.eu/media-press/newsroom/news/15-migrant-smugglers-arrested-in-multi-stage-operation?mtm_campaign=press-releases-just-published-20250514&utm_term=press-releases-just-published&mtm_source=newsletter&mtm_medium=email&mtm_content=title&mtm_group=news

аналізувати великі масиви даних, забезпечувати транскордонну співпрацю та реагувати на загрози у режимі реального часу.

Фахівці з комплаєнсу, міграційних служб, кримінальної розвідки та фінансового нагляду можуть сприймати ці операції як індикативні приклади того, як у 2025 році виглядають сучасні ризики — багаторівневі, цифрові, добре масковані, але вразливі перед скоординованою міжнародною реакцією.

Рекордне вилучення фентанілу: Як DEA завдала удару по картелю Сіналоа [18]

Пресреліз, опублікований Управлінням громадських зв'язків Міністерства юстиції США, висвітлює безпрецедентну за масштабом операцію Управління з боротьби з наркотиками (DEA), проведену 6 травня 2025 року, яка стала найбільшим в історії вилученням фентанілу. Ця операція була спрямована проти однієї з найвпливовіших і найнебезпечніших організацій з торгівлі наркотиками, пов'язаної з мексиканським картелем Сіналоа.

В результаті правоохоронці арештували 16 осіб і конфіскували величезну кількість фентанілу, інших наркотичних речовин, готівки, вогнепальної зброї та транспортних засобів у п'яти штатах США: Нью-Мексико, Орегон, Юта, Аризона та Невада. Операція стала частиною загальнонаціональної ініціативи «Operation Take Back America», яка має на меті боротьбу з незаконною імміграцією, ліквідацію картелів і транснаціональних злочинних організацій, а також захист громад від насильницьких злочинів.

У ході операції правоохоронні органи провели скоординовані обшуки в кількох штатах, що призвело до вилучення рекордної кількості фентанілу, зокрема 396 кілограмів фентанілових пігулок і 11,5 кілограмів фентанілового порошку в Альбукерке, Нью-Мексико, що еквівалентно понад трьом мільйонам пігулок. Крім того, в Альбукерке було конфісковано 49 одиниць вогнепальної зброї, включаючи саморобну зброю та пристрої для безшумної стрільби, 610 тисяч доларів готівкою, а також 1,5 кілограма кокаїну, 3,5 кілограма героїну, 7 фунтів метамфетаміну та два транспортні засоби вартістю 140 тисяч доларів. У Салемі, Орегон, вилучено 2,8 мільйона доларів готівкою, ювелірні вироби вартістю 50 тисяч доларів і два автомобілі вартістю 150 тисяч доларів. У Лейтоні, Юта, конфісковано 780 тисяч доларів готівкою та транспортний засіб вартістю 150 тисяч доларів. У Фініксі, Аризона, правоохоронці вилучили 390 тисяч доларів, 13 кілограмів фентанілових пігулок, 72 фунти метамфетаміну, 2,4 фунти героїну та 5 кілограмів кокаїну. У Лас-Вегасі, Невада, було вилучено 93 тисячі доларів, 2,7 кілограма кокаїну, 1 фунт метамфетаміну, а також здійснено арешт і депортацію нелегального іммігранта.

Операція мала значний юридичний резонанс. Лідером злочинної організації був Геріберто Саласар Амая, 36 років, якого разом із 12 іншими особами звинуватили у змові з метою розповсюдження фентанілу. Деякі з підозрюваних, зокрема Сесар Акуна-Морено, Брюс Седілло, Браян Санчес, Кейтлін Янг, Алан Сінгер і Ніколас Таннер, отримали додаткові

[18] https://www.justice.gov/opa/pr/largest-fentanyl-bust-dea-history-authorities-seize-over-400-kilograms-fentanyl-record

звинувачення у розповсюдженні фентанілу. Окремі особи, такі як Хосе Луїс Маркес і Брюс Седілло, звинувачені у володінні фентанілом із наміром його розповсюдження, а Седілло також звинуватили у використанні вогнепальної зброї для підтримки наркоторгівлі. Саласар Амая отримав додаткові звинувачення, пов'язані з імміграційними порушеннями, включаючи незаконне повернення після депортації, перевезення нелегальних іммігрантів і змову з метою їх переховування. Крім того, троє осіб — Філіп Ловато, Роберта Еррера та Мішель Лопес Рубіо — були арештовані за окремими кримінальними скаргами. У Санта-Фе, Нью-Мексико, у Ловато вилучили 110 тисяч фентанілових пігулок, у Еррери — 365 тисяч пігулок, 1,5 кілограма героїну, 569,9 грама кокаїну та 24 одиниці вогнепальної зброї, причому в її квартирі перебувала неповнолітня дитина. У Лопеса Рубіо конфіскували 165,5 кілограма фентанілових пігулок.

Ця операція стала наймасштабнішим вилученням фентанілових пігулок в історії DEA, що, за словами виконуючого обов'язки адміністратора DEA Роберта Мерфі, є не просто вилученням наркотиків, а «перемогою на полі бою» проти мереж, які постачають смертельні речовини в американські міста. Прокурор США по округу Нью-Мексико Раян Еллісон підкреслив, що операція підвищила безпеку громад і надіслала чіткий сигнал наркоторговцям про невідворотність покарання. Вилучення такої кількості фентанілу, що становить мільйони летальних доз, завдало значного удару по діяльності картелю Сіналоа та зменшило доступність цього небезпечного наркотику на вулицях США.

Як передбачувальне врядування може призвести до політики щодо AI, яка витримає випробування часом [19]

У статті розглядають концепцію передбачувального врядування як ключовий підхід до формування ефективної політики у сфері штучного інтелекту. Цей підхід базується на п'яти основних елементах: спільні цінності, стратегічна аналітика, залучення заінтересованих сторін, гнучке регулювання та міжнародна співпраця.

Першим кроком є визначення спільних цінностей для врядування AI, таких як справедливість, прозорість та відповідальне використання, водночас відкидаючи практики, що порушують приватність, сприяють упередженості або порушують права людини. Принципи AI від OECD, вперше погоджені у 2019 році та оновлені у 2024 році, слугують гнучкою основою для розробки політики та є глобальним орієнтиром для надійного AI.

Другим елементом є стратегічна аналітика, яка передбачає збір інформації з поточних спостережень для кращого уявлення про майбутнє AI. Моніторинг інцидентів та небезпек, як це здійснюється через OECD AI, допомагає встановити колективне розуміння моделей ризику та їх складності, що дозволяє ефективніше передбачати та запобігати майбутнім проблемам.

Третім аспектом є залучення заінтересованих сторін. Створення простору для змістовного діалогу та участі стейкхолдерів на ранніх етапах розробки інновацій або під час використання систем AI сприяє формуванню кращої політики. Це включає інформування громадськості, збір різноманітних перспектив від технічних експертів до вчителів, а також співпрацю з урядами та фахівцями для спільного створення рішень.

[19] https://oecd.ai/en/wonk/how-anticipatory-governance-can-lead-to-ai-policies-that-stand-the-test-of-time

Четвертий елемент - гнучке регулювання, яке дозволяє інноваціям розвиватися, забезпечуючи при цьому відповідні запобіжники. Такі підходи, як "пісочниці" та інші контрольовані регуляторні середовища, надають компаніям з ШІ тимчасову юридичну можливість тестувати передові ідеї, дозволяючи регуляторам бачити, де потрібно адаптуватися. Адаптація встановлених інструментів, таких як Керівні принципи OECD щодо відповідальної ділової поведінки для багатонаціональних підприємств, або нова рамка звітності в рамках Кодексу поведінки Хіросімського процесу з AI, може допомогти спростити дотримання вимог у різних країнах та інтегрувати практичний досвід компаній у регулювання.

Нарешті, п’ятий елемент — міжнародна співпраця. Визнання того, що транснаціональний та міжсекторальний розвиток, використання та вплив AI вимагають співпраці між політиками та іншими зацікавленими сторонами. Універсальний підхід до врядування AI ніколи не буде достатнім. Однак зусилля щодо використання переваг AI та пом’якшення його ризиків будуть успішними лише за умови, що різноманітні ініціативи працюватимуть узгоджено, а не конкуруватимуть чи суперечитимуть одна одній. Глобальна співпраця, як це видно у партнерстві між OECD та Глобальним партнерством з AI (GPAI), є важливою для ефективного врядування.

Ваша думка важлива!

1. Як Україна може використати елементи передбачувального врядування у регулюванні ШІ для фінансового сектора — особливо в аспекті раннього виявлення ризиків ПВК/ФТ/ФР?
2. Яким чином український державний сектор може використати блокчейн для прозорого розподілу соціальних виплат і грантів у післявоєнній відбудові, з урахуванням ризиків ВК і кіберзагроз?
3. Яким чином Україна може посилити кібербезпеку фінансових установ для запобігання використанню її банківської системи в транснаціональних кіберзлочинах, враховуючи обмежені ресурси через війну?
4. Як вплине масове впровадження стейблкоїнів на фінансову стабільність і здатність центральних банків реалізовувати монетарну політику? Чи готовий Національний банк України до таких викликів у своїй нормативній і інституційній структурі?
5. Чи доцільно законодавчо заборонити в Україні використання анонімних стейблкоїнів або запровадити обов'язкову ідентифікацію для усіх користувачів таких активів, враховуючи міжнародні тренди?
6. Як війна в Україні впливає на зростання ризику розповсюдження синтетичних наркотиків, і які превентивні заходи можуть бути вжиті для захисту вразливих груп населення, зокрема ветеранів і переселенців?
7. Яким чином українські компанії обходять податкові зобов'язання через офшорні юрисдикції на кшталт Люксембургу, та як Україна може посилити або доповнити наявні механізми протидії таким схемам?
8. Чи достатньо ефективно інтегровані ВНУП у національну систему ПВК/ФТ в Україні, і як посилити регуляторний нагляд за ними без надмірного тиску на бізнес?

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-2025-20

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].