Методологічний бюлетень

Серійний номер: МінФін-AML-2025-40

Жовтень 2025

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

Джон Вуден

Мета

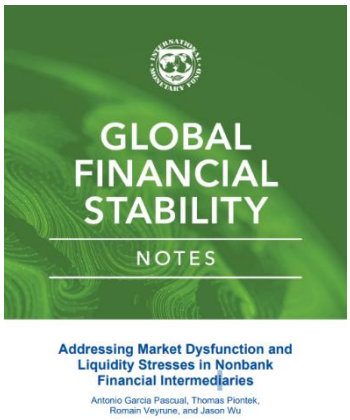
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Вирішення проблем ринкової дисфункції та ліквідності у небанківських фінансових посередників [1]



Документ МВФ детально аналізує проблеми, пов’язані з дисфункціями ринку та стресами ліквідності у секторі небанківських фінансових посередників (НБФП), а також роль центральних банків у подоланні цих ризиків. Він підкреслює, що після глобальної фінансової кризи та пандемії COVID-19 саме НБФП стали ключовими учасниками фінансової системи, акумулюючи майже 50% світових фінансових активів. Зростання їхньої ваги посилює системні ризики через поєднання значних боргових зобов’язань та проблем із швидким доступом до грошей та зростаючої взаємопов’язаності з банками, ринками та транснаціональними потоками капіталу. Автори наголошують, що швидке згортання позицій НБФП за умов

[1] https://www.imf.org/en/Publications/global-financial-stability-notes/Issues/2025/09/23/Addressing-Market-Dysfunction-and-Liquidity-Stresses-in-Nonbank-Financial-Intermediaries-570543

поганої ринкової ліквідності може призводити до "спіралей" примусових розпродажів активів, дестабілізуючи як внутрішні, так і глобальні фінансові ринки.

Документ приділяє увагу критеріям визначення системної важливості НБФП: розмір, взаємопов'язаність та замінність. На цій основі центральні банки мають заздалегідь визначати, які сегменти або інституції можуть бути кандидатами на підтримку. Потенційно системними визначено центральні контрагенти, інвестиційні та пенсійні фонди, фонди грошового ринку та дилери цінних паперів. Особливу небезпеку становлять інвестиційні фонди з невідповідністю ліквідності між активами та зобов'язаннями, а також надмірне використання деривативів, що збільшує прихований левередж.

Центральний банк, як монопольний емітент ліквідності, може виступати постачальником ліквідності для НБФП, але лише у випадках системної загрози. У документі розглянуто інструментарій втручання: операції з кредитування та купівлі активів, механізми "lender of last resort", постійні кредитні лінії та надзвичайна ліквідна допомога (ELA). Важливим є розмежування між проблемами фінансування (наприклад, розширення спредів у репо-ринках) та проблемами ринкової ліквідності (падіння обсягів торгівлі, зростання спредів bid/ask), оскільки від цього залежить вибір інструменту: або кредитування під заставу, або прямі покупки активів. Приклади Fed (PDCF, TSLF) та Bank of England (операції 2022 року для підтримки ринку гілтів) демонструють, що ефективність залежить від таргетованості, часових обмежень та прозорої комунікації з ринком.

Водночас надання доступу НБФП до постійних кредитних інструментів центральних банків може створити значні ризики морального ризику, якщо вони не супроводжуватимуться "банкоподібними" регуляторними вимогами та високими критеріями допуску. Саме тому документ акцентує на пріоритетності суворого регулювання та нагляду: вдосконаленні управління ризиками в НБФП, пропорційному регулюванні різних бізнес-моделей, запровадженні інструментів управління ліквідністю (swing pricing, redemption gates), проведенні регулярних стрес-тестів та нарощуванні аналітичних можливостей регуляторів.

Окремий блок присвячений регуляторним прогалинам у даних. Вони особливо виражені у сфері ліквідності фондів, обліку левереджу, похідних інструментів пенсійних фондів та крос-кордонних взаємозв'язків. Відсутність якісної та деталізованої інформації обмежує можливості регуляторів і центральних банків своєчасно реагувати на стреси. Автори підкреслюють необхідність кращого обміну даними між наглядовими органами, у тому числі через меморандуми про взаєморозуміння, а також розвитку

Висновки:

- **Центральні банки повинні втручатися лише для ліквідаційних проблем, а не проблем платоспроможності.** Усі програми підтримки мають бути чітко таргетовані, обмежені у часі та мати механізми виходу з ринку.
- **Системна важливість НБФП вимагає попереднього визначення потенційних кандидатів на підтримку.** Особливу увагу слід приділяти інвестиційним фондам, пенсійним фондам і дилерам цінних паперів, які є найбільш уразливими до ліквідних та левереджних шоків.
- **Регуляторні та наглядові рамки повинні передувати інтервенціям.** Необхідно посилити управління ризиками в НБФП, запровадити пропорційне регулювання, систематичні стрес-тести та обов'язкове використання інструментів управління ліквідністю.
- **Закриття прогалин у даних є критичним пріоритетом.** Без доступу до деталізованої інформації про структуру активів, зобов'язань, левередж та взаємопов'язаність НБФП центральні банки не зможуть ефективно оцінювати ризики й ухвалювати рішення про підтримку.

міжнародної координації, зокрема для управління ризиками транскордонних потоків у країнах з ринками, що формуються.

Злочини у ланцюгах критичних мінералів: загроза кліматичним цілям і глобальній безпеці [2]

Документ представляє собою комплексне дослідження проблеми кримінального впливу на ланцюги постачання критично важливих мінералів для енергетичного переходу (CETMs), таких як літій, кобальт, мідь, нікель, графіт та рідкоземельні елементи. У центрі уваги звіту — взаємозв'язок між зростанням глобального попиту на ці ресурси, їх обмеженою географічною доступністю та концентрацією переробних потужностей у кількох державах, що створює вразливі умови для проникнення організованої злочинності, поширення корупції та виникнення масштабних фінансових злочинів. Автори наголошують, що кримінальне втручання у цей сектор є вже не поодиноким явищем, а системною загрозою, яка підриває прозорість ринку, призводить до втрат державних доходів, послаблює довіру до урядів та корпорацій і ставить під ризик досягнення кліматичних цілей, закріплених Паризькою угодою.

Звіт детально описує, що кримінальна діяльність проявляється на всіх етапах ланцюга постачання — від етапів геологічної розвідки та ліцензування до видобутку, транспортування, експорту й переробки. Основним рушієм злочинності визнається корупція, яка діє як універсальний «каталізатор» усіх інших форм зловживань. Саме завдяки корупційним схемам компанії отримують ліцензії та доступ до земель, уникають дотримання екологічних і соціальних стандартів, використовують підроблені документи й обходять митний контроль. Важливим є те, що не тільки організовані злочинні угруповання проникають у цю сферу, а й формально легальні корпорації, які через відсутність належної перевірки ланцюгів постачання або свідомо, або мимоволі стають учасниками злочинних схем. У деяких випадках спеціально створюються фіктивні компанії, які займаються виключно відмиванням доходів і нелегальною торгівлею мінералами. Попри наявність законодавчих норм щодо корпоративної відповідальності у понад сотні країн, застосування таких норм залишається слабким, а міжнародні стандарти мають переважно добровільний характер, що фактично дозволяє бізнесу уникати відповідальності.

Особливою вразливістю відзначається сегмент кустарного та дрібномасштабного видобутку (ASM), який у контексті CETMs значною мірою лишається невидимим для державного регулювання. Нечіткі або відсутні правові режими, конфлікти з великими компаніями за доступ до ресурсів та економічна уразливість місцевих громад створюють ідеальні умови для експлуатації організованими злочинними групами. Цей сектор, який у майбутньому може зростати через виявлення нових родовищ, становить особливий ризик як з точки зору кримінального впливу, так і з точки зору соціально-економічних наслідків для місцевих спільнот.

Важливим акцентом документа є опис контрабанди й нелегальної торгівлі мінералами, які здійснюються здебільшого не через фізичне приховування вантажів, а через системні зловживання: підробку сертифікатів походження, маніпуляції з даними про вагу та склад,

[2] https://www.unodc.org/documents/data-and-analysis/Crimes%20on%20Environment/Minerals_Crime/Critical_minerals_2025.pdf

хабарництво на митницях, використання режимів вільних економічних зон. Особливо небезпечними є ті випадки, коли державні політики, спрямовані на захист внутрішнього ринку чи стимулювання національної переробки, створюють непередбачувані стимули для нелегального вивезення сировини. Ці процеси підривають легальну торгівлю та сприяють формуванню паралельних «сірих» ринків.

Автори наголошують, що однією з ключових перепон у протидії злочинності в секторі критичних мінералів є дефіцит якісних даних і обмежений доступ до інформації. У багатьох юрисдикціях відсутня прозорість у питаннях ліцензій, обсягів видобутку та зовнішньої торгівлі, особливо у випадку ASM, що створює «сліпі зони» для регуляторів і правоохоронців. Наявні міжнародні дослідження зосереджуються переважно на золоті та дорогоцінному камінні, тоді як ризики в секторах літію, кобальту чи рідкоземельних елементів залишаються недостатньо дослідженими. Це не тільки ускладнює належне виявлення та попередження злочинів, а й підриває можливості для розробки ефективної політики відповідального постачання.

У практичному вимірі документ пропонує низку рекомендацій: інтегрувати антикорупційні заходи та фінансові розслідування у всі етапи ланцюгів постачання, створювати більш жорсткі механізми корпоративної відповідальності, розробляти законодавчі та інституційні рамки для регулювання дрібномасштабного видобутку, забезпечувати права місцевих громад на землю та доступ до ринку, а також пропонувати альтернативні джерела доходу для зниження залежності від нелегального ASM. Значна увага приділяється необхідності посилення міжнародної співпраці, координації правоохоронних органів, створення регіональних платформ обміну даними й інформацією в реальному часі. Водночас документ підкреслює, що політики мають розроблятися не універсально, а з урахуванням специфіки кожного мінералу, адже кожен з них має власні шляхи видобутку, переробки й торгівлі, а отже і власні кримінальні ризики.

Висновки:

- **Корупція — головний рушій злочинності у секторі CETMs.** Вона дозволяє компаніям і злочинним угрупованням обходити регулювання, що веде до незаконного видобутку, контрабанди, відмивання коштів і втрат державних доходів.
- **Компанії можуть виступати як підґрунтя для злочинності.** Відсутність обов'язкових міжнародних стандартів належної перевірки та слабке правозастосування дозволяють корпораціям уникати відповідальності, зберігаючи легітимність на папері.
- **ASM є найбільш вразливим сегментом.** Його неформальний характер, конфлікти з великим бізнесом і відсутність належного правового регулювання створюють «сліпі зони» для організованої злочинності.
- **Міжнародна співпраця та прозорість даних — критично важливі.** Лише посилений контроль на кордонах, обмін розвідувальною інформацією та уніфіковані системи збору даних можуть знизити ризики злочинності й забезпечити відповідальний ланцюг постачання.

У підсумку, звіт підкреслює, що злочинність у ланцюгах постачання критичних мінералів для енергетичного переходу є системним явищем, яке не можна ігнорувати. Воно ставить під загрозу не лише добробут і розвиток країн-виробників, а й глобальну енергетичну безпеку, зусилля зі сталого розвитку та кліматичні цілі. Для ефективної протидії потрібен комплексний підхід, який об'єднує держави, міжнародні організації, бізнес і місцеві громади в рамках спільних ініціатив із забезпечення прозорості, підзвітності й безпеки у глобальних ланцюгах постачання мінералів.

Глобальний звіт 2025 про Ціль сталого розвитку 16: виклики миру, справедливості та інклюзії у світі зростаючих конфліктів і нерівності [3]

Глобальний звіт про прогрес у досягненні Цілі сталого розвитку 16 на 2025 рік являє собою комплексний аналіз тенденцій і викликів у сфері розбудови мирних, справедливих та інклюзивних суспільств. Він підготовлений трьома ключовими агентствами ООН – OHCHR, UNDP та УНЗ ООН – і базується на найновіших доступних даних усіх міжнародно погоджених індикаторів SDG16. У вступі наголошується, що світ переживає період безпрецедентних потрясінь, де війни, внутрішні конфлікти, економічні кризи й кліматичні виклики переплітаються і створюють «глобальну надзвичайну ситуацію розвитку». Водночас підкреслюється, що саме Ціль 16 є наріжним каменем усього Порядку денного 2030, адже без гарантій миру, правосуддя й інклюзії прогрес в інших напрямах є неможливим. Автори акцентують увагу на нерозривному зв'язку SDG16 з правами людини, які становлять основу для досягнення сталого розвитку.

У сфері миру дані показують змішану картину. З одного боку, спостерігається поступове зниження рівня умисних убивств у світі з 2015 по 2023 рік, однак ці темпи недостатні, щоб досягти цілі скорочення рівня вбивств удвічі до 2030 року. Регіональні відмінності залишаються значними: найвищі показники зберігаються в Латинській Америці та країнах Африки на південь від Сахари, тоді як у Європі та Східній Азії рівні убивств суттєво нижчі. Особливо гострою залишається проблема ґендерного насильства: майже 60% жінок, убитих у 2023 році, загинули від рук партнерів або членів сім'ї, тоді як більшість убивств чоловіків пов'язані з організованою злочинністю. У той же час конфліктне насильство зростає стрімкими темпами: у 2024 році життя людини забиралося кожні 12 хвилин, а кількість жертв сягнула понад 48 тисяч, причому кількість убитих жінок і дітей зросла в кілька разів. Саме війни й конфлікти стали основною причиною масштабного вимушеного переміщення, що у 2024 році охопило понад 123 мільйони осіб. Додатковим викликом є безперервні напади на правозахисників, журналістів та профспілкових активістів: у середньому кожні 14 годин у світі хтось із них був убитий або зник безвісти, а рівень нападів залишився критично високим попри незначне зниження у порівнянні з попереднім роком.

У сфері справедливості звіт фіксує системні проблеми доступу до правосуддя. Третина глобального тюремного населення, яке у 2023 році становило 11,7 мільйона осіб, перебуває у попередньому ув'язненні, що свідчить про затягнуті процедури та структурні вади судових систем. Рівень довіри до органів правопорядку є низьким: лише 15% жертв сексуального насильства повідомляють про злочини владі, тоді як для пограбувань цей показник становить 45%, а для фізичного нападу – 35%. Водночас з'являються перші результати щодо оцінки незаконних фінансових потоків, які показали їхні величезні масштаби й потенційний вплив на розвиток, якщо спрямувати ці кошти у легальну економіку. Прогрес відзначено у сфері контролю над незаконною зброєю: дедалі більший відсоток вилученої зброї маркується, реєструється й знищується, що створює кращі умови для протидії нелегальній торгівлі. Значну роль відіграють незалежні національні правозахисні інституції: з 2015 року кількість країн, які мають інституції з акредитацією «А» за Паризькими принципами, зросла з 70 до 89, а це означає, що майже половина світового населення живе у державах із визнаними правозахисними механізмами.

[3] https://www.unodc.org/documents/data-and-analysis/sdgs/2025_SDG16_Report.pdf

Додатково 70% парламентів мають спеціальні комітети з прав людини, що підсилює законодавчу підзвітність.

Що стосується інклюзії, загалом населення світу демонструє задоволення державними послугами – близько двох третин громадян позитивно оцінюють роботу органів влади у сфері документів, освіти й охорони здоров'я. Водночас понад 150 мільйонів дітей залишаються без свідоцтв про народження, що позбавляє їх доступу до базових прав і послуг. Жінки й молодь залишаються системно недопредставленими у політиці та державних органах: співвідношення жінок до чоловіків у парламентах становить лише 0,54, у судовій системі – 0,90, а у вищих урядових посадах – 0,80, що далеке від паритету. Попри певний прогрес серед молодших парламентарів, тенденції щодо ґендерної рівності й участі молоді у ключових політичних комітетах залишаються слабкими й нестійкими. На глобальному рівні країни, що розвиваються, досі недопредставлені у фінансових інституціях: їхній вплив у МВФ і Світовому банку становить лише близько 37–39% від голосів, хоча вони формують більшість членства. Політична участь у країнах з середнім і високим рівнем доходу сприймається населенням як обмежена: менше половини громадян вірять, що їхній голос впливає на ухвалення рішень. Нарешті, проблема дискримінації стає дедалі гострішою: одна з п'яти осіб у світі повідомляє про досвід дискримінації, причому в найбідніших країнах цей показник сягає чверті населення. Це особливо негативно впливає на жінок, бідні верстви й людей з інвалідністю, створюючи ризики соціальної дезінтеграції.

Звіт робить наголос на тому, що, попри певні здобутки – зниження рівня вбивств, реєстрацію понад 500 мільйонів дітей, зростання прозорості завдяки законам про доступ до інформації у 139 країнах, розширення роботи національних правозахисних інституцій і поступові кроки у сфері контролю над нелегальною зброєю – загальна динаміка реалізації Цілі 16 залишається незадовільною. Жодна з підцілей не перебуває на шляху повного досягнення до 2030 року, а темпи змін надто повільні й нерівномірні. Усе це підриває прогрес і за іншими Цілями сталого розвитку, оскільки мир, справедливість та інклюзія є базовими передумовами для подолання бідності, нерівності й захисту довкілля. Висновок документа однозначний: необхідно прискорити дії на національному рівні та зміцнити міжнародну співпрацю, спираючись на права людини, прозорість та інклюзивність. Лише так можна забезпечити, щоб бачення Порядку денного 2030 стало реальністю, а принцип «не залишати нікого осторонь» набув практичного змісту.

Висновки:

- **Ескалація конфліктного насильства:** Кількість загиблих серед цивільних, жінок та дітей різко зросла.
  Практична дія: терміново посилити міжнародні миротворчі ініціативи та захист цивільних, інвестувати у превентивну дипломатию й механізми раннього попередження.
- **Недостатній доступ до правосуддя:** Третина ув'язнених перебуває у попередньому триманні, а жертви сексуального насильства майже не повідомляють про злочини.
  Практична дія: реформувати судові системи, запровадити безоплатну правову допомогу й механізми захисту вразливих груп.
- **Інституційна нерівність та дискримінація:** Жінки, молодь і країни, що розвиваються, суттєво недопредставлені в управлінні національного та глобального рівня.
  Практична дія: розширити квоти та механізми участі для жінок і молоді, реформувати голосування в МВФ/Світовому банку, підсилити боротьбу з дискримінацією.
- **Зростання вимушеного переміщення:** Понад 123 млн осіб стали біженцями чи ВПО через конфлікти та переслідування.
  Практична дія: інтегрувати підхід SDG16 у політику щодо біженців, зокрема через захист прав людини, інклюзію й соціальну інтеграцію.

Санкції як зброя проти кіберзлочинців: нова стратегія Вашингтона [4]

Оприлюднене Міністерством фінансів США повідомлення про санкції проти транснаціональних кримінальних мереж у Південно-Східній Азії демонструє масштабність проблеми кіберзлочинності, яка дедалі частіше стає елементом глобальної безпеки. У центрі уваги — мережі шахрайських центрів у М'янмі та Камбоджі, які щороку завдають американцям збитків на десятки мільярдів доларів і водночас пов'язані з системними порушеннями прав людини. Санкції, накладені Управлінням контролю за іноземними активами (OFAC), спрямовані не лише на операторів таких схем, а й на їхні корпоративні структури, бенефіціарів та фінансових посередників, які сприяють відмиванню доходів і забезпечують функціонування злочинної інфраструктури .

Документ підкреслює, що за фасадом віртуальних «інвестиційних платформ» стоїть розгалужена система сучасного рабства. Тисячі людей з усього світу вербуються під приводом легальної роботи, але в підсумку опиняються у трудовому та сексуальному рабстві, змушені проводити цілодобові шахрайські операції онлайн. Звіт розкриває деталі роботи центрів на кшталт Yatai New City у Шве Кокко, де місцева збройна група Karen National Army (KNA) у співпраці з військовими М'янми створила ціле місто-анклав для відмивання коштів, онлайн-гемблінгу та примусової праці. Окремі компанії забезпечують охорону, постачання енергії та управління об'єктами, тоді як керівники злочинних мереж, такі як She Zhijiang, вибудовують складні корпоративні схеми, поєднуючи громадянства, псевдоніми та транснаціональні інвестиції, щоб уникати переслідування .

Камбоджійський кейс виглядає не менш показовим: готелі та казино у Сіануквілі, Баветі й Пурсаті перетворилися на осередки шахрайства, де «інвестиції у криптовалюту» стали прикриттям для експлуатації робітників і міжнародного відмивання коштів. Фігуранти цих справ — від власників готелів до великих банківських структур — мають кримінальне минуле, пов'язане з корупцією, незаконними азартними іграми й масштабними схемами відмивання. OFAC прямо вказує, що низка фінансових інституцій, включно з HH Bank у Камбоджі, стали інфраструктурними вузлами для злочинних операцій, що становить загрозу не лише для американських споживачів, а й для стабільності глобальної фінансової системи.

Цей пакет санкцій використовує цілу низку правових інструментів — від президентських указів проти транснаціональних кримінальних організацій і кіберзлочинців до Global Magnitsky Act, який передбачає переслідування за грубі порушення прав людини та корупцію. Це сигналізує, що кіберзлочинність у Південно-Східній Азії розглядається Вашингтоном не лише як питання боротьби з шахрайством, а як загроза національній безпеці США та міжнародній стабільності. З огляду на це, американська політика санкцій спрямована на руйнування не лише окремих схем, а й системної економічної бази злочинних мереж — власності, банківських каналів, інвестиційних фондів.

Однак у цьому документі є й інший важливий вимір — гуманітарний. Уряд США прямо пов'язує діяльність кібермереж із торгівлею людьми, насильством і сучасним рабством. Санкції позиціонуються не як каральний інструмент, а як засіб змінити поведінку суб'єктів і одночасно захистити потенційних жертв. При цьому зазначається, що жодна система санкцій не є незворотною: ті компанії й особи, які доведуть відмову від злочинної діяльності та готовність співпрацювати з міжнародною спільнотою, можуть бути виключені зі списків OFAC.

[4] https://home.treasury.gov/news/press-releases/sb0237

Висновки:

- **Санкції проти операторів шахрайських центрів** у М'янмі та Камбоджі демонструють необхідність цілеспрямованого тиску на корпоративні структури та фінансових посередників, що забезпечують роботу злочинних мереж.
- **Кіберзлочинність у Південно-Східній Азії** тісно пов'язана з торгівлею людьми, тому протидія має поєднувати фінансові інструменти з програмами захисту прав жертв і реінтеграції постраждалих.
- **Використання Global Magnitsky Act** у цьому контексті підкреслює ефективність інтеграції санкційних механізмів із боротьбою проти корупції та масових порушень прав людини.
- **Для досягнення стійкого результату** санкційна політика має супроводжуватися міжнародною координацією і підвищенням прозорості транскордонних фінансових потоків, що обмежить маневрові можливості кримінальних мереж.

Узагальнюючи, публікація демонструє подвійний характер глобальної боротьби з кіберзлочинністю: це водночас битва за фінансову безпеку громадян і за людську гідність тих, кого примусили стати знаряддям шахрайства.

Санкції проти Південно-Східної Азії у цьому випадку є частиною ширшої стратегії, де фінансовий тиск використовується як інструмент протидії організованій злочинності, корупції та масовим порушенням прав людини. І водночас вони нагадують, що ефективна боротьба з подібними викликами можлива лише за умови координації міжнародних зусиль, прозорості транскордонних фінансових потоків і готовності держав розглядати кіберзлочинність не як ізольовану проблему, а як глобальну загрозу безпеці та стабільності.

Звіти окремих інституцій та експертів

Грошові мули в Україні: зростаюча загроза фінансовій стабільності та безпеці [5]

Представлений дослідницький звіт, підготовлений Центром фінансової доброчесності (CFI) у співпраці з британським аналітичним центром RUSI, є комплексним аналізом проблеми використання грошових мулів в Україні. Документ розглядає це явище як зростаючу загрозу для фінансової стабільності та безпеки держави, особливо в умовах повномасштабної російської агресії. Автори зазначають, що схеми з використанням дропів не лише сприяють ухиленню від сплати податків та відмиванню коштів, що послаблює дохідну частину бюджету, але й можуть використовуватися для фінансування тероризму, диверсійної діяльності та прихованих російських операцій. Згідно з наведеними даними, через такі схеми щорічно проходить понад 200 мільярдів гривень, що призводить до потенційних податкових втрат у розмірі 50 мільярдів гривень.

У звіті детально розкрито механізм функціонування мереж грошових мулів, які можуть налічувати сотні й тисячі учасників, що ускладнює їх виявлення. Національний банк України (НБУ) визначає грошових мулів як осіб, що за винагороду надають третім особам свої банківські картки чи ідентифікаційні дані. Водночас автори підкреслюють, що частина людей втягується в цю діяльність несвідомо, тоді як інші діють цілком усвідомлено. Соціальний вплив проблеми є значним: втягнуті особи, часто молодь, стикаються з довгостроковим або навіть постійним

[5] https://cfi-ua.org/money-mules-in-ukraine-a-growing-threat-to-financial-stability-and-security/

виключенням із фінансової системи, що унеможливлює отримання кредитів, зарплат чи ведення бізнесу.

У відповідь на цю загрозу, українські банки та державні регулятори вживають низку заходів. НБУ посилив вимоги до фінансового моніторингу та запровадив обмеження на P2P-перекази, що, за попередніми оцінками, дозволило скоротити місячні обсяги таких операцій з 250 до 170 млрд грн. Важливим кроком стало підписання меморандуму між банками для обміну інформацією про підозрілих клієнтів, що є прикладом ефективного державно-приватного партнерства. Разом з тим, звіт висвітлює, як злочинні мережі адаптуються до нових умов: вони імітують звичайну споживчу поведінку, використовують штучний інтелект для підробки документів та відеоверифікації , а також активно залучають віртуальні активи для обходу обмежень, що, за оцінками експертів, завдає бюджету збитків близько 1 млрд грн щомісяця.

Окрему увагу в документі приділено правовій базі та правозастосовній практиці. В Україні відсутня окрема стаття Кримінального кодексу, що прямо карає за діяльність грошових мулів. Тому правоохоронці змушені кваліфікувати такі дії за статтями про шахрайство (ст. 190), відмивання доходів (ст. 209) або ухилення від сплати податків (ст. 212). Це значно ускладнює притягнення до відповідальності, оскільки вимагає доведення зв'язку з основним, більш тяжким злочином. У звіті також розглядається міжнародний досвід протидії грошовим мулам у Великій Британії, Польщі та США, де акцент робиться на публічно-приватних партнерствах, спеціалізованих базах даних та широких інформаційних кампаніях для населення.

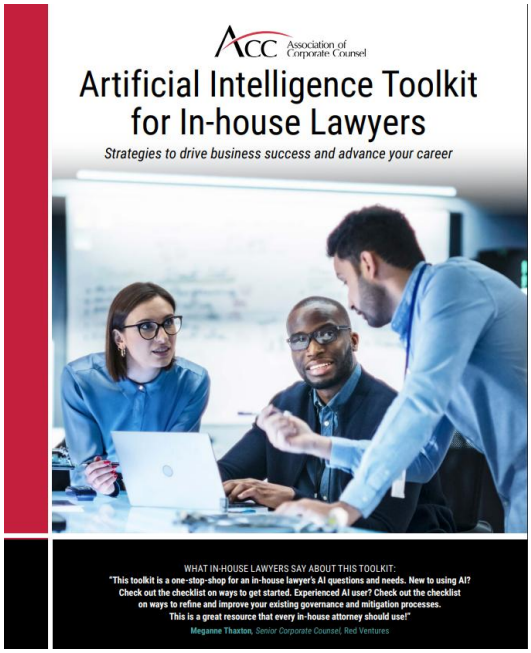
Висновки:

- **Регуляторні обмеження НБУ є дієвим інструментом.** Встановлення лімітів на карткові перекази (P2P) довело свою практичну ефективність, призвівши до скорочення місячних обсягів транзакцій на 80 млрд грн. Це підтверджує, що жорсткі адміністративні заходи є швидким та результативним способом протидії схемам, річний обіг яких завдає державі збитків на десятки мільярдів гривень.
- **Злочинні мережі активно адаптуються за допомогою технологій.** У відповідь на посилений контроль з боку банків та регулятора, організатори схем почали застосовувати штучний інтелект для підробки документів і проходження відеоверифікації, а також масово використовувати віртуальні активи для обходу обмежень на транскордонні перекази. Це вимагає від фінансових установ та правоохоронних органів невідкладного впровадження більш досконалих інструментів моніторингу та верифікації.
- **Відсутність спеціалізованої правової бази ускладнює притягнення до відповідальності.** В українському законодавстві немає окремої статті, яка б криміналізувала саме діяльність грошового мула. Правоохоронцям доводиться доводити причетність дропа до основного злочину (наприклад, шахрайства чи відмивання коштів), що є складним і ресурсозатратним процесом. Це створює правовий вакуум, який дозволяє багатьом учасникам схем уникати відповідальності.

Інструментарій штучного інтелекту для юристів [6]

Представлений документ, розроблений Асоціацією корпоративних юристів (ACC), є фундаментальним і всеосяжним посібником, що виконує роль стратегічної дорожньої карти для інтеграції технологій штучного інтелекту (AI) в діяльність сучасних юридичних департаментів.

[6] https://www.acc.com/sites/default/files/resources/upload/ACC-Artificial-Intelligence-Toolkit-for-In-house-Lawyers-FINAL.pdf



Його цільова аудиторія охоплює всіх штатних юристів, від початківців до керівників юридичних служб, а основна мета — заповнити критичний пробіл у готовності правників до викликів та можливостей, які несе з собою епоха AI. Ця проблема підкреслюється статистикою, згідно з якою лише 42% юрисконсультів вважають себе підготовленими до впливу генеративного AI на їхню професійну діяльність, що свідчить про гостру потребу в систематизації знань і розробці чітких методологічних підходів. Інструментарій детально аналізує подвійну природу AI: з одного боку, він відкриває безпрецедентні можливості для автоматизації рутинних завдань, підвищення ефективності аналізу величезних масивів даних та оптимізації робочих процесів , а з іншого — створює комплекс нових, значущих ризиків у сферах конфіденційності даних, захисту інтелектуальної власності, кібербезпеки та дотримання складного, фрагментарного регуляторного ландшафту, що стрімко розвивається.

Центральною віссю всього посібника є концепція побудови надійної та всеохоплюючої системи управління штучним інтелектом (AI Governance). Автори пропонують структурований шестикроковий підхід до розробки та впровадження цієї системи.

Крок 1: Проведіть аудит поточного використання AI у вашій організації

Перший і найважливіший крок — це зрозуміти, як і де штучний інтелект вже використовується у вашій компанії. Існує висока ймовірність, що ваші колеги вже експериментують з різними інструментами, зокрема з генеративним AI, для дослідження, підготовки документів чи автоматизації завдань.

Ключові дії на цьому етапі:

- Створення міжфункціональної команди: Для проведення всебічного аудиту необхідно зібрати команду, до якої увійдуть представники ключових підрозділів: інформаційної безпеки, IT, розробки продуктів, HR, фінансів, управління ризиками та, звичайно, юридичного департаменту.
- Проведення комплексного опитування: Найбільш практичний спосіб зібрати інформацію — це провести загальнокорпоративне опитування. Воно допоможе виявити, які саме інструменти використовуються, для яких завдань, та які плани щодо застосування AI існують у різних командах. Це дозволить ідентифікувати патерни використання та визначити потенційні зони ризику.
- Тимчасове призупинення ризикованих практик: Під час проведення аудиту доцільно розглянути можливість тимчасової паузи у використанні найбільш ризикованих інструментів AI, доки не будуть розроблені відповідні політики. Важливо комунікувати, що кінцевою метою є не повна заборона, а вироблення правил для безпечного та ефективного використання технології.

Крок 2: Картографуйте ваші регуляторні зобов'язання, пов'язані з AI

Регуляторний ландшафт у сфері AI є фрагментарним, швидко змінюється та відрізняється в різних юрисдикціях. Ваше завдання — чітко зрозуміти, які саме закони та норми застосовуються до діяльності вашої компанії.

Ключові дії на цьому етапі:

- Аналіз юрисдикцій: Створіть таблицю або карту, де будуть перелічені всі країни та регіони, в яких ваша організація веде бізнес або має співробітників.
- Ідентифікація застосовних норм: Для кожної юрисдикції визначте конкретні регуляторні вимоги до розробки та використання AI. Це можуть бути як спеціалізовані закони (наприклад, AI Act в ЄС), так і норми в межах існуючого законодавства (наприклад, GDPR, закони про захист прав споживачів, антидискримінаційні закони).
- Вибір єдиного стандарту комплаєнсу: Оскільки вимоги можуть відрізнятися і навіть суперечити одна одній, найкращою практикою є прийняття за основу найбільш суворих зобов'язань як єдиного загальнокорпоративного стандарту. Це спростить внутрішні процеси та забезпечить вищий рівень захисту.

Крок 3: Розробіть бізнес-орієнтовані карти ризиків та структури управління AI

На цьому етапі ви переходите від збору інформації до розробки стратегічної рамки, яка збалансовує інноваційні можливості AI з потенційними загрозами.

Ключові дії на цьому етапі:

- Створення карт ризиків: Спільно з міжфункціональною командою визначте та задокументуйте потенційні ризики, пов'язані з кожним сценарієм використання AI. До основних ризиків належать: порушення конфіденційності, упередженість (bias) та дискримінація, порушення прав інтелектуальної власності та загрози кібербезпеці.
- Інтеграція в загальну систему ризик-менеджменту: Ризики, пов'язані з ШІ, не повинні розглядатися ізольовано. Їх необхідно інтегрувати в існуючу в компанії систему управління ризиками, враховуючи встановлені процедури їх кількісної оцінки та пріоритезації.
- Розробка формальної системи управління: Створіть офіційну політику або рамковий документ з управління AI (AI Governance Policy). Цей документ повинен чітко визначати принципи етичного та прозорого використання технології, а також демонструвати регуляторам та партнерам відповідальний підхід вашої компанії.
- Інформування керівництва: Вкрай важливо донести до вищого керівництва та ради директорів інформацію про важливість управління AI та про конкретні ризики, які виникають у разі відсутності належних політик.

Крок 4: Встановіть чіткі ролі та обов'язки для команди управління AI

Ефективне управління неможливе без чіткого розподілу відповідальності. Кожен у компанії повинен знати, хто за що відповідає у сфері AI.

Ключові дії на цьому етапі:

- Призначення відповідальної особи або команди: Визначте конкретну особу (наприклад, AI Steward з юридичного департаменту) або команду, яка буде очолювати ініціативи з управління AI.
- Визначення ролей для різних підрозділів: Чітко пропишіть, яку роль в управлінні AI відіграють фахівці з обробки даних, інженери, юристи, HR-менеджери та комплаєнс-менеджери.
- Побудова системи підзвітності: Створіть прозору систему підзвітності за рішення, пов'язані з AI. Це не обов'язково має бути одна людина; скоріше, це може бути призначений лідер від кожної команди, яка інтегрує ШІ у свою діяльність. Як зазначає один з експертів, важливо «делегувати повноваження команді амбасадорів ШІ або зробити відповідальним рівень віце-президентів».

Крок 5: Оновіть існуючі політики, щоб врахувати аспекти AI

Багато проблем, пов'язаних із AI, не є принципово новими для бізнесу. Компанії вже мають політики щодо безпеки даних, конфіденційності, захисту інтелектуальної власності та протидії упередженості.

Ключові дії на цьому етапі:

- Аналіз існуючих політик: Перегляньте ваші поточні корпоративні політики та визначте, де необхідно додати специфічні положення щодо AI.
- Внесення доповнень: Замість того, щоб створювати окрему політику для кожного аспекту, спочатку спробуйте внести зміни до вже існуючих документів. Наприклад, політику конфіденційності можна доповнити пунктом про заборону завантаження корпоративних даних у публічні AI-інструменти. Це забезпечить кращу інтеграцію та уникне надмірної бюрократизації.

Крок 6: Створіть зручні та зрозумілі політики використання AI для всієї організації

Фінальний крок — це створення головної політики використання AI, яка буде простою, зрозумілою та практичною для всіх співробітників.

Ключові дії на цьому етапі:

- Чіткість та прозорість: Політика повинна бути написана простою мовою, без складного юридичного жаргону. Вона має чітко пояснювати ризики зловживання AI.
- Реалістичність: Документ повинен відображати реальну практику та культуру вашої компанії. Мета — заохочувати відповідальне використання, а не створювати надмірні бар'єри.
- Визначення сфери застосування: Чітко вкажіть, на кого поширюється політика (зазвичай, це всі співробітники, підрядники та треті сторони).
- Правила допустимого використання: Детально опишіть, які AI-інструменти дозволено використовувати, а які — заборонено, а також для яких конкретних завдань.

Висновки:

- **Формалізація управління AI є невідкладним пріоритетом.** Для ефективної мінімізації ризиків компанія повинна негайно ініціювати процес створення комплексної системи управління AI. Це вимагає проведення повного аудиту поточного використання AI, створення міжфункціональної робочої групи, розробки та впровадження чіткої корпоративної політики, яка б однозначно регулювала допустимі та заборонені способи використання AI, з особливим акцентом на захисті конфіденційних даних.
- **Людський нагляд та критична верифікація є абсолютно незамінними.** Технології AI, особливо генеративні моделі, схильні до так званих «галюцинацій» - генерування фактично невірної, але правдоподібної інформації. Юристи та інші співробітники несуть повну професійну та етичну відповідальність за кінцевий продукт своєї роботи. Тому будь-який результат, отриманий від AI, - чи то проект договору, чи юридичний висновок - має розглядатися виключно як чернетка, що потребує ретельної перевірки, редагування та підтвердження з надійних джерел.
- **Посилена перевірка постачальників та жорсткі контрактні умови - головний інструмент захисту.** В умовах, коли постачальники послуг масово інтегрують AI у свої продукти, першочерговим завданням стає управління ризиками третіх сторін. Необхідно вимагати від вендорів повного розкриття інформації про використання AI-технологій та включати в договори спеціалізовані додатки або положення, що регулюють права власності на дані, зобов'язання щодо конфіденційності, безпеки та дотримання законодавства, а також передбачають широкі зобов'язання постачальника щодо відшкодування збитків у разі виникнення будь-яких претензій, пов'язаних із використанням AI.

- Акцент на безпеці: Наголосіть на ключових вимогах до безпеки та конфіденційності, наприклад, використання VPN або захищених паролями корпоративних акаунтів для доступу до AI-інструментів.
- Відповідальність за недотримання: Поясніть, що недотримання політики може призвести до дисциплінарних стягнень, включно зі звільненням.

Особливу увагу в документі приділено детальному аналізу конкретних ризиків та стратегій їх мінімізації. У розділі про етичні зобов'язання юристів у США детально розглядається обов'язок компетентності, який тепер поширюється на розуміння сучасних технологій, та обов'язок збереження конфіденційності, порушення якого може статися через необережне завантаження клієнтської інформації у загальнодоступні AI-платформи, що може призвести до втрати адвокатської таємниці. Не менш важливим є блок, присвячений захисту інтелектуальної власності. Посібник попереджає, що контент, згенерований виключно штучним інтелектом без суттєвого творчого внеску людини, наразі не підлягає захисту авторським правом у США , а сам AI не може бути визнаний «винахідником» для цілей патентного права. Крім того, використання публічних AI-інструментів створює пряму загрозу ненавмисного розкриття комерційних таємниць, оскільки введені дані можуть використовуватися для подальшого навчання моделі. Окремий великий розділ присвячено взаємодії з постачальниками. Інструментарій наполягає на необхідності проведення поглибленої перевірки будь-яких третіх сторін, що використовують AI, та рекомендує включати до контрактів спеціальні положення: загальні заборони або вимоги щодо попереднього узгодження використання AI, детальні описи функціональності, гарантії дотримання законодавства та, що найважливіше, надійні пункти про відшкодування збитків для захисту компанії від можливих претензій.

Майбутнє грошей: роль стейблкоїнів у глобальній фінансовій системі до 2030 року [7]

Звіт є фундаментальним дослідженням майбутнього ролі стейблкоїнів у глобальній фінансовій системі та їхнього потенційного впливу на інституційну інфраструктуру грошей. Автори підкреслюють, що стейблкоїни стають рушійною силою цифрової трансформації фінансів. Вони називають цей етап «моментом ChatGPT» для блокчейну — тобто переломним моментом, коли технологія виходить за межі експериментів і починає широко використовуватися у повсякденних фінансових операціях та реальних грошових потоках. Протягом 2025 року відбувся стрімкий ріст емісії — з 200 млрд доларів на початку року до 280 млрд доларів у вересні, що підтвердило масштабність попиту на інструменти цифрових доларів. У цьому контексті Citi переглянула прогнози: у базовому сценарії до 2030 року ринок може сягнути 1,9 трлн доларів, у песимістичному — 0,9 трлн, а в оптимістичному — 4,0 трлн, що пояснюється швидким поширенням нових регуляторних рамок, підключенням великих корпорацій та розвитком нових блокчейн-платформ.

Звіт наголошує, що стейблкоїни не існують у вакуумі, а формують екосистему разом із іншими форматами цифрових грошей — токенізованими депозитами, депозит-токенами та CBDC. Хоча саме стейблкоїни є найбільш динамічним сегментом, Citigroup очікує, що за транзакційними обсягами банківські токени перевищать їх, оскільки вони поєднують технологічну ефективність

[7] https://www.citigroup.com/rcs/citigpa/storage/public/GPS_Report_Stablecoins_2030.pdf

із довірою, приватністю та регуляторним наглядом, що є визначальним для великих корпорацій та інституційних учасників. При цьому прогнозовані щорічні транзакції зі стейблкоїнами можуть сягати 100–200 трлн доларів, але транзакційні потоки банківських токенів оцінюються навіть вище — 100–140 трлн доларів, що свідчить про зміщення балансу між приватними емітентами та традиційною банківською системою у напрямку інтеграції, а не витіснення.

Особлива увага приділена регуляторному середовищу. У США ухвалення GENIUS Act стало переломним моментом, який забезпечив підґрунтя для масового використання стейблкоїнів, підвищивши попит на казначейські облігації США та посиливши роль долара у глобальних розрахунках. SEC запустила «Project Crypto» для модернізації законодавства у сфері цінних паперів, запровадивши нові ліцензійні режими та «швидку регуляторну смугу» (спеціальний спрощений режим, який створюють регулятори для іноваційних компаній) для інноваційних бізнес-моделей. В Європі у 2024 році набрала чинності MiCAR, а в Гонконзі у 2025 році впроваджено нову систему ліцензування для емітентів стейблкоїнів, що створило передумови для появи корпоративних токенів від таких гігантів, як Alibaba чи JD.com. У глобальному вимірі доларові стейблкоїни залишаються основним активом, але зростає інтерес до місцевих валютних стейблкоїнів у Азії, на Близькому Сході та в Європі.

У розділах, присвячених застосуванню, автори акцентують на кількох стратегічних сценаріях. Для малих та середніх підприємств стейблкоїни відкривають нові можливості у кросбордерних платежах, дозволяючи скоротити витрати, уникнути багатоденних затримок та зменшити залежність від посередників. У сфері корпоративних фінансів йдеться про концепцію «real-time everything», коли ліквідність переміщується безперервно між ринками, дочірніми компаніями та постачальниками, що змінює підхід до управління капіталом та скорочує фінансові цикли. На рівні ринку капіталу стейблкоїни поступово стають базовою розрахунковою валютою для токенізованих цінних паперів, а також ключовим елементом управління заставами та програмованих розрахунків. Корпоративні гіганти, серед яких PayPal, Amazon та Walmart, вже експериментують із власними стейблкоїнами, інтегруючи платежі у свої екосистеми та формуючи альтернативні інфраструктури для розрахунків.

Водночас у документі підкреслюються й системні виклики. Зростання стейблкоїнів створює ризик дезінтермедіації депозитів, адже кошти з банківських рахунків можуть перетікати у резерви стейблкоїнів, що повторює історію фондів грошового ринку у 1980-х. Це може призвести до моделі «Narrow Banking 2.0», коли банки втрачають частину ресурсної бази для кредитування, а економіка стикається з новими структурними ризиками. Додатковим бар'єром є фрагментація екосистеми: існування багатьох блокчейнів, відсутність єдиних стандартів інтероперабельності та підвищені ризики кіберзагроз. Хоча конкуренція між

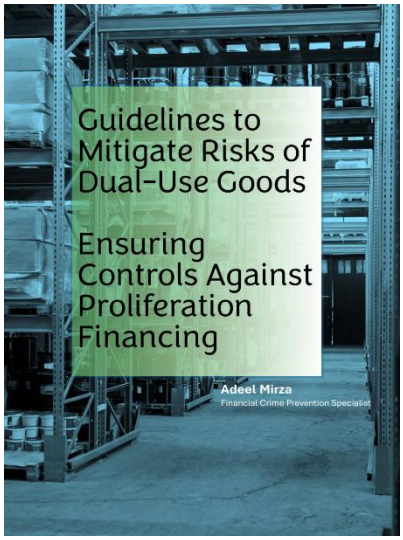
Висновки:

- **Прогноз Citi: $1,9 трлн ринку стейблкоїнів до 2030 р.** Це означає, що фінансовим установам та регуляторам необхідно вже зараз готувати інфраструктуру для інтеграції таких обсягів.
- **Банківські токени перевищать стейблкоїни за транзакційними обсягами.** Корпораціям варто зосередитися на розробці продуктів на базі токенізованих депозитів, оскільки вони більш привабливі з точки зору регуляції та довіри.
- **Кросбордерні платежі для малих та середніх підприємств (МСП) — ключовий драйвер зростання.** Стейблкоїни здатні закріпитися як стандарт для малого бізнесу, що зменшить витрати та прискорить інтеграцію до глобальних ринків.
- **Фрагментація та регуляторна невизначеність залишаються головними викликами.** Потрібні міжнародні стандарти інтероперабельності та прозорі механізми резервного забезпечення, щоб уникнути системних ризиків.

емітентами та мережами стимулює інновації, надмірна роздробленість може сповільнити масове прийняття та знизити ліквідність.

Загалом звіт підкреслює, що поява стейблкоїнів не означає зникнення банківської системи, а радше її трансформацію та інтеграцію з новими технологічними інфраструктурами. Подібно до того, як поява PayPal не знищила банки, а змусила їх адаптуватися, так і стейблкоїни та банківські токени співіснуватимуть, забезпечуючи користувачам швидші, гнучкіші й програмовані фінансові інструменти. У перспективі до 2030 року очікується не стільки конкуренція форматів, скільки поступове формування гібридної фінансової системи, де стейблкоїни зміцнюють роль долара, відкривають нові можливості для бізнесу та споживачів, але водночас потребують гармонізованого регулювання, міжнародних стандартів та продуманої інтеграції у традиційні фінансові інститути.

Контроль за товарами подвійного призначення: практичні настанови для запобігання фінансуванню розповсюдження [8]



Документ являє собою комплексні настанови щодо управління ризиками, пов'язаними з товарами подвійного призначення, і має на меті створення системного підходу для фінансових установ, постачальників логістичних та торгових послуг, а також надавачів послуг у сфері віртуальних активів. Його ключовою ідеєю є інтеграція ризиків, пов'язаних із подвійним використанням товарів, у ширшу рамку протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. У вступній частині окреслюються поняття, що становлять основу всього підходу: товари подвійного призначення як цивільні чи комерційні товари, здатні до військового застосування, фінансування розповсюдження як процес надання ресурсів чи логістики програмам створення зброї масового знищення, а також критично важливі категорії, такі як «кінцевий користувач», «кінцеве використання», «положення про загальний контроль» та «червоні прапорці». Автор наголошує, що розпізнавання ознак ризику на ранніх етапах є фундаментом ефективної системи, адже саме тут можна запобігти переорієнтації легального товарообігу у незаконні військові програми.

Важливе місце відведено деталізації ризикових напрямів. Зокрема, визначено групи товарів, які потребують особливої уваги через їхній потенціал до використання у програмах зі створення зброї масового знищення: електроніка та напівпровідники, що можуть застосовуватися у системах наведення чи управління ракетами; хімічні реагенти, які використовуються як прекурсори для виробництва хімічної зброї; безпілотні літальні апарати та комплектуючі до них; центрифуги й обладнання для роботи під тиском, здатні застосовуватися в ядерних процесах. Також документ виокремлює групу країн із високим ризиком, серед яких КНДР, Іран, Сирія, Венесуела та інші держави, що перебувають під багаторівневими санкціями, і підкреслює важливість підвищеної перевірки транзакцій із цими юрисдикціями. При цьому вказується, що навіть якщо країна чи товар на перший погляд не викликають занепокоєнь, сама природа транзакції може містити ознаки ризику, наприклад використання компаній-оболонок без

[8] https://media.licdn.com/dms/document/media/v2/D4D1FAQHPiDM0pwL3Bw/feedshare-document-pdf-analyzed/B4DZmO2URPHsAY-/0/1759038230830?e=1760572800&v=beta&t=2sSevWFstXNNvOib6-MhxdQLyj0QF6IeaWJQsbNGLfk

реальної присутності, транзит через треті країни з метою обходу контролю, розрахунки криптовалютами або надання нечітких декларацій щодо кінцевого призначення.

Суттєва частина документа присвячена методології оцінки ризиків. Пропонується інтегрувати фактори подвійного використання у широку систему оцінки ризиків на рівні установи, періодично оновлювати підхід з урахуванням змін у регуляторних режимах чи появи нових типологій, а також класифікувати клієнтів та угоди за рівнями ризику. Критеріями стають чутливість товару, географія походження, транзиту та кінцевого призначення, а також легітимність кінцевого користувача. Для управління ризиками наголошується на застосуванні належної перевірки клієнта. На базовому рівні CDD передбачає ідентифікацію клієнта та бенефіціарних власників, розуміння бізнес-моделі та постійний моніторинг. У випадках із підвищеним ризиком застосовується посилена перевірка, яка охоплює підтвердження особи кінцевого користувача та його можливостей, перевірку ліцензій, скринінг за міжнародними та національними санкційними списками, а також у разі необхідності проведення верифікації на місцях.

Документ наголошує на центральній ролі систем скринінгу як першої лінії захисту від взаємодії із забороненими сторонами або транзакціями, що стосуються ризикових товарів. Він закликає до використання оновлених списків санкцій ООН, OFAC, ЄС, Великої Британії та національних списків, а також до перевірки товарів через міжнародні контрольні переліки, як-от Wassenaar Arrangement, регламент ЄС про товари подвійного використання чи американські EAR/ITAR. Для підвищення прозорості рекомендується вимагати декларації кінцевого користувача/кінцевого використання з чіткими деталями про місце призначення, призначення товарів і підтвердження, що вони не будуть відхилені у військові програми. Важливим інструментом визначається й моніторинг транзакцій, який має бути спрямований не лише на стандартні параметри ПВК, а й на ознаки, характерні саме для фінансування розповсюдження: дроблення платежів, багаторазові дрібні транзакції з одним і тим самим контрагентом, складні маршрути платежів, залучення третіх сторін без видимої ролі.

Значну увагу приділено процедурам ескалації та звітності. Будь-яка підозріла транзакція повинна негайно передаватися працівнику відповідальному за комплаєнс, а у випадку підтверджених ризиків — звітуватися до фінансової розвідки у вигляді підозрілої транзакції.

Висновки:

- **Інтеграція ризиків подвійного призначення у систему ПВК/ФТ/ФР.** Фінансові установи та суб'єкти зовнішньо-економічної діяльності мають включати оцінку ризиків ФР у свої EWRA, класифікуючи клієнтів і транзакції за ризик-рівнями з урахуванням товару, юрисдикції та кінцевого користувача.
- **Обов'язковість посиленої перевірки (EDD) для високоризикових випадків.** Транзакції з високоризиковими товарами чи країнами повинні супроводжуватися EDD: перевіркою ліцензій, верифікацією кінцевого користувача, аналізом технічних можливостей та скринінгом за санкційними списками.
- **Запровадження ефективного моніторингу та скринінгу.** Інституції мають налаштовувати автоматизовані системи на виявлення індикаторів ФР (роздрібнення платежів, транзит через треті країни, крипто-платежі, компанії-оболонки), інтегрувати міжнародні та національні контрольні списки.
- **Системність ескалації, навчання та співпраці з органами влади.** Важливо забезпечити чіткі протоколи ескалації, регулярне навчання співробітників, аудит процедур та активну комунікацію з ПФР, митними та експортними органами для зміцнення ефективності національної та міжнародної системи контролю.

Обов'язковим елементом є ведення ретельної документації всіх перевірок, угод та звітів, причому мінімальний строк зберігання визначено у п'ять років. Окремий блок присвячений навчанню персоналу: щорічні тренінги для всіх співробітників, які працюють у ризикових сегментах, з акцентом на реальні типології, інструменти експортного контролю та порядок ескалації. Також визначається необхідність регулярних внутрішніх аудитів і тестувань систем, що дозволяють переконатися в актуальності процедур і точності скринінгу. Додатково підкреслюється важливість активної співпраці з органами державної влади — фінансовою розвідкою, митними та експортними органами — для підвищення ефективності контролю та вчасного реагування на спроби обходу.

Завершальна частина окреслює принцип безперервного вдосконалення: перегляд ризикових індикаторів відповідно до публікацій FATF і національних оцінок, оновлення політик та процедур з урахуванням нових тенденцій, розвиток технічних систем для зниження кількості хибнопозитивних спрацювань і використання досвіду розслідуваних справ для вдосконалення внутрішніх процесів. У підсумку документ позиціонується як дорожня карта для організацій, які прагнуть не лише виконувати регуляторні вимоги, а й активно протидіяти фінансуванню розповсюдження, захищати власну репутацію та робити внесок у збереження міжнародної безпеки і стабільності фінансових ринків.

Глобальні платежі 2025: цифрові валюти, агентний AI та миттєві транзакції як нові драйвери ринку [9]

Звіт фіксує переломний момент у розвитку глобальної платіжної індустрії, де технологічні інновації, регуляторні зміни, тиск інвесторів та геополітична нестабільність створюють нову складну, але динамічну екосистему. Основним висновком дослідження є те, що фундаментальні тренди, які раніше були на периферії — миттєві платежі, цифрові валюти, генеративний та агентний штучний інтелект, платформізація фінансових послуг — тепер набули системного масштабу і стають визначальними для структури доходів та стратегії компаній. Загальний обсяг доходів від платежів у 2024 році досяг 1,9 трлн доларів і до 2029 року прогнозується на рівні 2,4 трлн доларів, проте темпи зростання сповільняться через вичерпання ефекту високих відсоткових ставок, що стимулювали маржу на депозитах. При цьому транзакційні доходи залишаться основним рушієм, особливо у Латинській Америці, Східній Європі, на Близькому Сході та в Африці, де подвійні та навіть потрійні темпи зростання забезпечуються цифровізацією, активним впровадженням миттєвих систем і швидким поширенням мобільних фінансових сервісів.

Ключовим аспектом звіту є аналіз ролі цифрових валют, передусім стабількоїнів, які за кілька років перетворилися з експериментального продукту у масштабний фінансовий інструмент. Їхня капіталізація перевищила 270 млрд доларів у 2025 році, а транзакційний обсяг у 2024 році сягнув понад 26 трлн доларів, хоча реальні платежі становлять лише 1% від цієї суми. Стабількоїни, насамперед USDT і USDC, стали особливо затребуваними у кроскордонних транзакціях та в країнах із високою інфляцією або слабкими валютами, створюючи ефект доларизації. Це підштовхує банки та платіжні компанії до необхідності визначати свою стратегію

[9] https://web-assets.bcg.com/25/91/2269153c468ca43684442f055cb0/2025-global-payments-report-sep-2025.pdf

— чи ставати емітентами власних токенізованих депозитів, чи приєднуватися до консорціумів, чи зосереджуватися на інфраструктурних і кастодіальних послугах. Водночас центральні банки продовжують рухатися у напрямі цифрових валют, хоча ентузіазм щодо CBDC знижується у США та Великій Британії, тоді як Китай, ЄС, Індія та ОАЕ зберігають активність. Токенізація охоплює дедалі ширший спектр активів — від державних облігацій та фондів грошового ринку до приватного кредиту та золота — і створює нову архітектуру фінансової інфраструктури.

Окрема частина звіту присвячена агентному штучному інтелекту, який відрізняється від генеративного тим, що здатен діяти автономно, приймаючи рішення та виконуючи транзакції без прямого втручання людини. Очікується, що найближчими роками агентний AI забезпечуватиме понад 50% електронної комерції у США, перетворюючи спосіб взаємодії споживачів і бізнесу з фінансовими сервісами. Він візьме на себе управління особистими фінансами, планування бюджетів, оплату рахунків і навіть автоматичні покупки товарів, поступово перетворюючись на «фінансового асистента». Для банків, еквайєрів та платіжних мереж це означає радикальну зміну конкурентного поля: великі мережі отримають додаткові можливості для монетизації та встановлення стандартів, тоді як еквайєри будуть змушені зміцнювати аналітичні можливості та механізми запобігання шахрайству, аби залишатися релевантними. Проте зростає й ризик довіри та відповідальності: хто відповідатиме у випадку шахрайських транзакцій, здійснених самостійними агентами, і як вибудувати систему комплаєнсу у світі машинних транзакцій — ці питання ще потребують вирішення.

У сфері операційної ефективності звіт наголошує на тому, що «досконалість витрат» перестає бути лише про скорочення видатків і стає інструментом для стратегічного зростання. Оптимізація авторизаційних рішень, динамічна маршрутизація транзакцій, використання генеративного AI в маркетингу та продажах дозволяють підняти маржу на 30–40%, знизити витрати на залучення клієнтів на 60% та вивільнити ресурси для масштабування. Для цього компаніям рекомендується перебудовувати організаційні моделі, зменшувати кількість ієрархічних рівнів, активніше застосовувати автоматизацію та контролювати витрати на хмарні сервіси.

Ще одним глибоким трендом є платформізація торгових сервісів. Програмні платформи на кшталт Shopify, Toast чи Lightspeed поступово трансформуються у «фінансові операційні системи» для малого та середнього бізнесу, пропонуючи не лише обробку платежів, а й аналітику, кредитування, карткові продукти, управління зарплатою, маркетинг і навіть бухгалтерію. Їхня рентабельність

Висновки:

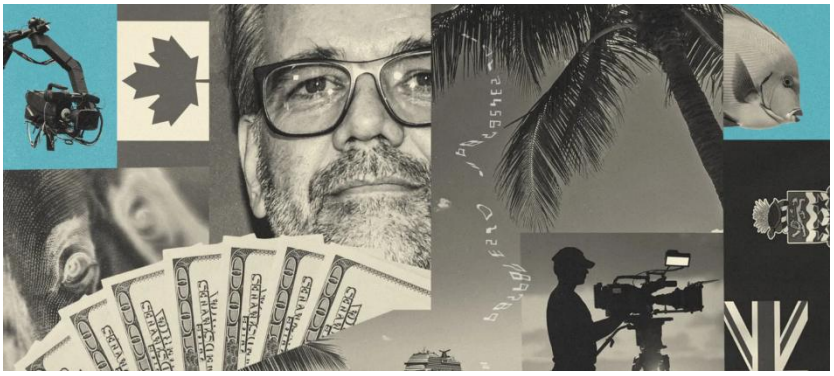
- **Стейблкоїни і токенізовані активи стають ядром нової інфраструктури платежів:** банки мають визначити свою роль у цьому ланцюжку – чи бути зберігачем активів, емітентом, учасником консорціуму чи надавачем інфраструктурних послуг – щоб не втратити ринкові позиції.
- **Агентний AI радикально змінить електронну торгівлю і платіжні сервіси:** компаніям варто вже зараз тестувати низькоризикові сценарії використання автономних агентів, вбудовуючи елементи контролю, безпеки й довіри.
- **Ефективність стає конкурентною перевагою:** інтелектуальна маршрутизація, аналітика на основі генеративного штучного інтелекту та організовані операційні моделі здатні підняти прибутковість на 30–40% і створити ресурс для масштабування бізнесу.
- **Миттєві A2A-платежі — головний вектор глобального зростання:** банкам слід готувати інфраструктуру до роботи у режимі цілодобової доступності 24/7, розвивати міждержавну сумісність і додаткові сервіси (Захист від шахрайства управління ліквідністю), щоб успішно монетизувати цей сегмент.

і темпи зростання вже перевищують показники класичних банків і еквайєрів, і, за прогнозами, до 2027 року до половини доходів у сфері еквайрингу у США формуватимуть вбудовані фінансові сервіси та додаткові (цінові) послуги. Це означає, що традиційні учасники повинні змінювати модель і переходити від масових послуг до нішевих вертикальних екосистем.

Миттєві платежі типу A2A (з рахунку на рахунок) стають глобальним стандартом і символом фінансового суверенітету. У 2024 році їх обсяг зріс на 40%, а частка у роздрібних цифрових платежах досягла 25%. Індія (Єдина платіжна системи, UPI) та Бразилія (Pix) уже довели, що масштаб може перевищити 50% усіх транзакцій, тоді як Європа поступово інтегрує SEPA Instant на рівні ЄС. Наступним етапом стає міждержавна інтеграція: ініціативи Project Nexus, EuroPA, Wero, UPI International та інші можуть створити глобальні «коридори» миттєвих транзакцій, що здатні відвоювати до 30% доходів у сфері міжнародних переказів. Проте для цього необхідна глибока регуляторна координація та розвиток інфраструктури кіберзахисту, адже зростання шахрайства за схемою авторизованих переказів (APP) є суттєвим викликом.

Звіт завершується акцентом на тому, що ризики та комплаєнс тепер є не лише операційним завданням, а й стратегічною вимогою. Санкційні режими, посилення правил кіберстійкості (наприклад, DORA в ЄС та Incident Notification Rule у США), складність у дотриманні вимог у сфері ПВК/ФТ у світі токенізованих грошей та транзакцій за допомогою AI створюють середовище, де здатність до ефективного управління ризиками визначатиме конкурентоспроможність компаній. Усе це формує нову реальність: ті учасники, які зможуть поєднати технологічні інновації з дисципліною витрат і зрілою системою управління ризиками, здобудуть стійку перевагу на світовому ринку платежів у найближче десятиліття.

Гламур проти правди: як індустрія кіно стала інструментом масштабного шахрайства [10]



В історії індустрії незалежного кіно рідко трапляється така суміш глянцю, юридичних лабіринтів і відвертої шахрайської винахідливості, як у справі Вільяма Сантора: його фінансова імперія навколо Productivity Media Inc. (PMI) виглядала зовні як типовий успіх — зірки, зйомки в екзотичних локаціях і щедрі інвестиції — але під поверхнею діяла ретельно спроектована схема, яка за своєю суттю була шахрайством подібним до «схеми Понці» із використанням інструментів фінансування фільмів й офшорної інфраструктури.

Сам Сантор умів створювати образ «легкого спонсора»: щедрі вечері для знімальних груп, персональні інвестиції у проєкти, робочі поїздки з акторами — усе це формувало довіру й знімало підозри, поки внутрішні аудити й кредитори не виявили розриви в документації та фіктивні зобов'язання. Ці обставини описані в журналістському розслідуванні, яке реконструює хронологію розкриття шахрайства та механіку ймовірних зловживань.

Схема ґрунтувалася на законодавчій та практичній особливості світового кінематографу: державні повернення витрат (refundable tax credits), попередні продажі дистрибуції та

[10] https://www.hollywoodreporter.com/movies/movie-features/inside-film-ponzi-scheme-william-santor-1236358644/

механізми «gap financing», що дозволяють переносити фінансування між фазами проєкту. PMI позиціонувала себе як «міст» — організатор коштів, що закриває прогалини бюджету продакшенів. Сам по собі цей бізнес має високу ризикованість, але також — при правильній звітності — прийнятну економіку.

У випадку Сантора модель була пристосована до шахрайської мети: створювалися «imposter corporations» — фіктивні компанії-партнери, підроблялися вебсайти й електронні адреси партнерів, а для частини угод вигадувалися неіснуючі позики та дистрибуційні контракти; ці документи служили підставою для виведення коштів на контрольовані ним рахунки. Потім частина виведених грошей використовувалася для часткових «погашень», щоб підтримати ілюзію платоспроможності та відтермінувати підозри — класична техніка Понці-схем, коли виплати одних інвесторів здійснюються за рахунок притоку від нових вкладників.

Ключові інструменти операції були простими, але ефективними: по-перше, експлуатація складності і непрозорості фінансування кіно — багато транзакцій виглядали правдоподібно саме через їхню юридично-бухгалтерську специфіку; по-друге, географічний та корпоративний арсенал офшорів і рахунків у Карибському басейні, зокрема Grand Cayman, який Сантор перетворив на базу реальних зйомок і, водночас, на майданчик для перерозподілу коштів; по-третє, створення штучного соціального капіталу — гучні вечірки, демонстрація розкоші, видимість успішного інвестора — усе це знижувало скепсис партнерів і постачальників. Зрештою, коли зовнішні аудити й контрагенти почали вимагати підтвердження платежів і виявили невідповідності (наприклад, неоприлюднені або неіснуючі чеки), ланцюг зламався.

Особливо показова психологія схеми: шахрай не лише маскував фінансові потоки, а створив «реальність» — реальні зйомки на Кайманах, зірки, працівники в гуртожитках і побутові витрати — усе це служило прикриттям для бухгалтерських маніпуляцій. Саме поєднання реального продакшену й фіктивних договорів давало змогу легітимізувати частину рухів коштів і відтерміновувати аудит. Як і в класичних Понці, «успіх» тримався на довірі та постійному притоку нових грошей; коли ринок або репутаційні шоки скорочували зовнішні вливи — система луснула. Фінансові наслідки для інвесторів виявилися тяжкими: у документах згадується принаймні $31.7 млн привласнених або неправильно спрямованих коштів, а загальна «портфельна» оцінка PMI у викривленому вигляді сягала десятків мільйонів доларів.

Не менш важливо розглянути елемент співучасті або, як мінімум, «пасивного сприяння» з боку довірених осіб і керівників; у матеріалах фігурує CFO компанії, котрий нібито підписував документи й отримував вигоди (зокрема придбав віллу в Іспанії), що піднімає питання про внутрішні контролі й комплаєнс у приватних фінансових структурах. Тут бачимо типовий ризик: коли одна людина або вузьке коло контролюють доступ до рахунків і одночасно відповідають за аудити та підтвердження угод, виникає проста можливість підтасувати відомості для особистого зиску.

Розпад схеми та його наслідки заслуговують окремого аналізу: зовнішні сигнали — звернення продюсерів, невідповідності у фінансових документах і втручання кредиторів — привели до банкрутства PMI, арештів активів і судових процесів, у тому числі й запровадження тимчасових заборон на розпорядження майном у Кайманах. Підсумком стало руйнування репутації фігурантів, матеріальні втрати для малозабезпечених інвесторів (зокрема канадських пенсіонерів, що вкладали у проєкти через приватні фонди) і, найвірогідніше, кримінальні наслідки для організаторів. Трагічний фінал самого Сантора — смерть, кваліфікована як самогубство на одному з його кайманських об’єктів — додає драматизму, але не відміняє юридичних і фінансових наслідків для постраждалих.

Що показує ця справа для фахівців і практиків? По-перше, вона підкреслює, що галузі зі складною фінансовою структурою (кіно, нерухомість, інфраструктурні проєкти) є потенційними майданчиками для маніпуляцій — особливо там, де діють державні інструменти стимулювання.

Висновки:

- **Використання складних фінансових інструментів у кіногалузі** створює ризик шахрайства, тому необхідні незалежні аудити й прозора верифікація кожного контракту.
- **Соціальний капітал і демонстрація розкоші** не можуть заміняти фінансової перевірки, отже інвесторам слід вважати «успіх» і публічність сигналами ризику, а не гарантіями надійності.
- **Концентрація контролю в руках вузького кола менеджерів** без зовнішнього моніторингу створює умови для масштабних зловживань, тому важливо запроваджувати багаторівневий контроль і ротацію відповідальних осіб.
- **Галузі з високим рівнем креативності та непрозорою бухгалтерією**, як кіноіндустрія, потребують спеціалізованих регуляторних механізмів моніторингу, аби мінімізувати можливості для повторення подібних схем.

По-друге, важливість прозорих і незалежних процедур підтвердження платежів, аудиту третьою стороною і контролю доступу до рахунків не може бути переоцінена; нагляду за CFO та іншими ключовими фінансовими ролями потрібно приділяти окрему увагу. По-третє, репутаційний капітал, який використовують шахраї — показові події, участь відомих персон, публічність — має розглядатися як «сигнал ризику», а не як доказ легітимності. І, нарешті, регулятори та фінансові посередники повинні посилити координацію в питаннях перевірки джерел фінансування, а також розвивати процедури швидкого реагування на «червоні прапори».

ВНУП

Найкращі практики щодо дотримання вимог з ПВК в гральному секторі США [11]

Це вичерпний посібник, призначений для галузі грального бізнесу США, включно з казино, спортивними букмекерами, а також операторами інтерактивних та мобільних ігор, який містить найкращі практики та регуляторні очікування для забезпечення відповідності федеральним вимогам щодо ПВК/ФТ відповідно до Закону про банківську таємницю (BSA). Казино, визначені як «фінансові установи» з 1985 року, зобов'язані впроваджувати та підтримувати ефективну, ризик-орієнтовану Програму ПВК/ФТ, яка відповідає вимогам BSA щодо звітності та ведення обліку.

Програма ПВК/ФТ має починатися з щорічної оцінки ризиків, яка є індивідуальною для кожного казино та враховує географічне розташування, продукти, фінансові послуги та клієнтську базу. У рамках оцінки ризиків слід розглядати такі загрози, як корупція, кіберзлочинність, шахрайство, наркоторгівля та торгівля людьми, а також специфічні для казино схеми, включаючи зловживання кредитними лініями для уникнення подання Звітів про операції з валютою (CTR), використання приватних ігрових салонів, chip-walking (коли злочинець приходить до казино з великою сумою готівки, купує фішки, а потім ходить від столу до столу, створюючи враження, що він має намір зіграти в азартні ігри. Потім він обналічує фішки, які майже не використовував, і гроші повертаються йому чеками казино або банківськими

[11] https://media.licdn.com/dms/document/media/v2/D4E1FAQER7cRauL3O7g/feedshare-document-pdf-analyzed/B4EZmebx_9GUAc-/0/1759299725826?e=1760572800&v=beta&t=jdlJCwCVLM6bGZwkqQxK3av3YJgIMHoG2ddVy-3MAyk

переказами) та маніпуляції з депозитами/виведенням коштів з мінімальною ігровою активністю. Для пом'якшення цих ризиків рекомендується запроваджувати превентивні заходи, такі як встановлення обмежень на викуп квитків Ticket-in, Ticket-Out (TITO) на кіосках, заборона обміну готівки на готівку та посилена перевірка платежів від третіх сторін або високоризикових суб'єктів, як-от юридичні чи благодійні організації.

Ключовим аспектом управління Програмою ПВК/ФТ є чітке визначення ролей: рада директорів та вище керівництво несуть повну відповідальність за дотримання BSA та мають формувати «культуру комплаєнсу», ставлячи його вище за комерційні інтереси. Призначається відповідальний працівник (AML Officer), який відповідає за щоденне дотримання вимог BSA, повинен бути незалежним від операційних відділів, мати відповідний авторитет та підпорядковуватися високопоставленим керівникам, як-от Головний юрисконсульт або Головний комплаєнс-директор.

Важливим елементом є ідентифікація клієнтів та належна перевірка (KYC/CDD). Перед проведенням транзакції, що підлягає звітуванню за BSA, або відкриттям рахунку, казино має зібрати та перевірити повне ім'я, постійну адресу та, якщо застосовно, номер соціального страхування (SSN) клієнта, використовуючи дійсний державний фотодокумент. Для онлайн-ігор, де неможлива особиста перевірка, оператори повинні використовувати не-документарні методи перевірки (third-party electronic ID verification service). Казино також зобов'язані проводити санкційний скринінг в Списку спеціально визначених громадян (SDN List) OFAC під час реєстрації та регулярно після цього, а також запроваджувати гео-блокування для юрисдикцій, що підпадають під всеосяжні санкції. Програма KYC має бути ризик-орієнтованою, вимагаючи посиленої перевірки для клієнтів з підвищеним ризиком, таких як особи, що займають політично значущі посади (PEPs), особи з високим обсягом ігор, або ті, що пов'язані з високоризиковими видами діяльності (наприклад, марихуана чи віртуальні валюти). Критичним є оцінювання Джерела коштів (SoF) для конкретних транзакцій і Джерела багатства (SoW) для підтримки загального рівня гри, використовуючи при цьому публічні записи та можливості обміну

Висновки:

- **Пріоритет незалежного комплаєнсу та ресурсного забезпечення:** Вище керівництво та рада директорів мають забезпечити, щоб відповідальна особа була незалежною, достатньо ресурсно забезпеченим (людськими та технологічними ресурсами) і мав повноваження для затвердження або відхилення рішень щодо подання SAR та обмеження відносин з клієнтами.
- **Застосування динамічної та цілісної належної перевірки:** Необхідно впровадити системи обміну інформацією в рамках усього підприємства (наприклад, між маркетингом, наглядом, операціями та комплаєнсом) для формування повного профілю клієнта, а також проводити обов'язкову, ризик-орієнтовану оцінку Джерела коштів та Джерела багатства для високоризикових клієнтів.
- **Встановлення чітких превентивних заходів для високоризикових транзакцій:** Для зниження ризику структурних операцій або відмивання коштів слід запровадити конкретні обмеження, такі як ліміти на викуп TITO (наприклад, нижче $3000), заборона обміну готівки на готівку та використання гео-блокування / аналізу неможливих поїздок для онлайн-платформ.
- **Суворе дотримання термінів SAR та правил конфіденційності:** Слід підтримувати документовану процедуру розслідування та прийняття рішень щодо SAR, забезпечуючи подання первинних звітів протягом 30 днів з моменту виявлення; необхідно суворо дотримуватись правил конфіденційності, обмежуючи доступ до інформації про SAR лише уповноваженим особам на основі принципу "потрібно знати".

інформацією відповідно до Розділу 314(b) BSA.

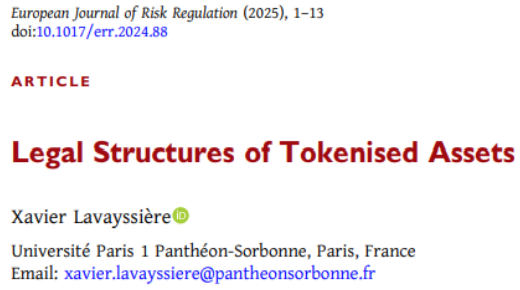
Казино зобов'язані подавати повідомлення про підозрілу діяльність (SAR) у разі виявлення або підозри щодо транзакції або спроби транзакції на суму від 5000 доларів США, яка, серед іншого, пов'язана з незаконними коштами, має на меті уникнути вимог BSA, або не має очевидної законної мети. SAR необхідно подати не пізніше ніж через 30 календарних днів з дати початкового виявлення підозрілих фактів, або до 60 днів, якщо підозрювану особу не ідентифіковано. Для подальшої подібної діяльності використовується «Звіт про продовження діяльності» (Continuing Activity Report), який подається протягом 120 календарних днів з дати останнього SAR. Важливою є конфіденційність SAR, їхнє розкриття суворо обмежене, з можливістю обміну інформацією лише в межах підприємства в США за принципом "потрібно знати" та з уповноваженими регуляторами.

Звітування про операції з валютою (CTR) є обов'язковим для кожної операції з готівкою (внесення або виведення), що перевищує $10 000 протягом будь-якого ігрового дня. Кілька операцій, здійснених однією особою або від її імені, підлягають сукупному звітуванню. CTR має бути поданий протягом 15 календарних днів.

Окрім внутрішніх процедур, казино повинні проводити незалежне тестування своєї Програми ПВК/ФТ принаймні щорічно, яке охоплює всі елементи програми, включаючи KYC, моніторинг транзакцій, звітність SAR та CTR. Персонал казино повинен проходити постійне, ризик-орієнтоване та специфічне для відділів навчання, що охоплює вимоги BSA, червоні прапорці, процедури звітності CTR/SAR та конфіденційність SAR, а також ознайомлення з ознаками торгівлі людьми.

Рекомендовані та навчальні матеріали

Правові конструкції токенізованих активів [12]


European Journal of Risk Regulation (2025), 1–13
doi:10.1017/err.2024.88

ARTICLE

Legal Structures of Tokenised Assets

Xavier Lavayssière

Université Paris 1 Panthéon-Sorbonne, Paris, France
Email: xavier.lavayssiere@pantheonsorbonne.fr

CAMBRIDGE UNIVERSITY PRESS

Стаття присвячена фундаментальному аналізу правових конструкцій токенізованих активів і пропонує систематизацію підходів до їхньої класифікації. Автор, виходячи з розриву між технологічними можливостями блокчейн- та DLT-систем і правовою визначеністю активів, розробляє таксономію, яка дозволяє зрозуміти, наскільки надійним є юридичний зв'язок між токеном та активом, що лежить в його основі. Визначено три ключові категорії: пряма токенізація, коли токени є первинною формою активу та наділені юридичною силою (наприклад, цифрові облігації, CBDC, токенізовані акції фондів); непряма токенізація, коли створюється проміжна юридична структура (SPV – Special Purpose Vehicle, траст, фонд), а токени відображають права на актив, що залишається у традиційній формі (наприклад, стейблкоїни, токенізована нерухомість чи кошти фондів); та неповна токенізація, де токени виступають лише "цифровими двійниками" і не забезпечують прав власності чи вимог.

У роботі наголошується, що ефективність токенізації безпосередньо залежить від якості юридичного ланцюга між власником токена та самим активом. Якщо токен справді прирівнюється до активу, його передача означає передачу права власності, що створює високу

[12] https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/legal-structures-of-tokenised-assets/5D3537D89F9AD858339424E1D60D7C43

правову визначеність і полегшує операції. У випадку непрямої токенізації юридична зв'язка ускладнюється додатковими рівнями (SPV, фонди), що породжує ризики непрозорості й можливих проблем у разі банкрутства або спорів. Неповна токенізація, хоч і не створює юридично обов'язкових прав, може застосовуватися для підвищення ефективності обліку та процесів управління, проте завжди вимагає паралельного існування традиційних інфраструктур.

Стаття також розглядає умови реалізації прямої токенізації: нормативне визнання цифрової форми активів (наприклад, французький ордонанс 2017 року чи німецький закон eWpG 2021 року), забезпечення юридичної передачі прав (особливо для цінних паперів та корпоративних прав) та наявність адекватної цифрової інфраструктури (реєстри нерухомості, ідентифікаційні системи, KYC-рішення на блокчейні). У контексті непрямої токенізації особлива увага приділена стейблкоїнам, які виступають проміжною формою, заснованою на резервах у традиційних грошових чи фінансових інструментах, і водночас мають претензію на роль "нативних" цифрових грошей. Автор зазначає, що саме у цій сфері спостерігається найбільший розрив між технологічною реалізацією та правовою визначеністю, а регулювання (наприклад, у рамках MiCA в ЄС) відіграє ключову роль у закритті цієї прогалини.

Окремий розділ присвячено аналізу ризиків. Автор виділяє моделі володіння (bearer чи registrar), співвідношення фактичного володіння токеном і юридичного права власності, а також питання правових колізій у випадках кроскордонних операцій і банкрутств. Технічна сумісність (composability) токенізованих активів, яка дозволяє створювати похідні токени ("wrapped assets", синтетичні інструменти), розглядається як джерело інновацій і одночасно як фактор нарощування системних ризиків. Використання токенізованих активів у DeFi-протоколах і для коллатералізації розширює можливості фінансових ринків, але створює виклики прозорості, ліквідності та правового захисту у випадку кризи.

У висновках підкреслюється, що токенізація здатна докорінно змінити підходи до передачі та управління активами, але успіх цих змін повністю залежить від юридичної стійкості обраної моделі. Прямі й непрямі форми токенізації можуть наділяти токени правовою визначеністю, тоді як неповні формати залишають їх у ролі допоміжних цифрових інструментів. Для збереження довіри учасників ринку й уникнення системних ризиків кожна нова інноваційна "ланка" у ланцюзі правових відносин має спиратися на міцні правові основи та прозорі регуляторні рамки.

Інші новини

Супермагістраль кокаїну: міждержавні виклики ірландського кейсу [13]

Стаття BBC описує одну з найбільших операцій європейських правоохоронців, яка стала одним із найгучніших прикладів протистояння між європейськими державами та транснаціональними наркокартелями. Ця операція, проведена ірландськими правоохоронцями у взаємодії з міжнародними партнерами, завершилася арештом восьми осіб та винесенням сукупного вироку у 129 років. Проте журналісти наголошують: цей успіх, попри символічну вагу, є радше винятком, ніж правилом, і він лише підтверджує, наскільки масштабною та стійкою залишається система трансатлантичного наркотрафіку.

Сьогодні Європа дедалі більше виступає кінцевим споживачем кокаїну, і тенденції останніх років демонструють стабільне зростання попиту. Великобританія вже зараз споживає

[13] https://www.bbc.com/news/articles/c5yvplyrrwno

щонайменше 117 тонн кокаїну на рік, що перетворює її на один із найбільших ринків у світі. Паралельно спостерігається стрімке зростання смертності, пов'язаної з вживанням цього наркотика: збільшення передозувань і довгострокових наслідків для охорони здоров'я створює ситуацію, коли наркотик перестає бути лише кримінальною проблемою, а стає суспільною кризою. Це означає, що будь-які успіхи правоохоронців на морі неминуче матимуть обмежений ефект, якщо не супроводжуватимуться системною внутрішньою політикою у сфері попиту.

Журналісти особливо наголошують на діяльності Maritime Analysis and Operations Centre (MAOC), яке займається моніторингом морських шляхів і координацією операцій із перехоплення наркотиків. Щодня аналітики відстежують сотні суден, використовуючи дані розвідки, супутникові знімки та координацію з національними флотами. Але ресурсні можливості центру не відповідають масштабам виклику: десятки суден, які потрапляють у поле зору, залишаються неперехопленими, адже бракує кораблів і персоналу для фізичного затримання. Це створює ситуацію «дикого заходу на морі», де картелі користуються кожною шпариною у міжнародній безпеці, а наявність нових схем транспортування, як-от перевантаження з «материнських» суден на дрібніші човни у відкритому морі, ускладнює ідентифікацію та перехоплення.

Ірландія у цій історії виступає слабкою ланкою, вразливість якої підкреслює дисбаланс між ресурсами держави і можливостями картелів. Військово-морські сили країни мають усього два придатні до використання кораблі, що явно недостатньо для контролю над величезною виключною морською економічною зоною. До цього додається фактор відкритого кордону з Великою Британією, який дозволяє наркотрафіку без значних перешкод проникати в глибину європейського ринку. Як наслідок, Ірландія перетворюється на своєрідного «троянського коня» — зручний і майже неконтрольований вхідний пункт для картелів, які шукають альтернативні маршрути, минаючи посилений контроль у портах Західної Європи.

У статті наводяться приклади того, як картелі постійно адаптуються до змін. Якщо раніше маршрути кокаїну переважно проходили через Іспанію та Португалію, то сьогодні дедалі активніше використовується Ірландія, що має слабшу інфраструктуру контролю. Цей зсув маршрутів пояснюється тим, що будь-який тиск на одній ділянці «супермагістралі» неминуче призводить до появи нових вузлів у менш захищених точках. Таким чином, боротьба з наркоторгівлею набуває характеру «гри», де картелі постійно виграють за рахунок гнучкості та масштабності ресурсів.

Зростання виробництва кокаїну в Південній Америці створює додатковий структурний тиск. Колумбія, Перу та Болівія — традиційні країни-виробники — нині демонструють рекордні врожаї коки та обсяги виробництва. Це означає, що навіть рекордні конфіскації в Європі практично не впливають на загальний обсяг постачання, адже картелі оперують у категоріях десятків і сотень тонн. Кожна перехоплена партія, навіть у 2–3 тонни, залишається лише частковим успіхом на фоні безперервного потоку.

Стаття також розкриває суспільно-політичний вимір цієї проблеми. Для Ірландії арешт судна MV Matthew став поштовхом для дискусії про необхідність збільшення оборонного бюджету та розбудови флоту. Але навіть ці кроки — за умови їхньої реалізації — не здатні радикально змінити ситуацію, адже картелі за масштабом доходів і гнучкістю логістики можуть конкурувати з малими державами. Боротьба за контроль над «супермагістраллю кокаїну» набуває характеру геополітичного виклику, у якому суверенні країни змушені діяти спільно, інакше вони приречені програвати у боротьбі з приватними кримінальними «корпораціями». Поки попит зростає, а держави реагують переважно точково, картелі зберігатимуть свою стратегічну перевагу.

Олігарх у вигнанні: як Ілан Шор створив криптоімперію для обходу санкцій [14]

Витік документів про діяльність молдовського олігарха-втікача Ілана Шора, який уже багато років перебуває під санкціями та звинувачується у відмиванні мільйонів доларів, демонструє надзвичайно небезпечний і водночас витончений приклад того, як поєднання кримінального досвіду, політичних зв'язків та сучасних фінансових інструментів створює цілком нову форму паралельної економічної системи.

Шор, відомий насамперед як головний фігурант «крадіжки століття» у Молдові, де було виведено з банківської системи близько $1 млрд, використав свою репутацію та підтримку Кремля для побудови компанії A7, яка стала платформою обходу санкцій проти Росії. Витік показує, що він не просто знайшов спосіб уникати міжнародних обмежень, а створив цілу екосистему, яка поєднує фінанси, криптовалюти, офшорні компанії, IT-структури та пропагандистські ресурси.

У центрі цієї системи — стейблкоїн A7A5, який використовується як альтернативний канал платежів для російських імпортерів товарів подвійного призначення, таких як мікроелектроніка, чіпи, оптика чи компоненти для дронів. Оскільки санкційні режими західних країн перекрили більшість офіційних каналів торгівлі, саме криптовалюти стали зручною оболонкою для трансакцій, які складно простежити або заблокувати.

A7A5 фактично став «тіньовим SWIFT» для російських компаній, які можуть розраховуватися через посередницькі структури у Центральній Азії чи на Близькому Сході, маскуючи реальних одержувачів платежів. У схемі задіяні банки та брокери з Киргизстану, які легалізують частину цих потоків і роблять їх зовні правдоподібними для партнерів. Таким чином, модель Шора — це не звичайне відмивання коштів, а довгостроковий інструмент створення паралельної фінансової системи, яка працює на забезпечення російського військово-промислового комплексу.

Особливе значення має кадровий склад A7. Витік демонструє, що Шор зміг залучити до керівництва компанією колишніх топ-менеджерів найбільших російських банків, включаючи Сбербанк, ВЕБ і «Русский стандарт». Це свідчить про те, що йдеться не про маргінальну структуру, а про системно вибудувану платформу, яка користується довірою з боку російських фінансових еліт. Присутність таких кадрів забезпечує професійний менеджмент, контроль ліквідності та здатність конструювати схеми, які важко розплутати західним регуляторам. Це також пояснює, чому Кремль демонстративно підтримує діяльність A7: відкриття їхнього процесингового центру у Владивостоці відбулося особисто за участі Володимира Путіна та голови «Промсвязьбанку» Петра Фрадкова. Тобто ми маємо справу не лише з приватною ініціативою корумпованого олігарха, а з частиною офіційної стратегії Росії з обходу санкцій.

Ширший контекст цієї історії показує, що Шор будує не лише фінансову інфраструктуру, а й політичний і медійний плацдарм. Частина його компаній у Молдові та сусідніх країнах фінансує проросійські медіа та громадські організації, які займаються пропагандою й підкупом виборців. Це означає, що схема A7 має подвійну функцію: з одного боку, вона підтримує російську економіку та військову машину, з іншого — фінансує політичні проекти, які дестабілізують демократичні процеси у країнах, що межують з ЄС.

[14] https://reporter.london/?p=1484

Для Молдови ця загроза є екзистенційною: Шор уже давно намагається використати своє фінансове становище для маніпуляції виборами й підриву євроінтеграційного курсу країни. Водночас міжнародні санкції, накладені США, ЄС і Великою Британією на A7 та її афілійовані структури, лише частково стримують діяльність компанії, адже її операції значною мірою здійснюються у юрисдикціях із низьким рівнем контролю та в криптосекторі, який залишається фрагментарно врегульованим.

Ще однією ключовою деталлю витоку є залучення московської IT-компанії Anykey, яка забезпечує технічну підтримку A7 та пов'язаних платформ. Через неї здійснюється цифрове адміністрування транзакцій, управління електронними гаманцями та навіть внутрішні комунікації. Цікаво, що Anykey одночасно обслуговує кілька структур, пов'язаних із Шором, включаючи проросійську НГО «Євразія». Це підкреслює взаємопов'язаність фінансових, інформаційних та політичних активів у «імперії Шора». За оцінками, близько 500 людей у різних країнах працюють у цій системі, і важко провести чітку межу між законним бізнесом та злочинною діяльністю. У цьому сенсі модель нагадує гібридні схеми російської розвідки, де поєднуються легальні структури та тіньові операції.

Таким чином, історія з A7 і діяльністю Ілана Шора демонструє, що ми стоїмо на порозі нового етапу глобальної фінансової злочинності. Якщо раніше ключовим інструментом ухилення від санкцій були офшори й підставні компанії, то тепер у гру вступають стейблкоїни й криптовалютні системи, які дозволяють створювати фактично незалежні платіжні екосистеми. У цьому випадку схема перестає бути локальним шахрайством і стає елементом геополітичної стратегії. Захід стикається з ситуацією, коли санкції втрачають частину своєї ефективності через появу альтернативних фінансових мереж, які працюють у паралельному правовому й технологічному просторі. Кейс Шора — це попередження, що для боротьби з подібними схемами потрібна нова архітектура міжнародного фінансового контролю, яка враховуватиме не лише банки та офшори, а й криптовалютні інструменти, пов'язані з політично мотивованими злочинцями.

Висновки:

- **Використання стейблкоїнів як альтернативних каналів платежів** доводить необхідність міжнародного моніторингу криптовалютних операцій у режимі реального часу.
- **Залучення колишніх топ-менеджерів російських банків** до схем обходу санкцій вимагає створення глобальних чорних списків фінансових фахівців і суворішого контролю за їхньою діяльністю.
- **Взаємопов'язаність фінансових, медійних та політичних структур** у схемі Шора показує потребу комплексного підходу, де санкції поєднуються з протидією дезінформації та політичному підкупу.
- **Щоб зберегти ефективність санкційної політики**, країнам слід інтегрувати криптовалютний сектор у міжнародну систему AML/CFT і забезпечити обов'язкову звітність для провайдерів стейблкоїнів.

У підсумку можна сказати, що схема Шора є не лише злочинною аферою, а й індикатором ширших змін у глобальній економіці злочинності. Вона доводить, що кримінальні угруповання та державні структури можуть зливатися в єдину систему, використовуючи криптовалюти як універсальну зброю проти санкційного тиску. Водночас ця історія показує межі ефективності традиційних інструментів контролю й підкреслює нагальну потребу у міжнародній координації, нових технологічних рішеннях і розробці правових рамок для моніторингу цифрових фінансових потоків. Інакше світ ризикує зіткнутися з появою паралельних «тіньових SWIFT», які забезпечуватимуть стабільне фінансування авторитарних режимів і їхніх військових кампаній.

Для загального розвитку

Чому глобальна система протидії фінансовим злочинам не працює [15]

Аналітична стаття, підготовлена дослідниками з RUSI, ставить під сумнів ефективність усієї глобальної архітектури боротьби з фінансовими злочинами, створеної під егідою FATF і національних регуляторів. Автори наголошують: попри понад три десятиліття роботи та безліч рекомендацій, ця система перетворилася на механізм формальних процедур, який витрачає колосальні ресурси, але фактично не досягає головної мети — запобігання відмиванню коштів і протидії фінансуванню злочинності. Нинішня модель нагадує складну бюрократичну конструкцію, яка орієнтована не на реальні результати, а на «tick-box compliance» — виконання формальних вимог без оцінки їхньої дієвості. Витрати приватного сектору на комплаєнс у сфері AML щороку перевищують $200 мільярдів, проте обсяг незаконних фінансових потоків у світі залишається стабільно високим, а в деяких регіонах навіть зростає.

Одним із найяскравіших прикладів неефективності є система Suspicious Activity Reports (SAR). У теорії це мало б стати інструментом швидкого реагування — банки та інші фінансові установи повідомляють про підозрілі транзакції, а правоохоронні органи використовують ці дані для розслідувань. На практиці SAR перетворилися на «потік паперу», що рідко призводить до реальних справ. Дослідження, наведені у статті, показують, що лише один із 16 SAR в Італії ставав корисним у вже наявних кримінальних провадженнях, і лише один зі 99 стимулював нове розслідування. Тобто більшість звітів або не містять реальної цінності, або подаються «про всяк випадок» — щоб інституція перестрахувалася від штрафів за неподачу. Це породжує парадокс: інструмент, покликаний підвищити ефективність боротьби з фінансовими злочинами, став доказом його формалізованої неспроможності.

Проблема має глибші корені у системі стимулів приватного сектору. Для банків і великих фінансових корпорацій головним ризиком стають не самі злочинні транзакції, а можливі штрафи від регуляторів у разі недотримання процедур. Тому стратегія часто зводиться не до пошуку справжніх схем відмивання, а до побудови бюрократичного щита: подати якнайбільше звітів, формально закрити всі перевірки і створити враження, що система працює. Більше того, дослідження 2022 року показало, що 79% керівників у сфері комплаєнсу в Європі, США та Азії були готові платити багатомільйонні штрафи, ніж вкладати ресурси у глибоку перебудову власних механізмів контролю. Це означає, що у нинішніх умовах чесність стає конкурентним недоліком: компанії, які намагаються справді викривати злочинні транзакції, витрачають більше ресурсів і стикаються з репутаційними ризиками, тоді як ті, хто обирає формалізм, продовжують працювати й зберігати конкурентоспроможність.

Автори закликають до радикального перегляду моделі глобальної протидії фінансовим злочинам. Вони підкреслюють, що нинішній підхід базується на припущенні, що достатньо уніфікованих стандартів FATF і регулярних оцінок взаємної відповідності для ефективної боротьби. Насправді ж кримінальні мережі виявилися значно гнучкішими: вони адаптуються до регуляції, використовують прогалини національних законодавств і виграють від відсутності координації. Географічна та правова фрагментація стає найбільшим союзником злочинців: дані залишаються розрізненими, країни обмежують доступ до фінансової інформації, а будь-які міжнародні розслідування буксують через бюрократію і політичні розбіжності. У цьому сенсі «глобальна система» існує лише на папері — фактично ж кожна країна бореться з тіньовими потоками самотужки, у кращому випадку ділиться обмеженою інформацією з партнерами.

[15] https://www.rusi.org/explore-our-research/publications/commentary/global-anti-financial-crime-system-broken

Замість збереження цієї неефективної архітектури, експерти пропонують шукати нові моделі. Прикладом можуть стати публічно-приватні партнерства (Public-Private Partnerships), коли держави, банки і технологічні компанії обмінюються даними у режимі реального часу, або спеціалізовані анти-шахрайські центри (Anti-Scam Centres), які працюють на стику фінансових і кібер-злочинів, блокуючи схеми ще до того, як вони завдадуть значної шкоди. Це доводить, що більш вузькі, спеціалізовані й технологічні моделі можуть бути ефективнішими, ніж гігантська й громіздка глобальна система.

Автори наголошують, що ключем є зміна парадигми оцінки ефективності: замість підрахунку SAR чи кількості виконаних вимог слід оцінювати реальний вплив — кількість заблокованих потоків, заморожених активів і розкритих злочинних мереж.

У підсумку, стаття малює картину структурної кризи. Глобальна система боротьби з фінансовими злочинами в її нинішньому вигляді працює за інерцією: витрачає мільярди, але дає мізерний результат, формально демонструє «відповідність стандартам», але фактично програє злочинним мережам, які діють у режимі швидкості й інновацій.

Вихід із цієї кризи, на думку авторів, можливий лише за умови сміливих рішень: перегляду стимулів для бізнесу, зняття бар'єрів для міжнародного обміну даними та створення систем, орієнтованих на якість результату, а не кількість процедур. Інакше фінансова злочинність залишатиметься тією сферою, де злочинці завжди на крок попереду держави, а глобальні правила залишатимуться ширмою, за якою приховується безсилля усього міжнародного співтовариства.

Висновки:

- **Система SAR має бути реформована** з акцентом на якість та аналітичну цінність звітів, а не їхню кількість, щоб реально підтримувати розслідування.
- **Необхідно змінити систему стимулів** для приватного сектору, створивши умови, за яких прозорість і співпраця з регуляторами будуть вигіднішими за сплату штрафів.
- **Міжнародна координація** повинна перейти від декларацій до створення технологічних платформ обміну фінансовими даними у режимі реального часу.
- **Країнам слід інвестувати** у нові партнерства і спеціалізовані центри протидії шахрайству, які вже довели свою ефективність у Сінгапурі та Австралії.

Ваша думка важлива!

1. Чи є необхідним негайне запровадження спеціалізованої кримінальної норми щодо мулів, і як ця норма має бути побудована, щоб забезпечити баланс між покаранням організаторів та реінтеграцією осіб, які втягнулися в схему несвідомо, водночас стимулюючи СПФМ до впровадження досконаліших інструментів моніторингу, що використовують технології?
2. Аналіз RUSI виявив, що глобальна система ПВК/ФТ страждає від "формального комплаєнсу", а більшість звітів SAR не мають реальної аналітичної цінності для правоохоронців. Які конкретні кроки мають зробити українські регуляторні та правоохоронні органи, щоб змінити парадигму оцінки ефективності: замість підрахунку кількості SAR перейти до оцінки реального впливу — кількості заблокованих незаконних потоків, заморожених активів та розкритих схем? Чи можуть публічно-приватні партнерства (PPP) з обміну даними, як пропонується у міжнародному досвіді, стати ключем до цієї трансформації?
3. Яким чином Україна, маючи власний потенціал видобутку літію, титану та рідкоземельних елементів, може убезпечити свої ланцюги постачання від корупції та кримінального впливу, враховуючи виклики воєнного часу та післявоєнного відновлення?
4. Чому попри зусилля ООН та інших інституцій доступ до правосуддя й надалі залишається обмеженим для мільйонів людей, і які інноваційні моделі правової допомоги могли б бути впроваджені в Україні для подолання проблеми затяжного попереднього ув’язнення та недовіри до судів?
5. Які стимули можна створити для українських банків і фінансових компаній, щоб прозорість та співпраця з державою стали вигіднішими за сплату штрафів чи мінімальне дотримання формальних вимог?
6. Які механізми контролю та прозорості варто впровадити у співпраці держави та приватних кіно-виробників, щоб залучення інвестицій у культуру не перетворювалося на інструмент відмивання коштів?

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-2025-40

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

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