Методологічний бюлетень

Серійний номер: МінФін-AML-2025-46

Листопад 2025

“Перемога починається з першого кроку”

Роберт Шуллер

Мета

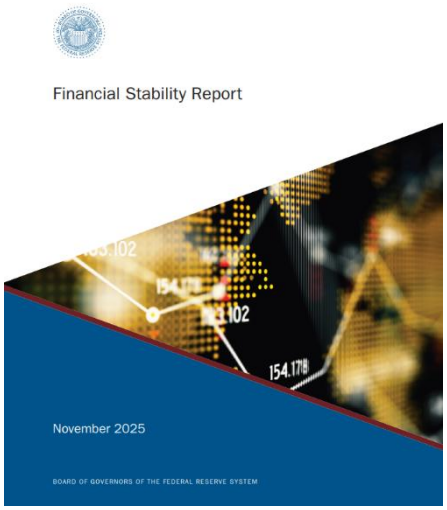
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Звіт ФРС про фінансову стабільність [1]



Документ є комплексною аналітичною оцінкою ФРС США щодо поточного стану фінансової стабільності країни, заснованою на даних до 23 жовтня 2025 року. У звіті подано системний огляд ключових вразливостей фінансової системи, динаміки ринків активів, боргового навантаження бізнесу та домогосподарств, рівня плеча у фінансовому секторі й ризиків фінансування, а також визначено потенційні короткострокові шоки, здатні взаємодіяти з накопиченими вразливостями та посилювати фінансовий стрес. Фундаментальним елементом рамки є розмежування між “шоками” та “вразливостями”: перші складно передбачити, тоді як другі накопичуються структурно та піддаються моніторингу. Звіт концентрується на чотирьох основних категоріях вразливостей: переоціненість активів, боргові

[1] https://www.federalreserve.gov/publications/files/financial-stability-report-20251107.pdf

навантаження бізнесу й домогосподарств, левередж фінансового сектору, ризики ліквідності та фондування.

У першому напрямі — valuation pressures — документ фіксує підвищені оцінки активів: фондові індекси знову наблизилися до верхніх меж історичних діапазонів цін до прибутків, премія за ризик у акціях знизилася до мінімумів 20-річного періоду, корпоративні спреди звузилися до рівнів нижче медіан, а ситуація на ринку державних цінних паперів стабілізувалася після стрибків волатильності в квітні 2025 року. Ринки нерухомості демонструють змішану картину: житлова нерухомість залишається переоціненою відносно орендних доходів, тоді як комерційна нерухомість лише стабілізується після попереднього глибокого падіння цін та зберігає ризики, пов'язані з рефінансуванням значних обсягів боргу у 2025–2026 рр.

У блоці щодо позик бізнесу та домогосподарств підкреслюється, що сукупний приватний борг відносно ВВП знизився до мінімумів за два десятиліття. Стан корпоративних балансів переважно стійкий: левередж публічних компаній дещо підвищений, але здатність обслуговувати борг залишається сильною завдяки стабільним показникам interest coverage. Проте слабкіші компанії — малі підприємства та ризикові приватні позичальники — стикаються зі зниженням боргової стійкості через удорожчання обслуговування боргу та більшу залежність від плаваючих ставок. У секторі домогосподарств ризики помірні: значна частка позичальників має високі кредитні рейтинги, іпотечні дефолти мінімальні завдяки великим подушкам домашнього капіталу, проте делінквентність за автокредитами та кредитними картками залишилася вище довгострокових медіан. Особливо виділяється зростання прострочень за кредитними картками серед субпраймових позичальників та різке підвищення прострочень за студентськими кредитами після відновлення обов'язкових платежів.

Третій блок — левередж фінансового сектору — демонструє, що хоча банківська система загалом стійка з високими нормативами CET1, у секторі зберігаються суттєві ризики. Уразливості формуються переважно поза банками: хедж-фонди мають рекордно високий левередж, активи під управлінням та обсяги позикових позицій зросли у різних торгових стратегіях, включно з використанням деривативів та операціями на ринку казначейських паперів. Левередж

Висновки:

- **Переоцінка активів суттєво підвищує ризики раптової корекції.** Фондові ринки, корпоративні облігації та житлова нерухомість залишаються істотно переоціненими, що вимагає підвищеної уваги регуляторів і учасників ринку до ризику різкого падіння цін та вторинних ефектів для фінансових інституцій і домогосподарств.
- **Уразливості концентруються серед малих підприємств і ризикових домогосподарств.** Попри загальну стійкість корпоративного та іпотечного портфеля, малі фірми та субпраймові позичальники демонструють погіршення боргової стійкості — це вимагає посиленого моніторингу кредитних стандартів і потенційних втручань для запобігання зростанню неплатежів.
- **Небанківські установи є ключовими носіями системного левереджу.** Хедж-фонди та страхові компанії формують зростаючі структурні ризики через рекордне плече, складні ринкові позиції та потенційний вплив на ліквідність ринку державних цінних паперів. Необхідна подальша макропруденційна координація на рівні FSOC.
- **Ризики фондування стабілізовані, але можуть швидко матеріалізуватися при шоках.** Зменшення обсягу незастрахованих депозитів у банках знижує ризики відпливів, однак сегменти короткострокового фінансування (зокрема окремі інвестиційні фонди і страховики) потребують постійного нагляду через їхню чутливість до ринкових шоків.

страхових компаній життя перебуває у верхньому квартилі історичного діапазону. Водночас банки несуть значні нереалізовані збитки в портфелях цінних паперів, особливо HTM і AFS, що підвищує чутливість до змін довгострокових ставок. Незважаючи на низький регуляторний левередж брокер-дилерів, їхня здатність підтримувати ліквідність на пікових навантаженнях залишається критичною вразливістю для ринку казначейських паперів.

У частині funding risks звіт підкреслює загалом помірний рівень ризику. Активи в грошових фондах (особливо державних MMFs) продовжили зростати, зберігаючи відносно низьку схильність до раптових вилучень. Банки суттєво зменшили залежність від незастрахованих депозитів порівняно з піками 2022–2023 рр., що підвищує стійкість системи. Разом з тим страховики життя збільшили обсяг нетрадиційних зобов'язань, хоча їх частка залишається малою. Загальна оцінка ризиків — стабільна, але з окремими сегментами, які можуть бути вразливими при стресі.

Заключна частина документа присвячена короткостроковим ризикам, які можуть слугувати каталізаторами стресу. За результатами опитування ринку найчастіше згадуються політична невизначеність, геополітичні ризики, стійка інфляція, а також можливе різке зниження цін активів, включаючи сценарій «перелому» в настроях щодо штучного інтелекту на ринках.

Документ підкреслює важливість продовження моніторингу системних вразливостей, удосконалення інструментів нагляду, застосування макропруденційних важелів, таких як контрциклічний буфер, та поглиблення взаємодії з іншими регуляторами для підтримання фінансової стійкості США.

Взаємодія монетарної та фіскальної політики після інфляційного шоку [2]

Документ ЄЦБ присвячений всебічному аналізу взаємодії монетарної та фіскальної політики в умовах різкого інфляційного шоку, який віддзеркалює події, характерні для періоду 2021–2022 років у Єврозоні. Використовуючи глобальну DSGE-модель EAGLE, автори досліджують, як різні варіанти реакції центрального банку та різні види дискреційних фіскальних заходів впливають на траєкторії інфляції, економічної активності та державного боргу в гіпотетичній структурі валютного союзу, що складається з країн із низьким і високим рівнем боргового навантаження. Звіт наголошує, що початковий інфляційний шок у моделюванні є глобальним cost-push-шоком, який підвищує витрати виробництва та призводить до зростання цін при одночасному падінні випуску — саме ця конфігурація є найскладнішою для поєднання монетарних і фіскальних інструментів, оскільки політики вимушені обирати між ціновою стабільністю та підтримкою економічної активності.

Автори виходять із того, що в умовах високої інфляції центральний банк стикається із класичною дилемою: агресивне підвищення ставок швидше повертає інфляцію до цільового рівня, але водночас поглиблює падіння економічної активності та збільшує державний борг через підвищення вартості запозичень; натомість затримка з підвищенням ставок може зменшити падіння економіки зараз, але водночас закріплює високу інфляцію та підвищує ризик того, що люди перестануть вірити у повернення цін до нормального рівня — тобто очікування "відірвуться" від цілі центрального банку. Використані сценарні симуляції показують, що

[2] https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3145~0849e36e60.en.pdf

трендова інфляція на піку шоку може зрости на 1 п.п., а вибір реакції монетарної політики суттєво визначає амплітуду та тривалість подальшої макроекономічної динаміки. При цьому механізм передавання впливу політики в моделі враховує різні категорії домогосподарств — Рікардіанські та нерікардіанські (ліквідно обмежені), — що дозволяє розрізняти їхню реакцію на податкові та трансфертні заходи.

Фіскальний компонент документа охоплює аналіз широкого набору заходів, які застосовували країни Єврозони для пом'якшення інфляційних наслідків для населення й бізнесу — від субсидій та зниження непрямих податків до підвищення соціальних виплат і державних інвестицій. Модель демонструє важливу властивість: більшість антиінфляційних фіскальних інтервенцій мають або тимчасовий, або другорядний ефект на інфляцію, але суттєво впливають на споживання. Так, зниження податків на споживання короткочасно знижує інфляцію, однак через стимулювання попиту ефект швидко вичерпується, а по завершенні заходу повернення ставки ПДВ створює протилежний імпульс. Підвищення трансфертів, особливо нецільових, підтримує споживання ліквідно обмежених домогосподарств, але водночас посилює інфляційний тиск, примушуючи центральний банк до більш жорсткої реакції. На відміну від цього, збільшення державних інвестицій, хоча й спричиняє незначний початковий інфляційний ефект, надалі посилює потенційний випуск і сприяє зниженню інфляції в середньостроковій перспективі через підвищення продуктивності.

Ключовим аспектом документа є детальний опис того, як поєднання монетарних і фіскальних рішень впливає на динаміку державного боргу. Модель чітко демонструє, що агресивна реакція монетарної політики приводить до значно більших витрат на обслуговування боргу, особливо у країнах із високим рівнем заборгованості, де так званий ефект "snowball" (різниця між ставкою за боргом та зростанням ВВП) стає критичним. Навпаки, затримка реакції дає більше «фіскального простору» завдяки номінальному ефекту інфляції та нижчій вартості обслуговування боргу, але потенційно поглиблює проблему тривалості інфляційного періоду. Фіскальні заходи, своєю чергою, по-різному впливають на борг: збільшення інвестицій має найменший негативний ефект завдяки спадному внеску до боргового співвідношення через розширення ВВП; цільові трансферти також є ефективними, оскільки впливають на найбільш вразливі домогосподарства за значно меншої бюджетної вартості; зниження ПДВ та нецільові трансферти є

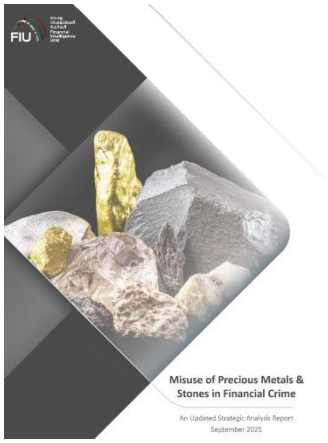
Висновки:

- **Оптимальна фіскально-монетарна комбінація — агресивна, але недеструктивна реакція ставок + тимчасові таргетовані фіскальні заходи.** Агресивне підвищення ставок швидко приборкує інфляцію, але істотно збільшує державний борг; натомість таргетовані трансферти мінімізують фіскальні витрати і не провокують надмірного інфляційного тиску.
- **Зниження ПДВ як антиінфляційний засіб має лише короткочасний і суперечливий ефект і не повинно застосовуватися як основний інструмент.** Ефект триває недовго, а скасування заходу створює зворотний інфляційний імпульс; одночасно цей захід суттєво погіршує баланс бюджету.
- **Інвестиційна фіскальна відповідь є найбільш ефективною в середньостроковому горизонті.** Державні інвестиції підвищують продуктивність, що зменшує інфляційний тиск і пом'якшує борговий ефект; саме це робить їх найкращим варіантом серед фіскальних стимулів.
- **Країнам із високим борговим навантаженням потрібен ще обережніший баланс політик.** Агресивна монетарна реакція в таких країнах створює сильніший «ефект сніжного кому» в обслуговуванні боргу, що може швидко зменшити фіскальний простір; у таких умовах сувора таргетованість фіскальних заходів є критичною.

найбільш фіскально затратними.

Окремо автори проводять тестування моделі. Показано, що зменшення жорсткості цін робить початкову інфляційну реакцію різкішою і вимагає сильнішої монетарної відповіді, тоді як збільшення жорсткості дозволяє згладити динаміку, але ціною більш затяжного коригування. Продуктивність державних інвестицій також має істотний вплив: за нижчої ефективності стимулюючий вплив на ВВП згасає, а боргове навантаження зростає подібно до інших заходів. Загальні висновки документа підкреслюють, що в умовах інфляційного шоку оптимальною є така конфігурація політик, де монетарна влада реагує рішуче, але не надмірно, тоді як фіскальні інструменти використовуються вузько-цільовим та тимчасовим чином, з акцентом на підтримку найбільш вразливих домогосподарств і на довгострокові інвестиції, здатні підвищити продуктивність.

Зловживання дорогоцінними металами та камінням у фінансових злочинах [3]



Представлений документ є комплексним оновленням стратегічного аналізу сектору торгівлі дорогоцінними металами та камінням (DPMS), який відіграє критичну роль в економіці ОАЕ, оскільки обсяг зовнішньої торгівлі у цій сфері сягнув понад 959 мільярдів дирхамів ОАЕ у 2024 році. Звіт базується на аналізі масиву даних за період з липня 2021 по червень 2025 року, що включає понад 1,4 мільйона звітів про порогові операції з готівкою, вибірку з близько 700 повідомлень про підозрілі фінансові операції (STRs/SARs), а також дані митниці та правоохоронних органів. Попри значне зростання кількості зареєстрованих дилерів у системі фінансової розвідки (збільшення на 81% до 8191 суб'єкта станом на червень 2025 року), аналіз виявив тривожну тенденцію зниження частки суб'єктів, які активно подають звітність. Лише близько 29% зареєстрованих дилерів подають звіти про порогові операції, і лише близько 3,2% подають звіти про підозрілі операції, причому левова частка (79%) усіх підозрілих звітів надходить лише від 10 суб'єктів, що свідчить про значне недозвітування у секторі.

Основна увага у документі приділяється виявленим типологіям відмивання коштів. Сектор залишається вразливим до використання готівки, яка є домінуючим інструментом розрахунків і дозволяє розривати аудиторський слід. Найпоширенішими методами зловживань є контрабанда золота, використання компаній-оболонок та фіктивних підприємств, які імітують легальну торгівлю, але мають невідповідність між заявленим оборотом та реальними фінансовими потоками. Особливий акцент зроблено на відмиванні коштів через торгівлю (TBML), де злочинці використовують підроблені документи, фальсифіковані сертифікати походження, маніпуляції з інвойсами (заниження/завищення вартості) та кругові схеми руху товарів для легалізації незаконних доходів або обходу санкцій. Хоча ризик потрапляння на ринок «конфліктного золота» дещо знизився завдяки запровадженню нових регуляторних вимог щодо належної перевірки (due diligence), він залишається актуальним, особливо через складні ланцюжки постачання та транзит через треті країни.

Окремий блок аналізу присвячено профілюванню суб'єктів, залучених до незаконної діяльності. Звіт ідентифікує широке використання третіх осіб та посередників для здійснення платежів, що ускладнює встановлення кінцевих бенефіціарних власників. Фіксується активна участь іноземних громадян, зокрема з Індії, Пакистану та Бангладеш, а також політично значущих осіб (PEPs), які використовують сектор для приховування статків. Також відзначається тенденція до

[3] https://www.uaefiu.gov.ae/media/xpyaznve/dpms-report-sanitized-version-final-october-20.pdf

«де-рискінгу» з боку фінансових установ, які обмежують обслуговування сектору DPMS, залишаючи лише великих клієнтів, що може виштовхувати менших гравців у тіньовий сектор або змушувати їх використовувати рахунки третіх осіб. На завершення, документ пропонує близько 60 індикаторів ризику для виявлення підозрілих схем, які охоплюють поведінкові аспекти клієнтів, аномалії в торговельних документах та транзакційну активність.

Висновки:

- **Посилення нагляду за звітністю та розширення охоплення суб'єктів.** Враховуючи, що лише 3,2% зареєстрованих дилерів (DPMS) подають звіти про підозрілі операції (STR/SAR), а 79% таких звітів генеруються лише 10 компаніями, регулятору та СПФМ необхідно терміново переглянути ефективність внутрішніх систем контролю.
  Рекомендація: Проводити прицільні перевірки та навчальні заходи для тих 97% дилерів, які не подають звіти, фокусуючись не лише на факті реєстрації в системі goAML, а на якості та своєчасності виявлення підозр, особливо щодо операцій з готівкою та третіми особами.
- **Впровадження поглибленої перевірки ланцюгів постачання для протидії TBML**. Звіт підтверджує високий ризик використання підроблених сертифікатів походження та інвойсів для легалізації «конфліктного золота» та TBML.
  Рекомендація: СПФМ повинні вимагати незалежного аудиту ланцюгів постачання та верифікації документів (наприклад, сертифікатів ICGLR) не лише на етапі започаткування відносин, а й під час моніторингу транзакцій, звіряючи обсяги торгівлі з реальними операційними можливостями клієнта та ринковими цінами.
- **Виявлення та блокування схем з використанням компаній-оболонок та третіх осіб.** Аналіз виявив системне використання фіктивних компаній, що мають невідповідність між заявленим видом діяльності та реальними фінансовими потоками, а також платежі від третіх осіб.
  Рекомендація: Фінансовим установам слід налаштувати сценарії моніторингу для виявлення транзиту коштів через рахунки компаній з непов'язаними видами діяльності та відмовляти в обслуговуванні або посилювати контроль у випадках, коли платежі за дорогоцінні метали надходять від непов'язаних третіх сторін без чіткого економічного обґрунтування.
- **Перегляд стратегії «де-рискінгу» фінансовими установами.** Скорочення клієнтської бази DPMS банками призвело до зниження кількості повідомлень про підозрілі операції від банківського сектору, але підвищило ризик переходу розрахунків у тіньовий сектор або використання підставних рахунків.
  Рекомендація: Банкам рекомендується перейти від відмови в обслуговуванні сектору DPMS до ризик-орієнтованого підходу, що дозволить зберігати видимість фінансових потоків та ефективніше контролювати їх через механізми EDD, замість того щоб виштовхувати їх у нерегульоване поле.

Регулювання

Від довіри до інновацій: архітектура британського режиму нагляду за стейблкоїнами [4]

Документ Банку Англії є ключовим стратегічним кроком у формуванні повноцінної нормативно-правової бази для використання стейблкоїнів у платіжній системі Великої Британії. Його поява відображає завершення етапу концептуальних дискусій, розпочатих у 2023 році, і перехід до практичного встановлення правил для учасників нового цифрового фінансового середовища. Банк Англії, як центральна фінансова інституція країни, обґрунтовує свою ініціативу необхідністю підтримання довіри до грошей, збереження фінансової стабільності та водночас створення умов для безпечних інновацій у сфері платежів. У преамбулі документа підкреслюється, що завдання регулятора полягає у забезпеченні того, щоб суспільство могло мати таку ж саму довіру до нових форм грошей, як і до традиційних — готівкових чи безготівкових фунтів стерлінгів. Банк визнає, що технологічний прогрес, зокрема розвиток блокчейн-інфраструктур і цифрових валют, відкриває можливості для створення «багатовалютної системи», у якій поряд функціонуватимуть токенізовані банківські депозити, комерційні гроші та регульовані стейблкоїни, підкріплені центобанківською ліквідністю.

Документ спирається на Financial Services and Markets Act 2023, який розширив компетенцію Банку Англії на сферу Digital Settlement Assets (DSA) — цифрових розрахункових активів, що включають системні стейблкоїни. Основний фокус зроблено на стейблкоїнах, номінованих у фунтах стерлінгів, які можуть бути використані у повсякденних платежах та операціях у фінансовій системі Великої Британії. Після їх офіційного визнання Міністерством фінансів (HM Treasury), такі емітенти підлягатимуть спільному нагляду Банку Англії та Фінансового управління (FCA), тоді як несистемні емітенти залишатимуться під виключною юрисдикцією FCA. Банк отримає розширені наглядові повноваження, зокрема право отримувати інформацію, запроваджувати кодекси практики, видавати директиви, здійснювати примусові заходи у разі невиконання вимог і накладати регуляторні санкції. Такий підхід формує основу для дворівневої системи регулювання, що охоплює і системні платіжні системи, і надавачів ключових послуг (постачальники послуг зберігання цифрових гаманців, платіжні шлюзи тощо), якщо вони мають системне значення або обслуговують системно важливих учасників.

Консультаційний документ містить детальний аналіз отриманих відгуків на попередню дискусію 2023 року та демонструє суттєві зміни у політиці Банку. Найпомітнішою серед них є ревізія політики забезпечення. Якщо раніше пропонувалося 100% забезпечення у вигляді незарахованих депозитів у Банку Англії, то тепер Банк пропонує гібридну модель: не менше 40% резервів у формі депозитів у центральному банку (без нарахування відсотків) та до 60% у короткострокових державних цінних паперах Великої Британії. Такий компроміс покликаний забезпечити баланс між ліквідністю, необхідною для швидкого викупу монет, і можливістю для емітентів отримувати прибуток від безризикових активів, що підвищує життєздатність їхніх бізнес-моделей. Банк вважає, що короткостроковий характер держоблігацій мінімізує ринковий ризик (зниження вартості активів), а депозити у центральному банку гарантують миттєву доступність коштів для погашення вимог користувачів. Водночас депозити

[4] https://www.bankofengland.co.uk/paper/2025/cp/proposed-regulatory-regime-for-sterling-denominated-systemic-stablecoins

залишатимуться безвідсотковими, оскільки стейблкоїни не повинні брати участь у трансмісії монетарної політики, а емітенти — не мають нараховувати виплата відсоткового доходу власникам стейблкоїнів. Для нових системних емітентів передбачено поступовий режим, який дозволить на початковому етапі зберігати до 95% активів у державних паперах з подальшим зниженням частки до 60% у міру зростання обсягів та системного значення.

У сфері капіталу та резервів Банк пропонує застосовувати міжнародні стандарти CPMI-IOSCO PFMI, адаптовані до специфіки стейблкоїнів. Емітенти повинні мати капітал, достатній для покриття загальних бізнес-ризиків (операційних, технологічних, управлінських), у розмірі більшому з двох показників — шість місяців поточних операційних витрат або витрати на відновлення після найбільш імовірного сценарію збитків. Крім того, запроваджується механізм двох окремих резервів, що утримуються на статутному трасті: перший — для покриття ринкових ризиків забезпечувальних активів (цінових коливань, дисконтування під час реалізації), другий — для фінансування витрат, пов'язаних із процедурою ліквідації або передачею активів власникам монет у разі неплатоспроможності емітента. Вимога зберігати такі активи на трасті підвищує рівень правової захищеності користувачів і гарантує, що резерви не будуть включені до загальної маси активів у разі банкрутства емітента. Капітал повинен бути у формі Common Equity Tier 1 (CET1), тобто оплачений статутний капітал, нерозподілений прибуток та інші розкриті резерви.

Важливе місце у документі посідає питання визначення системної важливості. Банк Англії пропонує багатоаспектний підхід, який включає кількісні та якісні показники: масштаб транзакцій, кількість користувачів, рівень інтеграції у фінансову систему, ступінь взаємозалежності з іншими інфраструктурами, можливість заміщення послуг, тип користувачів (роздрібний чи корпоративний сегмент), а також потенційний вплив на довіру до фунта стерлінгів як національної валюти. Для ілюстрації наведено умовні приклади («Coin Group», «Coin International», «Coin Exchange»), які демонструють, як Банк може визнавати платіжну систему системною «на старті» або відмовляти у такому статусі через обмежений вплив на реальну економіку. Такий підхід, заснований на аналізі кейсів, на думку регулятора, дозволяє уникнути хибних сигналів ринку, які могли б виникнути при встановленні жорстких кількісних порогів.

Окрему увагу приділено ризикам дезінтермедіації банківського сектору. Банк Англії визнає, що масове поширення системних стейблкоїнів може призвести до відтоку депозитів із банків та зменшення обсягів кредитування економіки. Щоб пом'якшити ці ризики, на перехідному етапі запропоновано тимчасові ліміти володіння: до £20 000 для фізичних осіб і до £10 млн для

Висновки:

- **Стратегічний баланс між інновацією та стабільністю.** Банк впроваджує модель, що одночасно забезпечує довіру до стейблкоїнів і підтримує їхню життєздатність, поєднуючи 40% резервів у центральному банку та 60% у короткострокових держпаперах.
- **Ризик-орієнтовані вимоги до капіталу.** Вимога до покриття бізнес-ризиків і створення двох трастових резервів підвищує захист власників монет та зменшує ймовірність масового вилучення коштів вкладниками з банків у цифровому форматі.
- **Перехідні ліміти володіння як інструмент макрофінансової безпеки.** Тимчасові обмеження £20 000/£10 млн покликані запобігти швидкому відтоку депозитів з банківської системи та дестабілізації кредитного ринку.
- **Поступова інтеграція з ринковою інфраструктурою.** Введення DSS і можливість центробанківської ліквідної підтримки створюють основу для безпечного впровадження стейблкоїнів у платіжну екосистему Великої Британії.

юридичних осіб, із можливістю винятків для бізнесів, які потребують більших обсягів для операційної діяльності. Ці обмеження мають стримати різкі зміни у структурі ліквідності банківської системи й дати змогу поступово адаптуватися до нової платіжної екосистеми. Банк наголошує, що ліміти є тимчасовими, будуть пом'якшені або скасовані після досягнення стабільності на ринку кредитування.

Документ також наголошує на важливості інтероперабельності — здатності стейблкоїнів взаємодіяти з банківськими депозитами, центробанківськими грошима та іншими платіжними системами. Для цього передбачено участь Банку Англії у розробці Retail Payments Infrastructure Board, яка створює наступне покоління платіжної інфраструктури країни. Крім того, у сфері оптових фінансових операцій тестуватиметься застосування стейблкоїнів у Digital Securities Sandbox (DSS), що має на меті перевірити можливість їх використання для розрахунків у фінансових ринках у поєднанні з токенізованими цінними паперами. У разі успіху ці механізми можуть бути інтегровані до основної регуляторної рамки.

Таким чином, консультаційний документ формує практичний фундамент для створення у Великій Британії регульованого ринку стейблкоїнів, який поєднує гнучкість інновацій із жорсткими стандартами стабільності та прозорості. Його стратегічна мета — забезпечити, щоб стейблкоїни, які набувають поширення у роздрібних і корпоративних платежах, могли функціонувати з такою самою надійністю, як і традиційні гроші, залишаючись при цьому під контролем державної фінансової системи. Банк Англії прагне запровадити пропорційний, ризик-орієнтований та прогнозований режим, який унеможливлює появу системних загроз, створює умови для відповідальної інновації та зміцнює позицію фунта стерлінгів у цифрову епоху, де межа між грошима, платіжними технологіями та фінансовими інфраструктурами стає дедалі тоншою.

Звіти окремих інституцій та експертів

Російська кіберзлочинність та мілітаризація держави [5]

Представлений звіт розкриває комплексну стратегію Російської Федерації щодо мілітаризації суспільства та інтеграції кіберзлочинності в державну гібридну війну, де цифрові операції стають невіддільним елементом примусу та психологічного тиску. Документ демонструє, як через поєднання історичних наративів, законодавчих ініціатив та державних інституцій створюється екосистема, в якій межа між «незалежними» хактивістами та державними структурами фактично стирається. Автор аналізує еволюцію російського громадянського суспільства, починаючи з культивації пам'яті про Другу світову війну та закінчуючи сучасними репресивними законами про «іноземних агентів», що створило ґрунт для повної консолідації влади та придушення інакомислення. Центральним елементом цієї системи виступає «Загальноросійський народний фронт» (ЗНФ) — кремлівський рух, створений за ініціативою Путіна, який функціонує як платформа для легітимізації державних пріоритетів, мобілізації волонтерів та збору коштів для військових потреб, зокрема через кампанію «Все для Перемоги!». Ця організація не лише діє у фізичному просторі, інтегруючи окуповані території через гуманітарні та інфраструктурні проєкти, але й активно розширює свою присутність у цифровому середовищі.

[5] https://analyst1.com/russian-cybercrime-state-militarization/

У звіті детально описано створення ініціативи «Кібердружина» (CyberSquad) під егідою ЗНФ, яка є механізмом «цифрового призову», залучаючи цивільних осіб до моніторингу інтернет-простору на предмет «русофобії» та блокування ворожого контенту. Використовуючи елементи гейміфікації, такі як присвоєння військових звань, нарахування балів та публічне визнання, держава трансформує звичайну активність у мережі на виконання громадянського обов'язку, фактично перетворюючи користувачів на «цифрових солдатів». Паралельно з цим документ досліджує феномен проросійських хактивістських груп, зокрема «Народної кіберармії» (Cyber Army of Russia - CARR), чия діяльність, риторика та символіка (використання літери Z, георгіївських стрічок) повністю синхронізовані з офіційними державними наративами. Аналіз вказує на високу ймовірність координації цих груп з боку спецслужб, оскільки їхні цілі (наприклад, атаки на інфраструктуру водопостачання в Техасі) та інформаційний супровід чітко відповідають геополітичним інтересам Кремля.

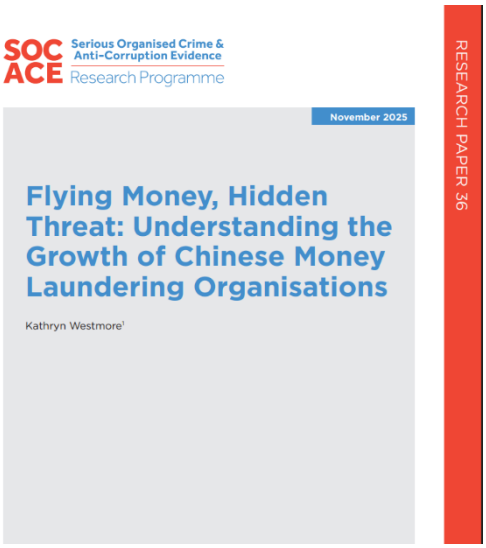
Особливу увагу в документі приділено взаємодії держави з професійними кіберзлочинцями та угрупованнями-вимагачами (ransomware groups). Зазначається, що Росія надає «безпечну гавань» кіберзлочинцям, які атакують західні цілі, відмовляючись від співпраці з міжнародними правоохоронними органами та навіть залучаючи хакерів до співпраці з ФСБ, як це було у випадку зі зламом Yahoo. Показовим є факт публічного нагородження та повернення засуджених на Заході хакерів у рамках обміну ув'язненими, що де-факто легітимізує кіберзлочинність як форму служіння державі. Звіт підсумовує, що російська стратегія полягає у використанні широкого спектра інструментів — від офіційних волонтерських рухів до кримінальних хакерських угруповань — для ведення перманентної інформаційної та кібервійни,

Висновки:

- **Ризик використання НПО для фінансування війни та кібероперацій:** Організації на кшталт ЗНФ діють як квазі-державні структури, що акумулюють значні фінансові ресурси через краудфандинг (кампанія «Все для Перемоги!») для підтримки військових дій та окупаційних адміністрацій.
  Рекомендація: Необхідно переглянути профілі ризиків неприбуткових організацій, що мають зв'язки з РФ, та запровадити посилений моніторинг транзакцій, які можуть маскуватися під гуманітарну допомогу, але фактично спрямовані на матеріально-технічне забезпечення збройних формувань або кіберугруповань.
- **Злиття кіберзлочинності та державних структур як індикатор для санкційного контролю:** Доведена координація між хактивістськими групами (CARR) та державними органами, а також політика «безпечної гавані» для угруповань-вимагачів (LockBit, REvil), свідчить про те, що доходи від кіберзлочинів можуть використовуватися в інтересах держави-агресора.
  Рекомендація: При розслідуванні інцидентів ransomware або ВК через криптовалюти, пов'язаних з російськими акторами, слід апріорі розглядати їх як потенційно пов'язані з державою. Це вимагає застосування жорсткіших санкційних механізмів до гаманців та інфраструктури, що використовуються такими групами, незалежно від їхньої заявленої незалежності.
- **Мобілізація цивільних ресурсів для гібридних атак:** Створення ініціатив на кшталт CyberSquad з системою гейміфікації та винагород створює масштабовану мережу для проведення скоординованих інформаційних атак та DDoS-кампаній.
  Рекомендація: Фінансовим розвідкам та підрозділам кібербезпеки слід відстежувати мікротранзакції та фінансові потоки, пов'язані з платформами винагород для таких «волонтерських» мереж, оскільки вони є елементом фінансування організованої злочинної діяльності в кіберпросторі під прикриттям громадської активності.

де будь-які дії проти «колективного Заходу» виправдовуються патріотизмом та захистом суверенітету.

Прихована загроза. Розуміння зростання китайських організацій з ВК [6]



Представлений документ висвітлює критичні аспекти еволюції та загроз, які становлять Китайські організації з відмивання коштів (CMLOs), що за відносно короткий час перетворилися на одну з домінуючих глобальних загроз відмивання коштів.

CMLOs використовують віковічні техніки, такі як неформальні системи переказу цінностей (IVTS), відомі як fei ch'ien («літаючі гроші»), які виникли ще за династії Тан (618–907 рр. н.е.) для полегшення торгівлі, але сьогодні вони еволюціонували у багатомільярдні операції, надаючи швидкі, дешеві та ефективні послуги транснаціональним організованим злочинним групам (ОЗГ). У деяких регіонах, як, наприклад, у США, CMLOs стали домінуючими гравцями на ринку відмивання коштів, а їхня діяльність продовжує зростати у Великій Британії та Європі. Головним чинником, що стимулює їхнє зростання та успіх, є запровадження суворих заходів контролю за капіталом у Китаї. Ці обмеження, зокрема річний ліміт у 50 000 доларів США на виведення коштів для фізичних осіб, створили величезний попит з боку заможних китайських громадян, які прагнуть перемістити капітал за кордон, і CMLOs, за невелику плату, можуть задовольнити цей попит коштами, які вони відмивають від імені злочинних груп. Це явище створює залучення аудиторії у Китаї, готову платити за доступ до західних валют.

Структура CMLOs описується як децентралізована та компартменталізована, що дозволяє їм гнучко масштабувати операції та знижує ризик виявлення. Їхні мережі є замкнутими і важкими для проникнення правоохоронними органами через мовні та культурні бар'єри, а також через використання зашифрованих комунікаційних платформ, зокрема WeChat. Робота цих мереж значною мірою ґрунтується на концепції guanxi — особистих, взаємовигідних стосунків, що є центральними для китайської культури. Центральне місце в операціях CMLOs посідає китайська діаспора, яку використовують як для залучення клієнтів, які бажають вивести капітал, так і для рекрутування «грошових мулів», часто китайських студентів. Ці мули відкривають численні банківські рахунки, на які злочинні доходи вносяться невеликими частинами (практика, відома як «смурфінг»), щоб уникнути ідентифікації підозрілих транзакцій. Діяльність CMLOs не обмежується традиційними IVTS, вони використовують цілий арсенал інструментів, включаючи відмивання грошей через торгівлю (TBML), купівлю нерухомості та інших предметів розкоші, а також активно інтегрують криптовалюти, такі як Bitcoin або Tether (USDT), які слугують як засіб переказу багатства за кордон для китайських громадян та як спосіб оплати прекурсорів фентанілу. Особливо помітна синергія у Північній Америці, де CMLOs стали «професійними відмивачами коштів» для мексиканських картелів, залучених до торгівлі фентанілом, надаючи їм надзвичайно ефективний і швидкий спосіб очищення величезних обсягів готівки.

Конкурентна перевага CMLOs полягає у їхній унікальній бізнес-моделі: вони стягують низькі комісії (близько 1–3%) або навіть пропонують свої послуги ОЗГ безкоштовно. Їхній фактичний прибуток генерується в Китаї, де вони продають західні валюти громадянам, які бажають обійти валютний контроль, часто стягуючи з них високі приховані збори. Це дозволяє CMLOs витісняти

[6] https://www.socace-research.org.uk/publications/chinese-money-laundering

традиційні мережі, які стягували 10–15% комісії, а також надавати послуги набагато швидше, часто протягом годин.

Важливим аспектом дослідження є аналіз зв'язку CMLOs з китайською державою. Незважаючи на часту риторику в США, яка розглядає діяльність CMLOs як державну загрозу, дослідження приходить до висновку, що немає доказів, які б свідчили про те, що діяльність CMLOs спрямовується китайською державою. Насправді, масовий відтік капіталу (за оцінками, до 254 мільярдів доларів США незаконно виведено з Китаю за 12 місяців до червня 2024 року) через CMLOs підриває інтереси Китаю та чинить тиск на його економіку, що вже бореться з уповільненням зростання. Хоча китайські схеми відмивання коштів можуть залучати урядовців та членів Комуністичної партії Китаю, це, як зазначається, не є доказом того, що ці схеми є державними. Проте, бездіяльність Китаю (попри знання про використання WeChat для координації операцій) може розглядатися як «принаймні мовчазна підтримка».

Навіть якщо CMLOs не є державною загрозою, їхня масштабна діяльність вимагає рішучої міжнародної відповіді, оскільки вони стали частиною ширшої транснаціональної проблеми незаконних фінансів. На даний момент спостерігається обмежена співпраця між західними правоохоронними органами та китайськими колегами, що ускладнює розслідування та розуміння повного ланцюжка транзакцій, особливо тієї його частини, що відбувається в Китаї. Це вимагає від Заходу посилення власної стійкості, покращення обміну розвідданими та розробки цільових кампаній.

Висновки:

- **Посилення фокусу на відтоку капіталу з Китаю як на основному драйвері:** CMLOs використовують жорсткий контроль капіталу в КНР (ліміт $50 000 на рік) для створення унікальної бізнес-моделі з низькими комісіями для ОЗГ Заходу.
  Практична дія: Фінансовим установам необхідно інвестувати у вдосконалення моделей моніторингу транзакцій, націлених на виявлення ознак обходу валютного контролю, зокрема, нетипової поведінки з обміну валюти та придбання активів (наприклад, нерухомості або оплати навчання) через канали, пов’язані з китайською діаспорою.
- **Захист вразливих груп діаспори:** CMLOs активно використовують китайську діаспору, зокрема студентів, як «грошових мулів».
  Практична дія: Необхідно розробити та реалізувати цільові інформаційні кампанії (наприклад, через університети та дипломатичні канали) для інформування китайських студентів та інших вразливих членів діаспори про ризики використання їхніх банківських рахунків для операцій CMLOs, а також посилити заходи протидії «смурфінгу».
- **Перехід від типологій до міждисциплінарних підходів:** Діяльність CMLOs є складною та інтегрує IVTS, TBML, використання криптовалют та традиційні фінансові канали.
  Практична дія: Правоохоронні органи та спеціалісти з ПВК/ФТ повинні відмовитися від ізольованого розгляду «типологій» (наприклад, окремо IVTS чи TBML) та застосовувати комплексний, транснаціональний підхід, який відображає гібридну природу операцій CMLOs, що часто координуються через зашифровані платформи, такі як WeChat.
- **Визнання обмежень міжнародної співпраці з КНР:** Відсутність суттєвої оперативної співпраці з китайськими правоохоронними органами обмежує видимість того, що відбувається на китайському кінці IVTS-транзакцій.
  Практична дія: Західні країни повинні зосередити зусилля на зміцненні внутрішнього та між'юрисдикційного обміну розвідданими між собою (США, Канада, ЄС, Велика Британія), щоб створювати повну картину загроз CMLOs, незалежно від готовності Китаю до співпраці.

Тіньовий флот: як росія перетворила українське зерно на зброю у гібридній війні [7]

Попри формальне запровадження міжнародних санкцій, російська система незаконного експорту українського зерна продовжує функціонувати практично безперешкодно. Нове розслідування Bellingcat доводить, що москва вибудувала складну мережу логістичних, фінансових та юридичних механізмів, які дозволяють системно красти українські аграрні ресурси з окупованих територій і продавати їх на світових ринках під виглядом «російського експорту». Це не просто поодинокі факти контрабанди — це масштабна державна політика, яка поєднує в собі воєнну логістику, фінансові схеми, маніпуляції з реєстраційними документами та політичну пропаганду.

За даними розслідування, контрабандна інфраструктура охоплює понад сотню суден, які регулярно здійснюють рейси з кримських портів — Севастополя, Феодосії, Керчі — а також із портів тимчасово окупованих Бердянська та Маріуполя. Переважна частина цих суден практикує вимкнення систем автоматичної ідентифікації (AIS), що унеможливлює їхнє відстеження в міжнародних базах. У багатьох випадках спостерігається зміна назв, прапорів і навіть міжнародних ідентифікаційних номерів (IMO), що створює враження постійного оновлення флоту. Насправді ж йдеться про ті самі судна, які раніше використовувалися у перевезеннях сирійської нафти, зброї або ж військових вантажів.

Зерно, награбоване на окупованих регіонах, транспортується до портів Чорного та Середземного морів, зокрема в напрямку Туреччини, Сирії, Єгипту, Лівану, а також ряду африканських держав. Саме ці країни залишаються «сірими зонами» санкційної політики — вони або не визнають незаконність окупації українських територій, або вдають, що не знають про походження вантажів. Російські посередники використовують це як можливість легалізувати крадене зерно через посередницькі компанії, зареєстровані у Дубаї, Лівані, на Кіпрі чи в Туреччині. Деякі з цих компаній створені спеціально для обслуговування таких операцій — вони не мають жодного іншого виду діяльності, окрім як змінювати документи про походження вантажу та оформлювати фіктивні контракти купівлі-продажу.

Особливу увагу Bellingcat звертає на спосіб фальсифікації документів. У більшості випадків вантажі оформлюються як зерно з російських регіонів — зокрема Краснодарського краю, Ростовської області або Криму, який у російських митних системах незаконно визнаний «російською територією». Водночас супутникові знімки та дані морського моніторингу свідчать, що завантаження відбувається безпосередньо на причалах окупованих українських портів. Часто судна здійснюють короткі «технічні» зупинки в Новоросійську чи Тамані, щоб отримати російські сертифікати походження, після чого прямують до портів призначення.

Цікаво, що деякі з суден, зафіксованих у перевезенні вкраденого зерна, раніше фігурували у розслідуваннях щодо «тіньового нафтового флоту» Росії, який використовується для обходу обмежень на експорт нафти. Це підтверджує, що російський режим використовує вже відпрацьовані схеми — створення фіктивних операторів, страхових компаній, реєстрацію флоту в юрисдикціях, що не приєдналися до санкцій (зокрема Танзанія, Сьєрра-Леоне, Ліберія). Через ці механізми Москва зберігає контроль над логістикою і водночас уникає прямої відповідальності, адже формально всі операції здійснюються «незалежними приватними компаніями».

У цьому процесі важливу роль відіграють і банки, що обслуговують розрахунки за такі операції. Bellingcat вказує на випадки, коли платежі за контрабандне зерно проходили через дрібні

[7] https://www.bellingcat.com/news/2025/10/23/russias-grain-smuggling-fleet-continues-undeterred/

фінансові установи на Кіпрі, у Вірменії та навіть у Сербії. Це створює ілюзію легальності угод і ускладнює відстеження кінцевих бенефіціарів.

Окремо у звіті наголошується, що незаконне вивезення зерна має подвійне значення для Кремля — економічне й політичне. По-перше, воно приносить росії мільярдні прибутки, які спрямовуються на підтримку військових дій. По-друге, контроль над аграрними потоками використовується як геополітична зброя. Москва цілеспрямовано намагається дискредитувати Україну як стабільного постачальника продовольства та посилити залежність країн Африки й Близького Сходу від «російського зерна». Саме тому російські чиновники активно просувають пропагандистський наратив про «гуманітарні поставки продовольства бідним країнам», намагаючись приховати факт, що це зерно — награбоване в Україні.

Ще однією ключовою проблемою залишається відсутність ефективного контролю на рівні міжнародних інституцій. Хоча ЄС і США неодноразово вносили підсанкційні судна до «чорних списків», у практиці морських перевезень це мало що змінює. Судна продовжують курсувати, оскільки більшість портів країн, що не мають політичних зобов'язань перед Заходом, не перевіряють бази даних санкцій перед прийомом вантажу. У результаті тіньовий флот функціонує практично безперебійно, а контрольні механізми з боку Міжнародної морської організації (IMO) фактично не працюють.

Для України наслідки цього процесу є багатовимірними. По-перше, це прямі економічні втрати: за оцінками аналітиків, росія вже вкрала зерна на сотні мільйонів доларів, що могло б поповнити український бюджет або стабілізувати валютні надходження. По-друге, це репутаційні ризики: на світових ринках з'являються великі обсяги «російського зерна», що демпінгують ціни та зменшують спроможність до конкуренції українських експортерів. По-третє, це створює довгострокову загрозу для відновлення аграрного сектору після війни, адже москва намагається встановити власну «монополію на постачання зерна з Чорного моря».

З точки зору глобальної безпеки, ця ситуація є тестом на дієвість міжнародного санкційного режиму. Незважаючи на декларації про «повну ізоляцію Росії», вона продовжує вести прибутковий бізнес завдяки слабким місцям у світовій системі контролю судноплавства. Bellingcat підкреслює, що без створення глобальної системи відстеження вантажів і уніфікації митних баз, зокрема з обов'язковим маркуванням походження зерна, зупинити контрабанду буде практично неможливо. Таким чином, нинішня ситуація демонструє не лише адаптивність російського режиму, а й стратегічну глибину його злочинної політики. Контрабанда зерна — це не тимчасова схема наживи, а складова частина гібридної війни, у якій економічні інструменти використовуються для досягнення військово-політичних цілей.

Висновки:

- **Російська контрабанда зерна стала системним державним механізмом** — Україні потрібно посилити міжнародні санкційні ініціативи проти суден і посередників, що беруть участь у таких схемах.
- **Використання фіктивних маршрутів і компаній вказує на слабкість глобального моніторингу** — слід ініціювати створення міжнародної бази відстеження суден, які перевозять сільськогосподарські вантажі з регіонів конфліктів.
- **«Гуманітарний» наратив Росії маскує воєнну економіку** — Україні та партнерам варто активніше викривати інформаційні маніпуляції Москви в міжнародних медіа та ООН.
- **Незаконний експорт українського зерна підриває продовольчу безпеку** — Україні необхідно закріпити в законодавстві механізми документування таких злочинів як воєнних та забезпечити подальші компенсаційні позови.

Контрабанда за підписом: як бюрократія та корупція створюють глобальні маршрути зброї [8]

Стаття, опублікована Global Initiative, розкриває один із найскладніших і найвитонченіших прикладів сучасного міжнародного кримінального бізнесу — схему, в якій поєдналися балканська військова промисловість, африканська корупція й латиноамериканський наркокартель.

Автор детально реконструює історію болгарського торговця зброєю Петара Димитрова Мірчева, який розробив багатомільйонну схему постачання зброї до мексиканського картелю Халіско (CJNG), використовуючи не контрабанду в класичному сенсі, а підроблену документацію — фальшиві сертифікати кінцевого користувача, що мали створити ілюзію легальної угоди.

Розслідування американських прокурорів викрило, що Мірчев і його партнери підготували "комерційну пропозицію" на суму понад 53,7 мільйона євро, до якої входили сотні одиниць стрілецької зброї, боєприпаси, а також важке озброєння — від гранатометів до бронетехніки. Використовуючи підроблені документи з печатками Міністерства оборони Танзанії, він намагався оформити експорт через болгарських виробників, маскуючи угоду під військову поставку до Африки. У липні 2024 року навіть було здійснено тестову відправку — 50 автоматів АК-47 та 140 тисяч патронів. Але американські фінансові слідчі відстежили банківські перекази на суму 38 тисяч доларів із рахунків у США до болгарських компаній, що мали зв'язки з Мірчевим. Цей ланцюг став ключем до його арешту в Іспанії у квітні 2025 року.

Попри очевидну тяжкість злочину, реакція в Болгарії виявилася вкрай млявою. Медіа зосередилися на фігурі мексиканського картелю, майже не зачепивши питання внутрішніх зв'язків між зброярськими компаніями, військовими й чиновниками. І це не випадковість: Мірчев — не нова особа у цій сфері. Його ім'я фігурує у звітах журналістських розслідувань і навіть у досьє спецслужб ще з 1990-х, проте він десятиліттями залишався недоторканним. Як пояснює автор, така "невидимість" можлива лише завдяки політичному прикриттю всередині болгарської системи, де оборонна промисловість має статус «недоторканної» сфери національної економіки. Ця інституційна закритість і є головною умовою, яка дозволяє діячам на кшталт Мірчева маніпулювати міжнародними сертифікатами та легалізовувати тіньові поставки зброї.

Стаття розкриває історичний контекст, без якого сучасні схеми виглядають лише епізодами. Після розпаду соціалістичного блоку Болгарія стала одним із головних джерел зброї для "сірих зон" світу — від Балкан до Африки. У 1990-х роках болгарські склади радянської зброї, разом із недореформованою системою контролю, забезпечили незаконні постачання до Боснії, Косова, Сьєрра-Леоне, Анголи та Судану. Після цього країна неодноразово фігурувала в операціях відомого російського контрабандиста Віктора Бута, якого Мірчев, за словами слідства, вважав своїм наставником. Їхня співпраця тривала ще з 1995 року, коли болгарські посередники забезпечували логістику та зберігання товарів, а Бут організовував авіаперевезення до зон конфлікту.

[8] https://globalinitiative.net/analysis/bulgaria-arms-trade-corruption-east-africa-mexico-cartels/

Далі автор простежує, як після 2010-х років болгарська зброя почала знову з'являтися у нових війнах — уже в Сирії, Лівії, Ємені. Формально це були "легальні" поставки, схвалені ЄС і США, але, потрапляючи до рук посередників у країнах Перської затоки, вони швидко осідали в арсеналах терористичних угруповань — від "Ісламської держави" до "Аль-Каїди". Зброя з маркуванням "Made in Bulgaria" ставала символом системної проблеми — коли формально законна торгівля перетворюється на кримінальний бізнес, прикритий дипломатією та бюрократією.

Кейс Мірчева — це лише вершина айсберга. Він показує, що сучасна торгівля зброєю майже не потребує контрабанди у звичному розумінні. Достатньо створити правдоподібний документальний ланцюг: сертифікат кінцевого користувача, дозвіл на транзит, рахунки-фактури. Все це створює ілюзію легітимності, тоді як реальне постачання відбувається у зовсім іншому напрямку. Цю практику автор влучно називає "контрабандою за підписом" — тобто схемою, де не потрібні сховані контейнери, достатньо лише підробленого документа з офіційною печаткою.

Стаття також наголошує на важливому парадоксі: Болгарія є членом ЄС і НАТО, підписантом Arms Trade Treaty (Договору про торгівлю зброєю), який вимагає суворого контролю за кінцевим користувачем, але на практиці контроль обмежується формальними звітами. Саме тому такі операції, як у справі Мірчева, стають можливими. У теорії система передбачає аудит і перевірку після поставки, однак у реальності "документи мають більшу вагу, ніж фактична перевірка". І поки держава демонструє співпрацю зі США, всередині країни жодних парламентських слухань чи офіційних розслідувань не проводиться.

Особливу увагу автор приділяє африканському компоненту схеми. Танзанія виступала не як активний партнер, а як "логістична тінь", де корупція забезпечила легалізацію підроблених сертифікатів. Це класичний приклад того, як африканські бюрократичні механізми стають частиною глобальних злочинних ланцюгів, де офіційний підпис чиновника має більшу вагу, ніж будь-який кордон. Саме ця "адміністративна корупція" — один із найнебезпечніших елементів глобальної торгівлі зброєю, адже вона перетворює злочин на бізнес із повним імунітетом.

Цей кейс розкриває принаймні чотири рівні ризиків, які взаємодіють між собою й створюють потенціал для масового поширення зброї серед недержавних і кримінальних акторів. Перший рівень — виробничо-історичний: Балканські країни, зокрема Болгарія, успадкували великі арсенали й виробничі компетенції після холодної війни, але часто не провели глибоких інституційних реформ у контролі за оборонною промисловістю; на практиці це означає доступ до реальних можливостей виробництва і зберігання зброї для суб'єктів, які формально діють в межах закону, але надають свої потужності посередникам.

Другий рівень — адміністративно-документальний: міжнародна система контролю (сертифікати кінцевого користувача, дозволи на експорт, транзитні документи) покладається на довіру до підписів і печаток, а не на обов'язкові оперативні перевірки «після поставки». Ця «вага підпису» робить документи цінним товаром, який можна купити або підробити, і саме так працювала схема Мірчева з «танзанійськими» підробленими сертифікатами.

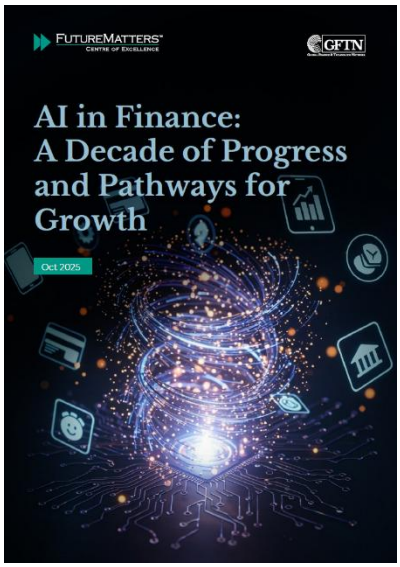
Третій рівень — корупційний: африканські бюрократичні вразливості використовувалися як адміністративна ширма, коли печатка і підпис чиновника Танзанії створювали правдоподібне підґрунтя для угоди, навіть якщо реального зв'язку з армією Танзанії не існувало.

І четвертий рівень — фінансовий: ключем для розкриття став банківський слід — грошові перекази, що пройшли через американські та європейські рахунки, і які дозволили міжнародним слідчим встановити ланцюжок зв'язків між Мірчевим, болгарськими виробниками й тестовою відправкою. Усі ці рівні працювали разом і роблять кейс показовим для розуміння сучасних ризиків торгівлі озброєннями.

Ключова теза публікації полягає в тому, що міжнародна торгівля зброєю сьогодні все більше нагадує транснаціональний корпоративний ринок, де обіг "легальних" паперів важливіший за реальне походження товару. Без прозорості й реальної політичної волі ці схеми продовжуватимуть існувати — від Балкан до Африки й Латинської Америки.

І поки документи з печатками замінюють контроль, "контрабанда підписом" залишатиметься ефективним інструментом збагачення для тих, хто володіє доступом до бюрократії, дипломатії та зброї одночасно. Стаття демонструє, що сучасна злочинність — це не завжди рух через кордони, а радше зловживання владою, довірою та системою міжнародного регулювання.

Штучний інтелект у фінансах: від автоматизації до епохи автономних фінансових систем [9]



Документ є комплексним аналітичним оглядом десятирічної еволюції штучного інтелекту (AI) у фінансовому секторі світу, який фіксує перехід від фази експериментальної автоматизації до етапу системного впровадження, інтегрованого управління ризиками та становлення принципово нової парадигми «AI-орієнтованих фінансів». У звіті узагальнено досвід, накопичений фінансовими установами, регуляторами, технологічними корпораціями та інвесторами у 2016–2025 роках, і представлено стратегічний погляд на майбутнє — десятиліття, у якому штучний інтелект перетворюється на центральну інфраструктуру глобальної фінансової системи. У цьому контексті AI постає не лише як інструмент підвищення ефективності, а як рушійна сила цифрової трансформації, формування нових джерел вартості, зміни ринкових структур і, водночас, джерело нових системних ризиків.

Від початкового етапу 2016–2018 років, коли AI у фінансах був представлений переважно у вигляді роботизованої автоматизації процесів (RPA), простих чат-ботів і моделей для виявлення аномалій, галузь пройшла шлях до повномасштабного впровадження предиктивної аналітики, глибинного навчання, генеративного AI та великих мовних моделей (LLMs), які сьогодні пронизують усі сфери — від банкінгу та страхування до управління активами, платіжних систем і регуляторного нагляду. У першій фазі автоматизація знижувала операційні витрати банків і страхових компаній на 40–75% завдяки RPA і алгоритмам, здатним обробляти масиви транзакційних даних і виявляти шахрайство. У другій фазі (2018–2022) інституції перейшли до побудови систем прогнозування, персоналізації послуг, кредитного скорингу на основі тисяч змінних, і активного використання RegTech — особливо у сфері ПВК/KYC. Цей період також позначився формуванням перших міжнародних етичних і нормативних рамок: принципи FEAT (Справедливість, етика, відповідальність, прозорість) Сінгапуру, OECD AI Principles 2019 року, які стали міжурядовим стандартом довірчого AI, та поява спеціалізованих програм SupTech для регуляторів.

У фінальній фазі (2022–2025) глобальну фінансову екосистему охопила ера генеративного AI, що започаткувала нову парадигму аналітики, комунікації з клієнтами та прийняття управлінських рішень. ChatGPT та інші LLM-системи радикально змінили підхід до обробки інформації, дозволяючи створювати тексти, коди, інвестиційні рекомендації та аналітичні звіти у реальному

[9] https://gftn.co/hubfs/AI%20in%20Finance%20-%20A%20Decade%20of%20Progress%20and%20Pathways%20for%20Growth-1.pdf

часі. Такі системи стали ядром роботи банків, інвесткомпаній і регуляторів: JPMorgan створив IndexGPT для AI-інвестиційних порад, BlackRock запровадив Aladdin Copilot — мультиагентну платформу для управління ризиками й аналізу портфелів у режимі реального часу, а RBC представив Aiden GenAI, який поєднує кілька AI-агентів для моніторингу новин, звітності та ринкових сигналів. У страхуванні генеративного AI автоматизував оцінку збитків, скоротивши час обробки на 20–30%, а у сфері капітальних ринків LLM вже виконують аналітику, яка раніше займала дні, протягом хвилин.

Розвиток технологій супроводжувався масштабним удосконаленням інфраструктури. Модельні архітектури еволюціонували від дерев рішень до глибинних нейронних мереж, трансформерів і мультиагентних систем. Впровадження підходів Data Fabric забезпечило єдине джерело достовірних даних для AI-аналітики, а відкриті стандарти та міжплатформна інтероперабельність стали ключовими вимогами. Паралельно формувалася глобальна хмарна інфраструктура, яка демократизувала доступ до обчислювальних ресурсів — Alphabet, Amazon і Microsoft інвестували понад 300 млрд доларів у розвиток датацентрів та AI-орієнтованих сервісів, створивши екосистеми для MLOps, API та Generative AI blueprints. Одночасно вартість інференсу моделей знизилася у десятки, а подекуди сотні разів, відкривши шлях до масштабування AI-рішень навіть для середніх і малих фінансових учасників.

На політичному рівні відбувалося формування нормативної архітектури штучного інтелекту у фінансовому секторі. Сінгапур, як лідер регуляторних інновацій, не лише запровадив принципи FEATта ініціативу Veritas, а й у 2025 році створив програму PathFin.ai — платформу для обміну знаннями щодо належного управління штучним інтелектом у фінансовому секторі. Європейський Союз ухвалив перший у світі всеохопний AI Act із ризик-орієнтованою системою класифікації, що визнає кредитний скоринг і страхування високоризиковими застосунками. Велика Британія розвиває концепцію «регулювання, спрямованого на підтримку інновацій» застосовуючи FCA Sandbox та AI Live Testing, що дозволяє тестувати алгоритми у контрольованих середовищах. США натомість обрали децентралізовану стратегію, представивши Національний план дій у сфері штучного інтелекту (AI Action Plan) і серію президентських указів про безпечний і етичний AI. На багатосторонньому рівні закріпилися OECD AI Principles, G7 Hiroshima Process, Bletchley Declaration та Резолюція ООН 2024 року про безпечний штучний інтелект для Цілей сталого розвитку.

Водночас розширення застосування AI породило нові системні виклики — ризики концентрації моделей, алгоритмічної упередженості, фрагментації регулювання, підвищеного енергоспоживання та відсутності глобальних стандартів інтероперабельності. Автори документа вказують, що подальший розвиток фінансового сектора вимагатиме переходу від реактивного до проактивного підходу — від постфактум-комплаєнсу (ex-post) до попереднього контролю моделей (ex-ante assurance), що включає аудит моделей до впровадження, оцінку їхньої прозорості, надійності й пояснюваності. Сінгапур, Індія, Велика Британія та інші юрисдикції вже розробляють системи «паспортів моделей» і аудиту пісочниць LLM, які спрямовані на створення довіри до автономних систем.

Звіт також акцентує на формуванні нового феномену — «AI-орієнтованих фінансів», побудованих на принципах автономного прийняття рішень і мінімальної участі людини. Це компанії, де AI виступає не інструментом, а ядром бізнес-моделі: кредитні та страхові рішення ухвалюються миттєво, а торгові платформи працюють у режимі самонавчання. Система «автономних фінансів» — наступний крок еволюції, коли мультиагентні AI-системи самостійно управляють портфелями, платежами, ризиками та ліквідністю. Проте така автономність вимагає переосмислення юридичної відповідальності, фідуціарного обов’язку та контролю за поведінкою алгоритмів. Регулятори починають створювати спеціалізовані інститути, як-от AI Supervisory Labs, для моніторингу динамічних ризиків і тестування сценаріїв ринкових збоїв.

Важливою тенденцією стало використання синтетичних даних — штучно згенерованих, але статистично еквівалентних реальним наборам, що дозволяє дотримуватися вимог конфіденційності (GDPR, PDPA) і тренувати моделі без ризику розкриття персональної інформації. Це має особливе значення для сфер ПВК/ФТ і кредитування, де конфіденційність клієнтських даних критично важлива. У той самий час AI став потужним інструментом фінансової інклюзії — прикладом є Tala, яка завдяки AI-алгоритмам надала понад 9 млн кредитів клієнтам без кредитної історії, скоротивши розрив у доступі до фінансів для MSME на 5 трлн доларів. Однак звіт наголошує: без належного контролю такі системи можуть відтворювати історичні упередження або створювати нові форми дискримінації, тому забезпечення алгоритмічної справедливості та прозорості стає обов'язковим компонентом стійкості фінансової системи.

Окрему увагу приділено синергії AI з «фронтирними» технологіями: квантовими обчисленнями, які в перспективі здатні радикально пришвидшити аналіз складних фінансових систем; нейроморфними процесорами для локальної обробки даних; та цифровій інфраструктурі нового покоління — API, цифровим ідентичностям, відкритим фінансовим платформам. Ці елементи формують основу «інтероперабельного фінансового простору», де AI може функціонувати без бар'єрів між державами, банками і ринками.

З фінансової точки зору, AI стає одним із найприбутковіших секторів глобальної економіки. У 2025 році венчурні інвестиції в AI сягнули 114,6 млрд доларів, а в генеративному AI — майже 50 млрд, що перевищило показники всіх попередніх років. Понад 79% компаній у сфері фінансів повідомили, що рентабельність їхніх AI-інвестицій відповідає або перевищує очікування. До 2030 року прогнозується зростання ринку AI до 1,8 трлн доларів, а щорічний приріст сягатиме 35,9%. Разом із цим звіт підкреслює трансформацію робочої сили: штучний інтелект не лише створює нові ролі (Менеджери з продуктів штучного інтелекту, фахівці з управління штучним інтелектом та тренери (наставники) агентів штучного інтелекту), а й вимагає появи нової категорії працівників — багатопрофільні фахівці (versatilists), які поєднують знання фінансів, технологій і етики. Масштабне перепідготовлення кадрів стає вирішальним фактором конкурентоспроможності, а формування міждисциплінарних команд з управління AI-ризиками — стандартом корпоративного управління.

Завершується документ висновком, що майбутнє фінансових ринків визначатиметься балансом між інноваційністю та відповідальністю. Якщо перше десятиріччя було епохою «AI як інструменту», то наступне стане епохою «AI як системи». Для цього потрібні міжнародна координація, гармонізація стандартів, створення етичних та юридичних гарантій і розвиток прозорої культури використання даних. Тільки поєднання технологічного прогресу з принципами підзвітності, інклюзії та людського нагляду дозволить забезпечити, щоб штучний інтелект у фінансах не лише

Висновки:

- **AI стає базовою інфраструктурою фінансів:** країнам слід інтегрувати платформу для обміну знаннями щодо належного управління штучним інтелектом у фінансовому секторі (аналогічно до MAS або ЄС).
- **Регулятори повинні переходити до ex-ante контролю моделей:** впроваджувати тестування, аудити і «паспорт моделей» перед впровадженням у фінансові процеси.
- **AI може зменшити нерівність, але лише за умов алгоритмічної справедливості:** потрібен нагляд за упередженістю моделей і справедливістю моделей у сфері кредитування та страхування.
- **Фінансові установи мають створити підрозділи з управління AI** (із залученням фахівців IT, комплаєнсу, етики, ризиків) та інвестувати у перепідготовку кадрів, готуючись до епохи фінансів, побудованих на основі штучного інтелекту.

підвищував ефективність, а й зміцнював довіру — головний актив світової фінансової системи у нову епоху.

Європейська цифрова трансформація: як токенізація змінює архітектуру капітальних ринків [10]

Документ являє собою ґрунтовне дослідження трансформаційного потенціалу токенізації як ключової технології майбутньої глобальної фінансової та публічної інфраструктури. У ньому токенізація розглядається не просто як технічний інструмент, а як стратегічна зміна парадигми, що здатна перевизначити принципи обігу вартості, управління активами та регуляторного контролю у цифрову епоху. Автори підкреслюють, що технологія розподіленого реєстру (DLT) стає фундаментом цифрової економіки, а токенізація — її функціональним ядром, яке забезпечує прозорість, автоматизовану взаємодію, незмінність записів і можливість працювати у режимі 24/7 без традиційних посередників.

Звіт детально пояснює, що токенізація дозволяє створювати цифрових «двійників» реальних активів — від нерухомості та цінних паперів до товарів, інтелектуальної власності й навіть адміністративних послуг. Такий підхід не лише мінімізує ризики контрагентів і прискорює розрахунки завдяки смартконтрактам, але й демократизує доступ до інвестиційних можливостей через фракційне володіння. Підкреслюється, що токенізовані ринки природно забезпечують повну трасованість транзакцій, відкриваючи потенціал для нових форм регуляторного нагляду — від автоматизованого комплаєнсу до безперервного аудиту. Водночас документ акцентує, що впровадження таких можливостей вимагає модернізації регуляторних підходів, адаптації правових рамок та узгодження технологічних стандартів між різними юрисдикціями.

У центрі звіту — аналіз європейського регуляторного поля, яке переживає суттєву трансформацію завдяки впровадженню MiCA, DLT Pilot Regime, MiFID II/MiFIR та низки національних актів, серед яких вирізняються Blockchain Law IV у Люксембурзі, eWpG у Німеччині, французька модель регулювання AMF (Орган з регулювання фінансових ринків Франції) та унікальний ліхтенштейнський «Token Container Model». Незважаючи на прогрес, автори визнають, що ЄС продовжує стикатися з фрагментацією регулювання, обмеженою сумісністю між DLT-інфраструктурами та недостатньо визначеною класифікацією цифрових активів. Вони підкреслюють важливість створення уніфікованої класифікації токенів, що дозволить забезпечити правову визначеність, інвесторську довіру та транскордонну інтероперабельність.

Велика частина документа присвячена прикладним кейсам, які демонструють реальний економічний ефект токенізації. Так, токенізація нерухомості на платформі RealT демонструє можливість автоматизованого розподілу орендного доходу, забезпечення юридично значущих прав власності та підвищення ліквідності раніше малорухомих активів. У Об'єднаних Арабських Еміратах запуск дирхам-забезпечених стейблкоїнів під контролем центрального банку ілюструє модель формування суверенної цифрової платіжної інфраструктури, де цифрові токени використовуються для внутрішніх розрахунків у регульованому середовищі. Експериментальна система Tokenized Micro Flat Tax (TMFT), що вбудовує податкові алгоритми у смартконтракти, демонструє революційну можливість для публічного сектору — автоматизоване, прозоре й миттєве виконання податкових зобов'язань без потреби у звітності та ручному контролі. Інші

[10] https://inatba.org/wp-content/uploads/2025/11/SubWG1_-Tokenization.pdf

приклади, такі як VeChain, Patientory або BeefChain, розкривають потенціал токенізації у логістиці, охороні здоров'я та агросекторі, показуючи універсальність технології для підвищення прозорості та довіри у різних галузях.

Звіт докладно описує бачення Європейського цифрового союзу капітальних ринків, яке передбачає радикальну модернізацію економічної інфраструктури ЄС шляхом інтеграції DLT у механізми торгівлі, оподаткування, публічних послуг та взаємодії держави з громадянами. Токенізація, як зазначається, дозволяє перейти від централізованих реєстрів до децентралізованих, що підсилює довіру та відкритість, а також створює підґрунтя для інклюзивного цифрового ринку капіталу. Але поруч із можливостями документ розглядає складні виклики, зокрема сумісність DLT з GDPR, адже незмінність блокчейну конфліктує з вимогами щодо видалення персональної інформації. Автори наполягають на терміновій адаптації законодавства ЄС до децентралізованих технологій, включаючи оновлення правил щодо приватності та динамічної згоди.

У заключній частині автори доходять висновку, що токенізація є передумовою створення нової фінансової екосистеми — відкритої, програмованої, стійкої та орієнтованої на громадян. Проте її повноцінна реалізація можлива лише за умов гармонізованих стандартів, узгоджених регуляторних рамок і активної участі держави та ринку. Успішна інтеграція токенізованих активів у глобальну економіку потребує чітких протоколів взаємодії, вирішення проблеми ліквідності, стимулювання ринкових учасників та формування середовища, де інновації співіснують зі стабільністю. Підкреслюється, що токенізація фактично є «швидкісною магістраллю» для модернізації сучасних економік, але лише за умови стратегічного, комплексного та відповідального підходу.

Висновки:

- **Єдина цифрова класифікація активів.** ЄС повинен розробити спільну класифікацію для всіх типів токенів, що стане основою для гармонізації законодавства та транскордонної сумісності.
- **Модернізація DLT Pilot Regime.** Необхідно підвищити ліміти та розширити сферу його дії, щоб залучити великі фінансові установи та збільшити ліквідність вторинних ринків токенізованих активів.
- **Впровадження програмованих державних сервісів.** ЄС та національні уряди можуть використовувати токенізацію для автоматизації податків, соціальних виплат і державних закупівель, створюючи прозору цифрову публічну інфраструктуру.
- **Інституційна співпраця та стимулювання ліквідності.** Регулятори й фінансові установи мають створити спільні стандарти, пілотні платформи та програми підтримки ліквідності, що дозволить токенізації стати реальним двигуном європейської цифрової економіки.

Цифрові активи 2025: як стейблкоїни, токенізація та DeFi змінюють архітектуру світових фінансів [11]

Документ являє собою комплексне, міжюрисдикційне дослідження сучасної екосистеми цифрових активів, її ринкової динаміки, технологічної еволюції та нормативного середовища, яке формує правила гри на глобальному фінансовому ринку у 2025 році. Звіт підкреслює фундаментальну зміну парадигми: цифрові активи, що починалися як експеримент у межах криптоспільноти, еволюціонували у розгалужену фінансову екосистему, яка інтегрується у

[11] https://gftn.co/hubfs/GFTN/Insights%20-%20Reports%20and%20Videos/Insights/GFTN%20Global%20Digital%20Assets%20Report/GFTN%20Global%20Digital%20Assets%20Report%20Combined%20-%2011%20Nov%202025.pdf

традиційні фінансові ринки, впливає на платіжну інфраструктуру, кредитування, ринки капіталу, комплаєнс-процеси та технології нагляду. Центральна ідея звіту полягає в тому, що цифрові активи перестали бути периферійним сегментом: вони перетворилися на один із основних векторів фінансової модернізації, а регулятори, фінансові установи та міжнародні організації вимушені адаптуватися до цих змін у реальному часі.

На тлі глобальної диджиталізації особливо швидко трансформується сфера цифрових грошей. Звіт демонструє, що стейблкоїни, токенізовані депозити та цифрові валюти центральних банків (CBDC) є трьома відмінними моделями цифрових грошей, кожна з яких розвивається власною траєкторією і під різним регуляторним контролем. Стейблкоїни — як приватно випущені активи з прив'язкою до фіатної валюти — стали найбільш поширеною формою цифрових грошей, що забезпечують разюче масштабування операцій: сумарний транзакційний обсяг перевищив 263 трильйони доларів з 2019 року, а за останні 12 місяців — понад 40 трильйонів доларів, що свідчить про стрімке зростання реального економічного використання не лише у криптоторгівлі, але й у міжнародних платежах, транскордонних розрахунках, казначейських операціях та роздрібних сервісах. Водночас стейблкоїни перебувають у фокусі регуляторів, і дедалі більше юрисдикцій — від ЄС до Японії та Сінгапуру — вибудовують цілісні режими регулювання, що вимагають прозорості резервів, процедур погашення та повної відповідності фінансовому моніторингу. Паралельно з цим банківські токенізовані депозити, що випускаються регульованими установами, демонструють швидке інституційне зростання, особливо в контексті міжбанківських розрахунків та автоматизованих операцій. CBDC продовжують розвиватися у пілотних чи частково впроваджених формах, причому особлива увага приділяється питанням приватності, інтеграції з банківською інфраструктурою та суспільної довіри.

Ще одним ключовим блоком звіту є токенізація реальних активів, яка перетворюється на один із найдинамічніших сегментів цифрової економіки. Станом на середину 2025 року ринок токенізованих активів демонструє вибухове зростання до понад 244 мільярдів доларів, із величезним попитом на токенізовані державні облігації, грошові ринкові фонди, комерційні інструменти, приватний кредит і навіть матеріальні активи. Аналітика GFTN показує, що саме інституційний сегмент рухає цю індустрію вперед, оскільки токенізація дозволяє суттєво знизити витрати пост-трейдингу, забезпечити цілодобовий DvP-розрахунок і підвищити ліквідність. Юрисдикції з найсильнішими нормативними режимами — ЄС, Швейцарія, Сінгапур, Гонконг, Японія — стають центрами тяжіння для фінансових інститутів, які прагнуть випускати або торгувати токенізованими цінними паперами в рамках чітких, передбачуваних правил.

Сфера криптобірж також демонструє рекордні масштаби: понад 750 мільйонів користувачів у світі здійснюють операції з цифровими активами, а ринкова капіталізація криптовалют перевищує 4 трильйони доларів. Звіт узагальнює розбіжності між повноцінними ліцензійними режимами (ЄС, Сінгапур, Гонконг, ОАЕ, Швейцарія) та фрагментованими режимами (США, Індія, Саудівська Аравія), що створює асиметрію у глобальній конкурентоспроможності майданчиків. Значна увага приділяється також інституційному кастодіальному сегменту, який зазнає радикального перегляду безпекових стандартів на користь MPC-технологій (технології, що дозволяють управляти цифровими активами без існування єдиного приватного ключа) та розподілених систем зберігання.

Значну частину звіту присвячено економіці докузу частки володіння (консенсусний механізм PoS) та ринку послуг стейкінгу. Близько 42% власників криптоактивів беруть участь у стейкінгу, а ринкова капіталізація PoS-мереж перевищує 800 мільярдів доларів. Регуляторні підходи у різних країнах залишаються нерівномірними: ЄС, Гонконг та Швейцарія дозволяють регульованим платформам пропонувати послуги стейкінгу, тоді як Сінгапур забороняє їх для роздрібних інвесторів, а США вперше окреслили межу між «протокольним» та «інституційно-посередницьким» стейкінгом, що створило чіткіші правила для ринку.

У сфері DeFi звіт відзначає стрімке зростання: понад 312 мільйонів користувачів, майже 50 мільярдів доларів активних кредитів та інтенсивна інтеграція з токенізованими активами і стейблкоїнами. У цьому контексті GFTN підкреслює системні ризики: глибоку технологічну вразливість смартконтрактів, залежність від оракулів, швидке масштабування незабезпечених протоколів, а також відсутність належних стандартів кібербезпеки. Водночас регуляторні підходи до DeFi здебільшого перебувають у зародковому стані: лише 9% юрисдикцій мають хоч якусь форму нагляду чи ліцензування DeFi-інфраструктури, і більшість країн лише починають обговорювати рамки нагляду, диференціюючи «справжню» децентралізацію та псевдодецентралізовані DINO-моделі.

Ключовим ризиковим блоком є ПВК/KYC, питання приватності та кібербезпеки. Звіт фіксує різке зростання санкцій за порушення вимог фінмоніторингу — понад 5,1 мільярда доларів штрафів у 2024 році, з тенденцією до подальшого збільшення у 2025 році. Висвітлюються численні інциденти витоку даних користувачів, масштабні хакерські атаки, уразливості приватних ключів використання вразливостей смартконтрактів, через які лише у першому півріччі 2025 року було втрачено понад 2,1 мільярда доларів. Незважаючи на рекомендації FATF, регуляторні підходи країн залишаються фрагментованими: ЄС, Сінгапур, Японія, Гонконг, Швейцарія, Бразилія та ОАЕ впровадили комплексні режими ПВК для цифрових активів, тоді як США, Велика Британія, Індія та країни Перської затоки переважно використовують традиційне законодавство у сфері ПВК, не адаптоване до специфіки цифрових активів.

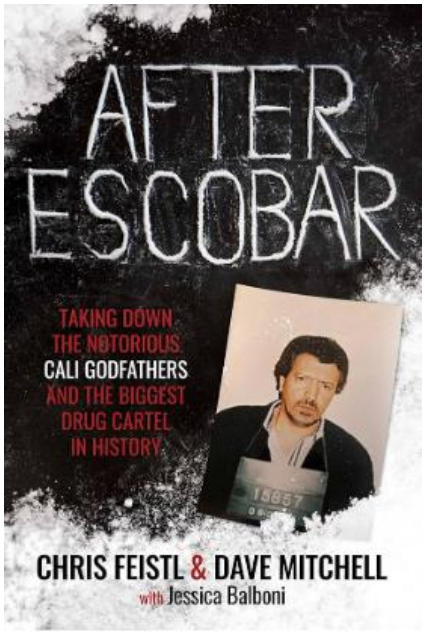
Наприкінці звіту розглянуто розвиток передових технологій, які формують наступну фазу цифрових фінансів. Особлива увага присвячена доказам з нульовим розголошенням (ZKP), повністю гоморфному шифруванню (FHE), мультипартійним схемам підпису, квантовій криптографії, системам самосуверенного цифрового ідентифікатора та новим формам міжланцюгової взаємодії. Ці технології стають ключовими як для інноваційних ринкових рішень, так і для регуляторів, які впроваджують моделі «нагляду в реальному часі» та «приватність-зберігаючого контролю». Звіт наголошує, що ефективне майбутнє цифрових активів залежить від здатності регуляторів інтегрувати ці технології у системи фінансового моніторингу, кібернагляду та управління системними ризиками, забезпечуючи баланс між інноваціями, стійкістю та захистом користувачів.

Висновки:

- **Цифрові активи перетворилися на стійку глобальну екосистему,** яка охоплює споживачів, бізнес і інфраструктурні платформи.
- **Основні ризики ринку зосереджені у технічних вразливостях,** зокрема смартконтрактах, оракулах, підробці ключів та складних схемах атак.
- **Блокчейн-аналітика стала ключовим механізмом виявлення незаконної діяльності,** дозволяючи ідентифікувати транзакції, пов’язані гаманці та робити замороження активів.
- **Регулятори посилюють взаємодію з ринком,** створюють узгоджені режими нагляду та впроваджують технологічні інструменти для роботи з цифровими активами.

Рекомендовані матеріали

Світ після Ескобара: як еволюціонував наркобізнес і чому він нагадує сучасну фінансову систему [12]



Книга від колишніх агентів Управління боротьби з наркотиками (DEA) Кріса Фейстла та Дейва Мітчелла — це не просто документальна розповідь про кінець легендарної епохи наркоторгівлі, а глибоке соціальне, політичне й економічне дослідження того, що сталося після знищення імперії Пабло Ескобара.

Вона демонструє, що смерть найвідомішого наркобарона означала не кінець ери насильства, а лише трансформацію злочинної системи у більш складну, гнучку й глобалізовану форму. Автори підходять до питання не як до чергової кримінальної історії, а як до аналізу соціального феномена, що змінив політику, економіку й навіть культуру Латинської Америки.

Після ліквідації Медельїнського картелю у 1993 році світ сподівався на нову епоху стабільності, але, як показує дослідження, вакуум влади породив не мир, а роздроблення злочинного світу на сотні дрібних, але високоорганізованих структур. Замість однієї централізованої організації виникла мережа картелів другого покоління — гнучких, технологічних і менш помітних. Вони позбулися культів особистості, характерних для епохи Ескобара, натомість перейшли до корпоративної моделі управління, де головну роль відіграє прибуток і контроль над логістикою, а не демонстрація сили. У цьому сенсі «після Ескобара» почалася не епоха занепаду злочинності, а епоха її еволюції.

Автори книги підкреслюють, що ключовим фактором цієї трансформації стала глобалізація. Якщо раніше наркотики вироблялися, транспортувалися та продавалися в межах одних і тих самих регіонів, то після 1990-х років відбувся справжній розрив географічних меж. Кокаїнова паста з Болівії і Перу потрапляла до рук мексиканських картелів, звідки через Карибський басейн або Західну Африку вона рухалася до Європи. Ці маршрути перетворилися на багаторівневі транзитні ланцюги, у яких брали участь міжнародні транспортні компанії, корумповані митники, брокери, морські оператори, банкіри та юристи. Сучасна наркосистема — це більше не вертикальна піраміда, а горизонтальна мережа, що нагадує транснаціональну корпорацію з диверсифікованими ризиками й прибутками.

Вражає те, як автори показують зміну природи влади у злочинному світі. Якщо Ескобар будував свою імперію на страху, показовому насильстві й контролі над територією, то сучасні кримінальні лідери володіють владою завдяки контролю над фінансами й інформацією. Гроші стали головною зброєю. Більше не потрібно воювати з державою — достатньо купити її представників. Тіньовий капітал почав проникати в легальні галузі: енергетику, агробізнес, логістику, будівництво, навіть спорт. У результаті, як підкреслюють автори, корупція перетворилася на форму економічної адаптації, а злочин — на частину офіційної економіки.

Особливо глибоко досліджується вплив наркоторгівлі на соціальні структури Латинської Америки. Після падіння Медельїнського картелю тисячі бойовиків, найманців і дрібних дилерів опинилися без засобів існування. Частина з них увійшла до нових угруповань, а частина — у політику та бізнес. У Колумбії, Венесуелі й Еквадорі виникли «гібридні» структури, які одночасно

[12] https://www.amazon.com/dp/B0DTGK4L19

контролюють незаконні копальні, аграрні підприємства й політичні партії. У книзі наведено приклади того, як колишні наркодилери фінансують виборчі кампанії, підтримують місцеві громади, роздають гуманітарну допомогу й навіть інвестують у школи, створюючи ілюзію соціальної відповідальності. Така мімікрія злочинності під «філантропію» — один із найнебезпечніших феноменів сучасності, що стирає межу між законним і незаконним.

Автори детально описують і роль міжнародних суб'єктів, насамперед США. Програма «Plan Colombia», запущена в 2000 році, мала на меті знищити наркотрафік через військову допомогу та зміцнення правоохоронної системи. Проте, як показує аналіз, ця політика мала подвійний ефект. Вона дійсно послабила великі картелі, але водночас посилила залежність держави від зовнішнього фінансування, що зробило уряд уразливим до політичного тиску. Мільярди доларів американської допомоги фактично легалізували нову форму «анти-картельного бізнесу» — приватні підрядники, консультанти з безпеки, аналітичні центри та політичні лобісти отримували надприбутки з антинаркотичних програм. Як іронічно зазначають автори, «боротьба з наркотиками стала бізнесом не меншим, ніж сам наркотрафік».

У книзі багато уваги приділено і зміні у світосприйнятті. Образ Ескобара став символом культури насильства, але водночас і міфом про соціального месника. Автори детально аналізують, як кінематограф, медіа та масова культура романтизували злочинця, створивши з нього поп-ікону. Цей «ескобаризм» поширився далеко за межі Колумбії — у Мексиці, Бразилії, навіть у США та Європі, де Ескобар став метафорою протесту проти системи. Автори застерігають: така героїзація злочину формує нову моральну кризу, у якій успіх оцінюється не за законністю дій, а за рівнем впливу й багатства.

Надзвичайно важливим є висновок книги про те, що сучасний наркотрафік більше не існує у вакуумі. Він тісно пов'язаний із фінансовими ринками, цифровими валютами, системою офшорів і глобальними банками. Тепер наркогроші відмиваються не через валізи готівки, а через криптовалютні платформи, фіктивні стартапи й благодійні фонди. Таким чином, злочинність перестала бути локальною — вона стала невидимою частиною світової економіки.

У своїх висновках Фейстл і Мітчелл наголошують: традиційні стратегії вичерпали себе. Сучасна система злочинності не має центру, отже, з нею не можна боротися методами ліквідації «голів картелів». Необхідні комплексні реформи, які включають прозорість фінансів, незалежність судів, міжнародну координацію моніторингу руху капіталів і реальний контроль над політичним фінансуванням. Лише тоді можна буде розірвати коло, у якому злочин і влада продовжують взаємно легітимізувати одне одного. Автори переконують, що сьогоднішня глобальна система наркобізнесу — це дзеркало сучасної економіки, у якій злочин і капітал стали невіддільними складовими однієї реальності.

Інші новини

Компанії-примари: як попри реформи Велика Британія залишається осередком корпоративних зловживань [13]

Попри масштабні реформи, спрямовані на посилення прозорості корпоративного сектору, серйозні зловживання британським корпоративним реєстром Companies House продовжують множитися. Розслідування опубліковане Compliance Corylated свідчить, що навіть після набрання чинності Законом про економічні злочини та корпоративну прозорість (Economic Crime and Corporate Transparency Act, ECCTA 2023), шахраї швидко адаптувалися до нових умов, знаходячи способи обходу перевірок особи та вимог до верифікації компаній. Нові правила

[13] https://www.compliancecorylated.com/news/serious-abuse-of-the-uk-corporate-register-continues-despite-reforms/

зобов'язали корпоративних сервіс-провайдерів (CSP) проходити авторизацію та виконувати функції з перевірки клієнтів, але навіть ці кроки не змогли повністю запобігти появі фіктивних утворень, що маскуються під легальні компанії.

Аналітики ринку фінансової безпеки, зокрема експерт із фінансових злочинів Рей Блейк, зафіксували появу нової хвилі компаній, які не просто приховують кінцевих власників, а й самі пропонують послуги з реєстрації фіктивних структур. Наприклад, компанія Register Your Meme Ltd, зареєстрована 3 жовтня 2025 року, пропонує оформлення юридичних осіб для так званих meme coins — криптовалют сумнівного походження, створених для спекуляцій. Вебсайт цієї фірми навіть генерує випадкові дані осіб для заповнення реєстраційних документів, фактично пропонуючи послугу створення компаній без будь-якої ідентифікації чи перевірки достовірності відомостей. Такий підхід підриває саму суть реформ, покликаних забезпечити прозорість корпоративного середовища та підвищити довіру до бізнесу, зареєстрованого у Великій Британії.

Попри офіційні заяви Companies House про те, що введення обов'язкової верифікації директорів і власників з істотною участю покликане покращити якість даних та боротися зі зловживаннями, експерти визнають, що злочинці залишаються на крок попереду. Як зазначає Кетрін Вестмор із Центру фінансів і безпеки RUSI, будь-яка система, заснована на декларативному принципі, створює можливості для обходу правил. За її словами, британські корпоративні структури залишаються привабливими для кримінальних груп, оскільки сприймаються як низькоризиковий інструмент для створення легального фасаду.

Блейк звертає увагу на ще небезпечнішу тенденцію: з'являються структури, що пропонують послуги з відкриття рахунків і переказу коштів під виглядом платіжних провайдерів, хоча насправді вони не мають відповідних ліцензій і не перебувають під наглядом фінансових регуляторів. Деякі з них зареєстровані одночасно як маркетингові-агенції чи IT-компанії, що дозволяє їм маскувати реальну діяльність. У цих випадках одна й та сама особа може фігурувати як засновник декількох таких фірм — і як власник, і як постачальник послуг, що створює складну мережу для фінансових махінацій і відмивання коштів.

Особливо тривожним є те, що деякі з цих структур реєструються за очевидно неправдоподібними адресами — зокрема, у будівлях історичних пам'яток. Так, нещодавні випадки показали, що низка компаній була зареєстрована у Вежі Лондона (Tower of London), де розташовані житлові приміщення для вартових (Beefeaters). Один із таких суб'єктів навіть заявляв, що надає послуги алгоритмічної торгівлі, попри відсутність ліцензії від Financial Conduct Authority (FCA) та наявність у списку попереджень цього регулятора. Попри це, компанія залишається у реєстрі, а її сайт продовжує функціонувати, що підкреслює неефективність контролюючих механізмів і недостатню координацію між FCA та Companies House.

Блейк застерігає, що ситуація може стати ще гіршою, адже в новій системі саме корпоративні сервіс-провайдери стануть основними агентами, відповідальними за перевірку ідентичності директорів і кінцевих бенефіціарів. Якщо частина таких суб'єктів сама діє у тіні, то ризики фальсифікацій лише зростатимуть. Тим більше, що закон не зобов'язує громадян Великої Британії користуватися послугами CSP — будь-хто може зареєструвати компанію самостійно, створюючи простір для маніпуляцій і зловживань. Кримінальні групи можуть оформлювати фірми на підставних осіб або навіть навчати клієнтів, як проходити перевірки, використовуючи викрадені дані чи підроблені документи.

Водночас самі регулятори визнають, що протидія такій діяльності є складною. Представники Companies House повідомляють про вдосконалення аналітичних систем, здатних виявляти аномалії на етапі подання даних, і про тіснішу взаємодію з правоохоронними органами. Проте результати цих зусиль поки що не відповідають масштабам проблеми. Більше того, навіть символічні випадки, як-от фіктивні компанії, зареєстровані за адресами урядових установ чи палаців, демонструють слабкість перевірочних процедур.

Таким чином, попри формальне посилення регулювання, Велика Британія продовжує залишатися уразливою до зловживань у сфері корпоративної реєстрації. Нові вимоги ECCTA — крок у правильному напрямку, але вони не усунули головну причину проблеми: низьку якість первинних даних та відсутність реального контролю за їх достовірністю. Без системної координації між Companies House, FCA і правоохоронними органами, а також без публічної підзвітності корпоративних сервіс-провайдерів, реформа ризикує залишитися косметичною.

Сучасна динаміка зловживань свідчить, що прозорість корпоративного реєстру — це не стільки технічне питання перевірки документів, скільки тест на здатність держави протистояти системним формам фінансової злочинності. Велика Британія, яка прагне відновити свою репутацію як безпечної юрисдикції для бізнесу, мусить зробити висновки: реальна ефективність реформ визначатиметься не обсягом ухвалених актів, а спроможністю їхнього реального застосування на практиці.

Для загального розвитку

Ринок викрадених даних: як тіньова економіка інформації перетворюється на глобальну загрозу безпеці [14]

Світова індустрія торгівлі викраденими даними перетворилася на один із найнебезпечніших і найменш контрольованих тіньових ринків XXI століття. Розслідування OCCRP розкриває масштаби цього явища, показуючи, що торгівля персональними, корпоративними й урядовими даними давно перестала бути сферою дрібного шахрайства. Це — глобальний нелегальний бізнес, який функціонує за законами ринку, має власну інфраструктуру, фінансові потоки, «фірмових» постачальників і навіть систему довіри між злочинцями. І головне — його наслідки виходять далеко за межі кіберпростору, впливаючи на безпеку держав, політику та фізичну безпеку людей.

Розслідування показує, що обіг викрадених даних тепер відбувається не лише у «даркнеті» — він має цілком легальні фасади. Створено розгалужену мережу компаній, які офіційно позиціонують себе як аналітичні або маркетингові агентства, проте насправді купують і продають інформацію, здобуту незаконним шляхом. Часто ці структури діють із країн, де законодавство про захист даних слабке або не передбачає міжнародного контролю — таких як ОАЕ, Сінгапур, Панама, Сербія чи Малайзія. Саме там відбувається «відмивання» даних: викрадена інформація агрегується, очищується від очевидних ознак злому і виставляється на продаж у вигляді «аналітичних масивів».

OCCRP виявило, що на цьому ринку діють сотні «дилерів» — посередників, які працюють за принципом комісійних агентів. Вони купують інформацію у хакерських груп або внутрішніх інсайдерів компаній, після чого перепродають її через спеціалізовані платформи. Деякі з цих

[14] https://www.occrp.org/en/feature/data-dealers-and-bomb-plots-inside-the-netherlandss-shadow-market-for-stolen-data

платформ функціонують як біржі: користувачі створюють акаунти, отримують рейтинги, можуть виставляти «товари» — цілі бази даних або окремі категорії персональної інформації. Цей процес набув настільки комерціалізованого вигляду, що в деяких випадках злочинці навіть пропонують гарантії повернення коштів, якщо дані виявляться «неповними або застарілими».

Особливо загрозливим є те, що масштаби викраденої інформації колосальні. Йдеться не про тисячі, а про мільярди записів, серед яких — повні біографічні профілі громадян, історії транзакцій, записи з мобільних операторів, логіни до корпоративних поштових скриньок, копії паспортів і навіть медичні дані. В OCCRP зазначається, що в багатьох випадках ці масиви зламуються не одинично, а «пакетами» — тобто одразу кілька великих систем стають жертвами нападу, після чого їхні бази інтегруються у спільні каталоги. Такий об'єднаний набір дозволяє зловмисникам відстежувати рух людей, будувати мережеві зв'язки між окремими особами та навіть створювати профілі з передбаченням поведінки.

Найбільш тривожним аспектом розслідування стало те, що ці бази почали використовуватися не лише для фінансових махінацій чи шахрайства, а й для реальної злочинної діяльності. Один із розкритих випадків показує, що злочинна група, яка планувала теракт у Західній Європі, придбала у даркнеті дані зламаних мобільних операторів і використала їх для відстеження переміщень своїх цілей. Завдяки цим даним злочинці отримували координати, дані GPS, записи про дзвінки та навіть інформацію про банківські операції. Це підтверджує, що торгівля даними перестала бути лише проблемою кіберпростору — вона стала загрозою національній безпеці.

Ще один аспект, висвітлений у матеріалі, — це напівлегальні витоки з боку самих компаній. Корпорації, що збирають великі обсяги персональної інформації (банки, телекомунікаційні оператори, страхові компанії, соціальні мережі), нерідко самі стають частиною «сірого ринку». Працівники цих структур продають дані клієнтів за винагороду, а керівництво заплющує очі на втрати, щоб уникнути скандалу. OCCRP вдалося ідентифікувати конкретні приклади, коли співробітники приватних охоронних компаній та IT-відділів передавали дані клієнтів «на сторону» через Telegram-канали або хмарні сервіси.

Розслідувачі також вказують, що активізація «чорного ринку даних» збігається з геополітичними тенденціями. Держави-агресори, зокрема Росія, Іран і КНДР, давно використовують кібератаки для шпигунства та дестабілізації. Однак сьогодні вони отримали новий інструмент — купівлю даних, викрадених не власними силами, а з відкритого тіньового ринку. Таким чином, зламані бази стають універсальним розвідувальним ресурсом: їх можна використати для виявлення посадовців, аналітиків, військових, або навіть для цілеспрямованого тиску й шантажу.

OCCRP вказує, що за останні роки сформувався цілий шар «дилерів», які співпрацюють із державними структурами. У росії, наприклад, такі компанії працюють під виглядом маркетингових агентств і водночас передають потрібну інформацію спецслужбам. Вони продають частину даних комерційним клієнтам, а іншу — надають «по запиту» ФСБ чи Міністерству внутрішніх справ. У такий спосіб створюється закрита екосистема, у якій кримінальні та державні інтереси повністю збігаються.

Особливу увагу розслідувачі звертають на використання штучного інтелекту у сфері торгівлі даними. Алгоритми навчаються на викрадених масивах інформації, автоматично створюють профілі, сегментують користувачів і навіть прогнозують, які записи матимуть найбільшу «ринкову цінність». Це робить тіньовий ринок даних ще більш живучим: тепер йому не потрібні хакери, які вручну викрадають інформацію — її аналіз, інтеграція та перепродаж відбуваються автоматично.

Розслідування також порушує питання про неефективність міжнародного законодавства. Навіть у країнах, де діє GDPR, санкції здебільшого накладаються на компанії, що не забезпечили належного захисту, а не на злочинців, які викрали дані. Тим часом глобальні платформи обміну

інформацією, такі як Telegram, Reddit або Discord, залишаються каналами поширення таких баз. Міжнародна поліція часто безсила — більшість серверів розташована у юрисдикціях, де не передбачено екстрадиції кіберзлочинців.

Варто також зазначити, що феномен ринку викрадених даних має і моральний вимір. Жертви часто навіть не знають, що їхня інформація циркулює на чорному ринку. Витік може включати все — від номерів документів до приватних фотографій і записів відеоспостереження. У результаті люди стають мішенями для шантажу, фішингу, соціальної інженерії або кампаній з дискредитації. Журналісти OCCRP наводять випадки, коли викрадені дані використовувалися для маніпуляцій із політичними опонентами, компрометації активістів чи тиску на дипломатів.

Таким чином, ринок викрадених даних — це не просто технологічна проблема, а глибоко політичний і соціальний феномен. Він відображає кризу довіри до цифрових систем і слабкість міжнародних механізмів контролю. Поки уряди зосереджені на захисті від конкретних хакерських атак, глобальна система злочинного обігу інформації розвивається як повноцінна індустрія.

У підсумку OCCRP робить однозначний висновок: викрадені дані — це нова форма зброї. Вони дозволяють контролювати, маніпулювати, шантажувати, а іноді — навіть знищувати. У світі, де інформація перетворилася на валюту, контроль над нею стає інструментом влади.

Ваша думка важлива!

1. Як фінансова розвідка та СПФМ мають адаптувати свої системи моніторингу для виявлення гібридного фінансування тероризму та військових дій?
2. З огляду на домінування CMLOs, які використовують IVTS та обхід валютного контролю, як західні СПФМ і правоохоронні органи можуть створити дієву модель протидії, враховуючи обмежену співпрацю з КНР?
3. Як регуляторам і СПФМ слід змінити підхід до нагляду, щоб ефективно боротися зі зловживаннями корпоративними реєстрами (як у Великій Британії) та забезпечити якісну звітність у високоризикових секторах (наприклад, DPMS)?
4. Які практичні кроки мають бути зроблені регуляторами (SupTech) та фінансовими установами, щоб перейти до ex-ante контролю AI-моделей та захистити фінансову систему від системних ризиків DeFi та алгоритмічної упередженості?
5. Чи готові українські інституції протистояти злочинним мережам, що мають політичне прикриття, і що потрібно змінити в системі фінансового моніторингу для цього?
6. Як Україна може запобігти тому, щоб її власна оборонна промисловість не стала частиною глобальних схем переозброєння через фіктивні документи та посередників? Як збалансувати національну безпеку, експортну політику та прозорість у сфері продажу зброї?
7. Яким чином штучний інтелект може стати інструментом підвищення фінансової інклюзії в Україні — особливо для мікро- та малого бізнесу, внутрішньо переміщених осіб та регіонів, віддалених від фінансових центрів?
8. Як токенізація реальних активів (нерухомості, землі, інфраструктурних проєктів) може вплинути на інвестиційну привабливість України та залучення капіталу, і чи готове чинне законодавство до такого рівня цифровізації прав власності?

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-2025-46

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].