



Міністерство
фінансів
України

Методологічний бюлетень AML

№42/2026



Зміст

Бангкокська програма МВФ і Світового банку: 12 ключових міркувань щодо стійкості фінансових послуг до кібершахрайства	3
Потоки стейблкоїнів у глобальній економіці: як валютний контроль та кризи прискорюють цифрову доларизацію	7
Загроза цифровому шифруванню: чому оновлювати криптографічний захист потрібно вже сьогодні	10
ESMA: постачальники послуг із криптоактивами мають припинити обслуговування tokenів, що не відповідають MiCA	13
Рекордні стягнення Мінфіну США з Bank of America: «аутсорсинг» виявлення підозрілих операцій як самостійне порушення	16
Пруденційний нагляд за крипторинком ЄС: практичні пропозиції ЕБА в межах ревізії MiCA	19
Новий санкційний пакет ЄС проти військово-промислового комплексу росії	22
Корупція та організована злочинність у Молдові: динаміка кримінальних ринків та межі відновлення держави	24
Багаторівнева рамка RUSI та місце фінансових інструментів у протидії ворожій кіберактивності	28
Тіньова логістика нарко-мереж Меконгу	32
Мілітаризація та кримінальні ринки: економічні вигоди учасників конфлікту на сході Демократичної Республіки Конго	35
Як корупція та організована злочинність трансформували Йоганнесбург	38
Бюлетені та кулі: анатомія ринку замовних убивств напередодні виборів	42
Кіберстратегія Китаю та прогалини західного стримування: відеокоментар RUSI	45
Як кіпрський офіс Deloitte переписував історію активів Романа Абрамовича	47

**Слухайте цей бюлетень
у форматі подкасту**



16:50



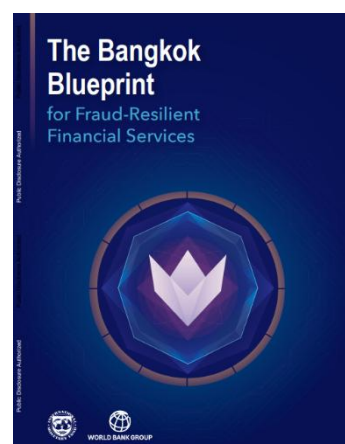
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для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

Бангкокська програма МВФ і Світового банку: 12 ключових міркувань щодо стійкості фінансових послуг до кібершахрайства¹

Міжнародний валютний фонд і Група Світового банку представили на щорічних зборах 2026 року в Таїланді спільний документ «The Bangkok Blueprint for Fraud-Resilient Financial Services» (далі – Бангкокська програма). Він розвиває Балійський порядок денний із фінтеху 2018 року, який свого часу заклав підходи до використання цифрових фінансових послуг з управлінням пов'язаними ризиками. Відправна теза авторів полягає в тому, що кібершахрайство у фінансовому секторі стало «системним політичним викликом, а не низкою ізольованих злочинних дій», а відтак потребує скоординованих дій у фінансовому секторі й за його межами. Документ прямо позиціонується як неприписувальна рамка, а не формальна політична настанова МВФ і Світового банку: 12 ключових міркувань (КС) не мають обов'язкової послідовності впровадження, але автори рекомендують починати з оцінки ризиків і прогалин та ухвалення національної стратегії, які задають логіку подальших кроків. Водночас програма слугуватиме орієнтиром для діалогу персоналу обох інституцій з національними органами влади та для їхнього внеску в роботу органів, що встановлюють стандарти.



Методологічно важливим є робоче визначення предмета. Кібершахрайство розуміється як використання цифрових технологій і психологічної маніпуляції жертвами, переважно споживачами, з метою отримання незаконної вигоди через авторизовані або неавторизовані операції із залученням суб'єктів у фінансовому секторі чи поза ним. Типологія розмежовує авторизоване шахрайство, тобто шахрайство, спричинене обманом (шахрайство з авторизованими кредитовими переказами (APP-fraud), інвестиційні та криптошахрайства, шахрайство з купівлею та видаванням себе за іншу особу), і шахрайство «першої сторони» (зловживання власним рахунком чи гаманцем, неправомірні оскарження та чарджбеки), від неавторизованого – масової компрометації платіжних систем, мереж еквайрингу, постачальників послуг і платформ, а також цільових неавторизованих операцій. Фішинг, компрометація облікових даних, SIM-swap чи захоплення рахунку розглядаються не як окремі види, а як методи, що можуть обслуговувати будь-який із них. Цьому відповідають два цикли: цикл шахрайства (підготовка,

¹ <https://documents1.worldbank.org/curated/en/099256510092673908/pdf/IDU-c601445e-3022-4b26-ade2-fdede483693c.pdf>

виконання, етап після виконання, коли кошти виводяться або приховуються) і цикл протидії (запобігання, виявлення, реагування й відновлення).

Емпірична база документа фіксує масштаб, який уже не дозволяє розглядати шахрайство як побічний ризик цифровізації. За останнє десятиліття кіберподії у фінансовому секторі становили близько 10% усіх кіберподій у світі й зросли вдсятеро, а кількість випадків кібершахрайства майже потроїлася. Аналіз FATF засвідчив, що 90% із 165 оцінених юрисдикцій вважають шахрайство значною загрозою відмивання коштів; 85% регуляторів у 60 юрисдикціях називають його головним ризиком для споживачів (дані ОЕСР). Національна оцінка ризиків відмивання коштів США оцінює фактичні втрати споживачів у 2024 році в 195,9 млрд дол. США проти лише 12,7 млрд зареєстрованих, що демонструє масштаб латентності. Глобальний альянс проти шахрайства (GASA) оцінив світові втрати 2025 року майже в пів трильйона доларів. Від 50 до 70% дорослих у світі стикалися зі спробами онлайн-шахрайства, причому найчастіше жертвами стають особи віком 29–60 років, а не лише літні люди. Попри це, на протидію шахрайству в провідних юрисдикціях припадає менше 1% ресурсів поліції.

Автори виокремлюють три структурні тенденції. По-перше, шахрайство стало транснаціональним злочином, нерозривно пов'язаним з організованою злочинністю та мережами професійного відмивання коштів, а також з торгівлею людьми (для утримання шахрайських центрів, де жертв примушують до шахрайства), наркотрафіком і тероризмом. По-друге, штучний інтелект, зокрема дипфейки, автоматизація через ботів і платформи «фішинг як послуга», діє як «мультиплікатор сили», а агентний ШІ та нові моделі взаємодії з клієнтом можуть відкривати нові вразливості. По-третє, загроза зміщується від неавторизованого до авторизованого шахрайства, де жертву змушують самостійно ініціювати й підтвердити платіж, а значна частина випадків починається в соціальних мережах і через SMS-фішинг. Звідси ключова теза: оскільки шахрайство переважно зароджується поза фінансовим сектором – на цифрових платформах, в електронній комерції та телекомунікаційних мережах, – заходи фінансового сектору є необхідними, але недостатніми, і потрібна відповідь «на рівні всієї екосистеми».

Перша опора (КС1–КС2) стосується стратегічних і правових засад. Національна стратегія має спиратися на актуальну оцінку ризиків, мати високий рівень політичної відповідальності, визначений провідний орган, вимірювані цілі, план дій, механізми моніторингу та стратегію публічної комунікації. Правова рамка, за КС2, має надати органам влади чотири групи повноважень: законодавчу основу для розподілу відповідальності за шахрайські операції між фінансовими установами, клієнтами й технічними постачальниками послуг (особливо у випадках, коли клієнта ошукали, але платіж формально авторизований); чіткі шлюзи для обміну інформацією між приватними установами, які нині, за оцінкою авторів, використовуються недостатньо через правову невизначеність і брак стимулів; прискорені повноваження щодо заморожування, арешту й повернення доходів від шахрайства, зокрема криптоактивів, і взаємне визнання рішень про заморожування між юрисдикціями; правила платіжних систем, які підтримують повернення коштів без підризу остаточності розрахунків. Наглядові процедури мають охоплювати метрики втрат від шахрайства, обсяги й зміст скарг, результативність і валідацію моделей виявлення, а також те, як установи мінімізують ризик рахунків-«дропів».

Друга опора (КС3–КС6) переносить акцент із реагування на проектування послуг. Органи влади можуть визначати мінімальні ризик-орієнтовані стандарти протидії шахрайству: безпечну ідентифікацію під час встановлення ділових відносин, автентифікацію операцій у застосунку, перевірку отримувача, скринінг у реальному часі, а також вимогу, щоб бізнес-модель не послаблювала контролі заради зручності клієнта. Принципово, що базовий захист від шахрайства має бути частиною безпечної послуги, «а не опцією, яку окремо оплачує кінцевий користувач». Для авторизованих платежів КС4 передбачає попередження, додаткові кроки підтвердження, періоди «охолодження» й тимчасові затримки високоризикових операцій, які мають реально переривати шахрайську операцію, а не просто перекладати відповідальність на клієнта через формальні застереження. Там, де контролів окремої установи недостатньо, рекомендовано спільні антифрод-утиліти: реєстри рахунків-«дропів» і шахрайських рахунків, централізовані бази даних про шахрайство, сервіси перевірки отримувача, антишахрайські центри. КС6 допускає активацію заходів стримування лише на підставі індикаторів ризику, без попереднього встановлення відповідальності.

Для сфери ПВК/ФТ ключовим є КС8. Національна оцінка ризиків має розкривати, які види шахрайства генерують найбільші доходи та як їх відмивають, а суб'єкти первинного фінансового моніторингу мають використовувати її результати для формування індикаторів підозрілості й правил моніторингу операцій. Документ наголошує на перетині превентивних заходів ПВК/ФТ і антифрод-контролів: моніторинг у реальному часі може бути налаштований на ознаки як відмивання коштів, так і шахрайства, а заходи належної перевірки мають бути динамічними й здатними розпізнавати згенеровані ШІ фото, відео та дипфейки. Наглядовим органам рекомендовано тематичні перевірки й горизонтальні огляди контролів, пов'язаних із шахрайством; зазначено, що в окремих країнах саме на органи нагляду у сфері ПВК/ФТ покладено нагляд за антифрод-заходами. Окремо підкреслено, що для повідомлення про підозрілу операцію не потрібен доказ злочину, що FATF вивчає можливість застосування свого інструментарію до шахрайства із залученням соціальних мереж і операторів зв'язку, а державам варто чітко врегулювати «безпечні гавані» для обміну інформацією між приватними установами із захистом від цивільної відповідальності. У врізці 3 нагадано, що частина країн досі відстає у впровадженні Стандартів FATF щодо віртуальних активів, а злочинці використовують ці прогалини для відмивання доходів від шахрайства.

Опора правозастосування (КС9) акцентує на пріоритизації справ, що руйнують транснаціональні угруповання та професійних відмивачів, на поверненні активів як пріоритеті розслідувань, участі в міжнародних механізмах (на кшталт механізму Інтерполу I-GRIP для оперативного зупинення платежів і Глобальної робочої групи щодо шахрайських центрів), притягненні до відповідальності юридичних осіб, зокрема компаній-оболонок, і криміналізації відмивання третіми особами, адже «відмивання як послуга» є ключовим чинником великого шахрайства. Як приклад результативності наведено операцію First Light у 61 країні, що завершилася вилученням активів на 257 млн дол. США. Для України програма має прикладне значення з огляду на законопроект № 16013 про реєстр осіб, платіжні операції яких потребують посиленого контролю, підтриманий Верховною Радою в першому читанні у вересні 2026 року: Бангкокська програма розглядає такі

реєстри саме як спільні антифрод-утиліти, ефективність яких залежить від правил обміну інформацією, захисту даних, пропорційності та чіткого розподілу відповідальності за збитки.

Висновки

Розподіл відповідальності за авторизоване шахрайство потребує законодавчої основи: КС2 вимагає закріпити в законі критерії розподілу збитків між банком, клієнтом і технічним постачальником саме для випадків, коли платіж формально авторизований під впливом обману; без цього судова практика залишатиметься непередбачуваною, а установи не матимуть стимулу інвестувати в запобігання.

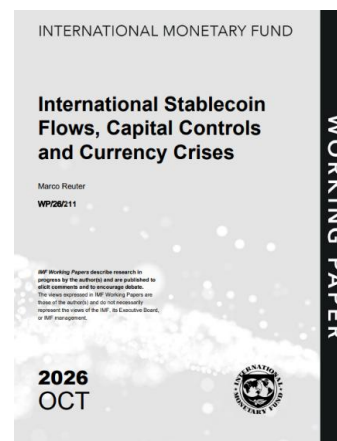
Національна оцінка ризиків має доходити до рівня індикаторів: за КС8 результати НОР щодо видів шахрайства, які генерують найбільші доходи, і способів їх легалізації мають перетворюватися на індикатори підозрілості й правила моніторингу операцій у СПФМ, а наглядові органи – перевіряти це через тематичні та горизонтальні огляди.

Реєстр рахунків-«дропів» варто проєктувати як спільну антифрод-утиліту: Бангкокська програма пов'язує ефективність таких реєстрів із «безпечними гаванями» для обміну інформацією, прозорими правилами фінансування, захистом персональних даних і пропорційністю обмежень, що прямо релевантно до доопрацювання законопроекту № 16013 до другого читання.

Злиття функцій протидії шахрайству, кібербезпеки та фінмоніторингу є очікуваною практикою: інтеграція цих підрозділів у фінансових установах, динамічна ідентифікація зі спроможністю виявляти дипфейки та заходи стримування на підставі лише індикаторів ризику мають стати предметом наглядової оцінки, а не добровільною ініціативою окремих банків.

Потоки стейблкоїнів у глобальній економіці: як валютний контроль та кризи прискорюють цифрову доларизацію²

Робочий документ Міжнародного валютного фонду (МВФ) представляє першу масштабну методологію оцінки глобальних транскордонних потоків стейблкоїнів на рівні країн та емпіричний аналіз їхньої ролі в обході заходів валютного контролю (CFMs) і заміщенні національних валют під час валютних криз. Робота ліквідує критичну «сліпу зону» в офіційній статистиці платіжних балансів, спираючись на аналіз понад 35 мільярдів ончейн-транзакцій у семи EVM-сумісних блокчейнах (Ethereum, Tron, Binance Smart Chain, Arbitrum, Base, Optimism, Linea) за період із 2018 до 2025 року. Сукупний обсяг проаналізованих валових переказів двох домінуючих доларових стейблкоїнів – USDT (84%) та USDC (16%) – сягнув 21,4 трлн доларів США, охопивши 188 юрисдикцій.



Методологічний прорив дослідження полягає в подоланні псевдонімності блокчейн-адрес за допомогою дворівневої системи машинного навчання, валідованої зовнішніми джерелами. На першому етапі було сформовано навчальну вибірку з 437 775 некастодіальних гаманців: за допомогою великої мовної моделі розпізнавалися лінгвістичні та культурні маркери 6 мільйонів доменних імен ENS (наприклад, суфікси чи китайські слова), а також виокремлювалися гаманці, що взаємодіють суто з регіональними криптобіржами. На другому етапі градієнтний бустинг дерев рішень класифікував активні адреси за поведінковими ознаками (погодинні патерни активності протягом доби, реакція на перехід на літній час DST та зв'язок зі смартконтрактами), після чого регіональні ймовірності розподілялися по країнах за частками вебтрафіку бірж (для Китаю застосовано окрему модель, що усуває викривлення від використання VPN). Точність методології було підтверджено співпадінням із точністю до 15% з офіційною статистикою імпорту стейблкоїнів Центрального банку Бразилії (єдиного центробанку світу, що веде такий облік через валютні контракти) та внутрішніми даними бірж Binance і KuCoin.

Емпіричний аналіз показав, що ринок стейблкоїнів набув макроекономічного масштабу: річний обсяг трансферів зріс із 1,2 млрд доларів у 2018 році до понад 7 трлн доларів у 2025 році. При цьому близько 90% усього обсягу переказів має саме транскордонний характер, а розмір медіанної транзакції становить 300 доларів США (проти середнього чека в 10 853 дол США), що вказує на масове роздрібне використання як альтернативи дорогим банківським переказам. Географічна структура використання стейблкоїнів виявилася дзеркальною протилежною до традиційної міжбанківської системи SWIFT: якщо у SWIFT 85% обсягів циркулює між країнами з розвинутою економікою (AEs), то у стейблкоїнах 86% транскордонних переказів залучають країни

² <https://www.imf.org/-/media/files/publications/wp/2026/english/wp202611-source-pdf.pdf>

з ринками, що формуються, та країни, що розвиваються. Найбільшим коридором стали операції між самими країнами, що розвиваються (33% обсягу), тоді як коридор між розвиненими країнами становить лише 14%.

Концентрація збереження вартості у стейблкоїнах у країнах, що розвиваються є ще виразнішою: із 200 млрд доларів США загальних накопичень, зафіксованих на кінець 2025 року, 75% припадає саме на ринки, що розвиваються. Усі 20 перших позицій у світі за співвідношенням обсягів утримання стейблкоїнів до розміру ВВП належать країнам, що розвиваються. Зокрема, обсяг володіння цифровими доларами сягає 5,6% ВВП у Венесуелі, 4,1% ВВП в Україні (8,6 млрд доларів США), 1,4% ВВП у Нігерії та 0,83% ВВП у Туреччині (13,3 млрд доларів), тоді як у США цей показник становить лише 0,04% ВВП. Це свідчить про те, що для громадян нестабільних економік стейблкоїни стали головним інструментом порятунку заощаджень від інфляції та девальвації, а не просто інструментом біржових спекуляцій.

Дослідження наводить перші строго доведені докази використання стейблкоїнів для обходу регуляторних обмежень за допомогою методу подвійних різниць на основі 217 випадків запровадження заходів контролю за рухом капіталу. Встановлено, що після посилення обмежень на відтік капіталу транскордонна активність зі стейблкоїнами в країні зростає на 4% вже в перший місяць, сягає пікових 30% через пів року (додаткові 205 млн доларів на місяць для медіанної країни) і залишається на цьому плато навіть через рік. Найсильніший сплеск (до +40%) викликають обмеження за операціями капітального рахунку. При цьому виявлено ефект «храповика»: подальше скасування або послаблення валютних обмежень не призводить до повернення бізнесу та громадян до попередніх моделей фінансової поведінки, оскільки вони вже понесли незворотні витрати на створення криптогаманців і освоєння цифрових каналів переказу коштів.

Аналогічний ефект гістерезису підтверджено на вибірці 21 валютної кризи: у перший рік після настання кризи накопичення стейблкоїнів резидентами зростає на 75% (в середньому на 0,07 процентного пункту докризового ВВП, або 7,9 млрд доларів США у грошовому вимірі). При цьому накопичення стартує безпосередньо з моменту падіння курсу і не відкочується назад після стабілізації. Таким чином, МВФ доводить, що доларизація економік набула нової форми – швидкої, цифрової та незворотної, що вимагає включення ончейн-потоків до макроекономічного моніторингу та перегляду ефективності традиційних інструментів валютного регулювання.

Висновки

Домінування країн, що розвиваються, у глобальних потоках цифрового долара: стейблкоїни перетворилися на глобальну транскордонну роздрібну платіжну систему, де 86% транзакцій і 75% усього обсягу накопичень зосереджено в країнах, що розвиваються (в Україні накопичення сягнули 4,1% ВВП), що відображає пошук надійного засобу збереження вартості.

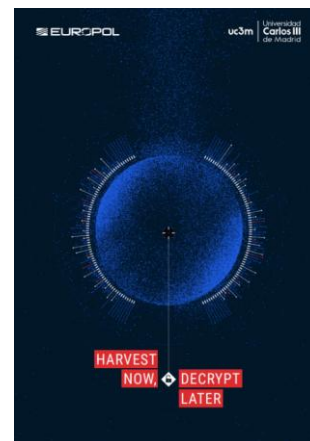
Необоротне зростання активності у відповідь на валютні обмеження: посилення обмежень на виведення капіталу зумовлює стрибок операцій зі стейблкоїнами на 30% протягом пів року; зворотне зняття бар'єрів не зменшує криптопотоки, демонструючи стійкий ефект звикання користувачів до нових інструментів.

Стрімка доларизація заощаджень під час валютних криз: входження країни у валютну девальвацію викликає чисте накопичення стейблкоїнів на 75% за рік, що значно випереджає історичні темпи зростання класичних валютних банківських депозитів і закріплюється на новому високому рівні.

Методологічне подолання анонімності для платіжного балансу: аналіз поведінкових патернів адрес довів можливість точного географічного картографування криптопотоків із верифікацією за даними центральних банків, що вимагає від фінансових регуляторів обов'язкового врахування ончейн-даних для оцінки зовнішнього сектору.

Загроза цифровому шифруванню: чому оновлювати криптографічний захист потрібно вже сьогодні³

Спільний звіт Європолу та Мадридського університету імені Карлоса III (UC3M) присвячений новій кіберзагрозі під назвою «Harvest Now, Decrypt Later» (HNDL) – «Перехопити зараз, розшифрувати пізніше». Суть цієї тактики проста: хакери або спецслужби вже сьогодні таємно перехоплюють і накопичують великі масиви зашифрованої інформації, хоча прочитати її зараз не можуть. Вони розраховують на те, що через кілька років або десятиліть з'являться потужні квантові комп'ютери, які легко зламують сучасний захист. Документ розроблено експертною групою Європолу для того, щоб оцінити реалістичність таких атак і дати державним органам, правоохоронцям, банкам та бізнесу чіткі інструкції, як захистити конфіденційну інформацію вже сьогодні.



Головна небезпека полягає в тому, що для цієї загрози зловмисникам не потрібен квантовий комп'ютер у даний момент. Вони діють як «колекціонери»: пасивно копіюють інтернет-трафік або викрадають зашифровані бази даних. Оскільки дані зашифровані, системи безпеки часто не бачать у цьому швидкої загрози, а жертва навіть не підозрює про витік. Проте класичні методи захисту, якими захищений увесь сучасний інтернет (зокрема алгоритми RSA та шифрування на еліптичних кривих ECC), тримаються на складних математичних задачах, які квантовий комп'ютер за допомогою алгоритму Шора зможе розв'язувати за лічені хвилини. Інший тип шифрування – симетричний (наприклад, стандарт AES-128, яким шифрують сам вміст файлів) – повністю не зламується, але його надійність зменшиться вдвічі, тому для безпеки треба переходити на довший ключ (AES-256).

У звіті детально розібрано, як саме ця загроза б'є по звичних цифрових інструментах. Популярний протокол безпечного інтернету TLS (який забезпечує безпечне з'єднання сайтів, роботу баз даних і VPN) залишається під ударом. Найбільш небезпечною є застаріла версія TLS 1.2 без механізму «прямої секретності» (PFS): якщо зловмисник збереже трафік, а в майбутньому квантовим шляхом розрахує головний ключ сервера, він зможе відкрити взагалі всі переговори та платежі за всі минулі роки. Сучасні версії, такі як TLS 1.3 та протокол для системних адміністраторів SSHv2, захищені краще, тому що створюють тимчасовий ключ для кожної окремої розмови. Але оскільки відкриті деталі цього обміну все одно записуються, потужний квантовий комп'ютер зможе підібрати ключі до кожного сеансу окремо. Така ж проблема є і в програмах для шифрування файлів та електронної пошти (OpenPGP): пароль від файлу ховається за допомогою відкритого ключа адресата, і якщо цей ключ колись зламують, відкриється весь архівний документ.

³ <https://www.europol.europa.eu/cms/sites/default/files/documents/Harvest-now-decrypt-later.pdf>

Зрозуміло, що не всі дані мають цінність через 10–20 років. Звичайні щоденні переписки чи одноразові паролі швидко втрачають актуальність. Проте є інформація, яка повинна залишатися таємною десятиліттями: державні секрети, дипломатичне листування, матеріали кримінальних розслідувань, імена таємних свідків та інформаторів, схеми критичної інфраструктури, медичні картки чи важливі комерційні патенти. Для оцінки ризику автори радять користуватися логікою «теорема Москви»: якщо час, протягом якого дані мають бути таємними, плюс час, потрібний державі на заміну всієї системи захисту, більший за час до появи квантового комп'ютера, то ці дані під загрозою вже сьогодні. Крім того, використання старих протоколів (як-от TLS 1.0 чи 1.1) небезпечно вже зараз без будь-яких квантових технологій, адже їх можна зламати звичайними сучасними комп'ютерами.

Щоб уберегтися від майбутнього зламу, Європол радить не чекати появи квантових машин, а впроваджувати заходи негайно. Найшвидший технічний крок – перейти на так званий «гібридний обмін ключами». Це спосіб, коли дані шифруються одночасно двома ключами: звичайним класичним і новим «постквантовим» (наприклад, алгоритмом ML-KEM/Kyber). Щоб прочитати такий файл, зломиснику доведеться зламати обидва замки одночасно. На організаційному рівні відомствам та компаніям необхідно перевірити всі свої програми на так звану «криптографічну гнучкість» (здатність швидко міняти шифри), припинити нескінченно зберігати старі архіви й видаляти непотрібну інформацію (принцип мінімізації даних), а головні електронні ключі тримати виключно на спеціальних фізичних чипах (HSM).

Висновки

Варто усвідомити реальність загрози випереджального перехоплення даних (HNDL) для інформації з тривалим терміном таємниці (державні таємниці, слідчі справи, медичні картки, патенти), адже для крадіжки та збереження зашифрованих масивів злоумисникам не потрібен квантовий комп'ютер сьогодні.

Необхідно терміново вимкнути застарілі інтернет-протоколи та відмовитися від небезпечних режимів без прямої секретності, перевівши корпоративні та державні мережі на мережі з обов'язковим створенням разових ключів для кожного сеансу.

Слід впроваджувати гібридні схеми шифрування, які поєднують звичайні цифрові ключі з новими постквантовими алгоритмами, щоб надійно захистити переписку й платежі від розкриття в майбутньому без збоїв у роботі наявних комп'ютерних систем.

Доцільно налагодити криптографічну гнучкість в установах : провести перевірку всіх використовуваних ключів і шифрів, надійно видаляти непотрібні старі архіви, а головні приватні ключі зберігати лише на захищених апаратних носіях (модулях HSM).

ESMA: постачальники послуг із криптоактивами мають припинити обслуговування tokenів, що не відповідають MiCA⁴



8 жовтня 2026 року Європейський орган з цінних паперів і ринків (ESMA) ухвалив висновок ESMA75-113276571-1742 щодо надання послуг із криптоактивами стосовно tokenів, прив'язаних до

активів (ART), і tokenів електронних грошей (EMT), які не відповідають вимогам Регламенту (ЄС) 2023/1114 про ринки криптоактивів (MiCA). Правовою підставою є стаття 29(1)(a) Регламенту (ЄС) № 1095/2010, що уповноважує ESMA надавати висновки національним компетентним органам (НКО) для формування спільної наглядкової культури та узгодженої наглядкової практики в Союзі. Документ адресовано насамперед НКО, однак його практичні наслідки безпосередньо стосуються всіх авторизованих постачальників послуг із криптоактивами (CASP), які працюють із клієнтами в ЄС, а отже, і операцій з найпоширенішими доларовими стейблкоїнами, емітенти яких не пройшли авторизацію за MiCA.

Висновок доповнює Питання-відповідь Європейської комісії № 2404 і попередню публічну заяву ESMA, які визначали, коли надання окремих послуг може становити публічну пропозицію, допуск до торгівлі чи розміщення ART або EMT. ESMA прямо зазначає, що не змінює цієї позиції та не стверджує, що будь-яка послуга щодо таких tokenів автоматично є публічною пропозицією чи допуском до торгівлі за статтями 16(1) або 48(1) MiCA. Натомість регулятор переносить аналіз в іншу площину – сумісності продовження послуг з обов'язками CASP за розділом V MiCA. «Невідповідними MiCA» визначено ART чи EMT, щодо яких не виконано умов законної публічної пропозиції або допуску до торгівлі в ЄС за розділом III чи IV MiCA, з урахуванням застосовних винятків і перехідних положень.

Центральне положення сформульовано однозначно: CASP не повинні надавати послуги з криптоактивами щодо ART чи EMT, які не відповідають MiCA. Обґрунтування спирається на статтю 66(1) MiCA – обов'язок діяти чесно, справедливо, професійно й у найкращих інтересах клієнтів. На думку ESMA, клієнт у такому разі зазнає ризиків, що впливають не з самої послуги, а з невідповідного статусу токена, тобто з відсутності гарантій на рівні емітента (права на погашення, вимог до резерву активів, корпоративного управління, розкриття інформації, нагляду). Ці ризики

⁴ https://www.esma.europa.eu/sites/default/files/2026-10/ESMA75-113276571-1742_Opinion_on_the_provision_of_crypto_asset_services_in_relation_to_non-MiCA-compliant_asset-referenced_tokens_and_e-money_tokens.pdf

не можуть бути належно виявлені, контрольовані чи пом'якшені засобами, які має CASP, тому надання будь-якої послуги за MiCA щодо такого токена створює презумпцію несумісності всіх послуг із вимогами статті 66(1): постачальник вважатиметься таким, що свідомо сприяє експозиції клієнтів до цих ризиків.

ESMA наводить три аргументи на користь такого підходу. Перший – запобігання систематичному обходу розділів II–IV MiCA: інакше активи однієї регуляторної категорії фактично підпадали б під різні стандарти залежно лише від того, чи були вони випущені відповідно до MiCA. Другий – рівні умови конкуренції: емітенти, що відповідають MiCA, несуть витрати на дотримання вимог щодо погашення, резервів, управління й розкриття інформації, тоді як невідповідні токени залишалися б на ринку без еквівалентних зобов'язань. Третій – довіра інвесторів, які не можуть розраховувати на однаковий рівень захисту, коли однакові активи підпадають під різні правові вимоги. Окремо зазначено, що обіг таких tokenів ускладнює для НКО контроль якості «білих книг», маркетингових комунікацій і того, чи не завдає торгівля шкоди роздрібним власникам.

Важливим є відхилення ESMA так званого «підходу розкриття інформації». Попередження, додаткові розкриття чи підтвердження з боку клієнта визнано недостатніми: вони не припиняють доступності й використання tokenів, а клієнт навряд чи здатен оцінити наслідки відсутності цілого комплексу гарантій, що діють колективно проти широкого спектра ризиків. Більше того, будь-яка оцінка, яку здійснює CASP, передбачала б складні правові та операційні судження, що різнитимуться за обсягом, методологією та висновками. Тому, на думку ESMA, захисту інвесторів, цілісності ринку й ефективності MiCA можна досягти «лише шляхом утримання від надання послуг», які полегшують доступ до таких tokenів або їх подальше використання.

Операційна частина висновку охоплює весь перелік послуг CASP: управління торговою платформою, обмін, виконання доручень, приймання й передавання доручень, розміщення, консультування, переказ, зберігання та управління портфелем. НКО мають оцінювати, чи дозволяють ці послуги окремо або в поєднанні клієнтам із ЄС набувати, торгувати, обмінювати, збільшувати експозицію чи іншим чином отримувати доступ до невідповідних tokenів або зберігати їх. CASP мають запровадити технічні, договірні й організаційні засоби контролю, які унеможливають набуття чи збільшення позицій клієнтами з ЄС. Допускаються лише «суворо обмежені залишкові послуги» для впорядкованого згорання – ліквідація, конвертація, виведення, переказ або зберігання наявних позицій – обмежені в часі, чітко повідомлені клієнтам і під посиленням наглядом.

Найбільш відчутним для ринку є строк: виявлені «успадковані» позиції НКО мають вимагати усунути якнайшвидше, але не пізніше трьох місяців від дати публікації висновку, тобто орієнтовно до початку січня 2027 року. На цей період послуги можуть обмежуватися лише продажем, конвертацією, переказом або виведенням. ESMA разом із НКО регулярно моніторитиме своєчасність застосування висновку. Для України цей документ є важливим орієнтиром у контексті наближення регулювання віртуальних активів до MiCA: за даними робочого документа МВФ, представленого в розділі 1 цього випуску, обсяг стейблкоїнів, якими володіють резиденти

України, оцінюється в 8,6 млрд дол. США, або 4,1% ВВП, що робить питання правового статусу токенів, емітенти яких не авторизовані за MiCA, одним із ключових для майбутньої моделі нагляду.

Висновки

Тримісячний строк фактично означає делістинг для клієнтів з ЄС: до початку 2027 року CASP мають припинити не лише торгівлю, а й обмін, консультування, переказ і нове зберігання невідповідних MiCA стейблкоїнів, залишивши тільки продаж, конвертацію, переказ або виведення наявних позицій.

Аргумент «ми попередили клієнта» більше не працює: ESMA прямо відкидає розкриття інформації та підтвердження ризиків клієнтом як заміну гарантій на рівні емітента, що варто враховувати при розробленні українських правил щодо токенів електронних грошей і токенів, прив'язаних до активів.

Для СПФМ і постачальників послуг віртуальних активів зростає значення гео- та продуктового контролю: необхідні технічні засоби, що не дозволяють клієнтам з ЄС набувати чи збільшувати позиції в невідповідних токенах, а також оновлення оцінки ризиків контрагентів, що можуть переносити такі операції в юрисдикції поза ЄС.

Українська модель регулювання має завчасно визначитися зі статусом стейблкоїнів, емітенти яких не авторизовані в ЄС: з огляду на оцінку МВФ у 4,1% ВВП відсутність чіткого правила створить ризик регуляторного арбітражу на користь українських платформ після запровадження європейських обмежень.

Рекордні стягнення Мінфіну США з Bank of America: «аутсорсинг» виявлення підозрілих операцій як самотійне порушення⁵



13 жовтня 2026 року Міністерство фінансів США оголосило про застосування до Bank of America, другого за розміром банку країни, заходів впливу за порушення законодавства у сфері протидії відмиванню коштів і санкційного законодавства. Мережа боротьби з фінансовими злочинами (FinCEN) наклала штраф у 1,2 млрд дол. США, Управління контролера грошового обігу (OCC) – цивільний грошовий штраф у 750 млн дол. США, Управління з контролю за іноземними активами (OFAC) уклало з банком мирову угоду на 11,6 млн дол. США. Сукупну суму стягнень Мінфін США

визначає як «понад 1,21 млрд дол. США», що з огляду на розмір окремих складників вказує на зарахування частини сум між відомствами (механізм зарахування прес-реліз не розкриває). Це третє за розміром стягнення в історії Мінфіну США і найбільше в історії OCC. Міністр фінансів Скотт Бессент наголосив, що фінансові установи перебувають «на передовій захисту економічної та національної безпеки», а недоліки банку такого масштабу створюють ризики для всієї фінансової системи США.

У межах урегулювання з FinCEN банк визнав умисне порушення Закону про банківську таємницю (BSA) за трьома напрямками: невідповідність програми ПБК мінімальним вимогам BSA, неналежна перевірка кореспондентських рахунків іноземних фінансових установ і неподання повідомлень про підозрілу діяльність (SAR). Найбільш показовим з методологічного погляду є висновок FinCEN про те, що банк, віддаючи пріоритет доходам і мінімізуючи навантаження на комплаєнс-ресурси, настільки покладався на запити правоохоронних органів, звернення інших фінансових установ та інші зовнішні сигнали замість власних автоматизованих засобів контролю, що фактично «передав на аутсорсинг третім особам» значну частину свого обов'язку з проактивного виявлення та звітування. Підозріла діяльність тривалий час накопичувалася без розгляду, а запізнілі повідомлення мали обмежену цінність для правоохоронців. Банк не вжив суттєвих заходів навіть після внутрішнього тестування, яке виявило значні проблеми.

Другий блок порушень стосується належної перевірки клієнтів. Процедури банку не враховували значної залежності клієнтів від платежів від невідомих третіх осіб, а банк не реагував своєчасно й предметно на накопичення «червоних прапорців», зокрема на можливі зв'язки з доходами від наркоторгівлі, навіть після того, як працівники комплаєнсу ескалували підозри щодо відмивання коштів через торгівлю та шахрайства. У підсумку банк своєчасно не повідомив FinCEN про

⁵ <https://home.treasury.gov/news/press-releases/sb0657>

підозрілі операції на суму понад 5 млрд дол. США, з яких понад 1 млрд дол. стосувався пріоритетних ризиків для національної безпеки: операцій, характерних для китайських мереж відмивання коштів, шахрайства та ймовірного відмивання через торгівлю, суттєво пов'язаного з південно-західним кордоном США.

Наказ за згодою FinCEN зобов'язує банк разом із третьою стороною провести ретроспективний перегляд (lookback) для виявлення й повідомлення про невиявлені підозрілі операції, а також пройти незалежну оцінку ефективності моніторингу підозрілої діяльності, належної перевірки клієнтів, перевірки іноземних кореспондентських рахунків і системи управління даними, які використовуються в програмі ПВК. Незалежні перевірки адаптовано до виявлених порушень і пріоритетних ризиків: південно-західного кордону, картелів і наркоторгівлі, Ірану та росії.

Стягнення OCC ґрунтується на порушеннях BSA та правил 12 CFR 21.21 і 12 CFR 21.11 і є наслідком невиконання припису про припинення порушень (cease-and-desist) від грудня 2024 року. За оцінкою OCC, система моніторингу операцій банку не забезпечила належного моніторингу операцій на трильйони доларів, що спричинило велику кількість запізнених SAR на мільярди доларів, багато з яких мали ознаки відмивання коштів. Банк роками знав, що не ескалує потенційно підозрілу діяльність до розслідувачів, але не виправив цього. Відповідальний працівник з питань BSA та персонал не мали достатньої кваліфікації, ключові працівники не пройшли належного навчання, а функція внутрішнього аудиту не виявила давніх проблем, які згодом знайшли інспектори. Через понад рік після припису банк і далі не ескалював підозрілу діяльність, а через системну прогалину в моніторингу проводив операції з ознаками відмивання через торгівлю.

Мирова угода з OFAC стосується 475 очевидних порушень кількох санкційних програм – щодо росії, Білорусі, Ірану, М'янми, Сомалі, наркотиків і глобального тероризму. Порушення виникли через проведення кореспондентських платежів через заблоковані банки внаслідок технічних і людських помилок, неналежне калібрування санкційних сповіщень, яке дозволило особам, включеним до санкційних списків, здійснювати платежі й знімати кошти, несвоєчасне оновлення списків після нових позначень OFAC і помилки в обслуговуванні рахунків, пов'язаних із заблокованими особами. OFAC визнав порушення неумисними («non-egregious») і переважно не розкритими добровільно; сума угоди не передбачає жодного зменшення базового штрафу, зокрема за виправні заходи чи співпрацю.

У розділі «Комплаєнс-міркування» Мінфін США формулює позицію, що виходить за межі окремої справи: фінансові установи не можуть ігнорувати «червоні прапорці» чи внутрішні застереження щодо неефективності контролів, зокрема «під виглядом інновацій», і не можуть розглядати запити правоохоронців чи звернення інших установ як заміну власного моніторингу. Профілі ризику клієнтів мають оновлюватися протягом усіх ділових відносин з урахуванням активності, продуктів і географії, а «просте документування занепокоєнь чи тривалі внутрішні перевірки без належних коригувальних дій» не є виконанням обов'язків. Окремо наголошено на конвергенції ризиків ВК/ФТ і санкційних ризиків та потребі інтегрувати відповідні функції. Мінфін нагадує й про

програму заохочення викривачів FinCEN: винагороду може бути виплачено за інформацію, що призвела до стягнення понад 1 млн дол. США.

Висновки

Залежність від зовнішніх сигналів може кваліфікуватися як самостійне порушення: справа Bank of America показує, що високу частку повідомлень, ініційованих запитами правоохоронців чи інших банків, регулятор розглядає як ознаку неефективності власного моніторингу, тому співвідношення «внутрішніх» і «зовнішніх» тригерів варто відстежувати як окремий показник.

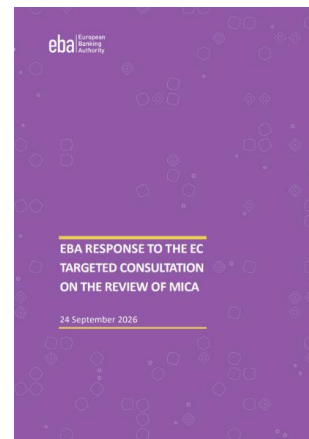
Накопичення нерозглянутих сповіщень є ризиком, який має контролюватися на рівні керівництва: запізнілі повідомлення про операції на понад 5 млрд дол. США стали наслідком ігнорування результатів тестування та внутрішньої ескалації; показники віку сповіщень і часу від виявлення до повідомлення доцільно включати у звітність для наглядової ради.

Невиконання попереднього припису суттєво обтяжує відповідальність: найбільше в історії ОСС стягнення накладено через те, що банк не виправив недоліків, визначених приписом від грудня 2024 року; для українських установ це аргумент на користь документованого й перевірюваного плану виконання вимог НБУ та Держфінмоніторингу.

Санкційний комплаєнс і фінансовий моніторинг мають працювати як одна система: 475 санкційних порушень стали наслідком калібрування сповіщень, запізненого оновлення списків і помилок у кореспондентських платежах, тобто тих самих вад даних і процесів, що й у моніторингу операцій.

Пруденційний нагляд за крипторинком ЄС: практичні пропозиції ЕВА в межах ревізії MiCA⁶

Документ Європейського банківського органу (ЕВА) щодо перегляду Регламенту (ЄС) 2023/1114 про ринки криптоактивів (MiCA) містить розгорнуту експертну позицію та законодавчі рекомендації банківського нагляду ЄС. Документ спирається на перші підсумки практичного застосування розділів III та IV MiCA: станом на 1 вересня 2026 року в ЄС було випущено 39 tokenів електронних грошей (EMT), переважно емітентами електронних грошей (EMI), та жодного авторизованого токена з прив'язкою до активів (ART). Аналіз адресований законодавчим органам ЄС, банківським наглядовим органам, фінансовим інституціям та емітентам стабільних tokenів, концентруючись на збереженні пруденційної стійкості, розмежуванні банківського й крипторегулювання, ліквідності резервів та мінімізації системних ризиків глобальних стейблкоїнів.



Головна теза звіту полягає у неухильному дотриманні принципу технологічної нейтральності («однаковий ризик – однакове правило»): токенизація активу сама по собі не повинна змінювати його регуляторну кваліфікацію. ЕВА наполягає на тому, що токенизовані традиційні фінансові інструменти мають залишатися суворо в межах законодавства про ринки цінних паперів (MiFID II, MiFIR, Регламент про капітальні вимоги CRR), а токенизовані депозити – у периметрі банківського регулювання (CRD/CRR), без штучного їх перенесення під норми MiCA. Водночас регулятор застерігає: відсутність повної гармонізації термінів «фінансовий інструмент» та «депозит» на рівні законодавства ЄС породжує суттєву фрагментацію, коли той самий token в одній державі-члені може трактуватися як цінний папір, а в іншій – як ART або бездокументарне зобов'язання.

Окрему увагу приділено складнощам класифікації tokenів, забезпечених сировинними товарами (зокрема золотом), синтетичних tokenів, вартість яких відображає ціну інших активів, а також tokenів, що представляють активи в інших блокчейн-мережах. ЕВА фіксує численні спроби структурувати пропозиції таким чином, щоб штучно замаскувати EMT під ART або уникнути суворої законодавчої заборони на нарахування відсотків за стейблкоїнами (Стаття 40 MiCA), що підриває регуляторну дисципліну. Для усунення невизначеності орган закликає спиратися на економічну сутність правовідносин над формою та запровадити єдине правове визначення поняття «депозит» у директивах CRD/CRR. Це створить надійне підґрунтя для безпечного розвитку транскордонних міжбанківських розрахунків токенизованими депозитами (зокрема через спільні ініціативи Євросистеми Pontes/Appia та експерименти Банку міжнародних розрахунків у проекті Agora).

У блоці вимог до резервів активів EMT та ART регулятор детально розбирає проблему високої взаємозалежності між сектором криптовалют та традиційним банківським сектором. З одного боку, чинна вимога розміщувати від 30% до 60% резервів у формі банківських депозитів гарантує негайний доступ до ліквідності для погашення за вимогами клієнтів. З іншого боку, раптове та масштабне виведення коштів емітентами стейблкоїнів створює загрозу гострого ліквідного стресу для банків-депозитаріїв, тоді як фінансові труднощі в самому банку можуть заблокувати доступ до резервів. З огляду на це, ЕВА рекомендує Європейській комісії провести ґрунтовний аналіз витрат і вигод від можливого зменшення встановленої частки банківських депозитів у структурі резервів на користь динамічних резервних портфелів, які забезпечуватимуть щоденну та щотижневу ліквідність і доповнюватимуться короткостроковими державними облігаціями найвищої кредитної якості. Водночас регулятор підтримує збереження правила, згідно з яким класичні комерційні банки звільнені від обов'язку окремого резервування під випущені EMT, оскільки їхній баланс уже контролюється значно жорсткішими банківськими коефіцієнтами LCR та NSFR.

Аналізуючи процедурні механізми захисту прав інвесторів, ЕВА пропонує законодавчо закріпити чіткі часові межі для викупу токенів у звичайних операційних умовах, що усуне небезпеку панічних «набігів» на окремих емітентів. Крім того, наглядовий орган наполягає на розширенні спектра кризових інструментів реагування щодо небанківських емітентів значущих стабільних токенів: регулятори повинні мати повноваження примусово ініціювати плани викупу та передавати бізнес разом із відокремленими активами резерву стороннім платоспроможним установам за зразком механізмів банківського врегулювання BRRD. Також регулятор закликає покласти край прихованим комісіям за погашення, коли емітенти формально декларують безкоштовний викуп, але вимагають відкриття платних внутрішніх гаманців.

Найбільшу системну загрозу ЕВА вбачає у транскордонних схемах мультिवипуску за участі емітентів із третіх країн (TCMIS). Через повну взаємозамінність токенів інвестори під час геополітичного чи ринкового стресу масово спрямовуватимуть запити на погашення до емітента в ЄС, чії резерви суворо захищені законодавством, що може призвести до миттєвого спустошення європейських резервів через проблеми в офшорних юрисдикціях. Щоб нейтралізувати ризик транскордонного зараження, орган пропонує додати участь у міжнародних мультिवипусках як окремий критерій «значущості» токена, запровадити режим обов'язкової еквівалентності регулювання третіх країн на засадах взаємності та надати наглядовцям право попереднього вето на вступ емітентів у такі пули.

На рівні інституційного нагляду ЕВА фіксує небезпечний регуляторний вакуум щодо багатопрофільних криптогруп, які одночасно поєднують емісію токенів, біржову діяльність, кастодіальні функції, кредитування та торгівлю за власний рахунок. Оскільки повноцінний консолідований нагляд наразі існує лише для банків, ЕВА наполягає на запровадженні постійних наглядових колегій, обов'язкової звітності на рівні материнських холдингів та праві наглядових органів вимагати створення проміжних материнських компаній в ЄС (IPU). У сфері криптокредитування та запозичень, зокрема у сфері децентралізованих фінансів (DeFi), регулятор закликає встановити обмеження на використання кредитного плеча, запровадити обов'язкову оцінку платоспроможності позичальників, заборонити використання стейблкоїнів, емітенти яких

не мають необхідного регуляторного дозволу, запровадити сертифікацію смартконтрактів і усунути прогалини у звітності щодо активів, які фактично перебувають у володінні резидентів ЄС.

Усунення технічних колізій між банківським та платіжним правом розглядається через призму взаємодії MiCA з новим платіжним пакетом PSD3/PSR. Регулятор застерігає від створення регуляторних асиметрій: якщо платіжним установам (PI) дозволяється надавати послуги з токенами EMT за спрощеним повідомленням без окремої ліцензії CASP, аналогічні правила еквівалентності мають діяти дзеркально, а кошти клієнтів мають бути чітко захищені від випадання з-під дії обох захисних режимів одночасно. Зрештою, ЕБА вказує на брак стандартизованих мандатів для оцінки ділової репутації керівників емітентів, що має бути розширено за межі фінансового права на всі сфери правопорушень, гарантуючи надійний фільтр для допуску учасників на європейський ринок.

Висновки

Токенізовані інструменти поза MiCA: цифрові депозити й токенізовані цінні папери мають регулюватися банківським законодавством і законодавством про фінансові інструменти (CRD/MiFID), із уточненням поняття «депозит».

Гнучкіші норми резервів стейблкоїнів: частку 30–60% обов'язкових банківських депозитів у резервах EMT варто замінити кошиками ліквідності з якісними держоблігаціями.

Бар'єри для глобальних стейблкоїнів (TCMIS): щоб ризики в офшорних юрисдикціях не виснажували резерви в ЄС, міжнародні схеми мультивипуску мають погоджуватися регулятором і відповідати вимогам режиму еквівалентності.

Консолідований нагляд за криптогрупами: поєднання одним холдингом емісії, бірж і кредитування потребує наглядових колегій, групової звітності та створення материнських компаній в ЄС.

Новий санкційний пакет ЄС проти військово-промислового комплексу росії⁷

Ухвалення Радою Європейського Союзу Рішення 2026/2279 від 12 жовтня 2026 року стало безпрецедентним кроком у системному розширенні санкційного тиску на російську федерацію та її військово-промисловий потенціал. Цей нормативно-правовий акт запровадив найбільший за весь період протистояння пакет індивідуальних обмежувальних заходів. До списку підсанкційних суб'єктів додано 1569 позицій, серед яких 826 компаній та 743 топменеджери й генеральні директори. Загальна кількість фігурантів європейських санкційних списків, розгорнутих для захисту територіальної цілісності, суверенітету та незалежності України, наразі наблизилася до позначки у 4600 осіб і компаній.



Політичним фундаментом для цього радикального кроку стали висновки Європейської Ради від 18–19 червня 2026 року, в яких було зафіксовано суворе засудження нової хвилі російської ескалації та ракетно-дронових ударів по цивільних цілях і критичній інфраструктурі, включаючи мости Києва, судна для перевезення зерна та об'єкти Національної академії наук України.

Аналіз якісного складу та економічного масштабу ухваленого пакету вказує на зміну стратегічних орієнтирів санкційної політики Брюсселя. Якщо попередні етапи переважно фокусувалися на макроекономічних обмеженнях і флагманських державних монополіях, то поточні заходи націлені на постачальників середньої ланки, які утворюють технологічне ядро російської оборонної промисловості. Підсанкційні підприємства сукупно генерують щорічний обіг щонайменше у 20 мільярдів євро та працевлаштовують понад 250 тисяч фахівців. При цьому понад половина доданих до реєстру суб'єктів безпосередньо інтегрована у ланцюжки розробки та виробництва балістичних ракет, застосовуваних агресором проти українського цивільного населення.

Секторальний зріз обмежень демонструє прицільну спробу блокувати критичні технологічні вузли російського виробництва зброї. Під дію санкцій підпали провідні виробники мікроелектроніки, напівпровідникових елементів, бортових обчислювачів, радіолокаційного обладнання, приймально-передавальної апаратури, оптики та систем точного позиціонування. Номенклатура підприємств також охоплює конструкторські бюро та заводські потужності в галузях авіоніки,

⁷ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202602279

ракетно-космічного приладобудування, суднобудування, гідроакустики, виробництва полімерів, композитних матеріалів, вибухових речовин і боєприпасів, розташованих у десятках регіонів росії. Позбавлення зазначених заводів доступу до зовнішніх ринків комплектуючих та фінансових інструментів має на меті створити нездоланні дефіцитні вузькі місця у відновленні парку ударних БПЛА, ракетних комплексів та пілотованої бойової авіації агресора.

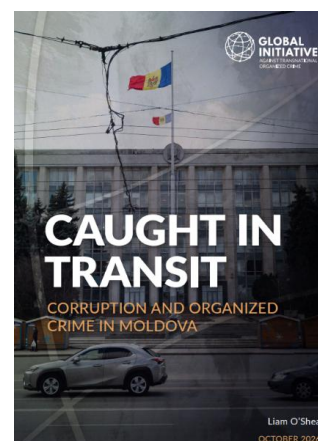
Значний інтерес становить правова конструкція та методологія, використана Радою ЄС для юридичної фіксації зв'язку фігурантів із війною. Європейський регулятор поклав в основу доказової бази офіційний реєстр підприємств військово-промислового комплексу, раніше сформований самим урядом держави-агресора. Включення компаній до цього державного списку наділяє їх правом на отримання федеральних бюджетних субсидій, зокрема прямої державної підтримки для покриття витрат працівників на житло. Європейська сторона розцінила статус отримувача подібних преференцій як прямий факт участі в забезпеченні воєнних дій і надання матеріальної підтримки агресії. Автоматично під персональні санкції підпали і керівники даних структур, чий управлінський контроль задіяний у забезпеченні функціонування мілітарного виробництва.

Запроваджений правовий режим тягне за собою повне блокування всіх активів зазначених осіб і підприємств у юрисдикціях держав Євросоюзу, категоричну заборону на надання їм будь-яких фінансових чи економічних ресурсів, а також пряму заборону на в'їзд і транзитне пересування територією ЄС для фізичних осіб. Одночасне внесення до реєстру як виробничих активів, так і їхніх генеральних директорів унеможливорює швидку адаптацію бізнес-структур за рахунок фіктивної перереєстрації прав власності чи зміни керівництва.

Таким чином, рішення Європейського Союзу свідчить про перехід до концепції глибокого структурного виснаження ворожої промисловості, спрямованого на системну руйнацію технологічних ланцюгів і підірив довгострокової спроможності Росії продовжувати ведення війни високої інтенсивності.

Корупція та організована злочинність у Молдові: динаміка кримінальних ринків та межі відновлення держави⁸

Документ міжнародної організації Глобальна ініціатива проти транснаціональної організованої злочинності (GI-TOC) присвячений комплексному дослідженню перетину політичної корупції, захоплення держави та організованої злочинності в Республіці Молдова. Дослідження ґрунтується на якісному аналізі політичної економії та кримінальних ринків за період із лютого до липня 2026 року. Методологія поєднує польові інтерв'ю з молдовськими посадовцями, суддями, антикорупційними прокурорами, журналістами-розслідувачами та західними дипломатами з перевіркою судових рішень, матеріалів преси й міжнародних звітів (зокрема GRETA, MONEYVAL, OECD, EUBAM). Документ адресований уряду Молдови, міжнародним донорам та інституціям ЄС у контексті переговорного процесу щодо вступу країни до Євросоюзу.



Центральний висновок дослідження полягає в тому, що Молдова не є самостійним великим центром продукування організованої злочинності, а її внутрішні кримінальні ринки залишаються відносно обмеженими. Проте географічне розташування на кордоні з Україною та ЄС перетворює країну на критично важливий транзитний коридор для незаконних товарних і міграційних потоків, що рухаються на захід. Провідним нелегальним ринком залишається контрабанда сигарет до ЄС (зумовлена різницею акцизів та цін), хоча її обсяги поступово зменшуються через перенесення виробництва нелегальних сигарет всередину Євросоюзу. Одночасно повномасштабна війна росії проти України кардинально змінила конфігурацію тіньових потоків: виник новий високодохідний ринок організації незаконного перетину кордону українськими чоловіками призовного віку (тарифи в якому зросли від початкових 1–3 тис. доларів до 5–20 тис. доларів США за особу), зростає транзит синтетичних наркотиків і прекурсорів, тоді як трафік жінок із метою сексуальної експлуатації пішов на спад, а очікуваний масовий витік зброї із зони бойових дій поки не матеріалізувався через її високе поглинання фронтом.

У структурі злочинного світу домінують локальні, дрібні та гнучкі молдовські мережі, тоді як фінансування та координацію великих транскордонних операцій здійснюють більш структуровані

⁸ <https://globalinitiative.net/wp-content/uploads/2026/10/Liam-OShea-Caught-in-transit-Corruption-and-organized-crime-in-Moldova-GI-TOC-October-2016.pdf>

транснаціональні синдикати (турецькі, українські чи румунські), що наймають громадян Молдови як кур'єрів, водіїв або підставних осіб завдяки наявності у багатьох із них румунських паспортів. Окрему загрозу становлять фінансовий кібершахрайський промисел (розгалужені нелегальні колцентри, що виманюють кошти у громадян ЄС та Молдови під виглядом інвестицій), а також використання криптовалют для гібридного іноземного фінансування. Зокрема, у березні 2026 року було розкрито криптогаманець на суму понад 107 млн доларів США у стейблкоїнах, які надходили з підсанкційної російської криптобіржі для мережі втікача Ілана Шора з метою підкупу виборців на виборах і референдумі 2024 року.

Окремим практичним викликом для фінансової системи залишається неповна відповідність регулювання віртуальних активів міжнародним стандартам, де MONEYVAL досі оцінює країну як лише частково відповідну нормам FATF. Попри активізацію Агентства з повернення злочинних активів (ARBI), яке у 2024 році арештувало майно на 75 млн доларів США, реальне виконання судових конфіскацій залишається вкрай низьким – менше 10% від вартості накладених арештів проти близько 50% у середньому по країнах ЄС. Постійні затримки у розгляді складних фінансових проваджень, що тягнуться по 8–10 років, у поєднанні з конституційною презумпцією законності набуття майна фактично знецінюють превентивну дію статей про незаконне збагачення.

Фундаментальним досягненням періоду 2021–2026 років названо демонтаж олігархічного захоплення держави проєвропейським урядом партії PAS під керівництвом Маї Санду. Якщо в період 2009–2019 років країна перебувала під тотальним неформальним контролем олігархічних кланів (кульмінацією чого стала «крадіжка століття» 1 млрд доларів із банківської системи у 2012–2014 роках за співучасті регуляторів і топпосадовців), то чинна влада зруйнувала захисний купол над організованою злочинністю. Це підтверджено вироком Володимиру Плахотнюку до 19 років ув'язнення у квітні 2026 року, заочними вироками Ілану Шору та Марині Таубер, проходженням процедури перевірки доброчесності суддів і прокурорів, а також очищенням керівництва антикорупційних органів.

Водночас процес відновлення держави залишається незавершеним і стикається з трьома системними ризиками. Перший ризик полягає у надмірній персоналізації реформ і слабкій інституціоналізації: значна частина рішень спиралася на надзвичайні виконавчі інструменти та просту парламентську більшість (зокрема суперечливі зняття партій з виборів чи багаторазові виправлення законів під поточні процедури), що створює прецедент легкого відкату змін у разі приходу до влади реваншистських сил за так званим «грузинським сценарієм». Падіння уряду Александара Мунтяну в липні 2026 року через корупційний скандал із непрозорим призначенням керівництва державної авіакомпанії MoldATSA продемонструвало крихкість політичного капіталу. Другий ризик – структурна бідність і стійка побутова корупція в поліції, прикордонній та митній службах через низькі зарплати (близько 700 євро), де реформи майже не проводилися. Третій ризик – безпековий: латентна загроза прориву нелегального трафіку зброї після завершення гарячої фази війни в Україні через відкриті молдовські кордони («очікування прориву греблі»).

Збереження значних корупційних ризиків на місцевому рівні та в публічних закупівлях додатково послаблює загальний ефект трансформації. За оцінками громадських організацій, близько 17% вартості публічних контрактів досі укладається напряму без використання електронної системи MTender, а практика штучного заниження сум угод нижче порогів прозорості та обмеження конкуренції під пов'язаних підрядників залишається непокараною. При цьому санкції Національного агентства з питань доброчесності є малоефективними, а більше половини виявлених порушень залишаються без реакції з боку органів влади.

Окремим чинником вразливості залишається Придністров'я. Хоча його роль як контрабандного хабу знизилася через блокування кордону Україною у 2022 році, припинення безкоштовного російського газу та падіння економіки, де-факто влада регіону і холдинг «Шериф» зберігають симбіотичний контроль над територією, використовуючи трафік ухилянтів для допитів співробітниками МДБ/ФСБ. Позитивним зрушенням є економічний примус Кишинева: скасування фіскальних пільг і переорієнтація 71% експорту регіону на ринок ЄС змусили понад 2400 придністровських підприємств зареєструватися за законами Молдови, звужуючи базу для нелегальної торгівлі.

Висновки

Транзитний характер злочинності за домінування зовнішніх синдикатів:

Молдова виступає передусім транзитним коридором до ЄС для контрабанди тютюну, синтетичних наркотиків і нелегальних мігрантів, де місцеві групи виконують лише сервісну роль перевізників та підставних осіб для іноземних кримінальних угруповань.

Послаблення політичного захисту організованої злочинності: судова реформа, перевірка доброчесності суддів і посадовців, а також притягнення олігархів до відповідальності сприяли послабленню механізмів централізованого захоплення держави та звуженню можливостей організованої злочинності використовувати політичні зв'язки для уникнення правоохоронного переслідування.

Вразливість реформ перед виконавчим суб'єктивізмом: успіхи антикорупційної трансформації спираються переважно на політичну волю правлячої більшості, а не на стабільні інституції, що створює небезпеку реваншу за «грузинським сценарієм» у разі зміни влади.

Економічна інтеграція Придністров'я як інструмент детінізації: поширення митного й податкового законодавства Молдови на підприємства сепаратистського регіону в обмін на доступ до ринку ЄС ефективніше звужує простір для контрабанди, ніж традиційні силові заходи.

Багаторівнева рамка RUSI та місце фінансових інструментів у протидії ворожій кіберактивності⁹



Королівський інститут оборонних досліджень (RUSI) опублікував аналітичну записку «Beyond 'Cyber' in Deterrence: A Multilevel Framework», підготовлену старшою науковою співробітницею д-р Луїзою Марі Юрель і науковим співробітником д-ром Гаретом

Моттом. Дослідження ґрунтується на 16 напівструктурованих інтерв'ю з чинними та колишніми представниками урядів держав НАТО й інституцій ЄС, двох експертних семінарах у Нью-Йорку й Таллінні за участі близько 30 учасників і двох брифінгів для урядовців, частина з яких була присвячена апробації рамки. Відправною точкою є гібридна ескалація росії в Європі: вторгнення близько 20 дронів у повітряний простір Польщі у вересні 2025 року, після якого Польща ініціювала консультації за статтею 4 Північноатлантичного договору, і скоординована кібератака на розподілені енергетичні об'єкти Польщі, здійснена угрупованням, відповідальним за атаки на українську енергосистему у 2015 і 2016 роках.

Головна теза авторів: відповіді, обмежені кіберзасобами (атрибуція, кібероперації, кіберсанкції), недостатні для того, щоб позбавити противника стратегічної переваги, що здобувається одночасно в кількох доменах. Кіберстримування запропоновано розглядати не як стратегію, а як результат – сукупні, ітеративні, часткові й інколи зворотні зміни поведінки держави-противника чи третьої країни, яких можна досягти із застосуванням будь-яких інструментів державної політики. Об'єктом стримування є саме зловмисна кіберактивність, але засоби її стримування не обов'язково мають бути кібернетичними. Звідси пропозиція перейти від дискусії, де кожне відомство обстоює цінність інструментів, які воно «має», до підходу, орієнтованого на результат і скоординованого на рівні всього уряду.

Рамка охоплює 36 інструментів, згрупованих за чотирма функціями. «Підвищення планки» – заходи, що ускладнюють, здорожчують і знецінюють атаки (стандарти безпеки, активний кіберзахист, експортний контроль, безпека ланцюгів постачання, міжнародні норми). «Накладання витрат» – проактивні чи каральні заходи (наступальні кібероперації, «hunt forward» операції, вилучення інфраструктури, таргетовані санкції, «фінансові порушення» через криптоактиви й інструменти ПВК, мита, публічна атрибуція, обвинувальні акти, висилання дипломатів). «Вигоди та стимули» – винагорода за стриманість (доступ до ринку, скасування санкцій, виключення із «сірих списків»). «Забезпечувальні чинники» – спроможність до атрибуції, державно-приватна співпраця, обмін розвідданими, розбудова спроможностей. Для аудиторії бюлетеня принципово, що фінансові інструменти – санкції, заморожування активів, позначення

⁹ <https://www.rusi.org/explore-our-research/publications/insights-papers/beyond-cyber-deterrence-multilevel-framework>

криптогаманців і бірж, посилена увага у сфері ПВК/ФТ – прямо віднесено до арсеналу кіберстримування.

Автори пропонують шість результатів кіберстримування з показниками для оцінки: дотримання задекларованих «червоних ліній»; зростання витрат противника на одну операцію (час на відновлення інструментарію після викриття чи вилучення інфраструктури); контроль ескалації; позбавлення стратегічної переваги; зміна поведінки третіх країн (готовність долучатися до атрибуції, скорочення розміщення шкідливої інфраструктури, співпраця щодо правоохоронних запитів); відновлення свободи дій союзників, тобто подолання «самостримування». Учасники досліджень зазначали, що західні уряди переоцінюють ймовірність непропорційної відповіді противника на наступальні кібероперації, а інструменти ЄС, що потребують одностайності, зокрема санкційні механізми, використовуються недостатньо саме через складність її досягнення.

Найбільш релевантний для сфери ПВК/ФТ/ФР розділ присвячено економічним інструментам. За висновком авторів, санкції, заморожування активів, позначення криптогаманців і бірж уже застосовуються для уповільнення й порушення діяльності зловмисних кіберсуб'єктів; прикладами адаптації є Інструментарій кібердипломатії ЄС 2017 року з горизонтальним режимом кіберсанкцій і окремий режим ЄС щодо гібридної дестабілізуючої діяльності росії, які можуть застосовуватися до одного й того самого суб'єкта. Проблемою залишається узгодження позицій держав-членів щодо дій поза російським напрямом. Автори пропонують шкалу економічних заходів, відкалібровану під поведінку держави: від стимулів (доступ до ринку, скасування санкцій) через «фінансове тертя» (посилений моніторинг у сфері ПВК/ФТ, неформальні сигнали) та таргетовані позначення (санкції щодо визначених осіб, позначення криптогаманців і бірж) до секторальних заходів і повної ізоляції. Шкала є оборотною: підтверджене поліпшення поведінки повертає відносини на вищий рівень.

Розширення економічного інструментарію запропоновано у двох вимірах: масштабу – від окремих осіб до серійних і секторальних пакетів – та змісту, коли умови щодо кіберповедінки закладаються в доступ до ринку, мита, закупівлі, експортне ліцензування й торговельні преференції. Автори визнають, що мита у відповідь на конкретний кіберінцидент досі не застосовувалися, а держави, здатні витримати економічний тиск, можуть не змінити поведінки. Тому такі інструменти можуть бути ефективнішими щодо «середніх» держав, які толерують чи приховують зловмисну діяльність. Ключове обмеження сформульовано так: економічні інструменти накладають відчутні витрати лише за умови колективного й послідовного застосування.

Окремо розглянуто ризик «інституційної сліпоти»: одна й та сама держава з дефіцитом спроможностей, що через бездіяльність дає притулок кримінальній інфраструктурі, може одночасно отримувати збільшену допомогу від міністерства розвитку, підвищену увагу від міністерства фінансів і демарш від міністерства закордонних справ, причому жодне відомство не знає про дії інших. Отримувач робить раціональний висновок, що жоден сигнал не є авторитетним. Для програм розбудови кіберспроможностей запропоновано градацію умов залежно від виду фінансування – офіційна допомога на розвиток, інші офіційні потоки, безпекова

допомога, комерційне та змішане фінансування – із застереженнями щодо ризику «шопінгу спроможностей» у країн, які не висувають умов.

Рекомендації згруповано за п'ятьма бажаними результатами: визначити координаційну функцію з мандатом на рівні всього уряду й вести національний реєстр інструментів із зазначенням власника, правової підстави, строку застосування та залежностей; публікувати короткі заяви про порогові неприйнятної кіберактивності, узгоджені з коаліцією, із заздалегідь визначеним переліком і послідовністю інструментів; створити механізми швидкої колективної дії, оцінивши для кожного інструменту правову підставу, стандарт доказування, спроможність забезпечити виконання та зворотність, і розглянути трансформацію країнових режимів санкцій щодо гібридних загроз у ширший інструмент; калібрувати економічні важелі й умови розбудови спроможностей щодо третіх країн; вибудовувати адаптовані до конкретного противника кампанії з регулярною оцінкою за індикаторами результату. До записки додано інтерактивний інструмент для картографування готовності держав до використання різних інструментів.

Висновки

Фінансові інструменти є складовою кіберстримування, а не лише реакцією на наслідки атак: RUSI прямо включає санкції, заморожування активів, позначення криптогаманців і бірж та посилений моніторинг у сфері ПВК/ФТ до арсеналу «накладання витрат», що передбачає залучення органів фінансової розвідки й санкційних органів до національних механізмів реагування на кіберзагрози.

Ефективність фінансових заходів залежить від доказової бази й зворотності: для кожного інструменту автори рекомендують заздалегідь оцінити правову підставу, стандарт доказування, спроможність забезпечити виконання та можливість скасування як стимулу, що для санкційних механізмів означає необхідність стандартизованих підходів до обґрунтування позначень, пов'язаних із кіберактивністю.

Режими санкцій щодо гібридних загроз потребують масштабування: пропозиція перейти від позначення окремих осіб до серійних і секторальних пакетів та розглянути розширення режиму ЄС щодо гібридних загроз з боку росії на інших суб'єктів задає орієнтир для узгодження українських санкцій з європейськими.

Міжвідомча неузгодженість знецінює сигнали державі-адресату: національний реєстр інструментів і координаційна функція, які пропонує RUSI, корисні й для системи ПВК/ФТ/ФР, де санкційні, наглядові та правоохоронні заходи щодо однієї юрисдикції часто ухвалюються без спільної оцінки їхнього сукупного ефекту.

Тіньова логістика нарко-мереж Меконгу¹⁰

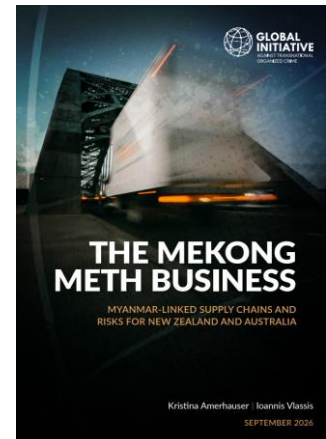
Метамфетамінова індустрія в басейні річки Меконг давно переросла статус локального кримінального явища, перетворившись на одну з найбільш організованих і стійких синтетичних наркомереж глобального масштабу.

Епіцентром масштабного виробництва залишається штат Шан та прилеглі райони М'янми, звідки наркотики поширюються сухопутними, річковими, повітряними та морськими коридорами по всьому світу. Поширений наратив, який пов'язує стрімке зростання обсягів вилучень наркотиків і падіння цін виключно з наслідками військового перевороту 2021 року в М'янмі, значно спрощує структурну картину. Звіт Глобальної ініціативи проти транснаціональної організованої злочинності свідчить, що сьогоднішня стійкість цього ринку є результатом багаторічної промислової трансформації, закладеної ще в 2010-х роках. Ця економіка спирається на інновації у хімічних ланцюгах постачання, збройний територіальний контроль, системну корупцію та високоадаптивну логістику.

Фундаментальною характеристикою метамфетамінового ринку Меконгу є відсутність єдиного вертикально інтегрованого картелю чи монопольного наркобарона. Ринок функціонує як децентралізоване бізнес-середовище. Синтез, постачання сировини, транспорт, охорона, оптове брокерство, відмивання коштів і кінцевий збут здійснюються автономними суб'єктами, які часто контактують лише зі своєю безпосередньою ланкою.

У М'янмі етнічні збройні формування, такі як Об'єднана армія держави Ва (UWSA), значною мірою переорієнтувалися з прямого виробництва на надання підконтрольних територій і захисту зовнішнім кримінальним лабораторіям в обмін на частку від прибутку. Безпосередню вигоду отримують також збройні формування та міліції, афілійовані з хунтою М'янми. При цьому виконавці нижчого рівня – прикордонні кур'єри та водії – є цілком замінними; їхній арешт чи ліквідація сприймається синдикатами як звичайні операційні витрати, що не загрожує ключовим бенефіціарам бізнесу.

Логістичні потоки демонструють надзвичайну маневреність і диверсифікацію маршрутів. Основними каналами виходу з М'янми є північний і північно-західний вектори до Таїланду, західний коридор М'яваді – Мае Сот, а також лаоський напрямок, через який трафік перенаправляється у разі посилення контролю на тайському кордоні. Усередині Таїланду вантажі рідко затримуються в самому Бангкоку: основними консолідаційними та перевалочними вузлами виступають провінції навколо столиці, передусім Аюттхая. Водночас Лаос і Камбоджа слугують стратегічними хабами для транзиту та перепакування, а також сполучення з портами В'єтнаму.



¹⁰

<https://globalinitiative.net/wp-content/uploads/2026/09/Kristina-Amerhauser-and-Ioannis-Vlassis-The-Mekong-meth-business-Myanmar-linked-supply-chains-and-risks-for-New-Zealand-and-Australia-GI-TOC-September-2026.pdf>

Паралельно відбувається диверсифікація асортименту: ринок насичується кетаміном, етомідатом у картриджах для вейпінгу («K-pods») і коктейлями наркотиків. Ба більше, виявлення промислових лабораторій із синтезу кетаміну у В'єтнамі та Камбоджі свідчить про зміщення виробничих потужностей за межі традиційного Золотого трикутника.

Наркобізнес Меконгу існує в тісній конвергенції з іншими транснаціональними кримінальними ринками та легальною економікою. Синтез наркотиків потребує сотень тон прекурсорів і так званих пре-прекурсорів, які постачаються з Китаю та Індії й беруться з легального промислового обігу Таїланду під прикриттям гірничодобувної та аграрної діяльності. Ця наркоіндустрія використовує ту саму інфраструктуру, що й промислові шахрайські кол-центри, нелегальні казино, схеми торгівлі людьми та відмивання грошей у спеціальних економічних зонах Бокео, Коканга та Шве Кокко. Отримані надприбутки легалізуються через неформальні системи розрахунків (хунді), криптовалютні канали, торгівлю золотом і комерційні структури прикриття. Комерційну стійкість системи забезпечує колосальна географічна різниця в цінах: якщо в лабораторіях М'янми кілограм кристалічного метамфетаміну коштує близько 400 доларів США, то в Таїланді його гуртова ціна сягає 3 000 доларів, у Малайзії – 15 000 доларів, а на ринку Австралії досягає орієнтовно 30 000 доларів США.

Для віддалених ринків збуту, зокрема Австралії та Нової Зеландії, метамфетаміновий трафік із Меконгу становить стратегічну загрозу. Незважаючи на те, що в публічних звітах цих країн фігурує значна частка вилучень мексиканського походження через активний обмін даними з партнерами з Північної Америки, меконгські мережі продовжують постачати стабільні обсяги завдяки вищій майстерності маскуванню та співпраці з місцевими кримінальними угрупованнями, насамперед бандами мотоциклістів (OMCG).

Звичайна концентрація правоохоронних зусиль на фізичному перехопленні партій на морських або поштових шляхах не вирішує проблеми, оскільки система готова до таких втрат. Сталий вплив на ситуацію можливий лише за умови цілеспрямованої боротьби з учасниками цієї індустрії: перекриття каналів постачання прекурсорів на дипломатичному рівні з Китаєм та Індією, подолання структурної корупції на митних і прикордонних пунктах, ліквідації конвергентної інфраструктури шахрайських хабів, а також інтеграції даних аналізу стічних вод і програм зменшення шкоди для оперативного моніторингу динаміки ринку.

Висновки

Децентралізована сервісна модель: Ринок контролюється не єдиним монопольним картелем, а системою автономних підрядників, де учасники контактують лише з найближчою ланкою, а кур'єри є витратним матеріалом, втрата якого закладається в операційні ризики.

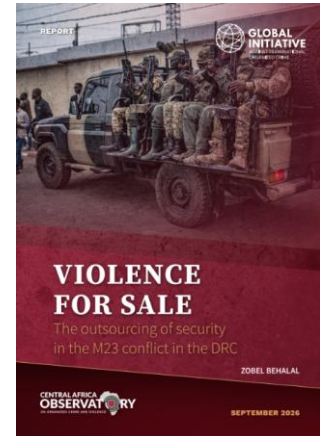
Конвергенція з іншими кримінальними ринками та легальною економікою: Наркобізнес використовує ту саму інфраструктуру, що й шахрайські кол-центри, нелегальні гральні зони та торгівля людьми; транспортування маскується легальними вантажами, а надприбутки відмиваються через готівкові розрахунки, золото, криптовалютні канали та неформальні системи передачі вартості.

Стрімка диверсифікація речовин і децентралізація лабораторій: Ринок Меконгу виходить за межі суто метамфетаміну – фіксується зростання обігу кетаміну, етомідату у вейп-картриджах («K-pods») і багатокомпонентних наркосумішей, а також виявлення промислових лабораторій із синтезу синтетичних речовин за межами М'янми – у В'єтнамі та Камбоджі.

Неефективність стратегії, орієнтованої виключно на фізичні вилучення: Колосальна різниця між собівартістю виробництва у М'янмі (\$400 за кілограм) та гуртовою ціною на ринках збуту в Австралії чи Новій Зеландії (близько \$30 000 за кілограм) покриває будь-які втрати від конфіскацій; стійкий результат можливий лише через тиск на учасників ринку: дипломатичний контроль постачання пре-прекурсорів з Індії та Китаю, ліквідацію хабів і руйнування корупційних мереж.

Мілітаризація та кримінальні ринки: економічні вигоди учасників конфлікту на сході Демократичної Республіки Конго ¹¹

Документ Глобальної ініціативи проти транснаціональної організованої злочинності (GI-TOC) присвячений комплексному дослідженню трансформації збройного протистояння на сході Демократичної Республіки Конго (ДРК) у самопідтримувану кримінальну екосистему через масштабне делегування (аутсорсинг) державою своїх безпекових функцій. Дослідження спирається на глибинні інтерв'ю з представниками силових структур, дипломатами, операторами видобутку, лідерами озброєних формувань, бійцями приватних військових компаній та громадянського суспільства, а також на перехресний аналіз торговельних даних і звітів Групи експертів ООН.



Центральна теза документа полягає в тому, що приватизація та аутсорсинг безпеки не вирішують конфлікт, а виступають головним рушієм насильства, нестабільності та розграбування природних ресурсів. Слабкість і хронічна корупція в лавах Збройних сил ДРК (FARDC), яку президент Фелікс Чісекеді публічно схарактеризував як «армію волоцюг», змусили уряд перекласти оборону на сторонніх акторів: місцеві коаліції ополченців «Вазалендо» (Wazalendo), армію сусідньої Уганди (UPDF) та численні іноземні приватні військові компанії. Одночасно повстанський рух M23 діє як прямий проксі-інструмент Руанди, що підтверджено розгортанням до 7000 військовослужбовців сил оборони Руанди (RDF) та застосуванням новітніх озброєнь – важкої артилерії, БПЛА, систем РЕБ і переносних ЗПК. Унаслідок взаємного делегування насильства публічна влада, приватний бізнес та організований кримінал остаточно злилися в єдину мережу, де збройне протистояння є лише прикриттям для комерційної наживи.

У документі детально задокументовано виникнення моделі «бізнес як безпека» через діяльність західних підрядників, зокрема засновника компанії Blackwater Еріка Прінса. Уклавши наприкінці 2024 року 5-річний контракт із Міністерством фінансів ДРК на суму 100–200 млн доларів США під виглядом логістичної та податкової оптимізації («фінансова бригада»/«гірнична поліція»), структури Прінса (Vectus Global, Quantum Global Consulting) фактично інтегрувалися у силові дії. Кульмінацією стала пряма участь його найманців, озброєних дронами з українським програмним забезпеченням компанії Swarmer, у січні 2026 року в боях за відбиття міста Увіра пліч-о-пліч із конголезьким спецназом. При цьому контракти з іноземними приватними компаніями (зокрема румунськими під проводом Гораціу Потри та французько-болгарською Agemira) використовуються

¹¹ <https://globalinitiative.net/wp-content/uploads/2026/09/Zobel-Behalal-Violence-for-sale-The-outsourcing-of-security-in-the-M23-conflict-in-the-DRC-GI-TOC-September-2026.pdf>

конголезькою правлячою елітою для корупційного збагачення та перерозподілу багатомільйонних «відкатів» через наближених посередників.

Тіньова економіка протистояння тримається на контролі над критичною сировиною: кольтаном, золотом і деревиною. Захопивши у квітні 2024 року родовище Рубая, що забезпечує близько 15% світового видобутку кольтану, угруповання M23 налагодило монопольний канал нелегального вивезення танталової руди до Руанди в обсягах до 120–195 тонн на місяць, генеруючи щонайменше 800 тис. доларів США прямого податкового доходу щомісяця. Отриманий мінерал «відмивається» в Руанді шляхом змішування з внутрішнім видобутком (експорт кольтану з якої зріс на 110% за відсутності нових копалин) та легально експортується переробникам у Китаї, Казахстані, ОАЕ та Гонконгу. Паралельно контингент армії Уганди (UPDF) у провінції Ітурі поєднує антитерористичні операції з кураторством контрабанди золота, скуповуючи його за завищеними цінами на військових базах і вивозячи військовим транспортом до Кампали, що підживило рекордний угандійський експорт золота до 6,4 млрд доларів США у 2025 році.

Усі учасники протистояння – M23, проурядові ополченці «Вазалендо» та підрозділи FARDC – сформували паралельні нелегітимні квазідержавні адміністрації. Вони самочинно призначають губернаторів, підміняють суди та обкладають населення й бізнес примусовими поборами на блокпостах уздовж торговельних артерій, викачуючи мільйони доларів також із незаконної вирубки цінних порід лісу в національних парках Вірунга та Кахузі-Бієга. Наслідком цієї приватизації насильства стала масштабна гуманітарна катастрофа: понад 10 мільйонів внутрішньо переміщених осіб, масові воєнні злочини, сексуальне насильство та вербування дітей-солдатів. Міжнародні мирні ініціативи (Вашингтонський, Дохійський та Луандійський процеси) зазнають фіаско, оскільки розглядають конфлікт крізь застарілі дипломатичні рамки (припинення вогню, деескалація), ігноруючи надприбуткові воєнні економічні моделі, в яких жодна зі сторін не зацікавлена у встановленні реального миру.

Висновки

Приватизація безпеки як пастка війни: делегування державних силових функцій іноземним приватним військовим компаніям, регіональним арміям і міліціям не розв'язує конфлікт, а руйнує суверенітет ДРК і перетворює бойові дії на бізнес-модель збагачення еліт.

Проксі-контроль Руанди над світовим кольтаном: підтримка M23 регулярними військами та новітньою зброєю спрямована на утримання шахт Рубая (15% світового видобутку) і нелегальне «відмивання» танталу через Руанду на міжнародні ринки електроніки.

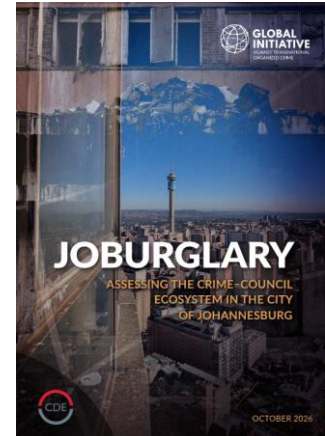
Подвійна роль Уганди у вивезенні золота: беручи участь в офіційних спільних операціях проти повстанців, угандійські військові водночас підтримують озброєні групи та контролюють трафік нелегального золота й лісу, що забезпечило рекордний експорт золота з Уганди до \$6,4 млрд.

Безсилля дипломатії без перекриття ресурсних потоків: мирні ініціативи зазнають краху через ігнорування економічних інтересів сторін; сталий мир можливий лише за умови ембарго на сумнівні мінерали та жорсткої дью-ділідженс перевірки ланцюгів постачання за нормами OECD.

Як корупція та організована злочинність трансформували Йоганнесбург ¹²

Масштабне дослідження, підготовлене міжнародною організацією GI-TOC на замовлення Центру розвитку та підприємництва (CDE) у 2026 році, розкриває феномен системного зрощення муніципального врядування Йоганнесбурга з кримінальними мережами.

Інституційне підґрунтя сучасної катастрофи виникло внаслідок реформ «iGoli» початку 2000-х років, коли управління життєзабезпеченням мегаполіса було розпорошене між тринадцятьма автономними муніципальними підприємствами під гаслом підвищення ринкової ефективності. Після муніципальних виборів 2016 року, коли правлячий Африканський національний конгрес (АНК) утратив монопольну більшість, місто поринуло в хронічну коаліційну турбулентність, змінивши за наступне десятиліття десять мерів та виконавців обов'язків.



Ця політична турбулентність повністю знищила спадкоємність стратегічного розвитку, стерла інституційну пам'ять і спровокувала безконтрольне розростання бюрократичного апарату з прихованим перевищенням зарплатних лімітів. До середини 2026 року муніципалітет опинився перед загрозою банкрутства з інфраструктурним відставанням у понад 220 мільярдів рандів, сформувавши замкнену «екосистему злочинності та ради», де руйнація міста стала передумовою тіньових надприбутків.

Ключовою опорою цієї деградації став перший аналітичний трек – інституційне захоплення, яке розпочалося з тотальної політизації рад директорів комунальних підприємств. Формальний захисний бар'єр, покликаний тримати політиків на «відстані витягнутої руки» від управління активами, був повністю знівельований через контроль членів мерського комітету (MMC) та міського менеджера над призначеннями керівних кадрів. У результаті наглядові органи перетворилися на корупційні вертикалі окремих партій, де професійні інженери та аудитори систематично заміщувалися політично лояльними фігурами.

До складу ради директорів компанії з управління майном Joburg Property Company (JPC) потрапляли колишні касири пунктів збору мита, секретарі та функціонери без завершеної шкільної освіти, а в радах водоканалу Johannesburg Water та енергетичного оператора City Power виникали періоди повної відсутності профільних інженерних спеціалістів. Таке знецінення управлінської експертизи супроводжувалося катастрофічним кадровим дефіцитом на технічному

¹²

<https://globalinitiative.net/wp-content/uploads/2026/10/Joburglary-Assessing-the-crime-council-ecosystem-in-the-city-of-Johannesburg-GI-TOC-October-2026.pdf>

рівні, де брак старших інженерів у City Power досяг 72%, що фактично паралізувало здатність структур запобігати технологічному колапсу.

Контроль над муніципальними агенціями дозволив перетворити публічні закупівлі на механізм масштабного перерозподілу бюджетних коштів, обсяг яких на так звані «контрактні послуги» перевищив 7 мільярдів рандів на рік.

Розслідування GI-TOC реконструювало типову десятикрокову схему тендерного шахрайства: інсайдерський злив цінових пропозицій фаворитам, дискваліфікація незалежних конкурентів за надуманими технічними критеріями, подальше різке завищення контрактної вартості та передача замовлень через ланцюжки фірм-прокладок. Кінцеві субпідрядники виконували роботи за мізерну частку первинного кошторису з найдешевших матеріалів або зовсім кидали об'єкти, як це трапилося з проектом міської оптоволоконної мережі Joburg Broadband, де вартість зросла з 780 мільйонів до 1,2 мільярда рандів через завищення розцінок консультантами. Виведені кошти регулярно перекачувалися у виборчі фонди політичних сил: від перерахування коштів підставними компаніями родичам партійних лідерів до справи Proton House, коли штучно завищена в тринадцять разів виплата 27 мільйонів рандів за ремонт офісів використовувалася для прямого підкупу депутатів міської ради під час зміни коаліційної влади.

Для безперешкодного викачування бюджетів корумповані групи планомірно знищили внутрішні та зовнішні механізми підзвітності. Муніципальний комітет публічних рахунків (MPAC) роками блокував повноцінні розслідування, перетворивши процедуру списання коштів на індульгенцію, внаслідок чого за останні п'ять років Йоганнесбург безкарно списав 45,16 мільярда рандів нерегулярних та марнотратних витрат. Це різко контрастує з практикою Кейптауна, де кожен факт порушень ретельно розслідується, а винні притягуються до фінансової та кримінальної відповідальності.

Кульмінацією захисту тіньових схем став цілеспрямований розгром власної антикорупційної служби мерії – Департаменту судово-медичних та слідчих послуг (GFIS), який розслідував понад 6000 проваджень на 35 мільярдів рандів. У 2023 році рада просто скасувала повноваження та попередні звіти GFIS, а у 2024 році провідного детектива підрозділу Зензеле Сітхале було демонстративно застрелено кілерами перед оприлюдненням доказів співпраці поліцейських із криміналом.

Другий аналітичний трек розкриває гібридну змову, де посадовці муніципалітету прямо координують дії зі злочинним світом задля експлуатації міського простору.

Найбільш прибутковим бізнесом стало захоплення нерухомості: за підтримки чиновників, які передавали конфіденційні дані з муніципальних реєстрів щодо заборгованостей та невіршених спадкових справ, рейдери захопили до 300 будівель не лише в центрі, а й у фешенебельних районах міста. Злочинні синдикати призначали власних комендантів, збирали мільйонні готівкові платежі з незахищених мешканців і за хабарі відновлювали комунікації в обхід лічильників, а суди відмовляли у виселенні через неспроможність міста надати тимчасове соціальне житло. Будь-які спроби власників повернути контроль блокувалися фізичним терором. Аналогічним чином

криміналітет колонізує муніципальні земельні ділянки, стихійно розбудовуючи сотні неформальних поселень та отримуючи сотні тисяч рандів орендної плати щомісяця для фінансування судового захисту від знесення.

Гібридна змова досягла критичних масштабів у сфері базових комунальних послуг, перетворивши нестачу життєво необхідних ресурсів на комерційний інструмент. Так звана «водна мафія» навмисно експлуатує аварійний стан мереж і нерідко штучно поглиблює дефіцит через саботаж клапанів, залякування ремонтних бригад та прямий злив води з автоцистерн, змушуючи владу виділяти сотні мільйонів рандів на закупівлі приватних водовозів за завищеними тарифами.

У сфері електропостачання розкрадання кабелів за участі важкої спецтехніки та навмисні пошкодження підстанцій часто організовуються пов'язаними з менеджерами фірмами заради отримання термінових ремонтних підрядів. Паралельно інфраструктурні майданчики міста тероризує озброєна «будівельна мафія», яка шантажем і силою вибиває до 30% вартості кожного контракту. Ватажки не просто знаходять спільну мову з чиновниками, а й самі проникають до владних кабінетів.

Завершальний трек – пряме обкрадання населення – проявляється у відкритому здирництві з боку муніципальної поліції JMPD та комунальників, що шантажують споживачів фальшивими боргами й загрозою знеструмлення у вечірній час вихідних днів.

При цьому поліцейські структури виявилися глибоко інтегрованими в організовані картелі. Матеріали судової Комісії Мадланги викрили співпрацю керівництва спецпідрозділів JMPD із синдикатом «Big Five»: патрульні забезпечували супровід вантажівкам із викраденою міддю, виводили цілі міські райони з-під нагляду, брали участь у грабежах дорогоцінного каміння та здавали службову зброю криміналу для здійснення розбійних нападів.

Ситуація, коли економічне ядро ПАР із часткою у 16% національного ВВП балансує на межі некерованого кримінального захоплення, доводить недієздатність суто косметичних та технократичних реформ. Порятунком Йоганнесбурга потребує радикального зовнішнього аудиту контрактів у реальному часі, безкомпромісного силового розчищення захоплених секторів і повної перебудови скомпрометованих муніципальних інституцій, інакше кримінальна екосистема остаточно поглине залишки міського суверенітету.

Висновки

Функціонування трирівневої кримінальної екосистеми: Злочинність і врядування в муніципалітеті злились через інституційне захоплення, гібридну змову та прямі побори і вимагання.

Руйнація та прямий саботаж критичної інфраструктури штучно генерують попит на надприбуткові екстрені тендери, а виведені кошти формують неформальні політичні бюджети, які використовуються для підкупу радників і зміцнення контролю над новими фінансовими потоками.

Спроможність контролюючих органів була паралізована через блокування розслідувань, позбавлення повноважень міського антикорупційного слідчого підрозділу GFIS та безперешкодне списання муніципальним комітетом коштів.

Муніципальна поліція (JMPD) зазнала структурного захоплення кримінальними картелями, що проявилось в системному вимаганні хабарів, супроводі краденого металу, наданні службової зброї в оренду для нальотів на інкасаторів та фізичному усуненні детективів.

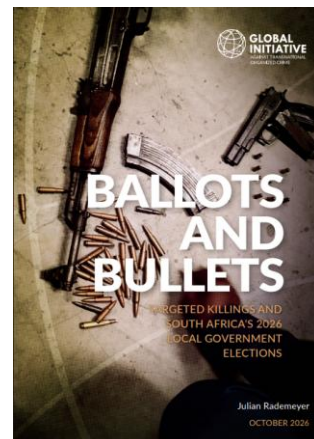
Бюлетені та кулі: анатомія ринку замовних убивств напередодні виборів ¹³

У Південно-Африканській Республіці спостерігається тривожний парадокс: у той час як загальний рівень навмисних убивств у країні демонструє тенденцію до зниження, кількість цілеспрямованих політичних ліквідацій стрімко зростає. GI-TOC оприлюднила масштабне дослідження, що фіксує критичне загострення кримінального насильства в період підготовки до муніципальних виборів, призначених на листопад 2026 року.

Політичні замовні вбивства досягли безпрецедентного історичного піка. З 1 січня до 30 вересня 2026 року зафіксовано 45 політичних нападів, у яких загинуло щонайменше 43 людини. Піковим періодом насильства став перший вікенд реєстрації виборців 20–21 червня 2026 року, коли за лічені години в чотирьох провінціях скоординованими нападами було ліквідовано шістьох політичних активістів і кандидатів. Червень загалом став найкривавішим місяцем року: 40 інцидентів у всіх категоріях, із них 12 – політичні.

Аналіз мотивів свідчить, що муніципальні вибори в ПАР є значно більш смертоносними, ніж національні перегони. Посада муніципального радника чи чиновника на місцях надає прямий доступ до розподілу бюджетів, контролю за списками соціального житла, працевлаштування та, передусім, до державних тендерів і системи публічних закупівель. У 2018 році Комісія під головуванням адвоката Марумо Моеране розслідувала причини політичних убивств у провінції Квазулу-Наталь і дійшла висновку, що головним драйвером насильства є корупційна система тендерів, у межах якої політики, посадовці та бізнесмени діють у злочинній змові. Комісія зафіксувала залучення кримінальних елементів для досягнення політичних цілей, маніпулювання органами безпеки та систематичну деградацію внутрішньої розвідки поліції. Однак через сім років після оприлюднення висновків рекомендації комісії залишилися невиконаними: незалежна панель врегулювання політичних конфліктів так і не запрацювала, деполітизація державної служби не відбулася, а тендерна економіка, заснована на патронажі та замовних убивствах, продовжила процвітати.

Географія та структура цілей у 2026 році демонструють загрозливу трансформацію. Якщо протягом останньої чверті століття політичні ліквідації були здебільшого внутрішньою міжусобицею в лавах правлячого АНК, то зараз насильство поширилося на широкий міжпартійний і громадський спектр. Водночас насильство різко поширилося на регіони, де воно раніше було рідкістю: Західний Кейп, Північно-Західну провінцію та Лімпопо.



¹³ <https://globalinitiative.net/wp-content/uploads/2026/10/Julian-Rademeyer-Ballots-and-bullets-Targeted-killings-and-South-Africas-2026-local-government-elections-GI-TOC-October-2026.pdf>

Доступність ринку замовних убивств зумовлена його низьким ціновим порогом та майже повною безкарністю. Згідно з дослідженнями GI-TOC, вартість найму кіллера в Південній Африці може коливатися від 145 до 8 700 доларів США. Лише близько 15% убивств у країні офіційно розкриваються. Навіть коли правоохоронцям вдається затримати виконавців – арешти чи звинувачення зафіксовані у 12 з 45 політичних нападів 2026 року – замовники майже ніколи не притягуються до відповідальності. Діяльність Спеціалізованої групи з розслідування політичних убивств (Political Killings Task Team), яку наприкінці 2024 року безуспішно намагалося розформувати керівництво поліції, наразі триває під пильним контролем Комісії Мадланги, що розслідує факти політичного втручання в діяльність силових структур.

Критичною загрозою для інституційної стабільності держави став прямий терор проти системи кримінальної юстиції. Зафіксовано щонайменше 14 нападів на осіб, пов'язаних із правосуддям: 13 із них були фатальними, забравши життя 17 людей у чотирьох провінціях. Під ударом опинилися вісім свідків у резонансних справах про наркотики та шахрайство зі страхуванням, троє співробітників поліції, один викривач і один адвокат. Свідки, що перебували під програмою захисту або мали давати свідчення в судах, були викрадені або застрелені у власних оселях, що завдає нищівного удару по спроможності держави доводити складні кримінальні процеси до вироків.

Новою тривожною мішенню криміналу стали працівники освітньої галузі. За дев'ять місяців 2026 року відбулося п'ять нападів на співробітників шкіл із характерними ознаками замовних дій, три з яких виявилися смертельними. Це продовжило хвилю кінця 2025 року, коли загинули чотири керівники шкільних закладів. Розслідування показують, що мотиви нерідко криються у внутрішній конкуренції за адміністративні посади директорів чи заступників, коли колеги замовляють одне одного кілерам, або в помсті місцевих кримінальних угруповань директорам.

Окремим загрозливим явищем 2026 року став вибуховий ріст масових розстрілів, пов'язаних із кримінальними ринками, які GI-TOC виокремила в окрему аналітичну категорію. Із січня до кінця вересня зафіксовано 45 таких інцидентів, у яких загинуло щонайменше 210 людей і ще 79 дістали поранення, тоді як за весь 2025 рік сталося лише 19 подібних масових нападів.

Цифри доводять, що реагування держави залишається суто реактивним. Безкарність замовників, параліч муніципального антикорупційного контролю, незахищеність свідків та деградація спецслужб дозволили кримінальному управлінню (criminal governance) проникнути в основу демократичного устрою. Якщо уряд не змістить фокус на розкриття фінансових мереж, припинення тендерного свавілля та демонтаж ринку кілерів, замовні вбивства остаточно підмінять собою результати народного волевиявлення, визначаючи зброєю, кому дозволено здійснювати публічну владу.

Висновки

Рекордне загострення політичного терору перед виборами: За перші дев'ять місяців 2026 року зафіксовано 45 політичних нападів і щонайменше 43 смерті, що вже перевищило загальні річні показники попередніх муніципальних і національних виборчих кампаній ще до початку найнебезпечнішої фінальної фази перегонів.

Тендерна корупція як головний стимул ліквідацій: Основним мотивом убивств на місцевому рівні є не політична ідеологія, а боротьба за доступ до муніципальних ресурсів, бюджетних потоків і державних тендерів через зрощування корумпованих політиків, чиновників та криміналітету.

Експансія на сектор юстиції та освіти: Насильство вийшло за рамки внутрішньопартійних конфліктів – замовні атаки спрямовуються проти широкого кола партій, традиційних лідерів, а також системно руйнують правосуддя через розстріли свідків, детективів, прокурорів і навіть освітян у конфліктах за адміністративні посади.

Зростання організованої злочинності та масового терору: Організований кримінал є джерелом найбільшої частки нападів, індустрія маршрутних таксі залишається каналом постачання зброї, а спалах масових розстрілів вказує на перехід кримінальних ринків від точкових ліквідацій до силового контролю над цілими територіями.

Кіберстратегія Китаю та прогалини західного стримування: відеокоментар RUSI ¹⁴



Королівський інститут оборонних досліджень (RUSI) 14 жовтня 2026 року оприлюднив одинадцятихвилинний відеокоментар «China's Cyber Strategy and Western Deterrence Gaps», присвячений тому, що урядам держав НАТО слід робити інакше у

відповідь на підхід Китаю до кібершпигунства. Співрозмовницями виступили старша наукова співробітниця групи кіберпитань і технологій RUSI д-р Луїза Марі Юрель та д-р Ахана Датта Фазель – колишня керівниця кібернапрямку Financial Times, яка обіймала посади у сфері кібербезпеки в Міністерстві юстиції, Кабінет-офісі та Національному центрі кібербезпеки Великої Британії, нині стратегічна радниця з питань національної безпеки й оборони UK Research and Innovation. Запис доступний на сторінці RUSI та на YouTube-каналі інституту.

Предметом обговорення є три взаємопов'язані теми: використання Китаєм кіберпростору як полігону для випробування меж ескалації; хибне сприйняття на Заході, коли китайські операції тривалий час трактувалися як ізольовані інциденти, а не як елементи скоординованої державної політики; і потреба вибудувати дієві стратегії стримування. Відеокоментар продовжує дослідження Юрель і Мотта, у якому обстоюється думка, що для протидії гібридним загрозам з боку росії та Китаю держави НАТО і їхні союзники не можуть розглядати кібербезпеку як ізольовану діяльність профільних кібервідомств. Потрібен підхід «усього уряду», що накладає витрати на противника не через створення нових інституцій чи інструментів, а через інтегроване використання наявних.

Контекст для розмови задає книга д-ра Фазель «Full Stack Spies: Cyber Espionage in the Age of US-China Competition», яка досліджує динамічні взаємозалежні відносини між хакерами, фахівцями з кіберзахисту, технологічними гігантами й державами, що формують і використовують кіберпотужність проти цілей у геополітиці, світовій торгівлі та фінансах, збройних силах і критичній інфраструктурі. Для членів RUSI також доступний запис годинного заходу «Cyber Espionage in the Age of US-China Competition».

Для фахівців у сфері ПВК/ФТ/ФР матеріал корисний як стисле введення в логіку, за якою фінансові інструменти – санкції, позначення криптогаманців і бірж, посилений моніторинг у сфері ПВК/ФТ –

¹⁴

[https://www.rusi.org/news-and-comment/video-commentary/chinas-cyber-strategy-and-western-deterrence-gaps;](https://www.rusi.org/news-and-comment/video-commentary/chinas-cyber-strategy-and-western-deterrence-gaps)
<https://www.youtube.com/watch?v=xRB7vFVSCU0>

розглядаються як повноцінна частина стримування державних кібероперацій. Відеокоментар доцільно переглядати разом зі звітом RUSI «Beyond 'Cyber' in Deterrence: A Multilevel Framework», який представлено в розділі 4 цього випуску.



Як кіпрський офіс Deloitte переписував історію активів Романа Абрамовича ¹⁵

Масштабний витік внутрішньої кореспонденції та фінансових документів у межах міжнародного журналістського розслідування Cyprus Confidential розкрив системну співпрацю між кіпрським представництвом міжнародної аудиторської компанії Deloitte, корпоративним провайдером MeritServus та менеджерами російського мільярдера Романа Абрамовича. Матеріали свідчать про те, що в середині 2000-х років, коли Кіпр готувався до вступу в Європейський Союз і суттєво посилював податкові вимоги та стандарти публічної фінансової звітності для приватних і підконтрольних іноземцям підприємств, аудитори та трастові керівники розробили механізми переведення активів на мільярди доларів до юрисдикції Британських Віргінських Островів (BVI). Ключовим інструментом цієї практики стало системне створення юридичної документації заднім числом.

Один із найбільш показових епізодів стосується кіпрської структури Kravin Investments Limited, створеної для обслуговування комерційних операцій олігарха ще наприкінці 1990-х років. У 2003 році ця компанія акумулювала мільярдні кошти від реалізації 20% акцій нафтового концерну «Сибнефть» компанії ЮКОС. До кінця 2003 року залишки на її банківських рахунках досягали близько 1,8 мільярда доларів, генеруючи значні відсоткові доходи. Законодавчі зміни на Кіпрі передбачали оподаткування пасивного доходу іноземних фірм за ефективною ставкою близько 15%. Щоб уникнути нарахування податкових зобов'язань, очільник MeritServus Деметріс Іоаннідіс

¹⁵ <https://www.occrp.org/en/project/cyprus-confidential/deloittes-office-in-cyprus-helped-abramovich-firms-relocate-billions-of-dollars-in-assets-in-apparent-bid-to-sidestep-tax-and-transparency>

разом із партнерами кіпрського офісу Deloitte Антонісом Таліотісом та Нікосом Хараламбусом розробили схему оформлення фіктивного ланцюга документів. У 2005 році сторони погодили створення угод, за якими Kravin нібито виплатила дивіденди своїй материнській компанії Kelvedon Worldwide Limited на BVI ще у травні 2003 року, а надалі лише утримувала ці депозити в довірчому управлінні. У результаті подана до кіпрського реєстру лише у 2016 році фінансова звітність за 2005 рік зафіксувала мізерні 15 тисяч доларів сплачених податків, а аудиторський партнер Deloitte офіційно завірив її як таку, що достовірно відображає фінансовий стан.

Аналогічну технологію було використано для виведення з-під вимог публічного розкриття особистих елітних активів через кіпрську компанію Amiscan Investments Limited. Початкові проекти звітності, складені Deloitte у 2005 році, фіксували володіння флотом супер'яхт на суму 354 мільйони доларів, повітряними суднами вартістю 142 мільйони доларів та елітною нерухомістю у Франції та Великій Британії на 127 мільйонів доларів. Побоюючись, що подання звітів до публічного реєстру Кіпру викриє майно бенефіціара, фінансові радники Millhouse та аудитори домовилися штучно створити угоду купівлі-продажу 19 дочірніх компаній 4 січня 2003 року, передавши їх структурам на BVI за собівартістю. Менеджер Deloitte Андреас Іоанну прямо вказував у листуванні, що головною метою формування звітності є мінімізація обсягу розкритої інформації та уникнення податкових зобов'язань. Згодом Deloitte офіційно підписав аудит Amiscan із нульовою балансовою вартістю активів.

Показовим прикладом маскуванню структури власності стала ситуація з головною кіпрською холдинговою компанією Electus Investments Limited, яка замикала на собі управління активами трасту Sara Trust на мільярди доларів. Прагнучи уникнути аудиторської звітності на Кіпрі, консультанти створили однойменну фірму-двійника на Британських Віргінських Островах та оформили передачу прав бенефіціарної власності станом на листопад 2003 року. Єдиним активом, який вимушено залишили на балансі кіпрської Electus, стала частка в британській філії Millhouse Capital UK вартістю близько 145 тисяч доларів, оскільки в публічних реєстрах Великої Британії вже містився незворотний прямий запис про її підпорядкування саме кіпрській компанії.

Провідні міжнародні експерти у сфері оподаткування, аудиту та комплаєнсу одноставно класифікують подібні маніпуляції з датами як фальсифікацію та потенційне ухилення від сплати податків, наголошуючи, що аудиторські фірми мають виступати гарантами доброчесності, а не архітекторами сумнівних схем. Захист Абрамовича відкидає будь-яку обізнаність олігарха щодо підробки документів, стверджуючи, що структури повністю поклалися на експертизу Deloitte. Тим часом сам Абрамович залишається суб'єктом розслідування правоохоронних органів острова Джерсі за підозрою у відмиванні доходів, отриманих від продажу акцій «Сибнефти». Деметріс Іоаннідіс та його компанія MeritServus у 2023 році опинилися під санкціями уряду Великої Британії за створення непрозорих структур для приховування майна підсанкційних осіб, а регуляторні органи Кіпру відкликали їхні ліцензії. Цей прецедент є свідченням того, як професійні юридичні й аудиторські посередники використовували прогалини міждержавного контролю для перетворення фінансової звітності на інструмент приховування капіталу.

Ваша думка важлива!

Які критерії внесення до реєстру «дропів», строки перебування в ньому та механізми оскарження дозволили б йому виконувати роль спільної антифрод-утиліти без надмірного обмеження доступу громадян до платіжних послуг?

Як має бути визначено в українському законодавстві про віртуальні активи статус доларових стейблкоїнів, емітенти яких не авторизовані за MiCA, з огляду на позицію ESMA та масштаби їх використання в Україні?

Як наглядовим органам відрізнити обґрунтоване використання запитів правоохоронців та інших банків як джерела інформації від фактичного «аутсорсингу» виявлення підозрілих операцій, описаного у справі Bank of America?

Як Україні оптимізувати передачу доказів до ЄС щодо іноземних мікросхем і вузлів, які знаходять у збитих ракетах і дронах, аби довести факти постачання компонентів до РФ через посередників у третіх країнах?

Яку відповідальність доцільно запровадити в Україні безпосередньо для посадових осіб юридичних компаній, які допомагають реструктурувати бізнес підсанкційних осіб або приховувати КБВ?

Контакуйте 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-2026-42

Архів

Бюлетень є аналітичною розробкою методологічної команди Департаменту антилегалізаційної політики Міністерства фінансів України, спрямованою на поширення кращих практик, дослідження новітніх типологій та глобальних регуляторних і правоохоронних тенденцій у сфері ПВК/ФТ/ФР. Видання призначене для підвищення інституційної спроможності всіх учасників AML системи України та сприяння ефективному управлінню ризиками ВК/ФТ/ФР з урахуванням міжнародних стандартів та актів права ЄС.



Міністерство
фінансів
України



AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE