Міністерство
фінансів
України

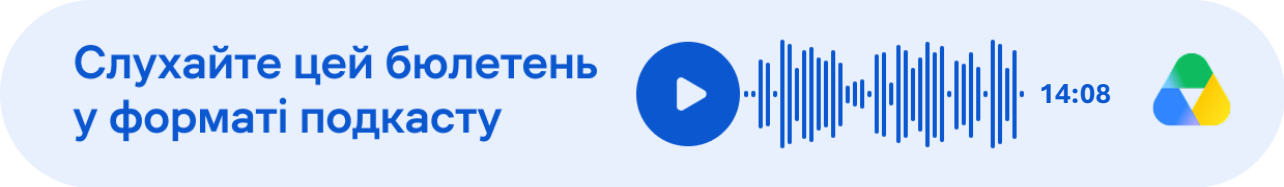
Методологічний бюлетень AML

№45/2026



Зміст

Звіт Європейської комісії щодо України 2026: стійкість антикорупційної системи, законодавчі затримки та прогалини у сфері ПВК/ФТ 3
FATF про скам-комплекси: наскрізна модель незаконних фінансових потоків і інструментарій протидії «епідемії шахрайства» 7
Стратегія протидії гібридним загрозам в Європі 12
Річний звіт AUSTRAC за 2025–26 роки: боротьба з фінансовими злочинами та реформування режиму ПВК/ФТ 15
Жовтневий випуск SARs Reporter Booklet 17
Чи справді стейблкоїни дешевші за традиційні грошові перекази? 20
Майбутнє платежів: трансформація платіжних систем, токенізація та ключові завдання для центральних банків 24
Баланс між анонімністю та регулюванням: дослідження криптографічних інструментів захисту приватності в цифрових валютах центральних банків 26
Злам Binance: анатомія найбільшого цифрового пограбування в історії 29
Санкційний фронт і тіньові мережі: як російська розвідка забезпечує війну в умовах ізоляції 35
Регулювання цифрових активів у мінливому глобальному ландшафті: еволюція інфраструктури та виклики для політики 37
Операція «Карфаген»: НАБУ і САП оприлюднили матеріали щодо нової злочинної організації та повідомили про підозру п'ятьом особам 39
Інституційні зміни антикорупційної архітектури США 43



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.

Звіт Європейської комісії щодо України 2026: стійкість антикорупційної системи, законодавчі затримки та прогалини у сфері ПВК/ФТ [1]

Європейська комісія оприлюднила робочий документ, який супроводжує щорічне Повідомлення про політику розширення ЄС. Звіт фіксує суттєве просування переговорного процесу: кластер 1 «Основи процесу вступу» формально відкрито на міжурядовій конференції 15 червня, кластер 6 «Зовнішні відносини» – 14 липня, кластери 2 «Внутрішній ринок» і 3 «Конкурентоспроможність та інклюзивне зростання» – 13 жовтня 2026 року, а всі інші кластери Комісія оцінила як готові до відкриття. У квітні 2026 року Україна ухвалила Національну програму адаптації законодавства до acquis ЄС (NPAA). Водночас Комісія прямо називає «предметом занепокоєння» уповільнення законодавчого процесу протягом звітного періоду і відзначає, що з кінця літа увага до реформ і до виконання умов Ukraine Facility та Ukraine Support Loan зросла; у жовтні 2026 року Україна та Комісія створили спільну Цільову групу для прискорення виконання проміжних контрольних показників (interim benchmarks) у сфері верховенства права й боротьби з корупцією.

Центральна оцінка розділу 23 «Судова влада та фундаментальні права» полягає в розмежуванні операційної ефективності спеціалізованих антикорупційних інституцій і браку структурних законодавчих рішень. Рівень підготовки у сфері боротьби з корупцією визначено як проміжний між «певним» і «помірним», при цьому Комісія підвищила загальну оцінку саме завдяки результатам НАБУ, САП і ВАКС: розслідуванням, обвинувальним актам і остаточним вирокам у справах корупції найвищого рівня, зокрема щодо чинних міністрів, керівництва Офісу Президента, суддів, прокурорів і народних депутатів. У звіті окремо згадано операцію «Мідас» щодо можливої корупції та відмивання коштів у закупівлях в енергетичному та оборонному секторах, нові повідомлення про підозру в серпні 2026 року, а також викриту НАБУ у вересні 2026 року організовану групу, яка, за даними слідства, налагодила систему неправомірної вигоди за невтручання в діяльність шахрайських колцентрів; ця справа, за текстом звіту, призвела до відставки Генерального прокурора, його першого заступника та до арешту високопосадових прокурорів. Комісія також відзначає, що у 2025 році десять обвинувачених у справах корупції високого рівня були звільнені від кримінальної відповідальності у зв'язку із закінченням строків давності.

[1] https://enlargement.ec.europa.eu/document/download/c817ca8c-4ddf-405d-896a-40becd42924a_en?filename=ukraine-report-2026.pdf

Водночас Комісія констатує, що протягом звітного періоду не ухвалено жодного закону, який суттєво посилював би антикорупційну законодавчу базу, а десять пріоритетних реформ, погоджених з українською владою 10 грудня 2025 року, здебільшого залишаються невиконаними. Ратифікація Конвенції ОЕСР про боротьбу з підкупом іноземних посадових осіб досі залежить від змін до кримінального законодавства. Україні рекомендовано утримуватися від законодавчих ініціатив, що містять корупційні ризики, – зокрема щодо політично значущих осіб (PEP), кримінальних процедур у справах про економічні злочини та безоплатної приватизації землі. Серед конкретних вимог – розширення підслідності НАБУ на всі посади високого ризику (керівництво Офісу Президента, голови обласних адміністрацій), запровадження гарантій від втручання інших правоохоронних органів у виключну підслідність НАБУ, самостійне ініціювання НАБУ і САП розслідувань щодо народних депутатів без погодження Генерального прокурора, незалежні спроможності НАБУ щодо зняття інформації з каналів зв'язку та доступ до неупередженої судової експертизи, скасування автоматичного закриття проваджень після спливу строків досудового розслідування і перегляд строків давності. Комісія фіксує, що НАБУ і САП продовжують повідомляти про тиск, зокрема про кримінальні провадження та стеження щодо працівників НАБУ з боку інших правоохоронних і безпекових органів, а також про медійні кампанії з дискредитації; строк повноважень чинного керівника САП спливає у липні 2027 року.

У розділі 24 «Юстиція, свобода та безпека» Комісія констатує відсутність прогресу в наближенні законодавства до acquis ЄС у сфері протидії тяжкій та організованій злочинності. Україна завершила оцінку загроз тяжкої та організованої злочинності (SOCTA) за 2021–2024 роки, проте досі не створила постійного національного координатора з протидії організованій злочинності, не ухвалила Стратегію фінансових розслідувань, а Стратегія повернення активів та план дій до неї втратили чинність у 2025 році без ухвалення наступних документів. Бюро економічної безпеки укомплектоване лише на 29 % (1 145 з 4 000 штатних посад), перша хвиля переатестації має завершитися до лютого 2027 року; конкурс на посаду керівника АРМА довелося оголосити повторно. Щодо СБУ Комісія відзначає відсутність суттєвих кроків реформування, рекомендує зосередити мандат служби на завданнях національної безпеки, обмежити її функції досудового розслідування і скасувати фактичну монополію на зняття інформації з каналів зв'язку. Щодо Національної поліції зазначено відсутність прогресу у запровадженні конкурсного добору керівного складу за участі незалежних експертів і наголошено на виявлених у звітному періоді корупційних справах щодо керівників поліції. Фінансові розслідування, за оцінкою Комісії, залишаються недостатньо використовуваним інструментом, за винятком НАБУ та БЕБ, а відсутність консолідованої статистики арештів і конфіскації активів унеможливлює оцінку їхньої ефективності.

Окремий блок присвячено кримінальному переслідуванню за відмивання коштів. У 2025 році кількість кримінальних проваджень за ст. 209 ККУ зросла до 3 454 (2024 – 3 187), обвинувальних актів – до 594 (496), вироків – до 271 (157), однак переважна й дедалі більша частка засуджених отримала покарання зі звільненням від відбування з випробуванням (188 проти 105). Кількість судових рішень про конфіскацію майже подвоїлася (96 проти 51), але в абсолютному вимірі залишається скромною, а залишок нерозглянутих справ у судах до кінця року зріс на 21 %.

Держфінмоніторинг у 2025 році передав правоохоронним органам і прокуратурі 1 441 матеріал (2024 – 1 053), проте Комісія фіксує суттєве скорочення кількості матеріалів, переданих до НАБУ, зменшення запитів до іноземних підрозділів фінансової розвідки (455 проти 621) і подальше падіння частки кримінальних проваджень, розпочатих на підставі матеріалів ДСФМ, – до 2,5 % від загальної кількості. Запланована оцінка MONEYVAL відкладена.

У розділі 4 «Вільний рух капіталу» Комісія пов'язує затримки у сфері ПВК/ФТ безпосередньо з перспективою приєднання України до географічного охоплення схем SEPA. У грудні 2025 року уряд повторно вніс до Верховної Ради комплексний пакет законодавства про наближення до acquis ЄС у сфері ПВК/ФТ, що передбачає створення реєстру рахунків та індивідуальних банківських сейфів фізичних осіб і реєстру бенефіціарних власників трастів та подібних правових утворень; Комісія наголошує, що затримка з його ухваленням «продовжує перешкоджати» наближенню до рамки ЄС, а в розділі 24 – що відповідні зміни «залишаються заблокованими» в парламенті й мають бути ухвалені без положень, які відтерміновують запуск реєстрів і доступ до них правоохоронних органів. Окремо зазначено, що в червні 2026 року парламент ухвалив норми, які обмежують фінансовий моніторинг колишніх PEP, і що в жовтні, до набрання ними чинності, їх було змінено; Україні рекомендовано подальше наближення до acquis ЄС щодо PEP. У сфері віртуальних активів законопроєкт про наближення до Регламенту про супровідну інформацію до переказів коштів і криптоактивів (TFR), ухвалений у першому читанні у вересні 2025 року, досі не прийнятий, як і законопроєкт про наближення до Регламенту MiCA.

Інституційна частина розділу 4 стосується Держфінмоніторингу. Комісія відзначає ухвалення у серпні 2026 року четвертої НОР ВК/ФТ і вимагає розробити на її основі комплексний національний план зменшення виявлених ризиків. У 2025 році ДСФМ отримав майже два мільйони повідомлень про фінансові операції (на 11 % більше, ніж у 2024 році), переважна частка яких надходить від банків, тоді як звітування нефінансового сектору залишається «дуже обмеженим». Того ж року надійшло 11 523 повідомлення про розбіжності у відомостях про КБВ, проте спроможність Міністерства юстиції їх опрацьовувати потребує посилення. Комісія фіксує ресурсні обмеження ДСФМ і те, що строк дії його стратегічних документів сплив, та рекомендує законодавчо гарантувати операційну незалежність, автономію й достатню спроможність підрозділу фінансової розвідки, зокрема через прозорий конкурсний добір його керівника з обмеженим строком повноважень і запровадження періодичних незалежних аудитів ефективності системи ПВК/ФТ.

Низка положень звіту має прямий стосунок до прозорості власності та санкційної політики. У сфері публічних закупівель із січня 2026 року обов'язок розкриття інформації про бенефіціарних власників поширено на всі види закупівель, проте рамкові угоди для окремих будівельних робіт без відкритих торгів обмежують прозорість і моніторинг. Рівень приєднання України до заяв Високого представника ЄС і рішень Ради ЄС щодо обмежувальних заходів станом на 1 вересня 2026 року становив 99 %, однак Комісія наголошує, що обхід санкцій досі не криміналізовано, і Кримінальний кодекс має бути відповідно змінений. Застосування національного санкційного режиму, за оцінкою Комісії, має залишатися в межах Європейської конвенції з прав людини.

У сукупності звіт формує чіткий порядок денний для системи ПВК/ФТ: Комісія розглядає ухвалення законодавчого пакета щодо реєстрів, приведення норм про PEP у відповідність до acquis, ухвалення законів про віртуальні активи та криміналізацію обходу санкцій як конкретні передумови подальшого просування, а підвищення ефективності ДСФМ – як питання інституційної незалежності й вимірюваних результатів, а не обсягу отримуваної звітності. Паралельно звіт пов'язує стійкість антикорупційної архітектури з усуненням тиску на НАБУ і САП та з реформуванням СБУ, Національної поліції, ДБР і прокуратури, що безпосередньо впливає на ефективність фінансових розслідувань і повернення активів.

Висновки

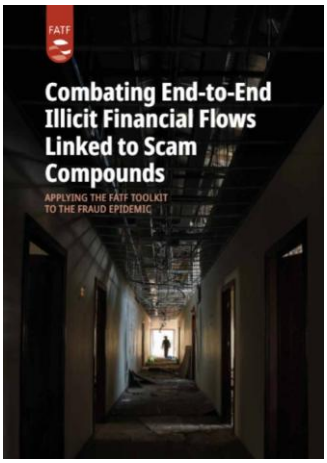
Законодавчий пакет ПВК/ФТ став критичним елементом переговорного процесу: Комісія пов'язує затримку з реєстром рахунків і сейфів фізичних осіб та реєстром бенефіціарних власників трастів із приєднанням до SEPA і наближенням до acquis, вимагаючи вилучити положення, що відтерміновують запуск реєстрів і доступ до них правоохоронних органів; створена в жовтні 2026 року спільна Цільова група робить ці кроки предметом безпосереднього моніторингу.

Ефективність ДСФМ оцінюватиметься за результатами, а не за обсягом звітності: майже два мільйони повідомлень на рік на тлі 2,5 % кримінальних проваджень, розпочатих за матеріалами ДСФМ, скорочення матеріалів до НАБУ і запитів до іноземних ПФР зумовлюють вимоги щодо періодичних незалежних аудитів ефективності, конкурсного добору керівника з обмеженим строком повноважень і нового національного плану за результатами НОР-4.

Регулювання щодо PEP перебуває у фокусі ЄС: Комісія двічі згадує ініціативи щодо PEP – як ризикове законодавство в розділі 23 і як предмет наближення до acquis у розділі 4, – тож будь-які зміни до строків і обсягу посиленого моніторингу колишніх PEP мають оцінюватися на відповідність Директиві та Регламенту ЄС з ПВК/ФТ, а також Рекомендації 12 FATF.

Прогалини у фінансових розслідуваннях і санкційному законодавстві потребують окремих рішень: відсутність Стратегії фінансових розслідувань і чинної Стратегії повернення активів, консолідованої статистики арештів і конфіскації, некриміналізований обхід санкцій та неухвалені закони про віртуальні активи (TFR, MiCA) формують конкретний перелік законодавчих і методологічних кроків, від яких залежить оцінка України як у процесі вступу, так і під час майбутньої оцінки MONEYVAL.

FATF про скам-комплекси: наскрізна модель незаконних фінансових потоків і інструментарій протидії «епідемії шахрайства» [2]



Документ є першим результатом «дорожньої карти» FATF з протидії шахрайству, визначеної пріоритетом головування Великої Британії, і підготовлений під керівництвом Великої Британії та США проєктною командою з експертів 32 юрисдикцій (зокрема 18 членів FATF) і 9 спостерігачів, серед яких Егмонтська група, Europol, МВФ, Інтерпол і УНЗ ООН. Емпіричну базу становлять відповіді 60 юрисдикцій на опитувальник серпня 2026 року та письмові внески 17 представників приватного сектору й громадянського суспільства. Звіт виходить з того, що шахрайство щороку завдає збитків близько 500 млрд доларів США, а 90 % оцінених юрисдикцій прямо визначають його як основний ризик відмивання коштів; у перших семи звітах п'ятого раунду взаємних оцінок тема шахрайства висвітлюється приблизно у 2,5 раза ширше, ніж у четвертому раунді, а звіт про взаємну оцінку Малайзії вперше називає скам-комплекси в сусідніх юрисдикціях окремим чинником ризику.

Методологічно важливою є термінологія. Термін «scam compounds» (скам-комплекси) FATF використовує як узагальнювальне робоче поняття для організованих шахрайських операцій індустріального й мережевого характеру – від великих фізичних комплексів, переважно в Південно-Східній Азії й пов'язаних із торгівлею людьми та примусовою злочинністю, до розосереджених «скам-осередків». Термін «scam centre» свідомо не використовується, щоб уникнути плутанини з державними «антискам-центрами», а для кримінальних операцій колцентрового типу запропоновано формулювання «fraudulent call centre operation», яке відмежовує їх від легальних послуг аутсорсингу. За даними звіту, скам-комплекси спеціалізуються переважно на інвестиційному шахрайстві, якому передує романтичне або довірче «опрацювання» жертви, націлене на осіб у понад 100 юрисдикціях, і поєднують вертикальну інтеграцію з економікою «злочин як послуга»: контролери можуть перебувати поза юрисдикцією фізичного комплексу, а окремі функції – від генерації діпфейків до відмивання – передаються на аутсорсинг спеціалізованим постачальникам. Під тиском правоохоронців операції дробляться й переміщуються, тоді як спільні контролери та фінансова інфраструктура зберігаються.

Ядром звіту є наскрізна модель незаконних фінансових потоків із семи етапів. На етапі створення операційних майданчиків та інфраструктури кошти спрямовуються на приміщення, телекомунікаційне та IT-обладнання, вербування, транспорт, документи, охорону, хабарі, підставні компанії, рахунки-«мули» та доступ до каналів віртуальних активів чи підпільного

[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/combating-illicit-financial-flows-linked-to-scam-compounds-fatf-2026.pdf.coredownload.pdf

банкінгу. Етап залучення працівників і жертв поєднує дві форми віктимізації: осіб, яких через фальшиві вакансії вербують, переправляють через кордон і примушують до шахрайства, та жертв, яких атакують через соцмережі, месенджери, сайти знайомств і фейкові інвестиційні платформи. Під час здійснення шахрайства та вилучення коштів використовуються фіктивні інвестиційні кабінети, невеликі початкові «виплати прибутку», повторні вимоги «поповнення», «податку» чи «розблокування», видавання себе за агентів із повернення коштів, а також «approval phishing», коли жертва підписує в блокчейні дозвіл на списання токенів зі свого гаманця. Збір і первинне розміщення охоплюють зарахування коштів на особисті, корпоративні та «мульні» рахунки, гаманці MVTS і BA, а також отримання готівки чи золота через кур'єрів; у колцентрових моделях збирачі передають готівку чи коштовності логістам для передачі вище. На етапі нашарування кошти розпорошуються через мережі «мулів», корпоративні рахунки, P2P-обмін, OTC-брокерів і «U-мерчантів», конвертуються в стейблкоїни, проходять через DeFi-мости, міксери, криптобанкомати й онлайн-гемблінг або через підпільний банкінг, за якого еквівалент виплачується за кордоном без прямого переказу тих самих коштів. Виведення та інтеграція включають зняття готівки, зворотну конвертацію через VASP і OTC, хавалу, фізичне переміщення готівки через кордон і вкладення в нерухомість, предмети розкоші, транспорт, дорогоцінні метали та підставні компанії. Сьомий етап — вилучення прибутку, реінвестування та розширення — замикає цикл: частина коштів стає прибутком контролерів, решта йде на оплату працівників, охорони й вербувальників, корупцію та нові операції. FATF наголошує, що модель є модульною, а не лінійним ланцюгом тих самих виконавців.

Окремо звіт оцінює 54 функціональні залежності скам-комплексів у восьми блоках щодо семи функцій їхнього життєвого циклу. 14 із них визначено як потенційно критичні, тобто такі, заміну яких складно, дорого або довго здійснити. У висхідній частині та в «платіжному вікні» це цифрова й телеком-інфраструктура, спеціалізовані послуги для шахрайства, спільні кримінальні зв'язки й фізична інфраструктура з охороною та корупцією; у низхідній — послуги «мулів» і професійного відмивання, фінансові установи та MVTS, канали BA/VASP/OTC і корпоративні структури.

Де зосереджені критичні залежності скам-комплексів



Джерело: FATF (2026), Combating End-to-End Illicit Financial Flows Linked to Scam Compounds, Infographic 2 (14 потенційно критичних залежностей)

Аналіз фінансових каналів демонструє, наскільки швидким є рух коштів. Мережі «мулів» залучають уразливих осіб – літніх людей, молодь, осіб у скрутному становищі, – а дедалі частіше

купують, продають або викрадають ідентифікаційні дані, щоб відкривати численні рахунки й гаманці в різних провайдерів і обходити контроль за збігом імен; у деяких випадках кошти переміщуються далі вже протягом двох хвилин. Віртуальні активи FATF визначає центральним каналом відмивання: офшорні VASP, P2P-перекази, OTC-брокери та криптобанкомати, а в окремих випадках – OTC-«каси» безпосередньо всередині комплексів. Звіт виокремлює USDT у мережі TRON і рекламованих у Telegram «U-мерчантів», які обмінюють стейблкоїни та фіат в обхід процедур KYC; у разі посилення контролю за ВА злочинці переходять до готівкових каналів і OTC-брокерів, що фактично діють як неліцензовані MVTS. Окремі блоки описують кейс камбоджійського конгломерату, який запустив власний доларовий стейблкоїн, рекламований як «стійкий до заморожування», та рішення FinCEN червня 2026 року поширити спеціальний захід на H-Pay Service PLC і будь-які майбутні структури-правонаступники, а також Telegram-маркетплейс Xinbi Guarantee, через який, за даними Мінфіну США, з 2022 року пройшло понад 24 млрд доларів США і щодо якого у вересні 2026 року було обмежено понад 52 млн доларів США.

Другий розділ звіту систематизує спільні виклики для компетентних органів і приватного сектору. Ключовим із них FATF називає невідповідність швидкості та видимості: кошти переміщуються між рахунками, гаманцями, класами активів і юрисдикціями за хвилини, випереджаючи звернення потерпілих, внутрішню ескалацію, подання повідомлень про підозрілі операції, їх аналіз і міжнародну співпрацю. Оскільки потерпілі здебільшого самі авторизують платежі, операції виглядають легітимними для фінансової установи, доки транзакційні дані не поєднано з контекстними сигналами ризику, якими володіють телеком-оператори, платформи чи правоохоронці. Розслідування ускладнюють багаторівневі потоки, непрозора бенефіціарна власність, електронні докази в різних юрисдикціях, корупція чи «офіційне прикриття», а розгляд торгівлі людьми і фінансових злочинів окремо, як зазначає FATF, залишає мережі вербування недоторканими та може призводити до кваліфікації жертв торгівлі людьми як правопорушників.

Третій розділ пропонує інструментарій реагування на двох рівнях – безпосередні дії проти мереж скам-комплексів та посилення загальної системи протидії шахрайству. FATF визнає, що найсильніша доказова база стосується «низхідних» заходів, тоді як «висхідне» руйнування спроможностей оцінено гірше. Антискам-центри, спільні інфраструктури даних про шахрайство, колаборативна аналітика й механізми швидкого реагування, зокрема у форматі державно-приватного та, де це дозволено, приватно-приватного партнерства, мають маршрутизувати достатньо надійні сигнали через чіткі правові підстави. Принципово важливо, що FATF покладає первинну операційну роль у втручанні в платіж на фінансову установу або VASP, яка безпосередньо контролює платіж, рахунок чи гаманець, тоді як ПФР і правоохоронні органи мають забезпечувати розвідувальну інформацію, координацію та, за потреби, формальні повноваження, а не втручатися в кожну транзакцію. Перші 24–72 години після виявлення визначено вирішальними для відстеження, повернення й відшкодування. Як моделі наведено механізм ПФР Угорщини, який з липня 2026 року може надавати суб'єктам моніторингу номери рахунків, IP-адреси, ідентифікатори пристроїв і дані про осіб на строк до 90 днів, та аналогічні повноваження ПФР Люксембургу з липня 2026 року; юрисдикціям із суттєвою загрозою запропоновано розглянути визнання шахрайства пріоритетом національної безпеки.

Кейси звіту демонструють масштаб узгоджених дій. Скоординовані заходи США та Великої Британії щодо Prince Transnational Organised Crime Group з жовтня 2025 року включали санкції, арешт активів на суму понад 15 млрд доларів США та обвинувачення її керівника у США; Корейський ПФР (KoFIU) у листопаді 2025 року запровадив обмеження щодо 15 фізичних і 132 юридичних осіб, пов'язаних із Prince Group і Huione Group, а Національний банк Камбоджі відкликав ліцензію Prince Bank. Для України показовим є кейс спільної слідчої групи Туреччини та Чехії: після передання чеської справи через Інтерпол було встановлено розміщений у Туреччині колцентр, який ошукував громадян Чехії, видаючи себе за посадовців і працівників банків; спільний аналіз у Празі дозволив ідентифікувати 100 підозрюваних, а операція в Стамбулі в липні 2026 року завершилася затриманням 56 осіб, 45 із яких узято під варту.

Додаток 1 консолідує висновки у шість Принципів FATF щодо протидії незаконним фінансовим потокам, пов'язаним зі скам-комплексами: діяти проти ширшої злочинної екосистеми та її критичних залежностей, а не лише проти фізичного майданчика; руйнувати фінансові потоки наскрізно – як на висхідній, так і на низхідній ділянках; поєднувати розвідувальні дані та спроможності між секторами й кордонами; діяти швидко через транскордонні канали, заздалегідь налагоджені для збереження «вікна втручання»; ставити в центр захисту як жертв онлайн-шахрайства, так і осіб, яких примусили працювати в комплексах, з гарантіями непокарання; адаптуватися до еволюції загрози й вимірювати результати, а не активність. Останній принцип FATF деталізує окремо: успіх має оцінюватися не кількістю сповіщень, розслідувань, арештів, закритих рахунків чи заморожених активів, а відверненими збитками, конфіскацією, поверненням і відшкодуванням коштів потерпілим та тривалим підривом складно замінних кримінальних спроможностей, з урахуванням ефектів переміщення та ребрендингу. FATF зазначає, що звіт визначатиме наступний етап її роботи щодо шахрайства, зокрема оцінку того, чи ефективно застосовуються наявні Стандарти до ризиків, пов'язаних зі скам-комплексами.

Висновки

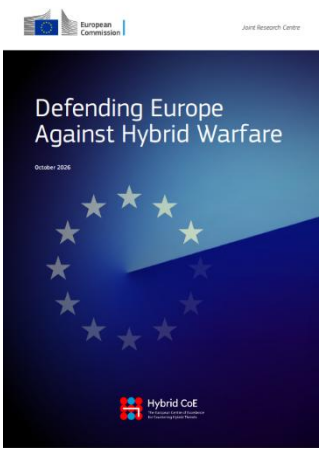
Модель наскрізного потоку варто інтегрувати в оцінку ризиків: FATF пропонує визначати схильність юрисдикції до ролі країни розташування, жертви, вербування, транзиту, відмивання, зберігання активів чи розміщення інфраструктури; для України з її досвідом колцентрового шахрайства це означає необхідність відобразити відповідні типології та залежності (рахунки-«мули», P2P/OTC, корпоративні структури, «прикриття») у секторальних оцінках і плані заходів за результатами НОР.

Вікно втручання в 24–72 години потребує заздалегідь створених механізмів: первинна роль у зупиненні, відкликанні й обмеженні платежів покладається на банки та VASP, тому критичними стають правові підстави для обміну індикаторами між ПФР і суб'єктами моніторингу (за прикладом Угорщини й Люксембургу), єдині контактні точки та процедури швидкого реагування з правоохоронними органами й органами повернення активів.

Канали віртуальних активів потребують цільового нагляду: USDT у мережі TRON, P2P-обмін, OTC-брокери як фактично неліцензовані MVTS і структури-правонаступники під санкційними чи спеціальними заходами (кейси H-Pay і Xinbi) визначають пріоритети для моніторингу VASP і банків, зокрема для виявлення транзитних рахунків, швидкої конвертації та виведення коштів за кордон.

Ефективність слід вимірювати результатами для потерпілих і злочинних мереж: перехід від показників активності (кількість повідомлень, арештів, заблокованих рахунків) до відвернених збитків, конфіскації й відшкодування, поряд зі скринінгом на ознаки торгівлі людьми та гарантіями непокарання для примушених працівників, задає нову рамку для оцінки ефективності як національної системи, так і майбутніх взаємних оцінок.

Стратегія протидії гібридним загрозам в Європі [3]



Звіт, підготовлений Об'єднаним дослідницьким центром Європейської комісії (JRC) спільно з Європейським центром передового досвіду з протидії гібридним загрозам (Hybrid CoE), фіксує фундаментальну зміну безпекового середовища Європи. Його центральна теза полягає в тому, що гібридні загрози більше не є фоновим явищем, а переросли в повноцінну гібридну війну – ескалацію, яка вимагає від демократій не лише пасивного опору, а й активної стратегії стримування.

Документ пропонує цілісну рамку – стратегію стримування (RD strategy), яка поєднує проактивне передбачення, активну оборону та реактивну відповідь.

Ключовим аналітичним ядром дослідження є декомпозиція сучасного операційного рівня гібридних загроз за трьома змінними: обсягом, часом та інтенсивністю.

Обсяг описується як результат масштабних операцій, часто скоординованих між державними та недержавними акторами, мета яких – перевантажити оборону цілі, виснажити її ресурси та підірвати зв'язки кооперації всередині демократичних альянсів. Автори наголошують, що принцип «vincit qui patitur» (хто витримує, той перемагає), який демонструє Україна, демократії часто недооцінюють, тоді як автократії свідомо будують кампанії на виснаження.

Каскадні ефекти (час) визначаються як негативні наслідки операції, що виходять за межі початкової мети і можуть бути зброєю для нових атак. Звіт підкреслює, що каскадні ефекти можуть використовуватися навіть після відбитих або поглинутих атак, а їхня небезпека зростає з часом: чим довше триває первинний вплив, тим легше розгортати вторинні удари.

Нарешті, операції високого впливу (HIO) – це атаки, покликані завдати значної шкоди, шокувати суспільства та паралізувати здатність ухвалювати рішення, використовуючи обман і несподіванку. Вони можуть бути як кінетичними, так і нематеріальними, і саме інфраструктура – енергетика, зв'язок, транспорт – є найпривабливішою ціллю, оскільки її колапс здатен паралізувати цілі держави на рівні ЄС і НАТО.

На стратегічному рівні документ констатує безпрецедентну інтенсифікацію гібридних кампаній росії проти ЄС і НАТО після 2022 року, які офіційні особи ЄС вже відкрито називають гібридною війною. Автори фіксують дві паралельні тенденції: зростання інтенсивності в усіх площинах (політичній, дипломатичній, кібер-, інфраструктурній, розвідувальній, військовій) та появу нових інструментів – від замахів на вбивства і підпалів до глушіння супутникової навігації, дронів над військовими базами та порушення повітряного простору. У цьому контексті документ наголошує:

[3] https://op.europa.eu/en/publication-detail/-/publication/0b1feb2b-cdbd-11f1-8b4c-01aa75ed71a1/language-en

покладатися лише на стійкість недостатньо, оскільки її здатність поглинати загрози має межі, а відсутність стримування агресор сприймає як слабкість і запрошення до подальшої ескалації.

Концептуальне ядро доповіді – це розрізнення первинних і вторинних концепцій стримування. Первинні – класичні: стримування шляхом відмови (deterrence by denial), яке унеможливлює або робить малоймовірним успіх атаки, та стримування шляхом покарання (deterrence by punishment), яке накладає витрати, що перевищують вигоди агресора.

Вторинні концепції значно розширюють інструментарій: абсолютне стримування (запобігання атаці через нарощування спроможностей), обмежувальне (constraining intensity), кумулятивне (обмеження порогу шкоди), стримування через розкриття (deterrence by disclosure – публічне викриття підготовки атак, як це робили США перед вторгненням росії в Україну), стримування через стратегічну комунікацію, інтегроване стримування (поєднання технологій, концепцій і спроможностей), інтерналізоване (тихе внутрішнє приготування) та розширене (колективна безпека для захисту союзників).

Стратегія RD, запропонована авторами, працює як цикл із трьох кроків:

Перший – проактивне передбачення (proactive anticipation). Автори формулюють десять операційних вимог до проактивного передбачення – стратегічна глибина, інтеграція руйнівних подій, управління складністю, переосмислення усталених знань, впровадження передбачення, швидкість адаптації, політична рішучість, стратегічна рішучість, підхід «усього суспільства» та норми й взаємозалежність (entanglement).

Другий крок – активна оборона (active defence), яка розгортається під час атаки та одразу після неї й організована навколо трьох етапів (виявлення – ідентифікація – визначення) і двох додаткових елементів (відновлення та атрибуції). Автори наголошують, що виявлення не може обмежуватися розвідкою: цивільний простір – журналісти, OSINT-аналітики, неурядові організації, оператори критичної інфраструктури – є критично важливими для раннього попередження.

Третій крок – реактивна відповідь (reactive response), яка настає після атаки, є вимірюваною та пропорційною, але завжди болючішою за початкову агресію, щоб досягти стримувального ефекту. Автори наводять широкий перелік контрзаходів – від санкцій проти установ і компаній, залучених до гібридних операцій, і регуляторних дій у межах міжнародних організацій до розгортання військових сил і кібероперацій заради колективного захисту.

Особливої ваги документу надає передмова єврокомісара з питань оборони і космосу Андрюса Кубілюса, який прямо пов’язує гібридну війну з підтримкою України: росія прагне зірвати виробництво й постачання зброї, атакуючи європейські заводи, енергомережі та транспортні маршрути. Його теза фактично є політичним маніфестом доповіді: недостатньо витримувати удари, потрібно робити їх складнішими для виконання, викривати відповідальних і накладати законні та пропорційні санкції, не чекаючи формального запуску колективної оборони.

У цьому сенсі документ є рамкою, яка пропонує європейським політикам і практикам конкретні інструменти – від освітніх і медіапрограм до військових навчань і санкційних механізмів – для переходу від пасивного виживання до активного формування поведінки агресора.

Головний висновок звіту можна сформулювати так: європейські демократії здатні перемогти в гібридній війні лише за умови, що стійкість і стримування розглядатимуться не як альтернативи, а як єдина система, що працює на випередження, під час і після атаки – і що політична рішучість буде не менш важливою за технологічну та інституційну спроможність.

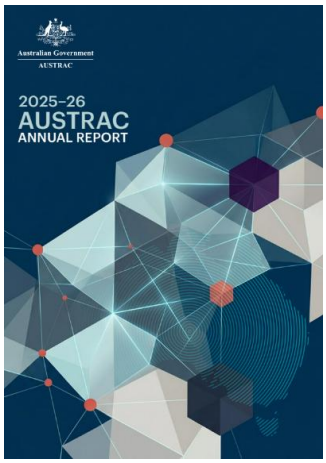
Висновки

Гібридні загрози переросли у гібридну війну, і сама лише стійкість більше не здатна забезпечити безпеку – необхідне поєднання стійкості зі стримуванням агресора.

Сучасні гібридні операції характеризуються трьома взаємопов'язаними тенденціями: перевантаження оборони, каскадними ефектами (використання наслідків атак) та операціями високого впливу, що паралізують цілі суспільства.

Ефективна протидія вимагає циклічної стратегії, яка поєднує проактивне передбачення, активну та реактивну відповідь із пропорційними, але відчутними втратами для агресора.

Річний звіт AUSTRAC за 2025–26 роки: боротьба з фінансовими злочинами та реформування режиму ПВК/ФТ [4]



Річний звіт Австралійського центру звітності та аналізу транзакцій (AUSTRAC) за 2025–26 роки відображає ключові результати діяльності агентства як національного підрозділу фінансової розвідки (ПФР) та регулятора у сфері протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ). Звітний період став визначальним для австралійського режиму ПВК/ФТ через масштабне впровадження законодавчих реформ та підготовку до суворої взаємної оцінки Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF). Агентство зосередило свої зусилля на зміцненні стійкості фінансової системи та захисті суспільства від складних схем фінансових зловживань.

У рамках імплементації реформ «Траншу 2» AUSTRAC здійснив безпрецедентну роботу з підготовки як наявних, так і новорегульованих секторів бізнесу (юристів, бухгалтерів, ріелторів, постачальників послуг для трастів і компаній тощо), які мали інтегруватися в режим до середини 2026 року. Агентство опублікувало понад 130 керівних документів, розробило світові стандарти практичної підтримки (програмні стартові набори) та провело тисячі роз'яснювальних заходів і вебінарів, щоб забезпечити високий рівень розуміння новими суб'єктами своїх обов'язків.

Як ПФР, AUSTRAC продемонстрував значне зростання обсягів оброблених даних: протягом 2025–26 років було зібрано понад 574 тисячі звітів про підозрілі операції (SMR, що на 27% більше порівняно з минулим роком) та понад 285 мільйонів звітів про міжнародні перекази коштів (IFTI). Завдяки новітнім аналітичним інструментам і робочому середовищу Analyst Workbench (AWB), до якого мають доступ понад 5000 користувачів із 44 партнерських відомств, ці дані перетворюються на практичну розвідувальну інформацію для правоохоронних органів.

Діяльність державно-приватного партнерства Fintel Alliance стала центральним елементом у боротьбі з транскордонною та організованою злочинністю. Завдяки зрілій роботі Колаборативного аналітичного центру (CAH), партнери успішно реалізували низку ініціатив: від викриття масштабних схем готівкового відмивання коштів та ідентифікації системних ризиків іпотечного шахрайства в рамках «Операції CLAW» до протидії мікро-відмиванню коштів, пов'язаному зі скамами та нелегальним онлайн-гемблінгом.

Особливу увагу агентство приділило протидії фінансовій інфраструктурі тіньової торгівлі тютюновими виробами та захисту вразливих категорій громадян, зокрема розслідуванню

[4] https://www.austrac.gov.au/sites/default/files/2026-10/AUSTRAC_AnnualReport_2025-26.pdf

злочинів, пов’язаних із матеріалами про сексуальну експлуатацію дітей та кібервимаганням (секс-вимагання щодо неповнолітніх). У співпраці з банками та правоохоронними органами ці заходи дозволили ініціювати тисячі розривів відносин із ризикованими клієнтами, заблокувати незаконні грошові потоки та підтримати низку арештів і екстрадицій серйозних правопорушників.

Фінансовий та адміністративний стан AUSTRAC характеризується збільшенням ресурсів для забезпечення реформ: загальний обсяг видатків програми становив близько 225,6 млн австралійських доларів, а середня штатна чисельність працівників зросла до 787 штатних одиниць. Закріпивши нові показники результативності (зокрема базові індекси залученості партнерів на рівні 78.8 та цільові пропорції регуляторного нагляду за секторами високого ризику), AUSTRAC підтвердив свою готовність і надалі гарантувати безпеку економіки та захист австралійського суспільства від фінансових злочинів.

Висновки

Імплементація реформ «Траншу 2»: AUSTRAC успішно підготував нові сектори бізнесу (юристів, бухгалтерів, ріелторів тощо) до інтеграції в національну систему ПВК/ФТ відповідно до стандартів FATF.

Зростання обсягів розвідувальних даних: Зафіксовано суттєве збільшення кількості звітів про підозрілі матеріали (SMR) та міжнародні перекази, які за допомогою аналітичних платформ перетворюються на дієві кейси для правоохоронців.

Ефективність кампанії Fintel Alliance: Державно-приватне партнерство та Колаборативний аналітичний центр (CAH) забезпечили успішне проведення спільних операцій проти іпотечного шахрайства, мікро-відмивання та тіньового ринку тютюну.

Цільовий регуляторний нагляд: Понад 62% регуляторних зусиль агентства було спрямовано на суб’єктів із найвищим ризиком (криптоактиви, банки, гральний бізнес) із використанням ризик-орієнтованого підходу та примусових заходів.

Жовтневий випуск SARs Reporter Booklet [5]



Бюлетень, опублікований у жовтні 2026 року Підрозділом фінансової розвідки Великої Британії (UKFIU) при Національному агентстві боротьби зі злочинністю (NCA), являє собою ґрунтовний аналітичний зріз того, як фінансова розвідка трансформується у реальні правоохоронні дії.

Цей документ не лише демонструє статистику, а й наводить детальні приклади того, як вчасне та якісне інформування про підозрілі транзакції дозволяє запобігати легалізації доходів, викривати організовані злочинні угруповання та захищати вразливих осіб. Головний меседж документа, підкріплений словами керівника UKFIU Вінса О'Брайена, полягає в тому, що SARs є критично важливим інтелектуальним ресурсом, який надає правоохоронцям необхідні дані – від номерів телефонів і адрес до деталей інвестиційної активності та банківських рахунків – для ініціювання нових розслідувань та підтримки вже існуючих.

Центральною темою бюлетеня є практична цінність запитів на захист від звинувачень у відмиванні коштів (Defence Against Money Laundering – DAML). Аналіз наведених кейсів демонструє складний механізм взаємодії між фінансовими установами та правоохоронними органами. У випадках, коли підзвітні суб'єкти виявляють аномальну активність на рахунках, вони ініціюють DAML-запити для отримання дозволу на закриття рахунку та переказ залишку коштів. UKFIU, діючи як національний координатор, часто відхиляє такі запити, якщо вбачає у них потенційну цінність для слідства. Це дозволяє передати інтелектуальні дані правоохоронцям, які, спираючись на цю інформацію, ініціюють розслідування, домагаються отримання дозволів на заморожування рахунків (Account Freezing Orders – AFO) та подальшої конфіскації активів. Показовим є приклад, де бізнес-рахунок, що використовувався для відмивання коштів через фіктивні SIC-коди, був заморожений на суму понад 65 000 фунтів стерлінгів, а злочинні кошти – конфісковані, що засвідчує ефективність системи у запобіганні подальшій легалізації.

Окрему увагу в документі приділено боротьбі з використанням підставних осіб (money mules) та захисту вразливих категорій населення. Бюлетень описує випадки, коли репортери виявляли ознаки того, що клієнти стають жертвами шахраїв, які використовують їхні рахунки для "відбілювання" злочинних доходів. Наприклад, у кейсі з романтичним шахрайством, де клієнт, раніше визнаний жертвою, почав отримувати кошти від третіх осіб та переказувати їх на онлайн-сайти знайомств, DAML-запит від банку дозволив не лише заморозити понад 3000 фунтів, а й провести перевірку добробуту клієнта та забезпечити його захист. Ще один яскравий приклад ілюструє, як завдяки пильності репортера вдалося врятувати вразливу особу від подальшого фінансового насильства: шахраї, використовуючи викрадені особисті документи, змушували

[5] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/833-sars-reporter-booklet-october-2026/file

клієнта переказувати кошти, але завдяки SAR та втручанню правоохоронців вдалося запобігти подальшій шкоді та конфіскувати понад 8000 фунтів.

Бюлетень також висвітлює успішність боротьби з відмиванням коштів через складні схеми, зокрема у сфері управління відходами та використання фіктивних компаній. У випадку з компанією, що займалася управлінням відходами, численні SARs від різних репортерів дозволили правоохоронцям виявити не лише ухилення від сплати податків, а й роботу без ліцензій та ознаки легалізації доходів, що призвело до конфіскаційного розслідування. Інший кейс демонструє, як шахраї створюють фіктивні бізнес-рахунки для отримання платежів від державних установ: завдяки DAML-запиту вдалося заблокувати понад 150 000 фунтів, а згодом конфіскувати 160 000 фунтів, які були незаконно привласнені та повернуті державному органу. Це підкреслює важливість SARs не лише для виявлення злочинів, а й для відшкодування збитків.

Крім фінансових злочинів, документ акцентує увагу на використанні SARs для розкриття злочинів, пов'язаних з наркотиками та сексуальним насильством над дітьми. У справах про наркотики аналіз транзакцій – округлені суми, посилання на вуличні назви наркотиків, відсутність легального доходу – дозволяє правоохоронцям заморожувати та конфісковувати кошти, а також висувати обвинувачення. Наприклад, у справі про підозрюваного у збуті наркотиків, чиї рахунки використовувалися для відмивання коштів, вдалося конфіскувати понад 10 000 фунтів готівки та понад 1000 фунтів з рахунку. Ще більш резонансним є кейс, де SAR, заснований на аналізі цифрового гаманця та відкритих джерел, призвів до виявлення матеріалів сексуального насильства над дітьми, арешту підозрюваного та вжиття заходів для захисту вразливих осіб, що демонструє міждисциплінарний потенціал фінансової розвідки.

Підсумовуючи, жовтневий бюлетень UKFIU 2026 року є переконливим свідченням того, що система SARs у Великій Британії функціонує як потужний та динамічний інструмент. Вона не обмежується пасивним збором даних, а активно сприяє ініціюванню розслідувань, заморожуванню та конфіскації злочинних активів, а також захисту найвразливіших верств населення. Документ наголошує на важливості співпраці між фінансовими установами та правоохоронними органами, заохочуючи репортерів до подальшого вдосконалення якості своїх звітів, адже саме від їхньої пильності та точності залежить ефективність боротьби з організованою злочинністю та фінансовими махінаціями.

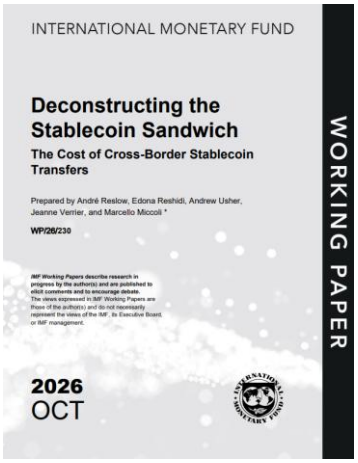
Висновки

Захист вразливих осіб як пріоритет: Значна частина кейсів демонструє, що SARs дозволяють не лише виявляти фінансові злочини, а й ідентифікувати жертв шахрайства, забезпечуючи їм захист та запобігаючи подальшому фінансовому насильству.

Міждисциплінарний потенціал фінансової розвідки: SARs виходять далеко за межі суто економічних злочинів – вони стають ключовим доказовим інструментом у справах про наркоторгівлю, ухилення від сплати податків, шахрайство з державними коштами та навіть у розслідуваннях, пов'язаних з матеріалами сексуального насильства над дітьми.

Цінність якісного звітування: Документ підкреслює, що ефективність системи залежить від пильності та точності самих фінансових установ – виявлення аномалій та вчасне подання SARs є критичним.

Чи справді стейблкоїни дешевші за традиційні грошові перекази? [6]



Світова система транскордонних платежів десятиліттями залишається синонімом повільності, дорожнечі та непрозорості. За даними Світового банку, середня глобальна вартість відправлення 200 доларів США у третьому кварталі 2025 року становила 6,36%, що більш ніж удвічі перевищує цільовий показник G20 у 3%. У багатьох платіжних коридорах, особливо тих, що обслуговують країни з низьким рівнем доходу, витрати сягають значно вищих позначок. На тлі цієї хронічної неефективності стейблкоїни, насамперед доларові USDT та USDC, почали розглядатися як ледь не панацея – швидкий, дешевий та доступний альтернативний канал.

Однак, як показує нове дослідження фахівців Міжнародного валютного фонду, загальноприйняте уявлення про дешевизну стейблкоїнів є суттєво спрощеним, а іноді й оманливим.

Дослідження пропонує перший систематичний вимір повної вартості транскордонного переказу на базі стейблкоїнів. Автори розробили методологію обліку витрат, яка простежує транзакцію через п'ять етапів: фіатний депозит (вхід у систему), купівля стейблкоїна, переказ по блокчейну, продаж стейблкоїна та фіатне зняття (вихід із системи). Ключовий висновок полягає в тому, що фокусування виключно на низькій вартості блокчейн-транзакції є фундаментальною помилкою, адже основні витрати формуються не в мережі, а на рівні доступу до фіатних грошей та біржової інфраструктури.

Емпірична база дослідження вражає своїм масштабом. Автори вручну зібрали дані про витрати з публічно доступних джерел, охопивши 270 платіжних коридорів між 18 країнами, 29 криптовалютними біржами, двома стейблкоїнами (USDT та USDC) та п'ятьма блокчейн-мережами. Це дозволило сформувати 4005 повних маршрутів переказу. Методологія передбачає, що користувач обирає найдешевші опції для входу та виходу з фіатної системи на кожному кінці маршруту. Такий підхід дає змогу оцінити базовий рівень витрат, який домінує на ринку.

Результати дослідження демонструють, що середня вартість переказу номіналом 200 доларів США становить близько 2,18% (медіанне значення – 1,99%). Це нижче цільового показника G20 у 3% і, на перший погляд, підтверджує тезу про економічну перевагу стейблкоїнів над традиційними каналами, середня вартість яких у вибірці становила 5,81%. Однак за середніми цифрами ховається надзвичайна гетерогенність: вартість коливається від негативних значень (-2,18%) до понад 8% у найдорожчих випадках. Більше того, в приблизно третині платіжних коридорів, де доступна детальна інформація про традиційні маршрути, найдешевший традиційний провайдер

[6] https://www.elibrary.imf.org/downloadpdf/view/journals/001/2026/230/001.2026.issue-230-en.pdf

пропонує нижчу вартість, ніж найдешевший маршрут через стейблкоїни. Це означає, що стейблкоїни не є універсальним рішенням, а їхня перевага значною мірою залежить від конкретних умов у країні відправлення та отримання.

Найважливішим внеском роботи є детальна декомпозиція витрат. Автори розкладають загальну вартість на чотири основні компоненти: комісії фіатних шлюзів (депозити та зняття), торгові комісії бірж, витрати на криптопереказ (комісії) та ринкові цінові спреди й премії. Виявляється, що найбільшою складовою середньої вартості є торгові комісії (0,85%), за ними йдуть комісії фіатних шлюзів (0,67%) та витрати на криптопереказ (0,48%). Компонент премії та спреду в середньому становить лише 0,18%, але саме він відзначається найбільшою варіативністю (від -3,07% до 4,51%) і є головним драйвером різниці у витратах.

Цей висновок має принципове значення. Блокчейн-комісії, які зазвичай асоціюються з економією витрат, становлять менше чверті середньої загальної вартості. Основні ж витрати лежать у площині доступу до фіатних грошей (банківські перекази, картки, платіжні системи) та біржової інфраструктури (торгові комісії, спреди). Іншими словами, стейблкоїни не усувають традиційну фінансову інфраструктуру, а лише змінюють її роль: банки та платіжні провайдери залишаються критично важливими на входах і виходах із криптосистеми, і саме їхні комісії формують левову частку витрат кінцевого користувача.

Окрему увагу в дослідженні приділено феномену премії – відхиленню локальної ціни стейблкоїна від обмінного курсу. Цей компонент відіграє ключову роль у формуванні асиметрії. Якщо в країні відправлення стейблкоїн торгується з премією (наприклад, через обмеження на доступ до іноземної валюти або високий попит на доларові активи), це здорожує придбання стейблкоїна для відправника. Якщо ж премія існує в країні отримання, це, навпаки, здешевлює переказ, оскільки отримувач продає стейблкоїн за вищою локальною ціною. У коридорах, де премія на стороні отримувача достатньо велика, вимірювана вартість переказу може стати навіть негативною. Класичним прикладом є Південна Корея, де купівля стейблкоїнів для відправника є дорожчою, але отримання коштів у Кореї – вигіднішим.

Автори наголошують, що негативна вартість не означає, що користувачі отримують гроші за переказ, або що сама технологія генерує вартість. Це радше відображення цінового викривлення відносно курсу, спричиненого сегментацією ринку, сильним локальним попитом на доларові активи або обмеженнями арбітражу. Таким чином, премія є не стільки технологічним, скільки макроекономічним і регуляторним феноменом, що відображає глибину та відкритість локальних фінансових ринків.

Аналіз за групами країн підтверджує цю логіку. Середня вартість платіжних коридорів між розвиненими економіками становить 2,31%, тоді як у напрямку з ринків, що розвиваються, до розвинених – 3,05%, а у зворотному напрямку – лише 1,61%. Це переконливо доводить, що премія є головним джерелом варіативності, а не середнього рівня витрат.

Порівняння з традиційними каналами, за даними Remittance Prices Worldwide, показує, що стейблкоїни в середньому дешевші майже на 5% у 33 випадках, де доступні обидва набори даних.

Однак при порівнянні найдешевших опцій у кожному випадку традиційні провайдери залишаються дешевшими приблизно в третині випадків. Це підкреслює, що стейблкоїни пропонують перевагу в типових умовах, але не домінують одноманітно, особливо там, де вже діють ефективні традиційні оператори.

Важливим обмеженням дослідження є те, що воно зосереджується виключно на переказах між централізованими біржами (CEX-to-CEX), не охоплюючи альтернативні шляхи, такі як децентралізовані фінанси (DeFi), однорангові перекази або гібридні моделі. Крім того, аналіз враховує лише транзакційні витрати і не бере до уваги швидкість, нефінансові бар'єри, контрагентський ризик чи регуляторні та комплаєнс-витрати, які несуть посередники. Оцінки вартості відображають зріз комісій та ринкових умов на певний момент часу, і структура витрат може змінюватися в міру еволюції екосистеми стейблкоїнів, зокрема внаслідок інтеграції технології традиційними платіжними провайдерами.

Підсумовуючи, дослідження МВФ пропонує реалістичний та методологічно обґрунтований погляд на економіку транскордонних переказів у стейблкоїнах. Воно руйнує спрощений наратив про «дешевизну блокчейну», показуючи, що основні витрати формуються в традиційних фіатних шлюзах та на біржовій інфраструктурі, а цінові премії на локальних ринках є головним джерелом відмінностей між коридорами.

Для регуляторів це означає, що оцінка стейблкоїнів як платіжного засобу повинна базуватися на повному обліку витрат, включаючи внутрішні фіатні перекази, а не лише на вартості блокчейн-транзакції. Для користувачів – що стейблкоїни справді можуть бути дешевшими, але не завжди і не скрізь, і що вибір найдешевшого маршруту вимагає розуміння локальних ринкових умов.

Висновки

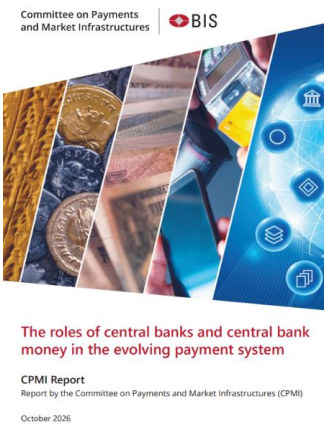
Середня вартість переказу в стейблкоїнах становить 2,18%, що нижче цільового показника G20 (3%) і дешевше за традиційні канали (5,81%), однак у третині досліджених випадків традиційні платіжні провайдери залишаються дешевшими.

Основні витрати формуються не в блокчейні, а на рівні доступу до фіатних грошей та біржової інфраструктури: торгові комісії (0,85%) і комісії фіатних шлюзів (0,67%) разом становлять більшість вартості, тоді як блокчейн-комісії – менше чверті (0,48%).

Головним драйвером різниці у витратах є премія – відхилення локальної ціни стейблкоїна від курсу, що відображає сегментацію ринків і обмеження доступу до іноземної валюти.

Вартість переказу суттєво залежить від розміру суми та обраного фіатного методу: середня вартість падає з 4,12% для 50 доларів до 1,54% для 5000 доларів через фіксовані комісії, а використання медіанного замість найдешевшого фіатного методу підвищує середню вартість переказу з 2,18% до 3,04%.

Майбутнє платежів: трансформація платіжних систем, токенізація та ключові завдання для центральних банків [7]



Аналітичний звіт, підготовлений Комітетом з питань платежів та ринкових інфраструктур (CPMI) при Банку міжнародних розрахунків (BIS), присвячений глибокій трансформації глобального платіжного ландшафту. У документі зазначається, що стрімкий розвиток технологій, зміна вподобань користувачів (запит на миттєві та цілодобові платежі) та поява нових небанківських учасників (емітентів електронних грошей і стейблкоїнів) докорінно змінюють структуру платіжних систем. Попри ці інновації, фундаментальні економічні характеристики платіжних систем залишаються незмінними: наявність мережевих ефектів, динаміка концентрації та фрагментації ринку, а головне – необхідність підтримання довіри до грошей.

У звіті детально розглядаються традиційні та новітні конфігурації платіжних систем, зокрема ті, що базуються на токенізації та програмованих платформах. Автори аналізують наслідки розмежування функцій випуску, обліку й переказу активів, а також об'єднання різних фінансових послуг на спільних платформах. Окрему увагу приділено ризикам ліквідності, проблемам взаємоопераційності та механізмам забезпечення номінальної конвертованості між різними формами грошей. Підкреслюється, що гроші центрального банку є найнадійнішим і найліквіднішим засобом розрахунку на верхівці багаторівневої платіжної структури, що слугує якорем довіри та забезпечує стабільність всієї фінансової системи.

Окрім аналізу загальних ринкових тенденцій, документ приділяє значну увагу питанню доступу нових учасників ринку до розрахункових рахунків і послуг центральних банків. Уряди та регулятори постають перед складними дилемами: з одного боку, розширення доступу для небанківських провайдерів платіжних послуг може стимулювати конкуренцію та інновації, з іншого – це створює потенційні канали передачі ризиків, підвищує загрозу регуляторного арбітражу та може посилити моральний ризик через очікування прямої підтримки з боку держави у часи криз. У зв'язку з цим центральні банки по всьому світу ретельно зважують переваги та недоліки запровадження диференційованих типів рахунків, спеціальних захисних рахунків або єдиних платформ для роботи з цифровими активами.

У фінальній частині документа систематизовано ключові інструменти та політичні міркування для центральних банків, які виступають в ролі емітентів, операторів, наглядових органів та каталізаторів ринку. Центральні банки переглядають політику доступу до своїх рахунків і послуг, модернізують наявну інфраструктуру (включаючи подовження операційного часу систем валових

[7] https://www.bis.org/publications/roles-central-banks-and-central-bank-money-evolving-payment-system_1.pdf

розрахунків у режимі реального часу (RTGS) та розвиток систем швидких платежів), адаптують нагляд під нові цифрові форми активів та координують зусилля з міжнародними партнерами й приватним сектором для забезпечення безпеки, ефективності та стійкості майбутніх платіжних систем.

Висновки

Незмінність ролі грошей центрального банку: Попри технологічну еволюцію, гроші центрального банку залишаються надійним ядром, яке забезпечує конвертованість за номіналом, остаточність розрахунків та стабільність фінансової системи.

Складність токенізації та розмежування функцій: Технологія токенізації відокремлює емісію від обліку й переказу, відкриваючи шлях новим небанківським провайдерам, але водночас створюючи виклики для управління ризиками та підзвітності.

Ризики ліквідності та фрагментації: Поширення нових платформ і закритих контурів може призвести до фрагментації ліквідності, що вимагає від центральних банків адаптації інфраструктури та забезпечення взаємоопераційності.

Комплексна політика регуляторів: Для збереження безпеки платіжних систем центральні банки мають комплексно поєднувати ролі емітента, оператора, наглядовця й каталізатора, адаптуючи правила доступу та посилюючи міжнародну співпрацю.

Баланс між анонімністю та регулюванням: дослідження криптографічних інструментів захисту приватності в цифрових валютах центральних банків [8]



Аналітичний звіт, підготовлений Інноваційним центром Банку міжнародних розрахунків (BIS) спільно з Валютним управлінням Гонконгу (HKMA) в межах другої фази проєкту Aurum, досліджує можливості технічного забезпечення приватності для цифрових грошей центральних банків (CBDC). Головне питання проєкту полягає в тому, чи можуть цифрові готівкові гроші забезпечити повсякденну конфіденційність, подібну до фізичної готівки, і водночас повноцінно підтримувати державні політичні цілі – протидію відмиванню коштів, фінансуванню тероризму, запобігання шахрайству та підтримання фінансової стабільності. Автори підкреслюють, що розробка цифрової готівки не повинна бути вибором за принципом «або-або» між повною анонімністю та тотальною прозорістю транзакцій.

Для вирішення цього завдання в межах проєкту було створено експериментальний прототип, який реалізує принцип «конфіденційності за дизайном», інтегруючи технології підвищення конфіденційності (PETs) безпосередньо в базову архітектуру системи. Двошарова архітектура розділяє оптовий рівень на базі розподіленого реєстру (DLT) та роздрібний рівень банківських електронних гаманців. Завдяки такій структурі центральний банк здійснює емісію та розрахунки, не маючи прямого доступу до персональних даних користувачів та деталей роздрібних транзакцій, що виключає ризик масового стеження чи централізованих витоків інформації.

Водночас технічне уточнення: BBS+ – це схема криптографічних підписів, яка підтримує вибіркове розкриття атрибутів і доведення їхньої автентичності. Сама собою вона не гарантує автоматичної зміни ідентифікатора під час кожної транзакції – це залежить від архітектури системи та способу реалізації псевдонімізації. Користувачі проходять стандартну процедуру ідентифікації (KYC) лише у свого ліцензованого комерційного банку, після чого отримують зашифровані криптографічні облікові дані. Це дозволяє створювати унікальні псевдоніми, повністю відв'язані від реальної особистості для зовнішніх спостерігачів і контрагентів, але водночас забезпечує можливість законної ідентифікації правоохоронними органами за допомогою банку у випадках, передбачених законодавством.

Для забезпечення незв'язності транзакцій та захисту від відстеження історії платежів у протоколі активно застосовуються докази з нульовим розголошенням. Завдяки їм валідатори та сторонні

[8] https://www.bis.org/publications/project-aurum-phase-2-exploring-privacy-enhancing-technologies-digital-cash.pdf

спостерігачі можуть перевірити легітимність платежу, коректність сум і відсутність подвійного витрачання коштів, не бачачи при цьому ані імен платника й отримувача, ані точної суми переказу. Унікальні теги запобігання подвійному витрачанню та двокрокова генерація доказів дозволяють перенести важкі криптографічні обчислення на інфраструктуру банків, роблячи систему зручною для використання на звичайних мобільних пристроях.

Звіт також детально аналізує політичні компроміси, які виникають при посиленні приватності. Зокрема, максимальний захист конфіденційності може ускладнювати резервне копіювання і відновлення втрачених гаманців (подібно до втрати фізичної готівки), обмежувати складну програмованість фінансових продуктів та збільшувати час обробки транзакцій через генерацію криптографічних доказів. Водночас розробники передбачили гнучкі інструменти налаштування політик, такі як вибіркова деанонімізація, контрольовані анонімні гаманці для туристів із лімітами, а також механізми «фракційного блокування» підозрілих коштів замість повного заморожування рахунку.

Наприкінці дослідження наголошується, що застосовані технології підвищення приватності мають синергетичний ефект і можуть використовуватися для інших завдань фінансового сектору. Зокрема, вони сумісні з методами федеративного навчання та багатосторонніми обчисленнями, що дозволяє комерційним банкам спільно виявляти схеми відмивання коштів та шахрайства на глобальному рівні без розкриття чутливих даних клієнтів. Проєкт Aurum Phase 2 доводить технічну спроможність поєднання приватності та комплаєнсу, надаючи центральним банкам практичну базу для проєктування національних систем цифрових грошей з урахуванням локальних законодавчих вимог.

Висновки

Архітектурні гарантії конфіденційності: Проєкт підтверджує, що замість сподівань на інституційну стриманість приватність цифрової готівки можна прозоро та міцно закласти безпосередньо у саму криптографічну основу системи за допомогою інструментів PETs.

Поєднання анонімності та безпеки: Використання спеціальних підписів і доказів із нульовим розголошенням захищає користувачів від стеження, водночас дозволяючи комерційним банкам законно перевіряти транзакції для запобігання злочинам.

Ціна приватності: Посилення конфіденційності ускладнює масштабування системи, уповільнює розрахунки через генерацію доказів, обмежує програмованість смарт-контрактів та ускладнює відновлення втрачених ключів.

Архітектурне розмежування даних: Поділ оптового та роздрібного рівнів унеможливлює доступ центробанку до персональних даних і платежів громадян, суттєво зменшуючи ризики кібератак та витоків.

Злам Binance: анатомія найбільшого цифрового пограбування в історії [9]



Події 29 жовтня 2026 року назавжди змінили уявлення про безпеку централізованих криптовалютних бірж. У той час як світова фінансова спільнота ще оговтувалася від наслідків злому Bybit у лютому 2025 року, який коштував 1,5 мільярда доларів, на горизонті з'явилася загроза, що перевершила всі попередні рекорди у чотири рази.

Ввечері 29 жовтня 2026 року з гаманців найбільшої у світі криптовалютної біржі Binance було виведено активів на суму приблизно 6,36 мільярда доларів. Ця блискавична операція стала наймасштабнішою крадіжкою криптовалют в історії, а її виконавцем, з високою вірогідністю, виступило елітне хакерське угруповання TraderTraitor, що діє під егідою розвідувальних служб Північної Кореї.

Атака розпочалася о 20:05 за всесвітнім координованим часом (UTC) і охопила десять різних блокчейн-мереж, включаючи Ethereum, Bitcoin, Tron, XRP Ledger, Solana, Arbitrum, Avalanche, Optimism, Base та Polygon. Протягом перших двадцяти хвилин зловмисники здійснили серію транзакцій, які повністю спустошили гарячі гаманці біржі на більшості цих мереж. Друга хвиля атак відбулася близько 23:05 UTC, коли постраждали гаманці на Avalanche та Polygon. Керівництво Binance було змушене визнати наявність інциденту безпеки та тимчасово призупинити виведення коштів на кількох мережах як запобіжний захід, запевняючи користувачів, що їхні активи в безпеці. Однак масштаб події та швидкість, з якою кошти залишали гаманці, свідчили про безпрецедентний рівень підготовки та компрометації інфраструктури.

Ключовим елементом цього безпрецедентного пограбування стала не просто фішингова атака чи викрадення приватних ключів, а використання новітніх механізмів смарт-контрактів Ethereum, зокрема оновлення EIP-7702, впровадженого в мережі під час хардфорку Pectra у травні 2025 року. Ця технічна особливість дозволяє звичайному гаманцю виконувати код смарт-контракту шляхом накладення спеціального підпису. Хакери підготували 50 підписів, кожен з яких вказував на контракт, що приймає команди виключно від оператора атаки. Оскільки кожен гаманець веде облік своїх транзакцій, а авторизація діє лише за конкретного значення цього лічильника, зловмисники, розуміючи, що гарячий гаманець Binance постійно обробляє безліч виведень

[9] https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history

коштів, підготували підписи для 50 послідовних транзакцій. Це гарантувало, що принаймні одна із них спрацює в момент виконання.

О 20:20 UTC оператор відправив єдину транзакцію, що містила ці 50 підписів, і один з них збігся з поточним станом гаманця. Через 3 хвилини і 24 секунди після цього, хакери дали команду гарячому гаманцю Binance переказати весь його баланс на контрольовану ними адресу. Ця єдина транзакція перемістила 167 464 ETH та 63 інших токени, включаючи 1,615 мільярда USDT. Делегування залишалося активним, і кожного разу, коли на гаманець надходили нові кошти, оператор автоматично змітав їх на свої адреси – це відбувалося о 20:41, 20:59, 21:04, 21:44, 22:39 та 23:56 UTC. Крім того, скомпрометований гаманець виконував роль виконавця для окремого смарт-контракту Binance, що дозволило зловмисникам витягнути додаткові 823 мільйони USDC.

Водночас із атакою на Ethereum, яка вимагала складної технічної підготовки, інші дев'ять мереж зазнали атак через звичайні підписані транзакції. Це свідчить про те, що компрометація не обмежувалася викраденням приватних ключів одного гаманця, а торкнулася самої інфраструктури Binance. Протягом тієї ж ночі п'ять гаманців на XRP Ledger, гаманці на Arbitrum, Avalanche, Optimism та Base, а також гаманці на Bitcoin, Tron та Solana відправляли кошти на адреси атакуючих через звичайні підписані перекази. Ще один гарячий гаманець Binance на Ethereum відправив 28 006 ETH, 55,7 мільйона USDT та 25,9 мільйона RLUSD тим самим шляхом, без використання делегування. Ця особливість вказує на те, що хакери, ймовірно, отримали доступ до системи підписання транзакцій біржі, що дозволило їм ініціювати перекази від імені гаманців на різних блокчейнах.

Підготовка до атаки розпочалася щонайменше за 36 годин до самої крадіжки. Операційний гаманець хакерів отримав три невеликі виведення з Tornado Cash – сервісу, що приховує походження криптовалюти – вранці 28 жовтня. Протягом 29 жовтня зловмисники розгорнули першу версію шкідливого коду, протестували її на двох гаманцях, а потім відпрацювали фінальну версію коду на третьому гаманці, повернувши тестові кошти собі. Лише через чотири години після цієї «репетиції» той самий код було відправлено на гарячий гаманець Binance.

Пост-мортем, який Binance оприлюднила 3 листопада 2026 року, свідчить, що виведенню коштів передувала багатомісячна кампанія соціальної інженерії. У червні інженер, відповідальний за гаманцеву інфраструктуру, шукаючи популярний інструмент програмування на основі штучного інтелекту, завантажив модифіковану інсталяцію зі шкідливим кодом; служба безпеки біржі замінила пристрій і змінила облікові дані, однак зловмисники вже встановили, хто з працівників обслуговує гаманцеву інфраструктуру. У вересні з іншим інженером через легітимну платформу пошуку роботи зв'язався фіктивний «директор проєкту»: після першої відеоспівбесіди з підставним HR-представником і другої – у месенджері з «генеральним директором» неіснуючої компанії – інженер завантажив «тестове завдання» зі шкідливим кодом, якого не виявили засоби захисту кінцевих пристроїв. 20 жовтня, використавши скомпрометований комп'ютер і внутрішній інструмент штучного інтелекту, нападники отримали контроль над комп'ютерами інших розробників гаманців тієї ж команди, а 29 жовтня, використовуючи викрадені облікові дані, запустили шкідливий скрипт і дісталися внутрішнього сервісу підписання транзакцій. Як

зазначає The Guardian, фіктивні співбесіди з використанням діпфейків є відомим елементом кіберарсеналу КНДР, проте зазвичай вони застосовуються у зворотному напрямку – коли підставні IT-фахівці влаштовуються на роботу, щоб спрямовувати кошти до Пхеньяна.

Обсяги викрадених активів вражають своєю різноманітністю. Найбільша частка припала на мережу Ethereum – близько 3,79 мільярда доларів, що включає 200 630 ETH та 185 інших токенів, серед яких 1,875 мільярда USDT, 823 мільйони USDC та 88,5 мільйона RLUSD. Біткоїн-гаманці втратили 18 270 BTC, що на момент крадіжки оцінювалося приблизно в 1,47 мільярда доларів. З мережі Tron було виведено 612,7 мільйона USDT та 46,4 мільйона TRX на суму близько 628 мільйонів доларів. XRP Ledger втратив 233,46 мільйона XRP (приблизно 296 мільйонів доларів), а Solana – 970 500 SOL (близько 96 мільйонів доларів). Менші, але все ж значні суми були виведені з Arbitrum, Optimism та Base (разом близько 39 мільйонів доларів, включаючи 74,6 мільйона ARB), Avalanche (28 мільйонів доларів) та Polygon (10 мільйонів доларів). Загальна сума в 6,36 мільярда доларів розраховувалася за ціною активів на момент їх викрадення.

Реакція фінансових структур на цю безпрецедентну подію була миттєвою. Емітенти стейблкоїнів, усвідомлюючи масштаб загрози, розпочали процес заморожування коштів, який тривав усю ніч. Станом на 00:30 UTC TRM Labs зафіксувала заморожування активів на суму близько 2,7 мільярда доларів. Зокрема, Tether заморозив близько 1,77 мільярда USDT: 971,1 мільйона USDT у головному гаманці-одержувачі о 21:01 UTC (лише через 37 хвилин після основного переведення коштів), а згодом ще 205 мільйонів USDT у двох інших гаманцях на Ethereum, 378,7 мільйона USDT на Tron та 8,4 мільйона USDT на Avalanche. Circle, у координації з правоохоронними органами, заморозила 823 мільйони USDC у головному гаманці о 21:04 UTC, а згодом ще 1,56 мільйона USDC, які хакери встигли обміняти з AVAX та перевести з Avalanche на Ethereum. Ripple заморозила 40,5 мільйона RLUSD о 22:01 UTC, а також заблокувала RLUSD у скомпрометованому гарячому гаманці Binance, щоб нові депозити не могли бути виведені. World Liberty Financial заморозила 27,8 мільйона USD1 у головному гаманці о 22:10 UTC. Крім того, Рада з безпеки Arbitrum, яка має повноваження вживати екстрених заходів у своїй мережі, о 00:08 UTC примусово заморозила 8 426 ETH та 74,6 мільйона ARB.

Попри безпрецедентні зусилля з боку емітентів та блокчейн-спільноти, значна частина викрадених коштів залишилася поза зоною досяжності. Хакери, усвідомлюючи, що стейблкоїни можуть бути заморожені, розпочали масштабну конвертацію активів у ті, що не підлягають блокуванню з боку емітентів. Протягом перших годин близько 325 мільйонів USDT було продано професійним маркет-мейкерам через UniswapX та інші обмінники на приблизно 122 300 ETH. Ця операція відбувалася за ціною близько 2 650 доларів за ETH, тоді як ринкова ціна коливалася в межах 2 300–2 350 доларів, що свідчить про дисконт понад 10% – хакери були готові втрачати кошти заради швидкості та анонімності. Другий гаманець надав 60 мільйонів USDT кредитному протоколу Aave і позичив під заставу близько 19 760 ETH, після чого Aave заморозив відповідні кошти. На Tron 300 мільйонів USDT перемістилися до гаманця, який розпочав надання коштів протоколу JustLend. Ще 200 мільйонів USDT пройшли через ланцюжок проміжних гаманців, де були обміняні на Uniswap, і 30 мільйонів USDT з цього ланцюжка було заморожено. 88,5 мільйона

RLUSD пройшли через два проміжні гаманці, перш ніж 48 мільйонів були продані через децентралізовані біржі в період з 21:42 до 22:01 UTC, доки Ripple не заморозив залишок.

У результаті цих операцій хакери зосередили в кількох гаманцях понад 420 000 ETH та 18 270 BTC, що станом на момент звіту оцінюється приблизно в 2,4 мільярда доларів. Ці активи перебувають поза зоною досяжності будь-якого емітента, оскільки не є стейблкоїнами і не підлягають примусовому заморожуванню. Біткоїни, викрадені з гарячого гаманця, одразу після надходження були розділені на круглі частини по 1 000 BTC та 100 BTC в межах одного блоку – ця техніка, відома як «peel chain», значно ускладнює відстеження руху коштів. Аналітики TRM Labs очікують, що наступним етапом відмивання стане використання крос-чейн мостів, обмінних сервісів та позабіржових брокерів (OTC). Фахівці компанії вже моніторять активи та гаманці зловмисників для відстеження подальших переміщень.

Оновлений аналіз TRM Labs від 3 листопада фіксує перехід до нових маршрутів відмивання тієї частини коштів, яку не було заморожено. У мережі TRON зловмисник створив власний токен, емісію якого може здійснювати лише його творець, і єдиний пул ліквідності для нього: «покупці» з гаманців, профінансованих із викрадених коштів, наповнювали пул, а безкоштовно викарбувані нові токени продавалися в цей пул з окремого гаманця, тож жодна пряма транзакція не пов'язувала дві сторони схеми. Другий метод передбачав передавання між гаманцями «квитанційного» токена кредитного протоколу, що підтверджує право вимоги на депозит, – відстеження лише за USDT не виявляє зв'язку між гаманцем, який вніс депозит, і гаманцем, що його погасив. Третій метод – послідовні крос-чейн обміни, за яких кошти з адреси відмивання спрямовуються безпосередньо на депозитну адресу другого мосту, що усуває проміжний гаманець, на якому зазвичай спрацьовує сповіщення або заморожування. Станом на 3 листопада основні залишки в ETH і BTC не переміщувалися, активний рух спостерігався в мережах TRON і Solana.

З огляду на цю ситуацію, TRM Labs надала низку рекомендацій для бірж та комплаєнс-команд. Зокрема, їм рекомендується перевіряти депозити та контрагентів за адресами, позначеними як пов'язані з атакуючими, оскільки кошти з гаманців, ймовірно, надійдуть на біржі, обмінні сервіси та OTC-платформи найближчими днями.

31 жовтня ФБР офіційно поклало відповідальність за атаку на КНДР і оприлюднило пов'язані з нею адреси гаманців в Ethereum, Bitcoin і Solana; Секретна служба США повідомила про роботу з відстеження, заморожування й повернення коштів. Північнокорейська сторона через агентство KCNA відкинула звинувачення. Binance заявила, що повністю покриє збитки за рахунок фонду SAFU, страхового фонду ф'ючерсів, біткоїн-резерву та корпоративних коштів, станом на 31 жовтня відновила 90 % втраченого обсягу, а 1 листопада поновила виведення коштів. Для сфери ПВК/ФТ визначальним є масштаб: за даними TRM Labs, КНДР з 2017 року викрала криптоактивів приблизно на 12,8 млрд доларів США, з них 7,4 млрд – у 2026 році, що становить 85 % вартості всіх криптозломів цього року, а 88 % викраденого припадає на компрометацію інфраструктури. Оскільки, за даними слідчих ООН, значна частина цих коштів спрямовується на ракетні програми, кожна біржа, OTC-платформа чи міст, через які проходять ці кошти, набуває санкційної експозиції.

У колонці для ACAMS від 4 листопада Арі Редборд (TRM Labs) формулює чотири уроки для підрозділів протидії фінансовим злочинам. Перший – посилити захист процесу найму та пов'язаних систем: верифікувати особу й місце перебування віддалених працівників, відстежувати округлені повторювані виплати на щойно відкриті рахунки, розглядати звернення рекрутерів, тестові завдання й інструменти розробників як частину периметра безпеки, а також розділяти інфраструктуру підписання за мережами, відстежувати неочікувані делегування EIP-7702 і відпрацьовувати процедуру відкликання до інциденту, оскільки Binance розробляла її вже під час атаки. Другий – обмінюватися інформацією в реальному часі: Tether заморозив 971,1 млн USDT через 37 хвилин після основного виведення, Circle – 823 млн USDC ще через три хвилини, тому участь у мережах оперативного сповіщення та повторний скринінг контрагентів за новими атрибуціями визначають обсяг заморожених коштів. Третій – використовувати механізм «заморожування – спалення – повторного випуску» стейблкоїнів, заздалегідь налагодивши контакти з емітентами, пакети доказів і розуміння правової процедури (судове рішення чи ордер на арешт), яка перетворює заморожування на повернення активів. Четвертий – здійснювати скринінг на кілька «стрибків» уперед: зловмисник продав близько 325 млн USDT маркет-мейкерам із дисконтом понад 10 % і позичав під заставу викрадених активів в Aave, а відстеження, що обмежується одним активом, бачить «чистий» гаманець там, де зв'язок проявляється лише через передавання квитанційного токена чи крос-чейн виплату, зіставлену за сумою і часом.

Цей інцидент є яскравим свідченням того, що кіберзлочинність, підтримувана державою, досягла нового рівня витонченості та масштабу. Північнокорейське угруповання TraderTraitor, яке раніше було викрито ФБР у зв'язку зі зломом Bybit на 1,5 мільярда доларів у лютому 2025 року, а також з атакою на KelpDAO у квітні 2026 року, підтвердило свою репутацію однієї з найнебезпечніших хакерських груп у світі.

Характерні риси цієї атаки – невеликі виведення з Tornado Cash для фінансування операційного гаманця, завчасна підготовка та тестування коду, а також отримання підписів заздалегідь з подальшим виконанням єдиним пакетом – збігаються з почерком попередніх пограбувань, пов'язаних із Північною Кореєю. Водночас методи відмивання, що спостерігаються цього разу, базуються на масштабних обмінах через маркет-мейкерів та кредитні протоколи, що відрізняється від схеми з використанням мостів, яка застосовувалася після злому Bybit.

Таким чином, подія 29 жовтня 2026 року стала не просто черговим зломом, а безпрецедентним за масштабом та складністю викликом для всієї криптовалютної індустрії. Вона продемонструвала вразливість навіть найбільших і, здавалося б, найзахищеніших гравців ринку перед обличчям добре підготовлених, добре фінансованих та технічно обізнаних атакуючих, які діють за підтримки держави.

Історія з Binance є тривожним сигналом про те, що методи кібератак еволюціонують швидше, ніж захисні механізми, і що навіть новітні технології, покликані підвищити функціональність та зручність, можуть бути використані як зброя проти тих, хто їх впроваджує.

Розслідування триває, і TRM Labs обіцяє ділитися подальшими висновками в міру розвитку подій, тоді як весь світ спостерігає за тим, чи вдасться правоохоронним органам та аналітикам повернути хоча б частину викрадених активів і притягнути винних до відповідальності.

Висновки

Масштаб: 29 жовтня 2026 року з гаманців Binance на десяти блокчейнах було виведено близько 6,36 млрд доларів, що робить цей інцидент найбільшим в історії криптовалют; TRM Labs з високою ймовірністю пов'язує атаку з північнокорейським угрупованням TraderTraitor.

Швидка реакція та заморожування: Емітенти стейблкоїнів (Tether, Circle, Ripple, World Liberty Financial) та Рада з безпеки Arbitrum оперативно заморозили активи на суму близько 2,7 млрд доларів, однак хакери встигли конвертувати частину коштів у ETH та BTC, зберігши контроль над активами приблизно на 2,4 млрд доларів.

Рекомендації для індустрії: Фахівці TRM Labs наголошують на необхідності моніторингу, запровадження політик відхилення неочікуваних транзакцій та посиленого скринінгу депозитів і контрагентів для запобігання подальшому відмиванню викрадених активів.

Периметр комплаєнсу охоплює найм, інструменти розробників і внутрішній ШІ: вектор атаки – модифікована інсталяція ШІ-інструмента, фіктивна співбесіда на легітимній платформі та внутрішній ШІ-інструмент – свідчить, що контроль ризиків інсайдерського доступу, верифікація віддалених працівників і сегрегація інфраструктури підписання мають бути частиною програм ПВК/ФТ і санкційного комплаєнсу VASP поряд із моніторингом транзакцій.

Санкційний фронт і тіньові мережі: як російська розвідка забезпечує війну в умовах ізоляції [10]



Аналітичний звіт, опублікований Міжнародним центром оборони і безпеки (ICDS), детально досліджує, зокрема еволюцію російських спецслужб в умовах повномасштабної війни та масштабних міжнародних санкцій. У документі підкреслюється, що попри масове вислання дипломатів і різке звуження операційних можливостей на Заході, розвідувальна екосистема росії переформатувала свою роботу, перетворивши обхід санкційних обмежень та забезпечення потреб військово-промислового комплексу на один із найвищих пріоритетів своєї діяльності.

Центральним елементом воєнної економіки рф стала розгалужена система незаконних закупівель, якою керують Служба зовнішньої розвідки та Головне управління Генштабу. Використовуючи глобальні мережі підставних компаній, фіктивних фірм та прихованих банківських рахунків по всьому світу, російські розвідники успішно постачають до росії мікросхеми, електроніку, компоненти боєприпасів та високоточні верстатні комплекси, необхідні для виготовлення ракет (зокрема гіперзвукових «Кинджалів»). Навіть після запровадження жорстких пакетів санкцій з боку США та ЄС (наприклад, проти компаній на кшталт «Сернія Інжиніринг» чи «Сертал») агентурні мережі знаходять нові способи фальсифікації країн кінцевого призначення товарів.

Окрім тіньових комерційних схем, російська розвідка активно використовує політичні та дипломатичні інструменти для підриву санкційного режиму зсередини Євросоюзу. Звіт наголошує на використанні рф лояльних політичних акторів і спеціальних каналів комунікації (наприклад, координації через дипломатичні відомства окремих держав на кшталт Угорщини) з метою політичного блокування, пом'якшення пакетів санкцій ЄС проти рф, а також виведення з-під ударів та захисту підсанкційних російських олігархів, банків і компаній.

Для диверсифікації ризиків та протидії тиску в країнах Глобального Півдня російські спецслужби перебрали під свій контроль активи та інфраструктуру ліквідованої ПВК «Вагнер» (зокрема структури на кшталт «African Politology»), поєднуючи проєкти з видобутку ресурсів, пропаганду та забезпечення безпеки авторитарних режимів в обхід фінансових обмежень. Водночас Головне управління Генштабу та Служба зовнішньої розвідки адаптували кадрову політику, ширше залучаючи до логістичних та закупівельних операцій нерезидентів, громадян третіх країн та кримінальні елементи, чиї дані не пов'язані напряму з державними реєстрами кадрових офіцерів.

[10] https://icds.ee/static/icds_report_constrained_yet_dangerous_hosaka_september_2026.pdf

Внутрішній контур екосистеми також підпорядкований воєнно-економічній мобілізації: 2-га служба Федеральної служби безпеки (Служба захисту конституційного ладу і боротьби з тероризмом) здійснює жорсткий тотальний контроль за інформаційним простором, науковою спільнотою та технологічним сектором, тоді як військова контррозвідка Федеральної служби безпеки (ФСБ) використовується як політичний інструмент рф для проведення масштабних чисток і перерозподілу фінансових потоків всередині Міністерства оборони після усунення колишнього керівництва.

Підсумовуючи, автор зазначає, що попри високу адаптивність у питаннях обходу санкцій та організації гібридних диверсій, російська розвідувальна екосистема страждає від глибоких системних вад: корупції, кумівства, а також дисфункційного циклу ухвалення рішень, коли розвіддані штучно підлаштовуються під політичні очікування вищого керівництва. Це створює серйозні виклики для західних країн, вимагаючи не лише точкових обмежень проти фіктивних фірм, а й жорсткого переслідування політичних технологів та посередників, які забезпечують роботу санкційних оклюзій.

Висновки

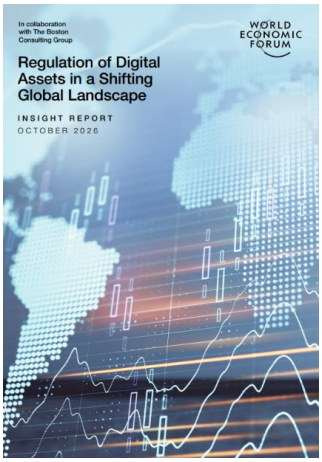
Пріоритет обходу санкцій та забезпечення ВПК: Попри масове висилання дипломатів на Заході, російські спецслужби переформатували свою роботу, створивши глобальні мережі підставних компаній для постачання мікросхем і високоточних верстатів (зокрема для ракет «Кинджал») в обхід західних санкцій.

Гібридний тиск та політичні «троянські коні»: рф активно залучає лояльних політичних акторів і використовує дипломатичні канали окремих країн ЄС (наприклад, Угорщини) для політичного блокування, пом'якшення пакетів санкцій проти рф та захисту підсанкційних олігархів.

Тотальний внутрішній контроль і чистки: 2 служба ФСБ здійснює жорсткий нагляд за інформаційним простором і наукою, тоді як військова контррозвідка використовується як політичний інструмент для проведення масштабних чисток і перерозподілу фінансових потоків у Міністерстві оборони.

Адаптація диверсійних мереж і тактик: Для мінімізації контррозвідувального тиску розвідка активно залучає до саботажу в Європі кримінальні елементи через соцмережі та громадян третіх країн, а також перерозподіляє активи ліквідованої ПВК «Вагнер» в Африці для підтримки авторитарних режимів.

Регулювання цифрових активів у мінливому глобальному ландшафті: еволюція інфраструктури та виклики для політики [11]



Аналітичний звіт, підготовлений Всесвітнім економічним форумом спільно з Boston Consulting Group, досліджує перехід цифрових активів із категорії ізольованого спекулятивного класу в саму основу глобальної фінансової інфраструктури. У документі підкреслюється, що справжнє значення цифрових активів полягає не в їхній ринковій капіталізації, а в їхній здатності трансформувати способи переміщення грошей, цінних паперів і забезпечення через технології розподіленого реєстру (DLT). За прогнозами, токенізовані реальні активи (RWA) можуть сягнути до 16% глобальних інвестиційних активів (близько $88 трильйонів) до 2035 року.

Інтеграція цифрових технологій стирає межі між традиційними фінансами (TradFi) та ринками криптоактивів, формуючи єдину ринкову архітектуру. Водночас цей процес суттєво впливає на суверенність держав, зачіпаючи три ключові виміри: монетарний контроль (ризики «цифрової доларизації» через стейблкоїни), нагляд за критичною фінансовою інфраструктурою та ефективність примусового виконання правил і санкцій. Регуляторні рішення тепер безпосередньо визначають, які форми цифрових грошей та токенізованих активів зможуть розвинутися до загальносистемного масштабного рівня.

Аналіз понад 25 типових видів діяльності в 35 юрисдикціях свідчить про те, що регуляторна зрілість є специфічною для кожного окремого напряму та сектора. Понад 70% досліджених юрисдикцій переходять від жорсткої прив’язки до юридичної форми активу до регулювання на основі виконуваної діяльності, що дозволяє охоплювати реальні ризики незалежно від того, як маркується токен. Різні моделі регулювання – від спеціалізованого законодавства до галузевих секторних рамок – успішно забезпечують інституційну участь за умови чіткості та юридичної визначеності.

Для подолання викликів фінансової системи автори звіту виділяють дев’ять вимірів ефективної нормативно-правової бази, поділених на три блоки: базові ринкові правила (периметр, юридична визначеність, захист клієнтських активів та інфраструктура), інтеграція у фінансову систему (цифрові гроші, монетарна стабільність, пруденційний і капітальний режим) та ринкові запобіжники (протидія фінансовим злочинам, ринкова цілісність і захист інвесторів). Цей підхід зміщує фокус уваги з простого питання «чи регулюється продукт?» на питання «чи здатна навколишня фінансова система підтримати його на інституційному рівні?».

[11] https://cisp.cachefly.net/assets/articles/attachments/97638_wef_regulation_of_digital_assets_in_a_shifting_global_landscape_2026.pdf

Звіт пропонує регуляторам практичний посібник, що складається з чотирьох кроків: ідентифікація матеріальних зон активності, оцінка наявних прогалин у нормативно-правовій базі, пріоритизація реагування на ризики та вибір адекватної регуляторної відповіді (адаптація чинних норм або використання пісочниць і тестових режимів). Наголошується, що масштабування ринків через кордони залежить не від ідентичності законів у різних країнах, а від взаємної довіри до регуляторних результатів та якості нагляду.

Законодавчі зміни неминуче трансформують усталені бізнес-моделі, засновані на регуляторному арбітражі та використанні переваг, зумовлених низькими транзакційними витратами, водночас зміщуючи конкурентні переваги на користь ліквідності, ефективного управління ризиками, довіри та розвинених мереж поширення послуг. Успішність реалізації реформ залежить від узгодженості нових регуляторних вимог із загальною системою фінансового законодавства, усунення перешкод у взаємодії із застарілими інформаційними системами та налагодження ефективних каналів міжнародної взаємодії між органами нагляду.

Висновки

Зміна ролі цифрових активів: Цифрові активи перетворюються з ізольованого спекулятивного класу на повноцінну фінансову інфраструктуру, що змінює способи випуску, обліку, торгівлі та розрахунків за цінними паперами і грошима.

Перехід до регулювання на основі діяльності: Більшість провідних юрисдикцій відмовляються від статичних визначень на користь функціонального підходу, охоплюючи правила емісії, зберігання, клірингу та розрахунків залежно від реальних економічних ризиків.

Дев'ять вимірів регуляторної архітектури: Побудова стабільних ринків вимагає комплексного вирішення завдань у дев’яти ключових сферах – від юрисдикційної визначеності та захисту активів до пруденційних норм, кіберстійкості та протидії відмиванню коштів.

Трансформація ринкового середовища: Чіткіші регуляторні вимоги поступово нівелюють відмінності між традиційними фінансовими установами та компаніями, що працюють на ринку криптоактивів, усуваючи неефективні бар’єри у здійсненні фінансових операцій та зміщуючи конкурентні переваги на користь ліквідності, довіри й належного рівня дотримання регуляторних вимог.

ІНШІ НОВИНИ



Операція «Карфаген»: НАБУ і САП оприлюднили матеріали щодо нової злочинної організації та повідомили про підозру п'ятьом особам [12]

4 листопада 2026 року Національне антикорупційне бюро України та Спеціалізована антикорупційна прокуратура повідомили про викриття в межах операції «Карфаген» злочинної організації, учасники якої, за даними слідства, налагодили систематичне надання неправомірної вигоди високопосадовцям правоохоронних органів за безперешкодну діяльність шахрайських колцентрів та інших незаконних видів діяльності. За версією слідства, організатором є раніше неодноразово засуджений чоловік, який залучив до злочинної діяльності чинних високопосадовців СБУ, Офісу Генерального прокурора, Національної поліції та представників кримінального середовища; до складу організації залучено щонайменше 12 осіб. Повідомлення супроводжується відео тривалістю 54 хвилини з фрагментами аудіо- та відеозаписів, листування й поясненнями детективів, структурованим за розділами: архітектура злочинної організації, колцентри, СБУ та ОГП, мережа U420, виготовлення підроблених євро, злочини проти життя і здоров'я, прикриття з боку правоохоронних органів і спроби позбавити НАБУ та САП незалежності. Оприлюднення є продовженням операції «Карфаген», у межах якої, як зазначено у звіті Європейської комісії щодо України 2026 року, у вересні 2026 року НАБУ викрило організовану

[12] https://nabu.gov.ua/news/operatciia-karfagen-vykryto-novu-zlochynnu-organizatciiu/

групу, що налагодила систему неправомірної вигоди за невтручання в діяльність шахрайських колцентрів; 22 жовтня 2026 року ВАКС узяв під варту з альтернативою застави 8 млн грн колишнього керівника одного з департаментів ОГП у цій справі.

У відео учасники організації позначені псевдонімами. Організатором («Кримінал») є особа, яка, за даними НАБУ, тричі засуджена, зокрема за грабіж, незаконне заволодіння транспортним засобом і хуліганство, і потрапила в поле зору НАБУ і САП у 2022 році у зв'язку з вимаганням від імені СБУ 1 млн доларів США за «неекстрадицію» особи. Співорганізатором названо громадянина РФ («Мексиканець»), якого слідство вважає засновником і керівником транснаціонального наркосиндикату «Хімпром»; за даними НАБУ, він прибув до України після того, як у 2016 році був оголошений у розшук, а з 2019 року перебуває в розшуку і в Україні. Виконавцями силових дій у відео названо осіб під псевдонімами «Боксер» і «Паша»; прикриття, за версією слідства, забезпечували «Прайс» – один із керівників Департаменту стратегічних розслідувань Національної поліції, «Консультант» – працівник поліції, який обіймав посаду заступника начальника відділу управління карного розшуку в Київській області, та «Акім» – високопосадовець СБУ у званні генерал-майора. За даними слідства, у 2022 – восени 2025 року організатор, використовуючи зв'язки з керівним складом СБУ, став співорганізатором злочинної організації; НАБУ також стверджує, що іноземний співорганізатор під час повномасштабної війни продовжував взаємодіяти з представниками ФСБ РФ, а учасники регулярно змінювали номери телефонів і акаунти в месенджерах.

Центральний епізод стосується мережі шахрайських колцентрів, які, за даними НАБУ, ошукували громадян України, ЄС та інших країн. Слідство встановило, що учасники організації координували діяльність щонайменше 52 колцентрів, у яких працювало щонайменше 2 700 осіб. За версією слідства, оскільки загрозу для колцентрів становили прокуратура, СБУ і Національна поліція, неправомірну вигоду передавали представникам усіх цих органів: стандартна сума становила 7 000 доларів США на місяць з одного колцентру, на початку місяця передавалися адреси колцентрів з їхніми ідентифікаторами, а до п'ятого числа відповідна сума сплачувалася у криптовалюті на заздалегідь наданий гаманець, після чого колцентр міг працювати місяць без ризику обшуків. Усі адреси, за даними слідства, обліковувалися на центральному рівні, що, за поясненням детективів, дозволяло контролювати систему й унеможливлювало самостійні дії правоохоронців на нижчих рівнях. Аналогічно, за версією НАБУ, вибудовувалася співпраця з представником ОГП, а щодо Національної поліції слідство досліджує період щонайменше з січня по липень 2026 року.

НАБУ окремо описує епізод, коли після помилки в адресі до одного з колцентрів прийшли з обшуком і вилучили техніку. За версією слідства, для її повернення використали судову процедуру: представник поліції надав контакт слідчого, який мав підготувати лист про відмову в поверненні майна, що стало підставою для скарги до суду; було рекомендовано подати кілька однакових скарг до Печерського районного суду м. Києва з метою впливу на автоматизований розподіл справ, а також обговорювалося питання оплати за ухвалення потрібного рішення. За даними НАБУ, вилучене майно було повернуто, а кошти перераховано на вказаний криптогаманець. Наприкінці липня 2026 року, після доручення Президента України активізувати

протидію колцентрам і наради в ОГП, учасники, за версією слідства, отримали від правоохоронців рекомендацію тимчасово припинити роботу колцентрів, перейти на конспіративні квартири та посилити конспірацію; у відео наведено повідомлення про припинення «робочої взаємодії» з 1 серпня 2026 року.

Другий напрям, за даними НАБУ, – мережа магазинів U420, яка була предметом публічного обговорення на початку 2026 року. За версією слідства, магазини належали іноземному співорганізатору, а організатор мав частку й щомісяця отримував відсоток від обороту; бізнес ґрунтувався на продажу розчину, що містить заборонену речовину, змішану з іншими речовинами за формулою, яка формально не підпадала під заборону українського законодавства. Через ризик визнання складу забороненим учасники, як стверджує НАБУ, шукали способи вплинути на рішення профільних міністерств, обговорювали пропозиції невстановлених осіб щодо «партнерства» з одноразовою виплатою 500 тис. доларів США та подальшим відрахуванням третини прибутку, а також розглядали варіант просування законопроєктів про легалізацію канабісу. За даними НАБУ, план підкупу не було реалізовано, зокрема на тлі журналістського розслідування Bihus.Info; у відео також наведено розмови про заздалегідь узгоджені «показові» обшуки та обговорення можливого тиску на журналістів і громадських активістів, зокрема фізичного. Чи були такі дії вчинені, у матеріалах не зазначено.

Третій напрям – виготовлення підробленої іноземної валюти. Детективи встановили, що протягом 2026 року члени організації облаштували в таємному місці цех зі спеціальним поліграфічним обладнанням і голографічними матрицями та виготовляли підроблені банкноти євро номіналом від 5 до 500 євро з імітацією захисних елементів. Основними учасниками цього епізоду НАБУ називає організатора, особу під псевдонімом «Паша» та чинного працівника поліції («Консультант»). Офіційне повідомлення НАБУ також згадує незаконне виробництво контрафактних цигарок.

Четвертий напрям стосується злочинів проти життя і здоров'я. За даними слідства, члени організації причетні до замовних катувань, викрадення людей і вимагання, використовуючи прикриття правоохоронців: отримували дані з баз даних, доступ до камер системи «Безпечне місто» (за даними НАБУ – з акаунта працівника Департаменту захисту національної державності СБУ) та матеріали обшуків. Детально описано епізод липня 2026 року, коли троє осіб у масках біля спортивного клубу в центрі Києва напали на чоловіка з металевою трубою; за версією слідства, підготовка тривала кілька тижнів, жертву відстежували через камери, а «Консультант» інформував про відсутність плану перехоплення та наступного дня – про кваліфікацію події як хуліганства (ч. 4 ст. 296 ККУ). Двох учасників, за даними НАБУ, раніше вже підозрювали у викраденні бізнесмена з вугільної галузі, утриманні його в підвалі й вимаганні 5 млн доларів США; група, як стверджується, виконувала замовлення й за кордоном, зокрема у Відні, а організатор отримував інформацію навіть про обговорення його діяльності на нараді європейських правоохоронних органів.

Окремий розділ відео присвячено прикриттю з боку СБУ. За версією слідства, високопосадовець СБУ знав про діяльність організатора та сприяв вирішенню питань як у СБУ, так і в ОГП: допомагав з оформленням непридатності до військової служби, автомобільними перепустками, наданням

водія й охоронця з посвідченням СБУ, отриманням даних з баз і довідок у кримінальних провадженнях, а також у судових справах і зняттях арештів. НАБУ наводить листування щодо знайомства організатора з новим керівником Департаменту стратегічних розслідувань Національної поліції, інформування про кадрові призначення в СБУ, про зустріч із міністром внутрішніх справ і керівником Національної поліції 28 травня 2026 року та про відвідування організатором будівлі центрального апарату СБУ 23 липня 2026 року. За даними слідства, з 16 жовтня 2025 року по 25 квітня 2026 року на вказаний організатором криптогаманець надійшло 3 750 000 USDT.

Завершальна частина відео стосується антикорупційних органів. За даними слідства, учасники злочинної організації були причетні до спроб позбавити НАБУ і САП незалежності влітку 2025 року; у відео наведено листування щодо можливої фальсифікації доказів у справі щодо працівників НАБУ та заходів, вжитих для того, щоб перешкодити особі, яка могла володіти відповідною інформацією, дати показання НАБУ. Детективи окремо зазначають, що більшість описаних злочинів не належать до підслідності НАБУ і мали виявлятися та розслідуватися іншими правоохоронними органами, однак діяльність тривала роками; питання, чому її не було припинено раніше, НАБУ називає відкритим.

5 листопада 2026 року НАБУ і САП повідомили про підозру п'ятьом учасникам злочинної організації: організатору (ч. 1 ст. 255, ч. 3 ст. 27 ч. 3 ст. 369, ч. 3 ст. 27 ч. 3 ст. 127, ч. 3 ст. 27 ч. 3 ст. 199, ч. 3 ст. 209 ККУ), першому заступнику начальника одного з департаментів СБУ (ч. 3 ст. 255 ККУ), керівнику одного з департаментів Національної поліції (ч. 3 ст. 255, ч. 4 ст. 368 ККУ), заступнику начальника відділу Управління карного розшуку ГУНП у Київській області (ч. 3 ст. 255, ч. 5 ст. 27 ч. 3 ст. 127, ч. 5 ст. 27 ч. 3 ст. 199 ККУ) та підлеглому організатора (ч. 2 ст. 255, ч. 3 ст. 127 ККУ). Кваліфікація охоплює створення злочинної організації та участь у ній, надання й одержання неправомірної вигоди, катування, підроблення грошей і легалізацію (відмивання) майна, одержаного злочинним шляхом. Того ж дня Вищий антикорупційний суд застосував до першого заступника начальника Департаменту стратегічних розслідувань Національної поліції запобіжний захід у вигляді тримання під вартою до 3 січня 2027 року включно з альтернативою внесення застави в розмірі 15 млн грн; прокурор просив тримання під вартою із заставою 20 млн грн, сторона захисту – домашній арешт або заставу в розмірі 998 тис. грн. Тимчасовий виконувач обов'язків Голови СБУ звільнив двох співробітників служби, які фігурують у справі, а Національна поліція відсторонила фігурантів від виконання службових обов'язків на час перевірки. НАБУ і САП вживають заходів для повідомлення про підозру іншим учасникам; досудове розслідування триває. Відповідно до ч. 1 ст. 62 Конституції України особа вважається невинуватою, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду.



Інституційні зміни антикорупційної архітектури США [13]

Напередодні проміжних виборів до Конгресу США, американське суспільство стоїть перед фундаментальним вибором, який виходить далеко за межі звичайної партійної боротьби. Згідно з OCCRP, країна стала свідком безпрецедентної трансформації самої архітектури антикорупційної політики. Адміністрація президента Дональда Трампа, після його повернення до Білого дому у січні 2025 року, розпочала системний демонтаж законів, інституцій та норм, які десятиліттями вважалися наріжним каменем американської демократії та глобальної боротьби з відмиванням брудних грошей. Цей процес викликає глибоке занепокоєння як серед експертів, так і серед міжнародних партнерів Вашингтона.

Аналізуючи внутрішню політику, варто відзначити, що перші кроки нової адміністрації були спрямовані на підрив незалежного нагляду. Однією з найрезонансніших дій стало масове звільнення 17 генеральних інспекторів – непартійних посадовців, чиїм обов'язком є розслідування фактів службових зловживань, марнотратства та шахрайства в різних урядових установах. Протягом перших 18 місяців перебування Трампа при владі було звільнено щонайменше 22 генеральних інспекторів, а станом на тиждень до проміжних виборів 27 таких посад залишалися вакантними. Адміністрація не надала жодних обґрунтувань для цих звільнень і не повідомила Конгрес, що згодом було визнано федеральним суддею незаконним. Це створило небезпечний вакуум підзвітності в урядових структурах.

Ще одним критичним ударом по фінансовій прозорості стало послаблення та фактичне призупинення дії Закону про корпоративну прозорість (Corporate Transparency Act), ухваленого у 2021 році. Цей знаковий закон вимагав від компаній звітувати про своїх кінцевих бенефіціарних власників, щоб запобігти використанню анонімних підставних компаній для приховування

[13] https://www.occrp.org/en/feature/defanging-laws-and-bringing-home-billions-how-trump-has-rewritten-the-corruption-rulebook-at-home-and-abroad

незаконно отриманих статків. Однак у серпні Міністерство фінансів США видало нове правило, яке скасувало вимогу щодо розкриття інформації для американських компаній та фізичних осіб, назвавши її "обтяжливою вимогою до звітності". Це рішення викликало хвилю обурення та призвело до судових позовів з боку понад 20 штатів, які аргументують, що закони, ухвалені Конгресом, не можуть бути скасовані шляхом підзаконних нормативних актів. Яскравим прикладом наслідків цього стало попередження американського наглядового органу про те, що відсутність таких даних ускладнює виявлення шахрайства в урядових контрактах, залишаючи "сотні мільярдів федеральних доларів" вразливими до ризиків, пов'язаних з бенефіціарною власністю. Крім того, минулого року Міністерство юстиції переслідувало 11 осіб, пов'язаних з російською транснаціональною злочинною організацією, яка скористалася слабкими вимогами до звітності.

Зовнішньополітичний вимір антикорупційної діяльності США також зазнав нищівних змін. Історично склалося так, що починаючи з 1960-х років, США були першопрохідцями у просуванні прозорості, належного врядування та програм боротьби з корупцією по всьому світу. Однак поточна адміністрація активно відступила від цих зусиль. Зокрема, було швидко ліквідовано Агентство США з міжнародного розвитку (USAID) – один з головних інструментів фінансування антикорупційних ініціатив за кордоном, а також заморожено виділення іноземного фінансування.

Крім того, було ліквідовано Офіс координатора Державного департаменту з питань глобальної боротьби з корупцією, створений у 2021 році для інтеграції антикорупційних зусиль у зовнішньополітичні цілі Вашингтона. Також припинила існування Цільова група KleptoCapture, створена Міністерством юстиції у 2022 році для переслідування тих, хто ухиляється від санкцій, особливо російських олігархів; Мін'юст пояснив це "переорієнтацією політики на боротьбу з картелями". Адміністрація також відмовилася від менш масштабних, але символічних зусиль, як-от виключення інформації про корупцію з щорічних доповідей Державного департаменту про права людини.

Особливу тривогу викликає суперечливе використання Закону Магнітського, ухваленого у 2012 році для запровадження санкцій проти іноземців, причетних до корупції або порушень прав людини. Президент шокував суспільство, коли використав цей закон для накладення санкцій на суддю Верховного суду Бразилії, який вів справу колишнього президента Жаїра Болсонару – союзника Трампа, згодом засудженого за планування державного перевороту після поразки на виборах 2022 року.

Ситуація, описана в документі, свідчить про те, що Сполучені Штати переживають глибоку кризу інституційної довіри.

Ваша думка важлива!

Які чинники найбільше пояснюють розрив між майже двома мільйонами повідомлень до ДСФМ і 2,5 % кримінальних проваджень, розпочатих за її матеріалами, на який указує Єврокомісія?

Які правові та технічні механізми потрібні банкам і VASP в Україні, щоб призупиняти платежі жертв шахрайських колцентрів у перші 24–72 години після виявлення?

Як Україні поєднати фінансовий моніторинг із соціальним захистом вразливих осіб, не порушуючи їхніх прав та не створюючи додаткових бар'єрів у доступі до фінансових послуг?

Як впливає поточна регуляторна база України на формування локальної премії на стейблкоїни та вартість крипто-переказів для українських громадян?

Які інструменти фінансового моніторингу дозволяють виявляти використання стейблкоїнів, зокрема USDT, як засобу систематичної передачі неправомірної вигоди посадовим особам?

Контактуйте щодо цього документу з Міністерством фінансів України:

Email: aml_bulletin@minfin.gov.ua
Поштова адреса: Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
Ідентифікація контакту: стосовно Методологічного Бюлетеня № МінФін-AML-2026-45

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