Методологічний бюлетень

Серійний номер: МінФін-AML-2026-34

Серпень 2026

“Майбутнє належить тим, хто вірить у красу своїх Мрій!”

Елеонора Рузвельт

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Національна оцінка ризиків Швейцарії щодо юридичних осіб і правових утворень [1]

Документ датовано 17 лютого 2026 року, Федеральна рада взяла його до відома 12 серпня 2026 року. Це третій за рахунком секторальний аналіз такого типу: він оновлює звіт CGMF 2017 року щодо юридичних осіб і доповнює дві загальнонаціональні оцінки ризиків 2015 і 2021 років. Заявлена мета – уточнити картину ризиків відмивання коштів, пов'язаних із юридичними особами та правовими утвореннями, виявити регуляторні прогалини й підтримати ризик-орієнтований підхід. Практична вага документа для України визначається двома обставинами: Швейцарія лишається однією з ключових юрисдикцій розміщення активів українського походження, а сама методологія оцінки одна з небагатьох, що поєднує реєстрові дані з даними фінансової розвідки й піддається відтворенню.

Методологічна еволюція порівняно з 2017 роком є найціннішою частиною документа. Аналіз 2017 року спирався виключно на кількісну обробку повідомлень про підозрілу діяльність (SAR). Оновлена оцінка зберігає цю основу, але додає три самостійні джерела: якісні матеріали поліцейських і прокурорських органів, дані нагляду за фінансовим ринком (FINMA) та результати опитування суб'єктів приватного сектору. Одночасно розширено предметне поле. До нього вперше включено фідуціарні домовленості, процедури створення компаній і передачі корпоративних прав, юридичних осіб, заснованих за кордоном, але таких, що мають

[1] https://cms.news.admin.ch/fileservice/sdweb-docs-prod-nsbcch-files/files/2026/08/18/a39fbcc9-3750-4471-a00d-8cf7204b8717.pdf

достатній зв'язок зі Швейцарією, окремі галузі економічної діяльності, а також асоціації та фонди, які раніше залишалися поза межами аналізу. Таке комбінування джерел прямо мотивоване методологічним обмеженням, яке CGMF формулює відверто: аналіз SAR фіксує лише ту протиправну активність, що пройшла через швейцарський банківський рахунок, і майже не бачить приховувальних операцій, які такого рахунку не торкаються.

Емпірична база охоплює період з 1 січня 2020 року по 30 червня 2025 року. За цей час до MROS надійшло близько 53 600 SAR. У 34,8 % із них фінансові посередники або торговці згадали юридичну особу чи правове утворення як релевантні для підозри, а в 31,0 % усіх повідомлень така особа була саме контрагентом за рахунком. Це дало робочий масив із 16 666 SAR, у якому фігурують 20 358 вітчизняних та іноземних юридичних осіб і правових утворень. Для порівняння, за той самий період було повідомлено близько 62 500 фізичних осіб як контрагентів або кінцевих бенефіціарів, тобто юридичні особи становлять 24,6 % усіх повідомлених суб'єктів – частка, майже незмінна від 2017 року. Кількість SAR, що надходять до MROS, зросла більш ніж уп'ятеро від 2017 року, тому нинішній масив суттєво ширший за попередній. Із вибірки свідомо виключено повідомлення щодо зловживання державними кредитами підтримки бізнесу періоду пандемії.

Щодо юридичних осіб швейцарського права масив містить 11 162 суб'єкти, причому 93,4 % повідомлень надійшли від фінансових посередників банківського сектору. За правовою формою переважають акціонерні товариства (Swiss AG) – 59,7 %, або 6 661 суб'єкт, і товариства з обмеженою відповідальністю (Swiss GmbH) – 37,4 %, або 4 180. Асоціації становлять 1,9 % (208), фонди – трохи менше 1 % (95), кооперативи – 0,2 % (18). Найцікавішим є не сам розподіл, а його зіставлення з фактичною поширеністю відповідних правових форм у торгових реєстрах. Таке зіставлення показує, що акціонерні товариства надпредставлені в повідомленнях на 15,7 відсоткового пункту, тоді як товариства з обмеженою відповідальністю недопредставлені на 12,2 пункту; кооперативи й фонди також дещо недопредставлені. CGMF пояснює це тим, що Swiss AG є суто капітальною і міжнародно орієнтованою конструкцією, вбудованою в транскордонні економічні й фінансові цикли, тоді як GmbH і кооперативи мають виражений персональний характер.

Розподіл предикатних злочинів щодо швейцарських юридичних осіб не виявляє специфічної загрози: найчастіше згадується шахрайство (51,0 % за всіма правовими формами), далі – ведення діяльності без дозволів і підроблення документів. Підкуп посадових осіб фігурує лише в 5,8 % випадків, організована злочинність – у 5,0 % (для Swiss AG – 5,6 %), тяжкі податкові злочини, які є предикатними лише з 1 січня 2016 року і не потрапили до даних 2017 року, – у 3,5 %. Разом із цими цифрами CGMF наводить методологічне застереження, яке має самостійну цінність для практики фінансового моніторингу: предикатні злочини різняться за способом їх встановлення. Шахрайство й підроблення документів зазвичай прямо випливають із доступних посереднику документів і записів, натомість вказівка на організовану злочинність з'являється у повідомленні здебільшого тоді, коли вже триває розслідування або ухвалено вирок. Отже, частки за предикатними злочинами не є однорідними величинами й не можуть інтерпретуватися як пряма міра поширеності відповідних явищ.

Картина щодо іноземних юридичних осіб принципово інша. Масив містить 9 062 такі суб'єкти; 72,0 % повідомлень надійшли від швейцарських банків і 25,0 % – від банків під іноземним контролем. За правовою формою домінують конструкції з обмеженою відповідальністю, аналогічні GmbH (німецька GmbH, американська LLC, британська Ltd тощо), – 62,7 %, або 5 680 суб'єктів; акціонерні товариства становлять 34,0 % (3 077), фонди – 2,3 % (208), філії іноземних компаній – 0,9 % (86). Вирішальна відмінність лежить не в правовій формі, а в структурі предикатних злочинів: підкуп посадових осіб згадується щодо іноземних осіб у 26,1 % випадків проти 5,8 % щодо швейцарських, а тяжкі податкові злочини – в 11,3 % проти 3,5 %. Іноземні юридичні особи систематично частіше пов'язані з тяжкими злочинами, більшими сумами, ширшим колом учасників, політично значущими особами та доміциліарними компаніями, а частина з них створена й управляється в юрисдикціях зі слабшими вимогами до контролю й прозорості.

Трасти проаналізовано окремо, хоч і за тією самою методикою. Фінансові посередники подали повідомлення щодо 134 трастів, що становить 1,5 % усіх іноземних правових конструкцій у масиві. Найпоказовіший результат тут – не структура предикатних злочинів, а її відсутність: у 40,3 % повідомлень щодо трастів предикатний злочин узагалі не вдалося класифікувати, тоді як у цілому по масиву цей показник становить 31,3 %. Сама неможливість встановити предикат є в цьому контексті самостійним індикатором непрозорості. Там, де предикат все ж визначено, підроблення документів (17,2 %) випереджає шахрайство (14,9 %), а підкуп, розтрата й тяжкі податкові злочини мають по 14,2 %. Приблизно 1 % трастів, про яких повідомлено, засновано в юрисдикціях сірого списку FATF. Ризик підвищують сума активів, кількість залучених осіб і використання трастів у багаторівневих схемах; особливо ризиковими є дискреційні трасти, у яких бенефіціари не розкриваються або постійно змінюються. Водночас CGMF наголошує, що вирішальним чинником є місце управління трастом: швейцарські трастові керуючі перебувають під наглядом наглядової організації та в периметрі дії закону про боротьбу з відмиванням коштів, що істотно знижує ризик.

Зведений індекс ризику розраховано за формулою, розробленою для національної оцінки 2015 року, на основі п'яти факторів за шкалою від 0 до 5. Іноземні юридичні особи й правові утворення отримали 2,5 бала (середній рівень), швейцарські – 1,6 (радше низький). Ще одне спостереження заслуговує на спеціальну увагу з методологічних міркувань: співвідношення іноземних і швейцарських осіб у повідомленнях перевернулося. У даних 2017 року понад дві третини повідомлень стосувалися іноземних структур, тепер швейцарських осіб у масиві більше (11 162 проти 9 062). CGMF прямо застерігає від прочитання цього як реального зростання внутрішнього ризику й називає дві причини: перехід на систему goAML у 2020 році, що змінив саму процедуру збору даних, і викривлення масиву 2017 року трьома групами гучних міжнародних справ – корупційними скандалами Petrobras/Lava Jato, 1MDB і PDVSA, масштабними витоками Panama Papers і Paradise Papers та справами «пралень» (азербайджанської, російсько-молдовської, Troika). Через це порівняння з 2017 роком у звіті свідомо подано як категоріальне, а не числове.

Змістове ядро висновків полягає в тому, що правова форма має другорядне значення, а вирішальною є операційність. Доміциліарні компанії, які існують без фактичної господарської діяльності, вважаються притаманно ризиковими; складні транскордонні структури з кількох доміциліарних компаній або структури без видимої економічної мети підвищують потенціал зловживання. Водночас звіт не абсолютизує цей поділ: операційно активні компанії теж несуть ризик і навіть ускладнюють виявлення, оскільки законна й незаконна діяльність переплітаються. За даними аналізу SAR підвищений ризик мають швейцарські компанії у будівництві, оптовій і роздрібній торгівлі, а також у сферах управлінського консультування, юридичних послуг, аудиту та фінансово-страхових послуг. Окремо відзначено, що більшість повідомлених швейцарських компаній є операційними, тоді як іноземні – переважно доміциліарними структурами для управління активами бенефіціара.

Щодо фондів і асоціацій характер ризику зміщується з відмивання коштів на фінансування тероризму. Швейцарські фонди недопредставлені в повідомленнях порівняно з їх фактичною поширеністю, проте частіше за інші форми пов'язуються з підозрами в корупції; з урахуванням наглядового режиму за фондами їх сукупний ризик оцінено як середній. Як вітчизняні, так і іноземні фонди визнано потенційно вразливішими до використання як каналу фінансування тероризму: кошти можуть потрапляти до терористичних організацій чи їх прибічників навіть без відома керівництва фонду, наприклад, через проєкти в регіонах підвищеної терористичної активності; існує також ризик інфільтрації фондів екстремістськими групами та створення фіктивних фондів. Сукупний ризик фінансування тероризму щодо фондів оцінено як середній. Ризик швейцарських асоціацій загалом низький, однак потенціал залучення до фінансування тероризму існує і пов'язаний саме зі збором пожертв і використанням коштів; асоціації, згадані в SAR, частіше мають зв'язок із високоризиковою країною.

Розділ про стійкість підсумовує заходи, вжиті від 2017 року: скасування акцій на пред'явника, уточнення обов'язку повідомляти про багаторівневі структури володіння, запровадження

обов'язку швейцарських торгових товариств вести реєстр акцій або часток і кримінальних та цивільних санкцій за його невиконання, поширення вимог прозорості на компанії, зареєстровані за кордоном, але фактично керовані зі Швейцарії, реорганізація нагляду й ліцензування трастових керуючих, нові правила щодо обов'язкового аудиту та заборона торгівлі «сплячими» компаніями. Асоціації з підвищеним ризиком фінансування тероризму тепер підлягають внесенню до торгового реєстру й зобов'язані вести реєстр членів. 26 вересня 2025 року парламент ухвалив Федеральний закон про прозорість юридичних осіб та ідентифікацію бенефіціарних власників (TLEA) і ревізію закону про боротьбу з відмиванням коштів, якими запроваджено реєстр прозорості та поширено дію закону на консультаційні послуги юристів, нотаріусів і фідуціаріїв у частині створення й структурування компаній та окремих високоризикових операцій з нерухомістю. Компанії відтепер зобов'язані зазначати осіб, що діють у фідуціарній якості в ланцюгу контролю, і вносити їх до реєстру прозорості.

Прогалини, які CGMF визнає невирішеними, окреслені так само чітко. Консультування операційно активних компаній не охоплюється законом про боротьбу з відмиванням коштів як таке. Доміциліація – надання адреси або приміщення для доміциліарної компанії, що зазвичай передбачає бізнес-адресу без реальної операційної присутності, пересилання кореспонденції, адміністративну підтримку й представництво, – не є фінансовим посередництвом і тому лишається поза дією закону, попри те що це визнано ризиковою діяльністю. Масштаб явища вимірюється реєстровими даними: приблизно 40 % доміциліарних компаній зареєстровані за адресою, за якою в торговому реєстрі значиться щонайменше ще одна така сама компанія, а майже 25 % мають іноземну юридичну адресу, спільну з кількома іншими компаніями, – що вказує вже на комерційний характер такої діяльності. Розмір відповідного сектору за даними Федерального статистичного управління станом на 2023 рік – 9 479 юридичних і нотаріальних фірм, 12 776 суб'єктів аудиту, податкового консультування, бухгалтерського обліку та фідуціарних послуг і 23 404 суб'єкти управлінського консультування; при цьому даних про те, як часто вони надають саме високоризикові послуги, немає, і CGMF змушений посилатися на німецьку оцінку 2022 року, за якою частка адвокатів, що працюють у сферах, охоплених антилегалізаційним регулюванням, становить 22 %.

Звіт завершується п'ятьма рекомендаціями: моніторити ефективність нових правил щодо консультаційних послуг і фідуціарної діяльності та за потреби розширити сферу їх застосування; забезпечити дієве впровадження реєстру прозорості з ризик-орієнтованим контролем його даних і залучити ці дані до майбутніх оцінок ризиків, зокрема щодо складних структур; посилити роз'яснювальну роботу щодо ризиків фінансування тероризму у секторі фондів і асоціацій; поширити результати самої оцінки серед органів влади, фінансових посередників і консультантів; регулярно переглядати послідовність застосування заходів проти «сплячих» компаній, зокрема у справах про банкрутство.

Висновки:

- **Правова форма майже не впливає на рівень ризику – вирішує операційність:** індекс ризику іноземних осіб 2,5 проти 1,6 у швейцарських за шкалою 0–5, а розрив між доміциліарною і реально працюючою компанією більший, ніж між будь-якими двома правовими формами.
- Підкуп фігурує у 26,1 % повідомлень щодо іноземних осіб проти 5,8 % щодо швейцарських, тяжкі податкові злочини – 11,3 % проти 3,5 %. Для трастів у 40,3 % випадків предикат узагалі не класифікується – сама неможливість класифікації є індикатором непрозорості.
- **Співвідношення іноземних і швейцарських осіб у повідомленнях перевернулося проти 2017 року**, але CGMF застерігає: причина – перехід на goAML і викривлення даних 2017 року трьома групами гучних справ, а не реальне зростання внутрішнього ризику.
- **Реєстр прозорості за законом TLEA від 26.09.2025 не закриває дві прогалини:** консультування операційно активних компаній лишається поза законом, а надання адреси для реєстрації компанії не є фінансовим посередництвом – при тому що 40 % доміциліарних компаній знаходяться за спільною адресою.

Національна стратегія Ірландії у сфері ПВК/ФТ/ФРЗ [2]

Уряд Ірландії оприлюднив Національну стратегію у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, підготовлену Керівним комітетом з питань боротьби з відмиванням коштів (Anti-Money Laundering Steering Committee, далі – AMLSC) під головуванням Міністерства фінансів. Документ визначає рамку державної політики на горизонт до 2030 року. Контекст, у якому він з'являється, задано масштабом фінансового сектору: Ірландія є третім експортером фінансових послуг у Європейському Союзі та восьмим у світі, а виміряні активи сектору перевищували 8,1 трлн євро станом на 2023 рік. Одночасно країна має високоінтегрований ринок праці, вільний рух капіталу та послуг у межах ЄС і розвинений сегмент юридичних і професійних послуг, TCSP, операторів ринку нерухомості – усі вони охоплені антилегалізаційним регулюванням.

Інституційна архітектура, описана в документі, побудована навколо AMLSC як органу національної координації та узгодження політики між відомствами. Постійними членами є Міністерство фінансів, Міністерство юстиції, внутрішніх справ і міграції, поліція (An Garda Síochána), підрозділ фінансової розвідки, Центральний банк Ірландії, Бюро з питань кримінальних активів (Criminal Assets Bureau), Сили оборони, Орган з питань корпоративного правозастосування, Офіс Директора публічних переслідувань та Орган регулювання грального бізнесу. До складу асоційованих членів входять податкова служба (Revenue Commissioners), Регулятор благодійних організацій, регулятори юридичних і ріелторських послуг, Консультативний форум приватного сектору, Товариство юристів та профільні бухгалтерські організації. Санкційний блок винесено за межі цієї конструкції: його веде Міжвідомчий комітет з міжнародних санкцій (CDISC) під егідою Міністерства закордонних справ і торгівлі. Стратегія передбачає створення нової підгрупи AMLSC з питань протидії фінансуванню тероризму та фінансуванню розповсюдження – саме тих напрямів, за якими в оцінюваннях FATF традиційно втрачаються бали за безпосередніми результатами.

Рамка політики спирається на три взаємопов'язані опори. Перша – політика та нагляд у широкому розумінні: оцінювання ризиків, розроблення національної та узгодженої з правом ЄС політики, стратегічний нагляд і координація між урядом і компетентними органами. Друга – запобігання та моніторинг: забезпечення, просування, нагляд і моніторинг дотримання вимог, а також збирання, аналіз і поширення фінансової та пов'язаної розвідувальної інформації. Третя – розслідування та правозастосування: виявлення, розслідування, кримінальне переслідування та застосування санкцій за відповідні правопорушення. Конструкція «трьох опор» сама по собі не є новацією, проте її цінність у документі полягає в тому, що кожен із подальших заходів прив'язується до конкретного відповідального органу в межах відповідної опори, що робить розподіл повноважень читабельним.

Змістовно стратегія прив'язана до Національної оцінки ризиків Ірландії 2026 року, яка застосовує чотирирівневу шкалу ризику (низький, помірний, значний, дуже значний). Загрозу відмивання коштів оцінено як помірну, фінансування тероризму – як низьку, фінансування розповсюдження – як низьку; ухилення від санкцій також оцінено як низький ризик із застереженням про потребу постійної пильності. Рейтинг джерел злочинних доходів очолюють злочини у сфері обігу наркотиків і шахрайство, за ними йдуть крадіжки та проникнення, незаконна торгівля й контрабанда, торгівля людьми та експлуатація, податкові злочини. Оцінка фіксує поєднання традиційних готівкових методів із цифровими інструментами – крипто-активами, мережами грошових мулів і складними схемами нашарування. Окремо від самої стратегії опубліковано План пріоритетних дій, що переводить виявлені в оцінці зони покращення у програму з 30 заходів.

[2] https://assets.gov.ie/static/documents/4dfbc163/National_AML_CFT_CPF_Strategy.pdf

Перша та друга стратегічні цілі стосуються координації та розуміння ризиків. Крім створення підгрупи з ФТ/ФРЗ, передбачено активніше використання AMLSC як майданчика для обговорення національного та європейського законодавства, укладення меморандумів про обмін інформацією між Регулятором благодійних організацій, поліцією та освітнім відомством, а також посилення домовленостей між наглядовими й правоохоронними органами щодо обміну інформацією про ризики відмивання коштів, фінансування тероризму та ухилення від санкцій. У частині оцінки ризиків заплановано вдосконалення інструментарію роботи ПФР із повідомленнями про підозрілі операції та аналітичної спроможності Офісу Директора публічних переслідувань, обговорення доцільності запровадження обов'язкової реєстрації суб'єктів у підрозділі фінансової розвідки, а також оновлення Центральним банком опитувальника оцінки ризиків як основного каналу збору секторальних даних і проведення цільового аналізу секторів, продуктів і транскордонних потоків.

Найнасиченішою є третя ціль, присвячена регуляторній рамці. Вона охоплює транспозицію Шостої антилегалізаційної директиви ЄС із внесенням змін до Закону про кримінальну юстицію 2010 року та підзаконних актів; роботу міжвідомчої групи з транспозиції, створеної у 2024 році; аналіз впливу єдиного зводу правил і Регламенту ЄС про запобігання відмиванню коштів на національну систему та визначення ролі наглядових органів і підрозділу фінансової розвідки у взаємодії з новостворюваним Органом ЄС з протидії відмиванню коштів (AMLA). Блок бенефіціарної власності передбачає посилення повноважень трьох реєстрів – реєстру бенефіціарних власників компаній і кооперативних товариств при Офісі реєстрації компаній, Центрального реєстру бенефіціарної власності трастів при податковій службі та реєстру бенефіціарної власності окремих фінансових утворень при Центральному банку, – а також запровадження обов'язкового розкриття кінцевих бенефіціарів для всіх командитних товариств. Окремо йдеться про приведення реєстру банківських рахунків, платіжних рахунків і сейфів (ISBAR) у відповідність до Шостої директиви з розширенням обсягу, наданням доступу AMLA та під'єднанням до загальноєвропейської системи взаємозв'язку реєстрів рахунків (BARIS), а також про створення єдиної точки доступу до інформації про нерухомість відповідно до статті 18 Директиви й Регламенту з граничним строком у липні 2029 року.

Третя ціль містить і низку вужчих, але операційно показових заходів. У частині віртуальних активів передбачено транспозицію Регламенту про ринки крипто-активів (MiCAR), яка вводить постачальників послуг з обігу крипто-активів до кола підзвітних суб’єктів, і Регламенту про перекази коштів (TFR), що поширює вимоги щодо супровідної інформації про ініціатора й отримувача на перекази крипто-активів – тобто імплементує Travel Rule. Щодо структур спеціального призначення заплановано законодавство, яке дозволить податковій службі публікувати перелік суб'єктів, що користуються режимом секції 110 Закону про консолідацію податків 1997 року, та запровадження вимоги щодо ідентифікатора юридичної особи для таких суб'єктів. У гральному секторі – підпорядкування казино-клубів із машинним гемблінгом жорсткішому режиму, вироблення галузевого стандарту щодо прийняття крипто-активів як джерела коштів і вимога «замкненого циклу» платежів, за якою виплати клієнту здійснюються на той самий рахунок, з якого надійшли кошти. Санкційний блок передбачає механізм невідкладної імплементації резолюцій Ради Безпеки ООН і запровадження уніфікованої форми подання пропозицій щодо включення до санкційних переліків ЄС і ООН.

Четверта ціль – розбудова спроможності та роз'яснювальна робота – містить кілька рішень, придатних до перенесення. Компетентні органи мають запровадити формалізований механізм щорічного перегляду ризик-орієнтованого наглядового підходу для звірки наглядових пріоритетів, ресурсів і інтенсивності нагляду з поточним профілем загроз. Профільні бухгалтерські організації створюють реєстр TCSP під власним наглядом із зовнішнім доступом, а також опрацьовують доцільність єдиного загальнонаціонального реєстру таких постачальників послуг. Центральний банк зобов'язується надавати секторам і окремим установам періодичний структурований зворотний зв'язок щодо ризиків, спираючись на оновлений опитувальник, а установи – враховувати його у власних оцінках ризиків. Партнерство з приватним сектором забезпечується через Консультативний форум, три групи

державно-приватного партнерства ПФР, європейське партнерство EFIPPP і спільну робочу групу підрозділу фінансової розвідки з бухгалтерськими організаціями. П'ята ціль присвячена міжнародній співпраці: участь у структурах ЄС, взаємодія з AMLA, Європолом і його Європейським центром з питань фінансової та економічної злочинності, Євроюстом, посилення ролі в Егмонтській групі, членом якої Ірландія є з 1998 року, підтримання відповідності санкційним режимам ООН і ЄС, повноцінна участь у процесах FATF із підготовкою до чергового взаємного оцінювання 2028 року та участь у Тематичному фонді МВФ з питань ПВК/ФТ.

Критичний аналіз документа дає підстави для двох застережень. Перше стосується вимірюваності: переважна більшість заходів сформульована як напрями діяльності без строків виконання та показників результативності, а механізм моніторингу описано лише через щорічну звітність AMLSC і згаданий вище щорічний перегляд наглядових підходів; сама стратегія визнає, що конкретизація винесена до окремого Плану пріоритетних дій із 30 заходів і до Стратегії протидії економічній злочинності й корупції Міністерства юстиції, побудованої навколо п'яти власних цілей. Друге застереження – аналітичне: документ не містить статистичних даних щодо кількості повідомлень про підозрілі операції, розслідувань, вироків чи арештованих активів і не посилається ані на попередню національну стратегію, ані на результати взаємного оцінювання Ірландії, що ускладнює оцінку прогресу. Для української практики цінність документа полягає передусім у самій конструкції: п'ятирічний горизонт прямо синхронізовано з циклом оцінювання FATF, кожен захід закріплено за конкретним органом, а стратегія свідомо розділена з планом заходів, що дозволяє оновлювати операційний рівень без перегляду рамки. Водночас ірландський досвід показує й ризик такої конструкції: без показників результативності на рівні самої стратегії відповідальність за результат розмивається між документами.

Висновки:

- **Стратегія побудована як макрорамка: заходи закріплено за відповідальними органами, але переважна більшість подана без строків і показників результативності**, а моніторинг описано лише через щорічну звітність AMLSC – це основна конструктивна слабкість документа.
- **П'ятирічний горизонт прямо синхронізовано з циклом FATF:** підготовку до взаємного оцінювання 2028 року винесено в окремий захід Цілі 5, а Ціль 1 створює підгрупу з ФТ і ФРЗ – саме тих напрямів, за якими традиційно втрачаються бали за безпосередніми результатами.
- **Трискладова архітектура реєстрів:** реєстр бенефіціарних власників, реєстр трастів при податковій службі та реєстр фінансових утворень при Центробанку, плюс ISBAR із під'єднанням до BARIS і єдина точка доступу до даних про нерухомість зі строком до липня 2029 року.
- **При активах сектору понад 8,1 трлн євро і статусі третього експортера фінпослуг у ЄС загрозу ВК оцінено лише як «помірну», а ФТ і ФРЗ – як «низьку»**; така асиметрія між масштабом сектору й рівнем оцінених загроз потребує окремого методологічного обґрунтування.

Банк міжнародних розрахунків про інтеграцію інформаційних систем нагляду [3]

Інститут фінансової стабільності Банку міжнародних розрахунків опублікував дослідження авторства Джона Чіу (Валютне управління Гонконгу) та Джермі Пренйо (БМР). Робота присвячена не наглядовим інструментам як таким, а інфраструктурі, що їх підтримує: автори виходять із тези, що ефективність наглядових навичок, процесів і технологій вирішальною мірою залежить від того, наскільки узгоджено працюють інформаційні системи органу. Поточні зусилля у сфері suptech, за їх оцінкою, здебільшого фрагментарні та прив'язані до

[3] https://www.bis.org/fsi/publ/insights77.pdf

окремих завдань, тоді як потрібен цілісний підхід, закріплений у стратегіях цифрової трансформації та врядування даними.

Методологія поєднує опитування та інтерв'ю. Опитування проведено з лютого по квітень 2026 року серед учасників Неформальної мережі suptech Інституту фінансової стабільності; відповіді надали 43 фінансові органи. Дещо більше половини респондентів (54 %) представляють країни з ринками, що формуються, та країни, що розвиваються, 46 % – розвинені економіки; ці частки розраховано без урахування шести респондентів, які не вказали назви установи. За мандатами найбільше органів мають повноваження з банківського нагляду (86 %), далі – з протидії відмиванню коштів і фінансуванню тероризму (51 %), нагляду за страховим ринком (44 %) і за ринками цінних паперів (33 %). Додатково проведено вісім інтерв'ю з органами, що перебувають на різних стадіях інтеграції. Методологічне застереження, яке варто тримати на увазі при прочитанні часток, полягає в тому, що вибірка формується з учасників профільної мережі suptech, тобто органів, уже зацікавлених у цій темі, – реальний загальносвітовий рівень зрілості радше нижчий за виміряний.

Концептуальна рамка документа має самостійну цінність. Наглядовий цикл автори описують через п'ять стадій: планування, оцінка ризиків, взаємодія з піднаглядними суб'єктами, застосування заходів і звітність. Цей цикл підтримують три системи. Система збору даних забезпечує збирання, валідацію, зберігання й управління даними – від адміністративної інформації про суб'єкт, регуляторної звітності та інших подань до ринкових і зовнішніх даних, записів комунікації з піднаглядними суб’єктами та відомостей про наглядові ресурси, заходи й графіки. Система керування робочими процесами підтримує планування, ведення й відстеження наглядових заходів, фіксацію висновків, рішень і вжитих заходів. Аналітична система забезпечує оцінку ризиків, моніторинг дотримання вимог і виявлення нових загроз; автори зазначають, що аналітика для оцінки ризиків і для моніторингу дотримання може бути розділена.

На цій основі побудовано модель зрілості з чотирьох поколінь. Перше – ручний нагляд: комунікація листами й телефоном, паперові подання, переважно описовий аналіз, відстеження процесів на паперових носіях. Друге – фрагментарний нагляд: цифрові інструменти в непов'язаних застосунках, комунікація електронною поштою, відстеження процесів у таблицях, подання через пошту, вебпортали або пакетне завантаження, аналіз у табличних чи статистичних застосунках на даних, що оновлюються вручну. Третє – пов'язаний нагляд: часткова інтеграція споріднених систем, захищений майданчик комунікації з централізованим зберіганням і автоматичним відстеженням, інтеграція подань із suptech-застосунками, візуалізація перебігу процесів, зв'язок систем структурованих даних з аналітикою. Четверте – інтелектуальний нагляд: повна інтеграція з «єдиним джерелом істини», спільна модель даних, за якої всі системи взаємодіють, а наглядовці працюють з ідентичною й актуальною інформацією.

Результати вимірювання зрілості є ключовим емпіричним внеском роботи. Лише вісім із 43 респондентів мають повністю інтегровані або взаємопов'язані системи, тобто досягли четвертого покоління; ще п'ятнадцять інтегрували системи щонайменше для двох процесів (третє покоління). Сумарно частка тих, хто відповів ствердно на питання про наявність інтегрованих систем, становить 53 % проти 47 %; з урахуванням тих, хто планує впровадження, частка органів третього й четвертого поколінь зростає до 70 %. Розрив між групами країн істотний: половина респондентів із країн, що розвиваються, не мають інтегрованих систем, тоді як серед розвинених економік таких менше чверті. Найпоказовішим є розподіл причин відсутності інтеграції: близько двох третин вважають, що наявні окремі системи вже задовольняють потреби організації, близько чверті – що інтеграція не є організаційним пріоритетом, невелика частка вказує на низьку технологічну зрілість, і жоден респондент не назвав причиною брак бюджету. Це прямо переносить проблему з площини фінансування у площину стратегії й організаційної культури.

Цілі інтеграції та її зв'язок зі стратегічною рамкою описано так само конкретно. Близько трьох чвертей респондентів назвали головною метою своєчасний доступ наглядовців до інформації та аналітичних висновків, на другому місці – узгодження й спрощення наглядових процесів, і лише 20 % згадали підвищення прозорості. Показовим є зв'язок зі стратегіями: приблизно дві третини органів з інтегрованими системами мають водночас стратегії цифрової трансформації, врядування даними та suptech, і в більшості таких випадків – ще й стратегію щодо штучного інтелекту, тоді як серед органів без інтегрованих систем повний набір цих стратегій мають лише 40 %. Автори також фіксують архітектурний зсув: органи переходять від систем, побудованих навколо управлінської інформаційної системи, до платформ на основі логіки управління відносинами з клієнтами (CRM), що краще підтримує керування робочими процесами й взаємодію з піднаглядними суб'єктами.

Розділ про штучний інтелект містить найсильнішу тезу документа: інтеграція є передумовою впровадження AI, а не його наслідком. Серед органів з інтегрованими системами понад половина використовує традиційні застосунки AI і майже половина – генеративні; серед органів без інтеграції ці показники становлять 40 % і 20 % відповідно. Інтегровані системи забезпечують стандартизовані робочі процеси, централізоване середовище даних і поліпшену якість та доступність даних, тобто саме ті передумови, без яких пілотні розробки не масштабуються й лишаються автономними застосунками. Окремо розглянуто агентний AI: агенти здатні оркеструвати дії між взаємопов'язаними системами, але не між ізольованими, тому за слабкої інтеграційної основи їх впровадження стає недосяжним. Наведено приклад органу, який застосував агента для опрацювання регуляторних заявок: агент перевіряє подання на відповідність вимогам до змісту, витягує дані про дотримання вимог заявником і ініціює наступний крок процесу – повернення на доопрацювання, скерування до наглядовця або погодження.

Виклики поділено на три групи. Технічні – застаріла інфраструктура, брак сумісності наявних систем і низька якість даних, кожен із яких назвали понад 40 % респондентів; сюди ж віднесено зростання кіберризику через розширення зовнішнього периметра та поверхні атаки в інтегрованих системах. Нетехнічні виклики автори вважають складнішими: опір новим способам роботи, негнучка організаційна культура, мислення наглядовців, скептичних до змін, що пропонуються постачальниками. Третя група – вендорна – виведена в документі на рівень системного ризику. Ринок має вузьку експертизу саме в наглядовій ніші; постачальники вбудовують у свої рішення пропрієтарні моделі та інструменти, що створює довгострокову залежність, ускладнює перехід на інше рішення і робить надлишковими власні напрацювання органу; вибір багатьма органами одного й того самого постачальника формує концентраційний ризик усередині наглядової спільноти. Автори прямо зазначають, що органам слід управляти ризиком третіх сторін на тому самому рівні вимог, який вони висувають піднаглядним установам, і пропонують три опори сучасної закупівельної стратегії: відкрита архітектура на відкритих стандартах та інтерфейсах прикладного програмування, що дозволяє замінювати компоненти; фундамент даних зі стандартизованими деталізованими моделями; галузева експертиза з урахуванням нішевого характеру нагляду.

Чотири кейси ілюструють різні підходи. Центральний банк Бразилії з 2015 року розвиває власну платформу SisAPS модульної архітектури з п'яти компонентів – репозиторію неструктурованої інформації про всі піднаглядні установи, системи комунікації та збору даних, панелей візуалізації наглядових заходів і ризикових сигналів, системи оцінки ризиків і контролів із стандартизованою методологією розрахунку наглядових рейтингів та модуля взаємодії з аудиторами кредитних спілок; модульність знизила ризик інтеграції й дозволила поетапне впровадження. Європейський центральний банк із моменту створення єдиного наглядового механізму у 2014 році розбудовує систему IMAS із трьох компонентів – ядра, порталу для піднаглядних установ і сховища даних для звітності й розширеної аналітики; система підтримує понад 70 % усіх наглядових процесів, через неї обмінено понад 50 000 повідомлень, а щороку близько 1 000 співробітників проходять навчання роботі з нею. Валютне управління Гонконгу побудувало платформу Supervision360 на CRM-основі з

суб'єктоцентричною архітектурою, у якій кожен банк є центральним профілем: понад 90 % цільових користувачів працюють у ній кілька разів на тиждень, платформа веде понад 1 000 наглядових заходів на рік і мільйони індексованих документів. Резервний банк Нової Зеландії створив власний застосунок на сторонній платформі даних за підходом мінімально життєздатного продукту з подальшими ітераціями.

Мандат у сфері протидії відмиванню коштів і фінансуванню тероризму мають 51 % респондентів – це другий за поширеністю мандат після банківського нагляду, – проте жодного окремого аналізу наглядових систем саме для цього напряму робота не містить: ані кейсів, ані обговорення специфічних потреб у даних, ані викликів інтеграції для антилегалізаційного нагляду. Прогалина суттєва, оскільки ПВК/ФТ-нагляд має принаймні три особливості, яких немає у пруденційному. По-перше, дані розподілені між підрозділом фінансової розвідки, який володіє масивом повідомлень про підозрілі та порогові операції, і наглядовими органами, які володіють даними про дотримання вимог, – тобто «єдине джерело істини» тут від початку є міжвідомчою, а не внутрішньоорганізаційною задачею. По-друге, нагляд у цій сфері розподілений між кількома органами за секторальним принципом, що робить проблему сумісності систем не технічною деталлю, а питанням архітектури національної системи. По-третє, значна частка вхідних даних є неструктурованою – описова частина повідомлень, матеріали виїзних перевірок, – і саме на таких даних дає найбільший приріст генеративний AI, впровадження якого, за висновком авторів, неможливе без попередньої інтеграції.

Проєкція цієї рамки на українську систему дає кілька практичних орієнтирів. Оцінка власних систем за шкалою чотирьох поколінь є відтворюваною самооцінкою, яку кожен наглядовий орган здатен провести самостійно й без зовнішнього консультанта; вона дає спільну мову для порівняння стану секторальних регуляторів. Висновок про те, що жоден із 43 органів не назвав причиною відсутності інтеграції брак бюджету, є прямим аргументом проти типового пояснення затримок з боку органів державної влади. Нарешті, те, що наглядові органи не конкурують між собою і не мають раціональних причин уникати спільної розробки або обміну відкритим кодом, є аргументом на користь спільних рішень для органів, що здійснюють нагляд у сфері фінансового моніторингу за різними секторами.

Висновки:

- **Жоден із 43 органів не назвав браком бюджету причину відсутності інтеграції:** дві третини вважають наявні розрізнені інструменти достатніми, чверть – не пріоритетом. Обмеження є стратегічними й організаційно-культурними, а не фінансовими.
- **Інтеграція є передумовою штучного інтелекту, а не його наслідком:** серед органів з інтегрованими системами понад половина використовує традиційний AI і майже половина – генеративний, серед неінтегрованих – 40 % і 20 %. Агентний AI без сумісності систем недосяжний.
- **Вендорний ризик винесено на рівень системного:** вбудовані пропрієтарні моделі створюють довгострокову залежність, а вибір багатьма органами одного постачальника формує концентраційний ризик усередині наглядової спільноти.

Стратегія MFSA щодо протидії фінансовій злочинності: ризик-орієнтований та результативний підхід до фінансового нагляду [4]

Стратегія Управління фінансових послуг Мальти (MFSA) щодо дотримання вимог у сфері протидії фінансовій злочинності визначає оновлений стратегічний підхід мальтійського регулятора фінансового сектору до запобігання та протидії фінансовим злочинам. Документ відображає суттєве розширення попереднього фокусу MFSA: якщо раніше стратегічний акцент переважно робився на протидії відмиванню коштів і фінансуванню тероризму, то нова стратегія охоплює ширше поняття дотримання вимог у сфері протидії фінансовій злочинності.

[4] https://www.mfsa.mt/wp-content/uploads/2026/08/MFSA-Strategy-on-Financial-Crime-Compliance-2026.pdf

MFSA виходить із того, що сучасні фінансові злочини стають дедалі більш взаємопов'язаними, складними та транскордонними, а тому не можуть ефективно розглядатися ізольовано. У межах документа поняття фінансової злочинності охоплює, зокрема, відмивання коштів, фінансування тероризму, фінансування розповсюдження зброї масового знищення, податкові злочини, ухилення від цільових фінансових санкцій та шахрайство. Такий підхід має забезпечити більш комплексне реагування на ризики та одночасно посилити стійкість фінансової системи Мальти.

Стратегія формується у контексті суттєвої трансформації європейської системи ПВК/ФТ. MFSA прямо пов'язує її із впровадженням нового пакета законодавства ЄС у сфері ПВК/ФТ, посиленням гармонізації регуляторних вимог та створенням Європейського управління з питань протидії відмиванню коштів та фінансуванню тероризму (AMLA). На думку регулятора, нова європейська архітектура створює не лише операційні та наглядові виклики, але й можливості для розвитку більш узгодженої системи нагляду. Відповідно, MFSA прагне не просто адаптуватися до нових вимог ЄС, а завчасно інтегрувати майбутні стандарти у власний наглядовий підхід, підвищуючи його послідовність, гнучкість та здатність реагувати на нові ризики фінансової злочинності.

Документ не розглядається як самостійна або ізольована політика. Він безпосередньо пов'язаний зі Стратегічною заявою та щорічними наглядовими пріоритетами MFSA і водночас враховує ширший національний та міжнародний контекст. Під час розроблення Стратегії MFSA брала до уваги рекомендації Національної оцінки ризиків Мальти, пріоритети рекомендації Національної оцінки ризиків Мальти, пріоритети Національного координаційного комітету з питань протидії відмиванню коштів та фінансуванню тероризму (NCC), а також Стратегію розвитку фінансових послуг Консультативної ради Мальти з питань фінансових послуг (MFSAC), документи європейських наглядових органів, а також керівні матеріали FATF і MONEYVAL. Таким чином, стратегія поєднує національну оцінку ризиків, міжнародні стандарти та практичні наглядові пріоритети самого регулятора, забезпечуючи їх інтеграцію в єдиний підхід до протидії фінансовій злочинності.

Ключовою метою Стратегії є глибше вбудовування питань протидії фінансовій злочинності у загальний регуляторний та наглядовий мандат MFSA. Як єдиний регулятор фінансових послуг Мальти, MFSA має не лише контролювати формальне дотримання спеціальних вимог ПВК/ФТ, а й використовувати ширший масив наглядової інформації для виявлення проблем у діяльності піднаглядних установ, які потенційно можуть створювати або посилювати ризики фінансової злочинності. Тому Стратегія передбачає системніше використання інформації, отриманої у межах пруденційного, операційного та іншого регуляторного нагляду, для оцінювання, ідентифікації та пом'якшення відповідних ризиків. Паралельно документ має забезпечити більшу прозорість і підзвітність самого регулятора, оскільки чітко окреслює роль MFSA у нагляді, контролі дотримання вимог та застосуванні регуляторних заходів. Це повинно надати учасникам фінансового сектору більш чітке розуміння наглядових очікувань і власних обов'язків.

Окреме місце у Стратегії відведено співпраці з національними та міжнародними партнерами. MFSA виходить із того, що ефективна протидія фінансовій злочинності потребує належного інформаційного обміну, узгоджених дій і послідовного застосування регуляторних вимог різними компетентними органами. Водночас співпраця має охоплювати не лише державний сектор. Стратегія передбачає активне залучення фінансових установ через роз'яснення, навчання та інші форми взаємодії, що повинні сприяти кращому розумінню ними ризиків, регуляторних очікувань і належних практик. MFSA підкреслює необхідність постійного перегляду своїх підходів з урахуванням технологічних змін, нових типологій та еволюції загроз фінансової злочинності.

Практична реалізація цієї політики пов'язується насамперед зі Стратегічним пріоритетом 17 MFSA, який передбачає впровадження національної та європейської стратегій у сфері ПВК/ФТ у фінансовому секторі в координації з відповідними органами, відповідальними за

формування політики та здійснення нагляду, а також подальшу адаптацію відповідних політик і систем на основі ризик-орієнтованого підходу. Для реалізації цього пріоритету MFSA планує продовжувати співпрацю з Підрозділом аналізу фінансової розвідки Мальти (ПФР Мальти), Радою з моніторингу санкцій (SMB), Реєстром підприємств Мальти (MBR), Управлінням з питань азартних ігор Мальти (MGA), іншими регуляторними та правоохоронними органами. Окреме значення надається взаємодії з AMLA щодо імплементації нового законодавчого пакета ЄС та гармонізації наглядових стандартів у межах Союзу.

При цьому Стратегічний пріоритет 17 не розглядається як автономна мета. Її виконання залежить від реалізації інших стратегічних пріоритетів MFSA, пов'язаних із міжінституційною взаємодією, ефективністю нагляду, застосування заходів впливу, технологічними інноваціями, управлінням та стійкістю фінансового сектору. Зокрема, Стратегічний пріоритет 12 передбачає зміцнення міжінституційних відносин, узгодження політичних позицій і забезпечення послідовності наглядових підходів. Стратегічний пріоритет 15 спрямований на виявлення регуляторних прогалин і перетинів, усунення дублювання у поданні даних і підвищення сумісності інформаційних інфраструктур. Інші пріоритети стосуються фінансової грамотності, взаємодії зі споживачами, підготовки кадрів та розвитку професійних компетентностей. Це свідчить про те, що MFSA розглядає протидію фінансовій злочинності як горизонтальну складову всієї системи фінансового регулювання, а не як окрему функцію спеціалізованих підрозділів.

Центральним елементом Стратегії є ризик-орієнтований підхід. MFSA виходить із того, що наглядові ресурси є обмеженими, тому вони мають спрямовуватися передусім на ті установи, види діяльності та сектори, де ризики фінансової злочинності є найбільш суттєвими або можуть спричинити найбільший негативний вплив. Визначення таких ризиків повинно спиратися на Національну оцінку ризиків Мальти, Рекомендації FATF, матеріали MONEYVAL та європейські наглядові стандарти. Інтенсивність контролю повинна бути пропорційною ризику, який недоліки системи протидії фінансовій злочинності конкретної установи можуть становити для споживачів фінансових послуг, цілісності фінансової системи, економічної стабільності та міжнародної репутації Мальти.

MFSA характеризує ефективну ризик-орієнтовану модель через три ключові якості. Регулятор повинен бути пильним, тобто здатним своєчасно виявляти передумови порушень, червоні прапорці та нові загрози; гнучким, тобто швидко адаптувати методи роботи до змін ризикового середовища, а не покладатися лише на підходи, сформовані на основі минулих ризиків; і компетентним, тобто забезпечувати працівників наглядових органів знаннями та інструментами, необхідними для належного реагування на нові типи ризиків. Така модель має забезпечити не статичний, а постійно адаптивний фінансовий нагляд.

Однією з найбільш змістовних новацій Стратегії є прагнення MFSA систематично використовувати дані з інших напрямів нагляду як індикатори можливих проблем у сфері дотримання вимог у сфері протидії фінансовій злочинності. Регулятор прямо наводить приклади інформації, отриманої під час застосування DORA та MiCA. Недоліки управління інформаційно-комунікаційними технологіями (ІКТ), проблеми зі звітуванням про операційні інциденти, слабкий контроль аутсорсингових відносин, недостатня якість регуляторних подань, неодноразова необхідність вжиття заходів з усунення виявлених недоліків або затримки з виконанням вимог можуть свідчити не лише про окремі операційні проблеми, а й про ширші структурні слабкості внутрішнього контролю. Аналогічно пруденційні показники, пов'язані з достатністю капіталу або концентрацією ризиків, можуть демонструвати тиск на бізнес-модель установи, за якого вона потенційно може спонукати установу до зниження рівня дотримання регуляторних вимог.

Завдяки поєднанню таких даних з інформацією щодо виконання вимог у сфері протидії фінансовій злочинності MFSA прагне своєчасно визначати слабкі місця ще до того, як вони переростуть у серйозні порушення. Особливе значення тут має здатність регулятора відрізняти установи, які формально виконують нормативні вимоги, від тих, де ефективні та стійкі

контрольні механізми справді інтегровані у корпоративне управління й повсякденну діяльність. Таким чином, загальна якість корпоративного управління та управління ризиками стає одним із важливих джерел інформації для оцінки ризику фінансової злочинності.

Ризик-орієнтований підхід реалізовуватиметься у двох взаємопов'язаних напрямах – через ризик-орієнтований нагляд та рекомендації, сформовані з урахуванням ризик-орієнтованого підходу. Ризик-орієнтований нагляд передбачає концентрацію обмежених наглядових ресурсів там, де вони можуть мати найбільший ефект. Рівень наглядового втручання залежатиме від ризикового профілю, масштабу та складності конкретної установи, а різний рівень ризику може передбачати різний характер і глибину взаємодії з регулятором. Водночас MFSA продовжуватиме публікувати ризик-орієнтовані рекомендації, які повинні пояснювати наглядові очікування та надавати фінансовим установам практичні й секторально орієнтовані рекомендації щодо виявлення, оцінювання та пом'якшення ризиків фінансової злочинності.

Другим важливим напрямом є нагляд, орієнтований на результати. MFSA підкреслює, що ефективність контролю не може визначатися лише фактом існування політик, процедур або формальним виконанням нормативних вимог. Необхідно оцінювати, чи досягають запроваджені установою заходи конкретних очікуваних регуляторних результатів. Такий підхід доповнює ризик-орієнтований нагляд: ризик-орієнтована модель визначає, де саме необхідно зосередити наглядові ресурси, тоді як нагляд, орієнтований на результати дозволяє встановити, чи забезпечили конкретні заходи бажаний результат. Нагляд при цьому розглядається як постійний процес моніторингу, оцінювання та адаптації, а не як одноразова перевірка.

MFSA вже застосовує цей підхід на практиці. У документі згадуються, зокрема, підготовка рекомендації для відповідальних працівників з питань ПВК/ФТ (MLRO) у секторі фінансових послуг та тематичне дослідження діяльності MLRO у корпоративних постачальників послуг. Надалі MFSA має намір проводити аналогічні тематичні заходи та повторні оцінювання, щоб встановлювати, чи привели попередні наглядові втручання до реального усунення виявлених проблем. Якщо бажаний результат не досягнуто, можуть застосовуватися додаткові заходи. Таким чином, формується циклічна модель нагляду: ідентифікація проблеми, регуляторне втручання, оцінювання змін та повторне коригування наглядової реакції.

Ще одним фундаментальним принципом Стратегії є охоплення наглядом усього життєвого циклу піднаглядної установи. MFSA очікує, що належні механізми ПВК/ФТ мають бути сформовані вже на момент створення та авторизації установи й підтримуватися протягом усього періоду її діяльності. На стадії авторизації установи повинні надати докази існування або запланованого впровадження відповідної системи заходів у сфері ПВК/ФТ. Регулятор оцінюватиме, наскільки заявник розуміє ризики фінансової злочинності, притаманні його бізнес-моделі, та чи здатний він ефективно їх контролювати. Після отримання дозволу така оцінка продовжуватиметься в межах постійного нагляду, а установи повинні постійно адаптувати свою систему контролю до зміни обставин і ризиків.

Особлива роль у забезпеченні ефективності системи відводиться вищому керівництву. MFSA наголошує, що саме керівництво має формувати належну культуру дотримання вимог та демонструвати відповідну поведінку, водночас відповідальність за запобігання, виявлення та стримування фінансової злочинності покладається також на працівників установи. Важливим інструментом допуску осіб до керівних посад у фінансовому секторі є оцінювання їх відповідності критеріям професійної придатності та доброчесності. У цьому контексті MFSA виконує функцію контролю допуску до фінансового сектору, не допускаючи до керівних посад осіб, які не відповідають установленим вимогам щодо доброчесності, компетентності та професійності. Відповідність таким критеріям має забезпечуватися на постійній основі: навіть після погодження особи можуть виникнути обставини, що потребуватимуть повторного оцінювання її придатності, а невідповідність установленим критеріям може стати підставою для відмови в погодженні або його відкликання.

Наступним напрямом є оптимізація регуляторного нагляду та зменшення його фрагментованості. MFSA прагне посилити координацію, співпрацю та узгодженість між компетентними органами у питаннях авторизації, контролю за дотриманням регуляторних вимог, застосування заходів впливу та здійснення загального нагляду. Національні механізми повинні розвиватися відповідно до нової європейської нормативної архітектури. Одним із ключових засобів досягнення цього результату стане розширення обміну інформацією між регуляторами, що повинно забезпечити більш комплексне розуміння ризиків і дозволити переходити від реактивного до проактивного їх виявлення. Передбачається також розвиток спільних інструментів і ресурсів, що мають підвищити ефективність нагляду та зменшити дублювання регуляторної роботи.

Координація і співпраця винесені у Стратегії в окремий стратегічний напрям. MFSA планує продовжувати обмін досвідом та інформацією з національними й міжнародними регуляторами, брати участь у міжнародних комітетах та форумах і активно взаємодіяти з європейськими наглядовими органами. Особливу увагу приділено AMLA: MFSA планує долучатися до її ініціатив та надавати технічний внесок у розроблення регуляторних технічних стандартів, керівних настанов, висновків та звітів Паралельно MFSA продовжуватиме орієнтувати свій нагляд на законодавство ЄС, стандарти FATF та міжнародні найкращі практики. Міжнародна співпраця розглядається не лише як спосіб виконання міжнародних зобов'язань, але і як засіб підвищення якості національного нагляду та зміцнення репутації Мальти як належно регульованого фінансового центру.

Важливою частиною моделі MFSA є також активна взаємодія з приватним сектором. MFSA планує розширювати інформаційно-роз'яснювальну та комунікаційну взаємодію з фінансовим сектором через спеціалізовані публікації, наглядові зустрічі, навчальні заходи, семінари, безпосередню комунікацію та нові формати співпраці, зокрема партнерства між державним і приватним секторами. Така взаємодія має бути двосторонньою і забезпечувати не лише передачу регуляторних очікувань фінансовим установам, але й кращий обмін практичною інформацією між регулятором та сектором. Установи повинні отримувати своєчасні орієнтири щодо нових ризиків, вимог і належних практик, що має сприяти формуванню сильної культури управління ризиками та підвищенню загального рівня дотримання регуляторних вимог. Інформаційно-роз'яснювальна та комунікаційна взаємодія також пов'язується з розвитком професійних компетентностей, підвищенням фінансової грамотності та співпрацею з освітніми установами.

Висновки:

- **MFSA передбачає посилення ризик-орієнтованого нагляду,** зосереджуючи наглядові ресурси на установах, секторах і видах діяльності з найвищими ризиками фінансової злочинності та адаптуючи наглядові підходи до нових загроз.
- **MFSA акцентує увагу на необхідності оцінювати фактичну ефективність систем контролю,** а не лише формальне дотримання вимог ПВК/ФТ, зокрема шляхом проведення повторних перевірок після виявлення недоліків.
- **Стратегія передбачає забезпечення постійного нагляду протягом усього життєвого циклу фінансової установи,** починаючи з етапу авторизації та охоплюючи системи управління, внутрішній контроль, керівництво й відповідність ключових осіб установленим вимогам.
- **MFSA планує розвивати міжвідомчу та міжнародну співпрацю,** посилюючи обмін інформацією, використання наглядових даних і координацію з національними та європейськими органами, зокрема AMLA, для підвищення ефективності нагляду та зменшення дублювання.

У підсумковій частині Стратегії MFSA ще раз підкреслює прагнення створити інтегровану систему протидії фінансовій злочинності, у якій спеціалізований нагляд за дотриманням вимог у сфері протидії фінансовій злочинності поєднується з інформацією, що надходить з інших регуляторних напрямів. Дані, отримані в межах DORA, MiCA та інших пруденційних режимів, повинні систематично використовуватися для раннього виявлення проблем, оцінювання

ризиків та коригування заходів наглядового реагування. Якщо така інформація є важливою для інших компетентних органів, MFSA передбачає її належну передачу. Саме такий інтегрований підхід має дозволити регулятору швидше виявляти системні слабкості, уникати ситуацій, коли різні види ризиків аналізуються ізольовано, і формувати більш повне уявлення про реальний рівень контролю в конкретній установі.

Загалом Стратегія відображає перехід MFSA від переважно формального контролю дотримання окремих вимог ПВК/ФТ до комплексної, динамічної та результативно орієнтованої моделі нагляду за ризиками фінансової злочинності. Її ключова логіка полягає у тому, що ефективний нагляд має одночасно бути ризик-орієнтованим, базуватися на фактичних результатах, охоплювати весь життєвий цикл установи, використовувати інформацію з різних напрямів фінансового нагляду, забезпечувати системний міжвідомчий та міжнародний обмін інформацією і підтримувати постійний діалог із приватним сектором. У результаті MFSA прагне сформувати систему, здатну не лише реагувати на вже виявлені порушення, а й своєчасно ідентифікувати передумови їх виникнення, концентрувати наглядові ресурси на найбільш суттєвих ризиках та забезпечувати фактичну, а не лише формальну ефективність заходів з протидії фінансовій злочинності.

Незаконне переправлення осіб і фінансова система: основні типології та індикатори ризику [5]

Аналітичний звіт підготовлений Управлінням з боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN) присвячений аналізу фінансових моделей, тенденцій та характерних індикаторів, пов'язаних із підозрілою діяльністю з незаконного переправлення людей. Документ ґрунтується насамперед на інформації, яку фінансові установи США подають відповідно до Закону США про банківську таємницю (BSA), та демонструє практичну цінність фінансової розвідки для встановлення способів фінансування, організації та забезпечення діяльності мереж незаконного переправлення людей. FinCEN нагадує, що незаконне переправлення людей включено до загальнонаціональних пріоритетів США у сфері ПВК/ФТ, а сам звіт підготовлено відповідно до законодавчого обов'язку FinCEN періодично оприлюднювати інформацію про моделі та тенденції загроз, виявлені на основі BSA-даних. Для дослідження було проаналізовано 67 540 BSA-звітів, поданих у період з 1 січня 2023 року до 31 грудня 2025 року та пов'язаних із підозрою на незаконне переправлення людей. Сукупний обсяг підозрілої фінансової активності, відображеної в цих повідомленнях, перевищив 4,9 млрд дол. США. Серед найбільш послідовних характеристик FinCEN виявив неможливість підтвердити зв'язок між відправником і отримувачем коштів, перекази вздовж поширених міграційних маршрутів та значну готівкову активність у районах, пов'язаних із незаконним переміщенням осіб, зокрема вздовж південно-західного кордону США.

Для формування аналітичної вибірки FinCEN використовував повідомлення, у яких фінансові установи застосовували спеціальний ключовий термін «FIN-2023-HUMANSMUGGLING», запроваджений у попередженні FinCEN щодо незаконного переправлення людей уздовж південно-західного кордону США від січня 2023 року, та/або позначали Human Smuggling як тип підозрілої діяльності. Загалом за визначеними критеріями було відібрано 67 540 повідомлень. FinCEN застосовував поєднання автоматизованого та ручного аналізу для встановлення найбільш поширених тенденцій, методів і моделей фінансової поведінки. При цьому автори застерігають від сприйняття зазначених 4,9 млрд дол. США як точного обсягу доходів від незаконного переправлення людей. BSA-звіти можуть містити як здійснені, так і лише заплановані або невдалі операції, дублікати транзакцій, а також фінансову активність, що відбулася до початку аналізованого періоду. Вибірка сформована за датою подання звіту, а не за датою здійснення відповідної операції, тому частина повідомлень могла охоплювати

[5] https://www.fincen.gov/system/files/2026-08/FTA-Human-Smuggling.pdf

багаторічну діяльність клієнтів або враховувати раніше встановлену негативну інформацію, зокрема відомості про арешти чи обвинувачення.

Окремо FinCEN наголошує на методологічних обмеженнях звітності про підозрілу діяльність. Вона відображає лише ті операції та моделі поведінки, які були ідентифіковані фінансовими установами як підозрілі та належним чином повідомлені, а тому не може розглядатися як повне відображення масштабів незаконного переправлення людей. В одному BSA-звіті можуть одночасно враховуватися завершені та незавершені операції, вхідні й вихідні платежі, перекази між рахунками, накопичена діяльність за тривалий період або операції розширеної мережі пов'язаних осіб. Крім того, загальна сума підозрілої активності може включати як незаконні, так і законні операції відповідного клієнта. Таким чином, найбільшу цінність представлені дані мають не як статистична оцінка злочинних доходів, а як джерело інформації для встановлення повторюваних фінансових моделей, ризикових характеристик та індикаторів, які можуть використовуватися фінансовими установами і правоохоронними органами.

У документі також чітко розмежовуються поняття незаконного переправлення людей і торгівлі людьми. У контексті законодавства США незаконне переправлення осіб охоплює дії або спроби, спрямовані на незаконне переміщення осіб до США, їх транспортування територією країни, переховування, сприяння незаконному в'їзду, а також змову з метою вчинення таких дій. FinCEN підкреслює, що мережі незаконного переправлення людей нерідко мають складну та децентралізовану структуру: окремі менші групи або особи виконують специфічні функції на різних етапах маршруту, тоді як частина таких мереж взаємодіє з великими транснаціональними злочинними організаціями. Особливо це стосується мексиканських картелів, які контролюють території вздовж ключових міграційних коридорів та отримують прибутки від незаконного переправлення, зокрема через стягнення так званого piso – територіальної плати з осіб або груп, які використовують контрольовані ними маршрути. Водночас торгівля людьми є окремим злочином, пов'язаним із вербуванням, перевезенням, утриманням або використанням людей для примусової праці чи сексуальної експлуатації із застосуванням сили, шахрайства або примусу. Незважаючи на різну правову природу цих злочинів, у BSA-звітах вони нерідко згадуються одночасно через частковий збіг фінансових типологій.

Однією з найбільш помітних тенденцій за аналізований період стала істотна зміна кількості повідомлень про підозрілу діяльність. У 2023 році було подано 27 256 BSA-звітів, пов'язаних із потенційним незаконним переправленням людей, що становило приблизно 40 % усієї вибірки. Піковим став 2024 рік – 29 266 повідомлень, або близько 43 % вибірки. Уже у 2025 році їх кількість різко скоротилася до 11 018, тобто приблизно 16 % від загального обсягу повідомлень за три роки. Таким чином, порівняно з 2024 роком скорочення становило близько 62 %. Масштаб зміни особливо виразний у квартальному вимірі: тільки у другому кварталі 2024 року було подано 8 663 повідомлення, що дорівнює приблизно 79 % усієї кількості BSA-звітів за 2025 рік. FinCEN співвідносить таку тенденцію зі значним зменшенням кількості незаконних перетинів південно-західного кордону США у 2025 році.

Географічний аналіз демонструє виражену концентрацію підозрілої активності навколо США та країн Латинської Америки. Сполучені Штати були найчастішою країною місцезнаходження суб'єктів: у 67 192 BSA-звітах було зазначено щонайменше одного суб'єкта з адресою у США. Водночас підозрювані особи були представлені в усіх американських штатах і територіях. Найбільша кількість повідомлень припадала на Техас, Каліфорнію, Нью-Йорк, Флориду та Нью-Джерсі. Поза межами США найбільш представленими юрисдикціями були Мексика, Гватемала, Гондурас і Колумбія. FinCEN розглядає таку географічну структуру як свідчення того, що значна частина повідомленої потенційно пов'язаної з незаконним переправленням людей фінансової активності відбувалася між США та Латинською Америкою, причому у вибірці представлені Карибський басейн, Центральна та Південна Америка.

Особливу аналітичну цінність має інформація про документи, що посвідчують особу, які використовувалися клієнтами під час проведення операцій через установи, що надають послуги з переказу коштів. FinCEN встановив, що суб'єкти найчастіше пред'являли документи, видані США та країнами Латинської Америки. Майже всі міжнародні операції у вибірці передбачали відправлення коштів зі США за кордон особами, які використовували іноземні документи. На думку FinCEN, така модель може свідчити про участь іноземних громадян, передусім вихідців із Латинської Америки, які тимчасово або постійно перебувають у США та здійснюють перекази на користь осіб за кордоном. У певних випадках це могли бути платежі, спрямовані на фінансування незаконного переправлення друзів або членів сім'ї. Особливо показовим є те, що майже у 7 % повідомлень, поданих установами з переказу коштів, клієнт прямо визнавав, що кошти спрямовувалися для допомоги у незаконному переправленні друга або родича до США. Серед країн видачі документів після США найбільш представленими були Гондурас, Мексика, Гватемала, Сальвадор, Еквадор і Нікарагуа.

Мексиканський напрямок є одним із центральних у всьому дослідженні. Найбільше BSA-звітів за адресою суб'єкта у Мексиці було пов'язано із Сьюдад-Хуаресом – 5 891 повідомлення. Серед інших важливих міст фігурували Мехіко, Монтеррей, Тапачула, Рейноса, Тіхуана, Тустла-Гутьєррес та низка міст, розташованих поблизу кордону зі США або вздовж маршрутів переміщення мігрантів із Центральної Америки. Географічна карта на сторінці 7 звіту наочно демонструє концентрацію повідомлень як у північних прикордонних містах Мексики, так і в південних районах поблизу Гватемали, що фактично дозволяє простежити фінансовий слід уздовж міграційного маршруту. FinCEN додатково наводить приклад Сьюдад-Хуареса, де у лютому 2025 року правоохоронні органи США та Мексики припинили діяльність транснаціональної організації, яка переправляла великі групи осіб, включно з дітьми, з Мексики до Техасу.

Водночас ризики не обмежуються маршрутом через мексиканський кордон. Окремий блок звіту присвячений незаконному переправленню людей через кордон США та Канади. У відповідних BSA-звітах фінансові установи фіксували великі обсяги підозрілих переказів між фізичними особами, операцій із готівкою та іноземною валютою, а також платежів за дебетовими картками, які відповідали моделям потенційного незаконного переправлення людей. Загальна сума підозрілих операцій через різні установи з переказу коштів у Канаді перевищила 32 млн дол. США. Окремі американські фінансові установи повідомляли про транзакції у Міннесоті та Північній Дакоті – штатах, розташованих уздовж північних маршрутів незаконного переправлення. Однією з ознак ризику була значна географічна віддаленість місця здійснення операції від місця проживання клієнта без економічно зрозумілого пояснення. В одному випадку клієнт регулярно обмінював канадські долари на долари США та переказав понад 250 тис. дол. США через P2P-сервіси особі, яку було обвинувачено у незаконному переправленні людей.

Ключове місце в аналітичних висновках FinCEN займають установи, що надають послуги з переказу коштів та інші грошові послуги (MSBs). На них припало близько 97 % усієї вибірки, або 65 238 BSA-звітів. При цьому ринок був надзвичайно концентрованим: три установи сформували 86 % усіх повідомлень MSB, а одна установа – близько 43 %, або 27 879 звітів. Сукупний обсяг підозрілої діяльності, здійсненої через MSB, становив близько 519 млн дол. США, середня сума на одне повідомлення – 7 961 дол., а медіанна – 3 560 дол. Така структура свідчить про характерну для цього сегмента модель великої кількості порівняно невеликих операцій, що суттєво відрізняється від фінансової активності, яку виявляли банки та кредитні спілки.

Аналіз типологій, які найчастіше зазначали MSB, дає практичне уявлення про набір індикаторів, які можуть свідчити про потенційне фінансування незаконного переправлення людей. Найчастіше – у 38 683 повідомленнях, або 57 % – фіксувалася неможливість встановити підтверджений сімейний зв'язок між відправником і отримувачем коштів. У 26 614 повідомленнях, або 39 %, рух коштів не відповідав типовій транзакційній поведінці клієнта. По 15 706 повідомлень стосувалися випадків, коли клієнт виявляв нехарактерну байдужість

до комісій, штрафів або податкових наслідків операції, а також коли перекази здійснювалися до географічних районів, які не відповідали звичайній поведінці клієнта. У 13 408 повідомленнях кошти спрямовувалися до високоризикових юрисдикцій, у 11 422 – різним непов'язаним отримувачам, у 9 018 – до місць уздовж відомих міграційних маршрутів. Ще 7 477 повідомлень містили ознаки структурування операцій для уникнення вимог щодо обліку та звітності. Також фіксувалися схеми, за яких один відправник здійснював перекази багатьом отримувачам або, навпаки, велика кількість відправників перераховувала кошти одному одержувачу. Один BSA-звіт при цьому міг містити одразу декілька таких індикаторів.

Важливе місце у звіті займає географічний аналіз відділень установ з переказу коштів та операцій із грошовими переказами. Серед країн розташування відділень найбільше повідомлень припадало на Мексику – 11 575, за нею майже на тому самому рівні перебували США – 11 455, а далі йшли Гватемала, Домініканська Республіка, Гондурас, Колумбія, Нікарагуа та Сальвадор. Аналіз міст , з яких здійснювалися грошові перекази показав концентрацію у великих містах США, насамперед Х'юстоні, Лос-Анджелесі, Далласі та Сан-Франциско. Натомість серед основних міст-отримувачів переважали мексиканські Сьюдад-Хуарес, Вільяермоса, Тапачула, Монтеррей, Тустла-Гутьєррес і Тіхуана, а також Гватемала-Сіті. На сторінках 11–12 звіту наведені відповідні таблиці, які демонструють, що аналіз місця походження і призначення переказу дозволяє встановлювати конкретні фінансові коридори, пов'язані з міграційними маршрутами.

Іншу картину демонструє сектор депозитних установ. Банки та кредитні спілки подали лише 2 075 повідомлень, тобто приблизно 3 % від загальної кількості BSA-звітів, проте на них припало близько 3 млрд дол. США, або 61 % усього заявленого обсягу підозрілої фінансової активності. Середня сума становила приблизно 1,5 млн дол. США, медіанна – 82 965 дол., хоча FinCEN уточнює, що середній показник значною мірою був зумовлений декількома повідомленнями на суми понад 100 млн дол. На відміну від MSB, банківська звітність значно рідше стосувалася міжнародних грошових переказів та була переважно зосереджена на операціях і суб'єктах усередині США. З 2 075 відповідних повідомлень 2 029 стосувалися американських суб'єктів, тоді як Мексика, яка посідала друге місце, фігурувала лише у 41 повідомленні. У банківській звітності підозріла діяльність частіше одночасно пов'язувалася з незаконним переправленням осіб та торгівлею людьми.

Серед характерних банківських індикаторів FinCEN виділяє часті внесення готівки, P2P-платежі та банківські перекази між різними особами й підприємствами без очевидного зв'язку, значні обсяги внесення та зняття готівки через банкомати вздовж кордону США і Мексики, а також невідповідність готівкової активності заявленому виду діяльності клієнта. В окремих випадках клієнти зазначали професії або види бізнесу, для яких значна готівкова активність не є типовою. Показовим є кейс рахунку, який міг функціонувати як рахунок для акумулювання коштів: на нього щомісяця надходили численні невеликі P2P-перекази більш ніж від 30 різних осіб. У період із березня до липня 2023 року фінансова установа виявила понад 500 підозрілих транзакцій загальною сумою близько 68 тис. дол. США. Клієнт використовував окремі поточний та ощадний рахунки, систематично переводив на ощадний рахунок отримані кошти, після чого знімав їх структурованими сумами нижче встановлених порогів звітності у різних банківських відділеннях та банкоматах.

FinCEN також демонструє, що фінансування незаконного переправлення людей може здійснюватися через значно складніші комерційні операції. Один із BSA-звітів стосувався підозрілих транзакцій, пов'язаних із чартерними авіарейсами, на суму понад 3 млн дол. США. Фінансова установа підозрювала, що ці кошти могли використовуватися для організації переміщення людей з Об'єднаних Арабських Еміратів до Нікарагуа з подальшим прямуванням до США. Серед ознак, що викликали підозру, були невідповідності між сумами платежів, незрозумілі повернення коштів та договори, які не відповідали фактичному руху коштів. Одну з компаній було пов'язано з випадками перевезення громадян Індії маршрутом через Єгипет, Ямайку, ОАЕ та Нікарагуа. FinCEN звертає увагу на роль Нікарагуа як одного з пунктів прибуття мігрантів, які згодом наземним шляхом прямують до американського кордону.

Інший випадок свідчить про важливість аналізу не лише переказів як таких, але й кінцевого використання коштів. Фінансова установа виявила понад 195 тис. дол. США нетипових готівкових внесків, які використовувалися для фінансування покупок за дебетовими картками у постачальника тактичного тепловізійного обладнання. Клієнтами були студент і власник компанії з продажу сільськогосподарської продукції, що не відповідало характеру таких закупівель. Вони також здійснювали значні зняття готівки через банкомати у Ногалесі та Фініксі та придбали майже на 30 тис. дол. США тепловізійні біноклі й цифрові прилади нічного бачення. FinCEN зазначає, що таке обладнання потенційно може використовуватися для забезпечення незаконного переправлення людей. Цей приклад демонструє необхідність співвідносити фінансові операції з економічним профілем клієнта, характером придбаних товарів та потенційною функціональною роллю цих товарів у злочинній діяльності.

Окремою типологією FinCEN визначає використання туристичних агентств. Мережі незаконного переправлення людей можуть організовувати для мігрантів комплексні маршрути, що передбачають придбання авіаквитків, автобусні перевезення та проживання у готелях на різних етапах шляху до кордону США. У BSA-звітах неодноразово фігурували особи, які позиціонували себе як власники туристичних агентств та здійснювали фінансові операції, характер яких був сумісний із потенційним незаконним переправленням людей. Водночас FinCEN наголошує, що не всі такі компанії обов'язково свідомо залучені до злочинних схем: легальні туристичні агентства в окремих випадках можуть ненавмисно використовуватися злочинними мережами. Один із наведених прикладів стосувався туристичного агентства із Сьюдад-Хуареса, на рахунок якого через банкомати та банківські відділення вздовж південно-західного кордону було внесено понад 150 тис. дол. США готівкою. Готівкові депозити практично повністю забезпечували фінансування рахунку, кошти вносили як власник агентства, так і невстановлені особи, а відсутність операцій із виплати заробітної плати додатково ставила під сумнів характер заявленої господарської діяльності.

В інших повідомленнях фінансові установи встановили підозрілу активність, пов'язану з міжнародною мережею незаконного переправлення людей та туристичними агентствами у Флориді, які могли бути залучені також до шахрайських схем із візами. Фінансова активність включала внесення готівки у різних штатах США, P2P-перекази від осіб, які, ймовірно, оплачували візові або туристичні послуги, а також численні повернення коштів за авіаквитки. Під виглядом звичайних туристичних платежів отримані кошти використовувалися для масового придбання авіаквитків для різних осіб через декілька авіакомпаній та для чартерування приватних літаків, що перевозили групи мігрантів. Це демонструє, що зовнішньо легітимна господарська діяльність може використовуватися як фінансова й логістична оболонка для організації незаконного переміщення людей.

Загалом звіт FinCEN показує, що фінансова діяльність, пов'язана з незаконним переправленням людей, є багаторівневою та

Висновки:

- **Необхідно посилити ризик-орієнтований моніторинг грошових переказів та переказів між фізичними особами,** враховуючи нетипову географію операцій, відсутність очевидного зв'язку між сторонами та ознаки структурування платежів. На установи, що надають послуги з переказу коштів, припало близько 97 % усіх проаналізованих повідомлень.
- **Доцільно застосовувати мережевий підхід до фінансового аналізу,** виявляючи схеми «багато відправників – один отримувач», «один відправник – багато отримувачів», транзитні рахунки для акумулювання коштів та подальше структуроване зняття готівки.
- **Варто розширити моніторинг на туристичні та авіаційні послуги,** масове придбання квитків, нетипові повернення коштів і придбання товарів, які можуть використовуватися для забезпечення незаконного переправлення людей.
- **Слід активніше використовувати географічний і маршрутний аналіз,** зіставляючи напрями руху коштів, місця здійснення операцій та відомі міграційні маршрути для виявлення потенційно пов'язаних мереж.

охоплює різні сегменти фінансової системи. Через установи з переказу коштів переважно проходять численні відносно невеликі міжнародні платежі між фізичними особами, часто без очевидного сімейного або економічного зв'язку та з вираженою прив'язкою до міграційних маршрутів. У банківському секторі частіше виявляються значніші обсяги коштів, рахунки для акумулювання надходжень від великої кількості осіб, структурування готівкових операцій, P2P-платежі, перекази між непов'язаними суб'єктами та використання бізнес-рахунків. Додатковий рівень ризику формують туристичні агентства, чартерні перевезення, масові закупівлі авіаквитків, нетипові повернення коштів та придбання обладнання, яке може забезпечувати діяльність злочинних мереж. Таким чином, основний практичний зміст аналізу FinCEN полягає в тому, що ефективне виявлення фінансових слідів незаконного переправлення людей потребує оцінки не окремої операції, а сукупності взаємопов'язаних характеристик: транзакційної поведінки клієнта, структури його контрагентів, географії платежів, каналів переказу, характеру використаних рахунків, економічного змісту операцій та їх можливого зв'язку з відомими міграційними коридорами. Саме поєднання цих елементів дозволяє фінансовим установам та органам фінансової розвідки переходити від виявлення одиничних нетипових платежів до встановлення ширших фінансових мереж, посередників і логістичної інфраструктури, що можуть забезпечувати функціонування схем незаконного переправлення людей.

Нові пропозиції SEC щодо ринку віртуальних активів [6]

Останні роки стали періодом безпрецедентного зростання та водночас викликів для ринку криптоактивів. Від появи біткоїна у 2008 році цей сектор еволюціонував від вузької ніші техно-ентузіастів до потужного глобального фінансового феномену, який привертає увагу як роздрібних інвесторів, так і інституційних гравців.

Однак, попри цю динаміку, регуляторна база Сполучених Штатів, зокрема Комісії з цінних паперів та бірж (SEC), тривалий час залишалася адаптованою до традиційних фінансових інструментів, не враховуючи унікальної природи цифрових активів. Ця прогалина створювала значні перешкоди для емітентів, ускладнювала планування транзакцій і, як наслідок, стримувала інновації та формування капіталу в межах американської юрисдикції. Деякі емітенти, зіткнувшись із цими регуляторними труднощами, обирали шлях проведення своїх операцій в офшорних зонах, що не лише звужувало інвестиційні можливості для громадян США, але й підвищувало рівень їхнього ризику через участь у ринках з менш надійним захистом прав інвесторів.

У відповідь на ці системні виклики SEC ініціювала низку кроків, кульмінацією яких стала пропозиція комплексного нормативного акту під умовною назвою «Regulation Crypto Assets». Цей документ є спробою створити спеціально адаптований режим для певних інвестиційних контрактів, пов'язаних із криптоактивами, які в тексті пропозиції іменуються «охопленими інвестиційними контрактами». Він базується на попередньому роз'ясненні SEC, випущеному в березні, яке мало на меті прояснити застосування федеральних законів про цінні папери до операцій з криптовалютами, та гармонійно доповнює зусилля Конгресу США щодо кодифікації цілісної структури регулювання ринку.

Запропонований регуляторний пакет є багаторівневим механізмом, який включає чотири ключові елементи, кожен з яких виконує власну функцію у спільній архітектурі регулювання.

По-перше, це так зване «стартап-звільнення» (startup exemption), яке пропонує емітентам тимчасове, одноразове звільнення від вимог реєстрації згідно із Законом про цінні папери 1933 року. Цей інструмент розрахований на початківців ринку – компанії, які перебувають на ранніх стадіях розвитку і потребують «дихаючого простору» для реалізації своїх бізнес-моделей. Воно дозволяє залучати до 5 мільйонів доларів протягом чотирирічного періоду за

[6] https://www.sec.gov/files/33-11434-fact-sheet.pdf

умови виконання низки прозорих умов, зокрема подання публічних звітів на початку та в кінці цього терміну. Такий підхід має на меті надати емітентам можливість зосередитися на виконанні тих управлінських зусиль, які вони обіцяли інвесторам у межах інвестиційного контракту, водночас зберігаючи для інвесторів достатній рівень інформованості та захисту.

Другим, більш масштабним рівнем є «звільнення для збору коштів» (fundraising exemption), яке за своєю структурою нагадує відомий у регуляторній практиці Регламент А, проте адаптоване до специфіки криптоактивів. Це дворівнева система, де перший рівень (Tier 1) дозволяє емітентам залучати до 20 мільйонів доларів протягом дванадцяти місяців, а другий рівень (Tier 2) – до 75 мільйонів доларів за той самий період. Така градація створює гнучку шкалу для середніх та великих проектів, які вже вийшли за межі початкового стартап-етапу. Важливою умовою для користування цим звільненням є публічне розкриття не лише тих самих даних про проект, що й у попередньому випадку, але й детального обговорення фінансового стану емітента з обов'язковим поданням фінансової звітності. Для другого рівня ця звітність повинна проходити обов'язковий аудит, що значно підвищує довіру до пропонованих інвестицій. Крім того, емітенти беруть на себе зобов'язання щодо постійного поточного звітування, що наближує цей режим до стандартів публічних компаній, однак у більш легкій формі, адаптованій до потреб ринку цифрових активів.

Третій і, мабуть, найбільш концептуально важливий елемент – це «безпечна гавань для інвестиційних контрактів» (investment contract safe harbor). Цей інструмент має на меті вирішити одну з найскладніших правових колізій, що виникають навколо криптоактивів – питання про те, коли такий актив перестає вважатися цінним папером у розумінні законодавства. Згідно з пропозицією, якщо емітент виконав або остаточно припинив усі суттєві управлінські зусилля, які він обіцяв здійснювати за контрактом, і не має наміру робити нових заяв чи обіцянок щодо таких зусиль у майбутньому, а також публічно підтвердив це через спеціальний сертифікаційний документ із розгорнутим аналізом, то інвестиційний контракт вважається таким, що припинив своє існування.

Відповідно, сам криптоактив більше не підпадає під визначення цінного паперу для цілей Закону про цінні папери та Закону про біржі. Це положення є критично важливим, оскільки воно створює передбачуваний шлях для децентралізації активу, коли його подальша доля вже не залежить від зусиль конкретної керуючої компанії, а визначається ринковими механізмами, що є наріжним каменем філософії багатьох криптовалютних проектів.

Висновки:

- **Створення багаторівневої системи полегшеного доступу до капіталу.** Пропозиція запроваджує диференційовані пороги залучення інвестицій, що дозволяє емітентам обирати найбільш доцільний режим залежно від стадії розвитку без повноцінної реєстрації.
- **Чіткий механізм припинення статусу цінного паперу через «безпечну гавань».** Пропонується прозора процедура, за якої криптоактив втрачає ознаки інвестиційного контракту (а відтак і статусу цінного паперу), що дає ринку довгоочікувану визначеність щодо моменту децентралізації активу.
- **Збереження антилегалізаційних норм при одночасному пом'якшенні реєстраційних вимог.** Регулятор свідомо відмовляється від жорсткого превентивного контролю на користь гнучких умов розкриття інформації, проте зберігає повноваження для реактивного втручання у разі зловживань – це зміщує акцент із бюрократичного дозволу на постійний моніторинг добросовісності емітентів.

Нарешті, четвертим елементом є механізм «випередження» державних вимог щодо реєстрації та кваліфікації цінних паперів. Пропонується запровадити визначення «кваліфікованого покупця» згідно із Законом про цінні папери, що автоматично усуває необхідність дотримання розрізнених регуляцій окремих штатів стосовно пропозицій та продажу охоплених інвестиційних контрактів, випущених у рамках Regulation Crypto Assets. Це стосується як первинних розміщень, так і певних транзакцій на вторинному ринку, за умови, що емітент продовжує виконувати інформаційні та звітні вимоги, передбачені цим режимом.

Такий підхід має на меті створити єдиний, уніфікований простір для обігу криптоактивів на території всієї країни, уникнути регуляторного арбітражу між штатами та значно спростити процедури для емітентів, які прагнуть залучати капітал на національному рівні.

Загалом, запропонований пакет «Regulation Crypto Assets» є знаковим кроком, що демонструє еволюцію підходу SEC від пасивного спостереження до активної побудови адаптивної регуляторної екосистеми. Його ключовим завданням є досягнення тонкого балансу між двома суперечливими цілями: з одного боку, стимулювання інновацій та полегшення формування капіталу, а з іншого – забезпечення надійного захисту інвесторів та підтримання цілісності ринку. Усі чотири запропоновані інструменти працюють у синергії: стартап-звільнення дає «пусковий козир» для молодих проектів, звільнення для збору коштів забезпечує масштабування, безпечна гавань вирішує проблему «переродження» активу з цінного паперу в товар або засіб обігу, а також створюється єдине поле для національної торгівлі. Важливо наголосити, що жодне з цих звільнень не скасовує дії антилегалізаційних норм федерального законодавства, що зберігає за SEC потужний арсенал для боротьби з шахрайством та зловживаннями.

Запровадження таких правил може мати далекосяжні наслідки для всього світового ринку криптоактивів. У разі схвалення, цей нормативний акт не лише спрямує потік капіталу з офшорів назад до американської юрисдикції, але й стане своєрідним еталоном для регуляторів інших країн, які також шукають шляхи інтеграції цифрових активів у свою правову систему.

Відкритість SEC до публічного обговорення, яке триватиме 60 днів з моменту публікації, свідчить про прагнення врахувати якомога ширше коло думок ринкових учасників, юристів та інвесторів. Разом із тим, успіх цієї пропозиції залежатиме не лише від формальних юридичних аспектів, а й від практичної імплементації та здатності регулятора оперативно реагувати на динамічний розвиток технологій та бізнес-моделей у сфері криптоактивів.

Цей документ відкриває нову главу в історії регулювання цифрових фінансів, де акцент зміщується від заборони та обмежень до створення зрозумілих, прозорих та працюючих правил гри, що є запорукою довгострокового здорового розвитку ринку.

Звіти окремих інституцій та експертів

Фінансування розповсюдження зброї масового знищення в Південно-Східній Азії: регіональні ризики, вразливості та практичні підходи до протидії [7]

Документ є практично орієнтованим посібником з аналізу ризиків фінансування розповсюдження зброї масового знищення (ФР) у Південно-Східній Азії. Він ґрунтується на результатах регіональної конференції, проведеної 7–8 жовтня 2025 року в Бангкоку за участю представників Індонезії, Камбоджі, Малайзії, В'єтнаму, Брунею-Даруссаламу, Лаоської НДР, Шрі-Ланки, Філіппін і Таїланду. Основна мета посібника полягає в узагальненні результатів цієї роботи, формуванні каталогу характерних ризиків ФР і наданні юрисдикціям практичних орієнтирів для їх виявлення, оцінювання та мінімізації. Вихідною тезою документа є те, що Південно-Східна Азія має особливий профіль ризику: ті самі характеристики, які забезпечують економічну конкурентоспроможність регіону – великі морські порти, інтенсивні торговельні маршрути, розвинені виробничі потужності, масштабні ланцюги постачання та інтеграція у світову економіку, – можуть використовуватися державними та недержавними суб'єктами для придбання матеріалів, технологій і фінансових ресурсів, необхідних для програм зброї масового знищення. Тому протидія ФР розглядається не як ізольоване питання фінансового контролю, а як комплексне завдання, що поєднує фінансовий моніторинг,

[7] https://www.global-amlcft.eu/wp-content/uploads/2026/07/PF-ASEAN-peignot-digital_compressed.pdf

експортний контроль, митне регулювання, корпоративну прозорість, морську безпеку, санкційні механізми, контроль віртуальних активів та міжвідомчий обмін інформацією.

Однією з найбільш істотних загроз документ визначає використання Південно-Східної Азії як транзитного, перевалочного та реекспортного центру незаконної торгівлі. Величезні обсяги контейнерних перевезень через основні порти регіону та стратегічні морські маршрути створюють своєрідне середовище, у якому незаконні вантажі можуть бути приховані серед значних потоків легальної торгівлі. Мережі, пов'язані з розповсюдженням, можуть направляти товари, включаючи контрольовану продукцію подвійного використання, через регіональні торговельні вузли, де вони перепаковуються та реекспортуються із зміненими або фальсифікованими документами. Для приховування реального походження, пункту призначення або кінцевого користувача використовуються змінені коносаменти, неправдиві сертифікати кінцевого користувача та інші маніпуляції з торговельною документацією. Додатковим методом є змішування незаконних товарів із легальними партіями вантажів, що істотно ускладнює їх виявлення без попередньої конкретної оперативної інформації. Особливу увагу приділено морському сектору, де ризики пов'язані з перевантаженням товарів із судна на судно, фальсифікацією суднових документів, змінами маршруту та використанням різних типів суден для транспортування чутливих або контрольованих товарів.

Важливе місце в регіональному профілі ризику займає виробництво та міжнародна торгівля товарами подвійного використання. Розвинена промислова база держав регіону означає, що значна кількість продукції має одночасно законне цивільне та потенційне військове або пов'язане із ЗМЗ застосування. До таких товарів у документі віднесено окремі електронні компоненти, високошвидкісні перемикачі, конденсатори й транзистори, вакуумні насоси, перетворювачі частоти, високоміцні метали, вуглецеве волокно та певні хімічні прекурсори. Сам по собі законний характер таких товарів ускладнює їх ідентифікацію в контексті ФР, оскільки ключове значення має не лише вид продукції, а й її технічні характеристики, кінцеве використання, покупець, маршрут постачання та структура операції. Ситуацію додатково ускладнює використання механізмів відмивання коштів через торговельні операції, зокрема неправильної класифікації товарів, завищення або заниження їх вартості та інших форм недостовірного декларування, які дозволяють одночасно приховувати характер товару і переміщувати кошти через кордони.

Мережі закупівель, пов'язані з ФР, за висновками документа, дедалі частіше застосовують складні способи обходу систем експортного контролю. Для цього можуть створюватися зовні легітимні комерційні компанії, які звертаються до виробників або постачальників, не розкриваючи справжнього кінцевого користувача чи фактичної мети придбання продукції. Однією з тактик є маніпулювання технічними специфікаціями, коли замовляється обладнання з характеристиками, формально дещо нижчими за порогові параметри експортного контролю, а після поставки воно модифікується. Інший механізм передбачає направлення товарів через треті країни з менш розвиненими системами експортного контролю з подальшим реекспортом до санкційної юрисдикції. Також великі закупівлі можуть штучно дробитися на декілька менших партій, а контрольовані товари – декларуватися під кодами Гармонізованої системи, характерними для схожої, але неконтрольованої продукції. Це демонструє, що ефективна протидія ФР потребує аналізу не лише окремих операцій, а й послідовності закупівель, торговельних маршрутів, технічних специфікацій та зв'язків між учасниками постачання.

Окремою складною категорією загроз є використання дипломатичної та державної інфраструктури. Передусім у документі аналізуються ризики, пов'язані з КНДР. Дипломатичні представництва, персонал, дипломатична пошта або приміщення можуть потенційно використовуватися для переміщення коштів, товарів чи організації операцій, пов'язаних із незаконними закупівлями. Державні підприємства у сфері судноплавства, торгівлі або будівництва можуть використовуватися як підставні компанії, забезпечувати отримання доходів або придбання необхідної продукції, водночас приховуючи зв'язок із державою, що перебуває під санкціями. Ще одним механізмом є залучення громадян третіх країн як формальних директорів компаній, посередників чи фінансових агентів. Протидія

таким схемам є особливо складною, оскільки потребує достатнього рівня розвідувальної інформації та здатності відрізнити законну дипломатичну чи комерційну діяльність від операцій, пов'язаних із ФР.

Значну увагу посібник приділяє зміні характеру ФР унаслідок розвитку віртуальних активів. Їх швидкість, транскордонний характер і псевдонімність створюють можливість переміщувати кошти без використання традиційних фінансових посередників. У документі виділено два основні напрями такого використання: обходження санкцій та безпосереднє генерування доходів через кіберзлочинність. Найбільш показовим прикладом визначено діяльність КНДР, яка використовує не лише традиційні механізми обходу санкцій, а й атаки на криптовалютні біржі, децентралізовані фінансові платформи та іншу цифрову інфраструктуру. Отримані в результаті таких атак активи можуть проходити через складні ланцюги транзакцій, після чого конвертуватися у фіатні кошти або використовуватися для подальших закупівель. Таким чином, віртуальні активи створюють принципово нову модель, за якої суб'єкти ФР здатні не тільки приховувати або переміщувати наявні фінансові ресурси, а й самостійно генерувати значні незаконні доходи.

На прикладі атак на Ronin Network та Harmony Bridge документ демонструє значні обсяги коштів, які можуть бути отримані внаслідок кібероперацій, пов'язаних із державними суб'єктами. Водночас посібник пропонує практичні підходи до відстеження таких активів. Зокрема, за допомогою публічних сервісів перегляду та аналізу блокчейн-транзакцій можна перевіряти відомі ризикові адреси, простежувати рух віртуальних активів між гаманцями, виявляти їх взаємодію з міксерами та міжмережевими мостами, а також відстежувати подальше надходження активів на централізовані криптовалютні платформи. У документі також представлено графік, що відображає зростання обсягів викрадених віртуальних активів, пов'язаних із діяльністю КНДР, та демонструє дедалі більшу роль таких активів як джерела фінансування програм розповсюдження зброї масового знищення.

Поряд із віртуальними активами окремо виділяються кіберзлочинність та атаки з використанням штучного інтелекту (AI). У контексті ФР вони знаменують перехід від традиційної моделі переміщення коштів до моделі безпосереднього створення незаконних фінансових ресурсів. AI може використовуватися для підвищення якості соціальної інженерії та створення переконливих локалізованих фішингових повідомлень, спрямованих, наприклад, на працівників банків або державних установ. Паралельно розвиток онлайн-маркетплейсів створює нові проблеми для експортного контролю, оскільки традиційні системи переважно були орієнтовані на значні за обсягом поставки, тоді як електронна торгівля дозволяє здійснювати велику кількість малих транскордонних відправлень. Анонімні продавці, компанії без реальної господарської діяльності та неправдиве декларування можуть використовуватися для придбання чутливих технологій без розкриття фактичного кінцевого користувача. Таким чином, автори розглядають сучасний ландшафт ФР як багатовимірний: традиційні торговельні й морські схеми співіснують із технологічно складними цифровими та кібернетичними механізмами.

Після аналізу загроз документ визначає структурні вразливості, які створюють умови для їх реалізації. Однією з них є нерівномірність регуляторних режимів для віртуальних активів та постачальників відповідних послуг. У частині держав існують прогалини у нагляді за такими суб'єктами, а недостатня спеціалізована підготовка регуляторів, фінансових установ і правоохоронних органів обмежує можливості виявлення ФР. Автори звертають увагу на значну асиметрію підходів: від фактичної заборони віртуальних активів в окремих країнах до існування значної кількості криптовалютних платформ із недостатнім рівнем нагляду в інших. Це дає змогу переміщувати діяльність до юрисдикцій із менш суворим регулюванням і слабшими механізмами контролю.

Іншою суттєвою вразливістю є функціонування морського сектору, вільних торговельних зон і спеціальних економічних зон. Спрощені процедури, запроваджені для прискорення торгівлі та залучення інвестицій, можуть одночасно обмежувати рівень фізичної перевірки вантажів і

документального контролю. Товари можуть ввозитися до таких зон, зберігатися, збиратися, перероблятися, перепаковуватися та реекспортуватися без застосування такого самого рівня експортного контролю, який діє на решті митної території. У результаті окремі компоненти подвійного використання можуть бути ввезені як неконтрольована продукція, зібрані в готове обладнання та вивезені без повноцінної перевірки необхідності експортної ліцензії. Масштаби торговельних потоків також означають, що митні органи не можуть фізично перевіряти кожну партію і значною мірою залежать від систем ризик-профілювання. Тому ефективність контролю прямо залежить від включення до таких систем специфічних індикаторів ФР, включаючи відповідні коди товарів подвійного використання, інформацію про відомі компанії-прикриття, ризикові маршрути та суб'єктів.

Документ також пропонує практичні інструменти для аналізу морських ризиків. Зокрема, дані систем автоматичної ідентифікації суден можуть використовуватися для моніторингу незвичайних переміщень у портах і на основних морських маршрутах, перевірки заявленого пункту призначення та зіставлення суден із санкційними чи іншими ризиковими переліками. Інформаційна система Міжнародної морської організації може використовуватися для перевірки історії конкретного судна, його зареєстрованого власника, менеджера й оператора, а також частих змін назви або прапора, які можуть виступати індикаторами обходу санкцій.

Ще одна вразливість пов'язана з неформальними фінансовими каналами, включаючи системи переказу вартості на зразок hawala, значний обіг готівки та діяльність незареєстрованих операторів грошових переказів. Хоча значна частина таких систем використовується для законних переказів, недостатність документування та регуляторного контролю створює можливості для їх використання у фінансуванні незаконної діяльності. У схемах ФР такі канали можуть мати особливе значення на завершальних етапах, наприклад для виплат місцевим агентам або посередникам без створення повноцінного фінансового сліду.

Суттєвим ризиком залишаються прогалини у законодавчій та регуляторній базі. Документ звертає увагу на принципову відмінність ФР від класичного відмивання коштів: для фінансування розповсюдження можуть використовуватися кошти цілком законного походження – наприклад, державні ресурси чи доходи від легальної торгівлі, – але спрямовані на незаконну мету. Відсутність спеціальних правових механізмів може означати, що навіть за наявності фінансової розвідувальної інформації про підозрілий платіж, пов'язаний із закупівлею товарів подвійного використання, компетентні органи не матимуть достатніх підстав для оперативного втручання, якщо зв'язок із санкційним суб'єктом ще не встановлено. Окремо наголошується на необхідності чітких національних переліків контрольованої продукції подвійного використання. Без таких юридично визначених переліків митним органам і приватному сектору складно встановити, які саме товари потребують спеціального контролю, що фактично створює прогалини для закупівельних мереж.

Найбільш наскрізною інституційною вразливістю автори вважають недостатній обмін інформацією та фрагментарну міжвідомчу координацію. Різні органи можуть володіти окремими частинами інформації про одну і ту саму схему: митний орган – даними про підозрілу поставку електроніки, ПФР – інформацією про фінансовий переказ від підставної компанії, а інші органи – відомостями про пов'язаних осіб або кінцевого користувача. Окремо кожен елемент може не виглядати достатньо ризиковим, тоді як їх поєднання здатне чітко вказувати на схему ФР. Відсутність правових і технічних каналів для оперативного обміну такими даними призводить до того, що інформація передається ситуативно та із запізненням, коли вантаж уже залишив країну або фінансова операція завершена. Тому документ фактично ставить здатність поєднувати різні масиви торговельної, фінансової, корпоративної та оперативної інформації в центр ефективної системи протидії ФР.

Додатковими вразливостями є географічне положення регіону, велика кількість островів, портів, прибережних територій і слабко контрольованих транскордонних маршрутів, недостатній рівень обізнаності державного та приватного секторів і дефіцит спеціалізованих ресурсів. Значна кількість працівників фінансових установ, митних органів та інших суб'єктів

не має достатньої підготовки щодо товарів подвійного використання, схем обходу санкцій та типологій ФР. Це обмежує можливості виявлення ризикової діяльності на операційному рівні. Водночас ПФР, митні та експортно-контрольні органи часто мають обмежені кадрові й технологічні ресурси для спеціалізованої роботи у сфері ФР.

Особливе значення має прозорість бенефіціарної власності. Недостатньо ефективні корпоративні реєстри, обмежена перевірка внесених до них даних та використання номінальних директорів дозволяють створювати мережі компаній-прикриттів і компаній без реальної господарської діяльності. Такі юридичні особи можуть використовуватися як формальні покупці, продавці, платники чи отримувачі коштів, приховуючи реального суб'єкта, який контролює операцію. Документ акцентує, що непрозорість корпоративних структур є не другорядною проблемою, а одним із фундаментальних чинників, які дозволяють закупівельним мережам приховувати зв'язок між фінансовими та торговельними операціями.

У посібнику також розглянуто потенційне використання неприбуткових і благодійних організацій. Вразливість цього сектору пов'язується з високим рівнем суспільної довіри, складністю транскордонних фінансових потоків та можливістю змішування законних і незаконних коштів. Особливий ризик може виникати у випадках, коли легітимна організація несвідомо співпрацює із закордонним партнером, який має приховані зв'язки із санкційними особами або іншими ризиковими суб'єктами. У такій ситуації гуманітарна чи благодійна діяльність може використовуватися як прикриття для обходу міжнародних фінансових обмежень.

Значна частина документа присвячена методології проведення національної оцінки ризиків ФР. Автори наголошують, що цей вид оцінювання залишається відносно новим порівняно з оцінками ризиків відмивання коштів і фінансування тероризму, а тому багато держав проводять лише першу або другу таку оцінку та не мають достатнього інституційного досвіду. За відсутності деталізованої методології існує ризик отримання надто загального документа, який не враховує специфічні для конкретної держави загрози та не трансформується у практичні заходи. Запропонована в посібнику модель не позиціонується як обов'язкова, але пропонує послідовну шестистадійну процедуру.

На першому етапі необхідно сформувати систему управління процесом та визначити межі оцінки. Початковою умовою є високорівневий політичний мандат, який повинен закріплювати повноваження щодо збору інформації, обов'язковість участі державних органів, строки проведення оцінки та необхідні кадрові й фінансові ресурси. Центральним координатором може виступати ПФР або міжвідомчий комітет. До процесу рекомендується залучати зовнішньополітичні органи, митницю, структури експортного контролю, морські адміністрації, правоохоронні органи, фінансових регуляторів, наглядові органи нефінансового сектору, органи у сфері промисловості й торгівлі, а також представників банків, торгово-промислових палат і судноплавного сектору. При цьому необхідні формалізовані правила роботи, механізми прийняття рішень, вимоги конфіденційності та угоди щодо обміну інформацією.

Паралельно створюються спеціалізовані технічні групи, відповідальні за збір даних, аналіз і оцінювання, взаємодію з приватним сектором та підготовку документа. Необхідно чітко визначити географічні й секторальні межі оцінки. Крім банків та інших фінансових установ, до неї мають включатися ВНУП, імпортно-експортні компанії, морські перевізники, авіаційний і наземний транспорт, а за наявності відповідної промислової бази – виробники напівпровідників, хімічної продукції, високоточного обладнання, ядерних технологій та продукції аерокосмічного сектору. Сама оцінка повинна бути адаптована до національного контексту та конкретних програм розповсюдження, які становлять найбільшу загрозу для відповідної юрисдикції.

Другий етап охоплює системний збір кількісних і якісних даних. Для різних груп учасників рекомендується розробляти окремі опитувальники. Від правоохоронних органів необхідно отримувати інформацію про розслідування, виявлені схеми, можливості та прогалини; від

регуляторів – інформацію про нормативну базу, нагляд, санкції та навчання; від фінансового сектору – дані про ризикові операції, повідомлення про підозрілі операції, внутрішні політики, системи скринінгу та індикатори підозрілості; від торговельного сектору – інформацію про обсяги торгівлі з ризиковими юрисдикціями, товари подвійного використання, способи оплати, транзитні пункти та належну перевірку клієнтів. Опитувальники повинні доповнюватися статистичними даними ПФР, інформацією про заявки та відмови в експортних ліцензіях, транскордонні перекази, торговельне фінансування, реєстрацію суден і портові операції.

Кількісні дані пропонується поєднувати із секторальними консультаціями, експертними інтерв'ю, міжвідомчими круглими столами та аналізом відкритих джерел. Контекст держави доцільно оцінювати за політичними, економічними, соціальними, технологічними, правовими та екологічними параметрами. Водночас повинні аналізуватися міжнародні кейси, матеріали щодо встановлених порушень, національні оцінки ризиків інших держав, взаємні оцінки FATF та міжнародна торговельна статистика. Окремим етапом є валідація інформації – перевірка її повноти, внутрішньої узгодженості та надійності, документування обмежень і формування єдиної структурованої бази для подальшого аналізу.

Третій етап передбачає безпосередню ідентифікацію та аналіз загроз і вразливостей. Загрози рекомендується оцінювати з урахуванням конкретних програм розроблення зброї масового знищення та засобів її доставки, географічного положення держави, наявності великих портів та аеропортів, транзитних пунктів, слабко контрольованих кордонів, історичних і сучасних торговельних відносин із санкційними юрисдикціями, непрямих торговельних потоків і складних мереж постачання. Для систематизації аналізу пропонується застосовувати матрицю, яка враховує ймовірність та вплив загрози, а географічний розподіл ризиків відображати за допомогою карт. Вразливості оцінюються з точки зору достатності законодавства, імплементації цільових фінансових санкцій, наявності визначень і переліків товарів подвійного використання, ресурсного забезпечення органів, якості координації, інформаційних систем і спеціалізованої експертизи. На секторальному рівні для фінансових установ оцінюються розуміння ризиків ФР, якість скринінгу, моніторинг транзакцій та якість повідомлень про підозрілі операції, а для торговельного сектору – обізнаність, належна перевірка клієнтів, можливості експедиторів та ефективність митного контролю.

Додатково може проводитися оцінювання наслідків реалізації ризиків. До безпекових наслідків віднесено сприяння розповсюдженню зброї масового знищення (ЗМЗ), послаблення регіональної та міжнародної безпеки та зростання геополітичної нестабільності. Економічними наслідками можуть бути міжнародні санкції, втрата кореспондентських банківських відносин, скорочення іноземних інвестицій і репутаційні втрати. Правові та репутаційні наслідки можуть включати негативні результати міжнародних оцінок та зниження довіри до юрисдикції.

Четверта фаза спрямована на інтеграцію результатів у загальну модель ризику, пріоритизацію проблем та визначення заходів реагування. У посібнику пропонується п'ятибальна шкала ризику та використання екторальних таблиць і графічного відображення рівнів ризику для відображення результатів. Водночас пріоритетність не повинна визначатися виключно числовим рейтингом: необхідно враховувати можливість практичного зменшення конкретного ризику, доступність ресурсів та потенційний ефект запланованих заходів. Заходи рекомендується розподіляти за строками: критичні проблеми мають вирішуватися у короткостроковій перспективі до шести місяців, заходи з розвитку спроможностей – у горизонті від шести до вісімнадцяти місяців, а масштабні структурні реформи – у період від вісімнадцяти до тридцяти шести місяців. Механізми зменшення ризику можуть включати законодавчі зміни, нове регулювання, секторальні керівництва, вдосконалення правозастосовних процедур, спеціалізоване навчання, технологічні інвестиції, протоколи обміну інформацією, нові стандарти звітування, міжнародне співробітництво та партнерство з приватним сектором.

Наступні етапи охоплюють підготовку, перевірку, затвердження, поширення та подальше оновлення національної оцінки. Проєкт документа повинен пройти технічну перевірку щодо точності даних і логіки методології, правову перевірку, безпековий аналіз щодо розмежування відкритої та закритої інформації, а також контроль якості. Перед остаточним затвердженням передбачається консультація з державними органами і, за необхідності, приватним сектором. Документ допускає підготовку кількох версій НОР – повної версії для обмеженого використання, публічної версії, стислого викладу основних висновків та англомовної версії для міжнародних партнерів. Після завершення оцінки має функціонувати постійний механізм моніторингу виконання плану заходів із регулярною звітністю та системою показників. Вони повинні охоплювати не лише формальні результати, такі як прийняті закони, охоплені регулюванням сектори або кількість навчених працівників, а й показники ефективності – кількість виявлених справ, заморожених активів, обвинувальних вироків та релевантних повідомлень про підозрілі операції. Дані рекомендується оновлювати щороку, а повну переоцінку проводити кожні три–п’ять років із можливістю оперативного перегляду у разі суттєвої зміни ризиків.

Окремий розділ посібника присвячено практичним труднощам, які вже виявлені у державах Південно-Східної Азії. Однією з них є недостатня кількість національних справ і документованих типологій ФР. За відсутності реальних прикладів ПФР, регуляторам і правоохоронним органам складніше формувати якісні індикатори ризику, розробляти профілі підозрілої діяльності та адаптувати ризик-орієнтовані підходи до специфіки власної держави. Ситуацію погіршують небажання окремих державних органів ділитися чутливою інформацією та відсутність постійних платформ для обміну розвідувальними даними, типологіями та практичним досвідом. Автори також звертають увагу на низьку ефективність традиційних опитувальників для приватного сектору: значна кількість анкет призводить до втоми респондентів і формальних відповідей, особливо коли самі учасники недостатньо розуміють специфіку ФР. Наслідком можуть стати загальні оцінки, які не відображають реальних ризиків конкретної юрисдикції.

Серед інших системних проблем визначено недостатнє залучення ВНУП, дефіцит кадрових і фінансових ресурсів, низьку якість повідомлень про підозрілу діяльність та підозрілі операції, інституційну фрагментацію, дипломатичні та політичні обмеження, географічну складність і непрозорість бенефіціарної власності. ВНУП, включаючи юридичні, бухгалтерські та корпоративні послуги, часто недостатньо інтегровані у національні механізми протидії ФР, що зменшує можливості раннього виявлення ризикових структур та операцій. Повідомлення від фінансових установ, ВНУП і постачальників послуг у сфері віртуальних активів нерідко містять недостатньо контексту і не відображають специфічні індикатори ФР. Окремою проблемою є відсутність у деяких країнах централізованої структури високого рівня, відповідальної за політику, координацію та практичну реалізацію заходів у сфері ФР. Документ також застерігає від перетворення національної оцінки ризиків на формальну процедуру, спрямовану лише на демонстрацію виконання міжнародних вимог, оскільки без залучення ключових секторів – зокрема судноплавства і високотехнологічної промисловості – оцінка може залишитися теоретичною та відірваною від реальних загроз.

Водночас у регіоні вже сформувалися практики, які документ оцінює як перспективні. Насамперед це забезпечення політичної підтримки найвищого рівня та застосування загальнодержавного підходу, за якого ПФР або інший визначений орган здійснює центральну координацію. Ефективними визнаються постійні національні робочі групи, координаційні комітети або спеціалізовані механізми з протидії ФР, які об’єднують ПФР, митні, правоохоронні, експортно-контрольні та розвідувальні органи. Значну роль відведено державно-приватному партнерству: фінансові установи, постачальники послуг у сфері віртуальних активів, судноплавні та логістичні компанії можуть не тільки виконувати нормативні вимоги, але й брати участь в обміні інформацією, підвищенні обізнаності та спільному формуванні індикаторів ризику. Замість створення повністю нової інституційної

системи рекомендується максимально використовувати вже наявну інфраструктуру та механізми взаємодії, сформовані у сфері ПВК/ФТ.

Не менш важливим напрямом є розвиток спеціалізованих компетентностей. Навчальні програми для ПФР, митниці, регуляторів і приватного сектору повинні мати практичний характер та включати сценарні вправи, посібники з індикаторами ризику, моделювання конкретних ситуацій і використання реальних справ та типологій. Регіональне та міжнародне співробітництво має забезпечувати регулярний обмін інформацією і практичним досвідом, оскільки мережі ФР за своєю природою є транскордонними, а їх окремі елементи можуть бути розподілені між кількома юрисдикціями.

У підсумку посібник формує бачення ФР як комплексного ризику національної безпеки та економічної доброчесності. Основна складність полягає в тому, що діяльність, пов'язана з ФР, часто маскується всередині цілком законної економічної активності: кошти можуть мати законне походження, компанії бути офіційно зареєстрованими, товари мати цивільне призначення, а торговельні операції окремо не демонструвати очевидних ознак порушення. Саме тому ефективність системи залежить від здатності держави поєднувати фінансову, торговельну, корпоративну, митну, санкційну, морську та розвідувальну інформацію, своєчасно встановлювати зв'язки між окремими елементами схеми та переводити результати оцінювання ризиків у конкретні заходи. Фінальний висновок документа полягає у необхідності подолання міжвідомчої фрагментації, залучення приватного сектору як повноцінного партнера, розвитку спеціалізованої експертизи та більшої узгодженості підходів між державами регіону. Саме такий перехід від формальної відповідності до практично орієнтованої, інтегрованої системи протидії розглядається як ключова передумова посилення спроможності держав запобігати, виявляти та припиняти ФР.

Висновки:

- **Необхідно посилити міжвідомчу координацію у сфері ФР,** забезпечивши оперативний обмін інформацією між ПФР, митними, правоохоронними, розвідувальними та експортно-контрольними органами.
- **Доцільно забезпечити практичну спрямованість національної оцінки ризиків ФР,** визначивши конкретні пріоритети, відповідальні органи, строки реалізації заходів та показники їх ефективності.
- **Слід посилити контроль за найбільш уразливими напрямами,** зокрема торгівлею товарами подвійного використання, морськими перевезеннями, віртуальними активами та структурами з непрозорою бенефіціарною власністю.
- **Важливо розширити взаємодію з приватним сектором і спеціалізоване навчання,** залучаючи фінансові установи, постачальників послуг у сфері віртуальних активів, ВНУП, логістичні та судноплавні компанії до розроблення типологій та індикаторів ризику ФР.

Стейблкоїни на перетині права, регулювання та монетарної політики: глобальні підходи, ризики та напрями регуляторної конвергенції [8]

Документ присвячений правовій природі стейблкоїнів, підходам до їх регулювання та потенційному впливу на монетарну систему. Основна теза дослідження полягає в тому, що стейблкоїни не є однорідним класом активів. Вони відрізняються механізмами стабілізації вартості, структурою резервів, моделями погашення та зберігання, а тому правовий і регуляторний режим має визначатися з урахуванням фактичної конструкції конкретного інструменту. Автори пропонують застосовувати диференційований підхід з урахуванням типу

[8] https://bdap.wharton.upenn.edu/wp-content/uploads/2026/08/Final_Stablecoin-Toolkit-Regulatory-Report-2.pdf

та структурних характеристик стейблкоїнів, за якого правова класифікація, регуляторні вимоги та монетарна політика узгоджуються зі структурними характеристиками стейблкоїна.

Стейблкоїни вже вийшли за межі суто криптовалютного ринку та використовуються для платежів, транскордонних розрахунків, торгівлі, забезпечення фінансових операцій і управління ліквідністю. Водночас їх правова характеристика залишається фрагментованою: залежно від юрисдикції один і той самий інструмент може розглядатися як електронні гроші, платіжний інструмент, майно, договірна вимога або окрема правова категорія. Це створює проблеми у сфері приватного і комерційного права, фінансового регулювання та монетарної політики.

У сфері приватного права ключовим є питання, чи може стейблкоїн визнаватися повноцінним об'єктом майнових прав. Від цього залежить можливість його передачі, використання як застави, встановлення забезпечувальних прав, захист добросовісного набувача та становище власника у разі банкрутства емітента або зберігача активів. На відміну від фізичних грошей, стейблкоїни існують як цифрові записи, управління якими здійснюється через криптографічні ключі або облікові записи. Тому традиційні концепції володіння та власності потребують адаптації до цифрового середовища.

Важливим елементом такого підходу є поняття контролю. Принципи UNIDROIT щодо цифрових активів і приватного права визначають контроль як можливість особи отримувати вигоди від цифрового активу, обмежувати доступ інших осіб до такого активу та передавати контроль над ним іншій особі. Подібний підхід закріплено у статті 12 Єдиного комерційного кодексу США (UCC) щодо контрольованих електронних записів. У цьому випадку контроль виступає функціональним аналогом володіння та може використовуватися для встановлення забезпечувальних прав і визначення їх пріоритетності.

Разом із тим автори наголошують на розриві між технічним контролем у блокчейні та юридичним визнанням права власності. Наприклад, у моделях самостійного зберігання користувач може повністю контролювати приватні ключі, тоді як у моделях із залученням зберігача активів фактичний контроль значною мірою належить платформі, яка може заморожувати активи або обмежувати здійснення операцій. У випадку регульованих фіатно-забезпечених стейблкоїнів користувач контролює сам токен, тоді як управління резервними активами здійснює емітент або зберігач активів. В алгоритмічних моделях власник контролює токен, але не механізм підтримання його вартості. Це означає, що однакова технологічна форма може приховувати різні правові та фінансові ризики.

Це механізм, за якого у разі дострокового припинення кількох фінансових договорів усі взаємні вимоги сторін оцінюються та зводяться до однієї підсумкової чистої суми, яку одна сторона має сплатити іншій. Міжнародна асоціація свопів і деривативів (ISDA) вже розробила рекомендації щодо використання токенізованих активів і стейблкоїнів як забезпечення, однак ефективність таких механізмів залежить від того, чи визнає національне законодавство відповідний цифровий актив об'єктом майнових прав. Водночас більшість систем на основі технології розподіленого реєстру (DLT), у яких використовуються стейблкоїни, не мають такого самого рівня правового захисту остаточності розрахунків, як традиційні платіжні та розрахункові системи. Віднесення стейблкоїна до еквівалентів грошових коштів, товарів або загальних нематеріальних активів безпосередньо впливає на можливість взаємозаліку фінансових зобов'язань у разі їх дострокового припинення.

Суттєвою проблемою є і транскордонний характер стейблкоїнів. Через відсутність фізичного місцезнаходження цифрового активу складно визначити право, яке має регулювати його передачу, власність, заставу, спадкування чи банкрутство. У США UCC передбачає спеціальну систему визначення застосовного права для цифрових активів, тоді як UNIDROIT пропонує міжнародні принципи для вирішення подібних колізій. Однак повної міжнародної гармонізації немає, тому автори рекомендують принаймні забезпечити чітке розкриття емітентами застосовного права та компетентного форуму для вирішення спорів.

У регуляторній частині звіту зазначається, що в основних юрисдикціях уже сформувалося спільне регуляторне ядро. США, Європейський Союз, Велика Британія, Японія, Сінгапур, Гонконг та ОАЕ переважно регулюють фіатно-референтні стейблкоїни, забезпечені ліквідними резервами та погашувані за номіналом. Водночас алгоритмічні та синтетичні стейблкоїни, а також стейблкоїни, забезпечені криптоактивами, часто залишаються поза межами спеціального регуляторного периметра або не відповідають установленим регуляторним вимогам.

Основними пруденційними вимогами стають повне резервне забезпечення, як правило у співвідношенні 1:1, використання високоякісних ліквідних активів, юридична сегрегація резервів від майна емітента, регулярна незалежна перевірка резервів, ліцензування та нагляд. Для системно значущих емітентів можуть застосовуватися посилені вимоги щодо ліквідності, капіталу, стрес-тестування та планування врегулювання. Такі заходи спрямовані, зокрема, на зменшення ризику масового погашення стейблкоїнів і вимушеного продажу резервних активів, що може створити негативний вплив на фінансові ринки.

Значна увага приділяється праву власника на погашення та захисту резервів у разі банкрутства емітента. Регламент MiCA надає власникам токенів електронних грошей право на погашення за номінальною вартістю. У Японії застосовується трастова модель, за якої власник має майнові права щодо резервних активів. У Гонконзі передбачено право на погашення та відповідні права на резервні активи у разі неплатоспроможності емітента, тоді як у Сінгапурі встановлено вимоги щодо відокремленого зберігання резервів і дотримання визначеного строку погашення. У США GENIUS Act передбачає 1:1 резервування, сегрегацію резервів, регулярне розкриття їх складу та спеціальний захист вимог власників у процедурі банкрутства.

Водночас подібність економічних функцій стейблкоїнів не означає однаковості їх правової класифікації. У Європейському Союзі токени електронних грошей прямо віднесено до електронних грошей, тоді як у Великій Британії стейблкоїни, що відповідають установленим критеріям, регулюються окремо від електронних грошей. У США для платіжних стейблкоїнів сформовано окрему спеціальну правову категорію, а в Японії застосовується поняття електронних платіжних інструментів. Гонконг і Сінгапур також запровадили окремі ліцензійні режими для стейблкоїнів поряд із чинним регулюванням електронних грошей. Такі відмінності безпосередньо впливають на порядок захисту прав користувачів у разі неплатоспроможності емітента, вимоги до ліцензування, остаточність розрахунків та здійснення транскордонних операцій.

Окремою проблемою залишається захист користувачів. Для традиційних електронних платежів у США та ЄС діють спеціальні правила щодо помилкових і несанкціонованих операцій, тоді як режими стейблкоїнів переважно обмежуються вимогами до розкриття інформації. Не існує також уніфікованого механізму оскарження замороження балансу стейблкоїнів. Крім того, не завжди зрозуміло, кого саме вважати «власником» стейблкоїна, якщо актив зберігається через біржу чи іншого посередника. У таких випадках кінцевий користувач може мати лише договірну вимогу до посередника, а не безпосереднє право до емітента чи резервів. Тому автори рекомендують чітко визначати статус бенефіціарного власника та запроваджувати вимоги щодо сегрегації клієнтських активів.

У сфері ПВК/ФТ документ підкреслює необхідність застосування до емітентів і посередників стейблкоїнів вимог, співставних із тими, що діють для традиційних фінансових установ. У США GENIUS Act зберігає застосування вимог Закону про банківську таємницю до емітентів стейблкоїнів, зокрема щодо моніторингу операцій та подання повідомлень про підозрілу діяльність (SAR). Водночас до відповідних операцій продовжують застосовуватися вимоги FinCEN щодо супроводження переказів інформацією про відправника та одержувача (Travel Rule), а також санкційні вимоги Управління з контролю за іноземними активами Міністерства фінансів США (OFAC). На міжнародному рівні ключовим орієнтиром залишається Рекомендація 16 FATF, однак підходи до імплементації Travel Rule суттєво відрізняються між юрисдикціями, зокрема щодо порогових значень операцій, некастодіальних гаманців та

децентралізованих фінансів (DeFi). Автори наголошують на необхідності забезпечення співставних вимог у сфері ПВК/ФТ для банківських і небанківських учасників, щоб не допустити отримання емітентами стейблкоїнів регуляторних переваг унаслідок менш суворих вимог.

Нерівномірність регуляторних вимог створює ризик регуляторного арбітражу, коли емітенти можуть структурувати діяльність через юрисдикції з менш суворими правилами щодо резервів, ліцензування, погашення або ПВК/ФТ. На думку авторів, це суперечить принципу «однакові ризики – однакове регулювання» та створює нерівні конкурентні умови. Особливо важливо забезпечити реальну еквівалентність режимів при допуску іноземних стейблкоїнів на внутрішні ринки.

Третій великий блок звіту стосується монетарної політики. Повністю забезпечений резервами стейблкоїн за своєю структурою може наближатися до моделі банку з повним резервуванням, що порушує питання щодо можливості надання емітентам таких стейблкоїнів доступу до резервів центрального банку. Такий доступ міг би зменшити кредитний і кастодіальний ризик, однак одночасно створив би приватний цифровий актив, близький за характеристиками до грошей центрального банку, і міг би посилити конкуренцію з банківськими депозитами.

Не менш важливим є питання процентних стейблкоїнів. З одного боку, можливість виплачувати дохід може сприяти конкуренції та інноваціям. З іншого – високоліквідний і повністю забезпечений процентний стейблкоїн може стимулювати відтік коштів із банківських депозитів, скорочувати ресурсну базу банківського кредитування, посилювати фінансову дезінтермедіацію та ускладнювати трансмісію монетарної політики. Документ не займає однозначної позиції, але наголошує, що це питання має вирішуватися на основі оцінки відповідних макрофінансових наслідків.

Висновки:

- **Необхідно запровадити ризик-орієнтований підхід до класифікації стейблкоїнів,** визначаючи регуляторні вимоги залежно від структури резервів, механізму погашення, моделі зберігання та фактичних ризиків конкретного інструменту.
- **Доцільно посилити захист власників стейблкоїнів** шляхом забезпечення резервування 1:1, юридичної сегрегації резервів, погашення за номіналом та чітких прав власників у разі неплатоспроможності емітента.
- **Слід гармонізувати транскордонні регуляторні вимоги та вимоги у сфері ПВК/ФТ,** зокрема щодо правил супроводження переказів інформацією про відправника та одержувача, діяльності іноземних емітентів, некастодіальних гаманців та взаємного визнання національних регуляторних режимів, щоб мінімізувати можливості регуляторного арбітражу.
- **Варто враховувати вплив стейблкоїнів на фінансову та монетарну стабільність,** зокрема ризики відтоку банківських депозитів, кредитної дезінтермедіації, валютного заміщення та посилення залежності від глобальних доларових стейблкоїнів.

Особливу увагу приділено глобальному поширенню стейблкоїнів, які прив’язані до долара США. Їх активне використання для платежів і заощаджень може посилювати валютне заміщення, особливо в країнах зі слабшими національними валютами, зменшувати ефективність внутрішньої монетарної політики та посилювати залежність від рішень Федеральної резервної системи США. Глобальні стейблкоїни можуть також прискорювати транскордонний рух капіталу та створювати додаткові ризики для країн із менш розвиненими фінансовими системами, тому їх поширення розглядається як питання монетарного суверенітету.

У рекомендаціях автори пропонують ширше закріплювати поняття контролю як цифрового аналога володіння, впроваджувати підходи UNIDROIT або аналогічні правові механізми, забезпечувати остаточність розрахунків і чітко врегулювати механізм взаємозаліку фінансових зобов’язань у разі дострокового припинення договорів, а також гарантувати власникам стейблкоїнів прямі права на резервні активи,

захищені у разі неплатоспроможності емітента. Регуляторні вимоги пропонується визначати відповідно до економічної функції та рівня ризику конкретного стейблкоїна, а не лише його формальної правової класифікації. Такий підхід має також охоплювати пропорційне регулювання алгоритмічних і синтетичних стейблкоїнів, а також стейблкоїнів, забезпечених криптоактивами.

На міжнародному рівні рекомендується гармонізувати мінімальні стандарти резервування, погашення, аудиту та ПВК/ФТ, удосконалити механізми визнання іноземних режимів і координувати підходи до Travel Rule та іноземних емітентів. Центральним банкам пропонується встановлювати прозорі критерії доступу емітентів до резервів, окремо оцінювати наслідки процентних стейблкоїнів, а меншим і відкритим економікам – приділяти особливу увагу ризику валютного заміщення та поширенню глобальних доларових стейблкоїнів.

У підсумку документ констатує, що у провідних юрисдикціях уже сформувалося спільне розуміння базової моделі регульованого стейблкоїна: це токен, прив'язаний до фіатної валюти, погашуваний за номіналом, забезпечений високоякісними ліквідними резервами, відокремленими від майна емітента, та випущений ліцензованою і контрольованою установою. Водночас значна фрагментація зберігається у питаннях правової природи стейблкоїнів, захисту кінцевих користувачів, регулювання нерезервних моделей, транскордонних колізій, ПВК/ФТ та монетарних наслідків. Головним завданням для законодавців, регуляторів, центральних банків і міжнародних організацій залишається узгодження правової класифікації, регуляторної архітектури та монетарної політики з фактичною структурою і ризиками конкретних стейблкоїнів.

Антинаркотична політика Талібану та системні злочини проти людяності [9]

З моменту повернення до влади в Афганістані у 2021 році, рух «Талібан» проголосив безкомпромісну війну з наркотиками, яка мала на меті викорінити виробництво та вживання заборонених речовин. Ця кампанія, що супроводжувалася знищенням полів опійного маку та лабораторій з виробництва метамфетаміну, на перший погляд, демонструвала рішучість нової влади. Однак, за фасадом боротьби з наркозлочинністю, розгорнулася значно похмуріша і трагічніша картина.

Масштабне польове дослідження, проведене Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC) у співпраці з організацією Coact, виявило докази систематичних зловживань, які за своїм характером та масштабом не мають аналогів у сучасному світі.

Дослідження, що охопило період з 2022 по 2025 роки, малює образ системи, яка функціонує не як мережа реабілітаційних центрів, а як розгалужена система таборів ув'язнення, де люди, які вживають наркотики, стають жертвами подвійного удару: спочатку від самої залежності, а потім – від жорстокої та нелюдської «допомоги». Режим Талібану, проголошуючи боротьбу з наркотрафіком, фактично створив інституціоналізовану машину для тортур та принижень, де головною метою є не зцілення, а ізоляція та покарання. Замість лікарень, ці установи функціонують як в'язниці суворого режиму, де тисячі людей утримуються в умовах, що межують із тривалими катуваннями.

Умови утримання в цих так званих «центрах лікування» є настільки огидними, що навіть побіжний опис викликає жах. Центри, які часто працюють далеко за межами своєї пропускної здатності, перетворюються на перенаселені, антисанітарні табори, де сотні, а інколи й тисячі людей, розміщуються у критих приміщеннях без належної вентиляції. Наприклад, в одному з центрів, розрахованому на 1000 місць, утримувалося від 4 до 5 тисяч пацієнтів, які спали на

[9] https://globalinitiative.net/wp-content/uploads/2026/08/Human-rights-abuses-in-the-Talibans-drug-control-regime-GI-TOC-August-2026.pdf

підлозі. Харчування, там, де воно було, ледь дозволяло уникнути голодної смерті, а доступ до чистої питної води та елементарних засобів гігієни був розкішшю. Відсутність належного одягу та опалення в холодну пору року робила ці центри місцями, де смерть від переохолодження чи виснаження була буденністю. Один з колишніх пацієнтів згадував, що в його центрі щоночі вмирало від п'яти до десяти осіб.

Проте, найбільш шокуючим аспектом цієї системи є повна відсутність будь-якої кваліфікованої медичної та психологічної допомоги. Медичне обслуговування, особливо в період гострої абстиненції, було або примітивним, або взагалі відсутнім. У кращому випадку пацієнтам робили ін'єкції глюкози або заспокійливих, але жодної системної терапії, спрямованої на полегшення фізичних страждань не проводилося. Лікування часто зводилося до примусового занурення в крижану воду, що мало «допомогти» подолати абстинентний синдром.

Реабілітаційні програми, якщо їх можна так назвати, обмежувалися примусовим вивченням Корану та релігійними лекціями про шкоду наркотиків, які часто набували форми залякування та моралізаторства. Психологічна підтримка була відсутня, а про професійну терапію чи програми соціальної реабілітації взагалі не йшлося. Замість цього, пацієнтів залучали до примусової праці, яка маскувалася під професійне навчання, де вони мили посуд, прибирали або виконували інші важкі роботи за мізерну винагороду. Весь цей «реабілітаційний» процес був спрямований на те, щоб фізично ізолювати людину від наркотиків, а не на усунення першопричин залежності чи надання інструментів для повернення до нормального життя.

Насильство та жорстоке поводження пронизують усю систему. Хоча дослідники не були безпосередніми свідками фізичних побиттів, розповіді пацієнтів малюють жахливу картину. Побиття батогами, катування холодною водою, тримання в ізоляторах без світла та кисню, приковування ланцюгами за ноги – це далеко не повний перелік покарань, які застосовувалися за найменшу провину, наприклад, за спробу втечі чи запізнення на молитву.

Особливо цинічним виглядає використання так званих «пацієнтів-представників», які наділялися владою над іншими ув'язненими. Ця система, запроваджена через брак персоналу, призвела до розквіту зловживань, де «старші» пацієнти вимагали гроші, займалися вимаганням та сексуально експлуатували новачків, особливо підлітків. Весь цей жах відбувався за мовчазної згоди або прямого потурання з боку персоналу та представників Талібану, які часто не мали жодної кваліфікації, а інколи й походили з аграрного чи ветеринарного середовища.

Процеси затримання та звільнення з цих таборів є ще одним свідченням їхньої антигуманної природи. Переважна більшість пацієнтів не потрапляла до центрів добровільно. Їх виловлювали під час поліцейських рейдів, часто

Висновки:

- **Системна дегуманізація замість лікування.** Афганські "реабілітаційні центри" функціонують не як медичні заклади, а як табори примусового утримання, де головною метою є ізоляція та покарання наркозалежних, а не їхнє зцілення.
- **Жорстокі умови утримання та висока смертність.** Перенаселення, антисанітарія, недостатнє харчування, відсутність чистої води та елементарних гігієнічних умов призводять до масових спалахів захворювань та щоденної смертності пацієнтів, що свідчить про свідоме нехтування правами на життя та здоров'я.
- **Інституціоналізоване насильство та безкарність.** Фізичні тортури, катування, приниження, сексуальна експлуатація та використання пацієнтів як наглядачів один над одним є повсякденною практикою. Особливо вразливими є жінки, діти та підлітки, які зазнають подвійного тиску – від самої системи та від інших ув'язнених, наділених владою.
- **Провал реабілітації та відсутність постлікувального супроводу.** Від 50% до 90% пацієнтів повертаються до вживання наркотиків через відсутність системи підтримки після звільнення, безробіття, стигматизацію та неможливість реінтеграції в суспільство. Система не дає людині інструментів для змін, а лише відтерміновує неминучий рецидив.

супроводжуваних насильством, або ж заарештовували за доносами родичів, які, ймовірно, бачили в цьому єдиний спосіб врятувати близьку людину від гіршої долі. Після затримання їх часто утримували у відділках поліції, де також застосовували тортури, перш ніж направити до табору.

Термін утримання, який зазвичай становив 45 днів або три місяці, визначався не медичними показниками, а адміністративним свавіллям. Для звільнення необхідно було пройти складну бюрократичну процедуру, яка вимагала залучення чоловіків-родичів, що мали поручитися за пацієнта та підтвердити його «одужання». Це створило замкнене коло для людей, які не мали сім'ї або були відрізані від неї, прирікаючи їх на багаторічне перебування в таборах.

Поширеною практикою було й вимагання хабарів за дострокове звільнення. Навіть після виходу на волю система забуває про своїх «пацієнтів». Жодної підтримки чи спостереження не проводиться, що призводить до того, що, за різними оцінками, від 50 до 90% пацієнтів знову повертаються до вживання наркотиків, стикаючись із тими ж самими злиднями, безробіттям та стигмою, які й привели їх до залежності.

Окремою та найбільш вразливою категорією в цій кризі є жінки та діти. Жіночі центри, яких і так існує вкрай мало, переважно значно менші та гірше обладнані, ніж чоловічі. Жінки-наркозалежні часто змушені одночасно доглядати за дітьми, які також страждають від впливу наркотиків. Вони стикаються з подвійною стигмою, ризиком сексуального насильства та переслідувань як усередині центрів, так і за їхніми межами. Багато жінок, через страх помсти, відмовлялися розповідати свої історії публічно, що свідчить про глибину їхнього безсилля. Діти та підлітки, які потрапляють до системи, часто піддаються тим самим жорстоким методам «лікування», що й дорослі, включаючи побиття та покарання. Лише в деяких центрах створюються умови, хоч трохи пристосовані для дітей, що робить їх жертвами не лише власної залежності, а й системної жорстокості дорослих.

Антинаркотична політика Талібану, незважаючи на її публічну риторику, виявилася глибоко провальною з гуманітарної точки зору. Вона не тільки не вирішує проблем, але й створює нові, більш жахливі форми страждань. Замість того, щоб будувати систему охорони здоров'я та соціальної підтримки, режим створив систему масового ув'язнення, яка є антитезою будь-якому поняттю про права людини.

Міжнародна спільнота, яка значною мірою закрила очі на ситуацію в Афганістані після виведення військ, несе відповідальність за те, що ці системні зловживання залишаються без належної уваги. Докази, зібрані у цьому звіті, є криком про допомогу, який вимагає невідкладного розслідування та тиску на владу Талібану з метою припинення цієї інституціоналізованої жорстокості.

Це не просто порушення прав людини, це – гуманітарна катастрофа, яка розгортається за зачиненими дверима десятків таборів, перетворюючи лікування на тортури, а надію на відчай.

Нова ера цифрових активів, яку фінансові установи не можуть ігнорувати [10]

Сучасний ландшафт кіберзагроз вимагає від організацій не просто технічного захисту, а й глибокого розуміння фінансових наслідків потенційних інцидентів. Традиційні підходи до оцінки кіберризиків, які часто базуються на розрізнених електронних таблицях та разових консультаційних звітах, стають не лише застарілими, а й відверто неефективними. Вони створюють ілюзію контролю, тоді як насправді залишають компанії вразливими до стрімких змін загроз та ускладнюють комунікацію між технічними фахівцями та вищим керівництвом.

[10] https://www.riskrecon.com/total-economic-impact-of-mastercards-cyber-quant-solution

Саме для вирішення цієї проблеми було розроблено платформу Mastercard Cyber Quant, яка позиціонується не просто як інструмент, а як стратегічний актив, що трансформує управління кіберризиками на рівні всього підприємства.

Згідно з дослідженням Forrester Consulting, проведеним на замовлення Mastercard, впровадження Cyber Quant демонструє переконливу економічну доцільність. Результати аналізу, заснованого на досвіді чотирьох компаній-респондентів та зведеного до показників узагальненої композитної організації, свідчать про значне зростання ефективності та суттєву економію коштів. Ключовим показником успіху є вражаюча рентабельність інвестицій (ROI) на рівні 112%, що досягається завдяки системному підходу до оцінки ризиків, який замінює хаотичні, трудомісткі та дороговартісні процеси. Чиста приведена вартість (NPV) інвестицій становить 255 000 доларів США за три роки, а період окупності, за прогнозами, не перевищує шести місяців. Ці цифри є вагомим аргументом для фінансових директорів та керівників з безпеки, які шукають обґрунтовані способи оптимізації бюджетів на кіберзахист.

Дослідження виокремлює три основні напрямки, де компанії отримують найбільш відчутні фінансові вигоди. Перший і найсуттєвіший – це підвищення операційної ефективності самої процедури оцінки ризиків. До впровадження Cyber Quant організації стикалися з низкою класичних проблем: ручне введення даних у застарілі Excel-файли, що призводило до втрати інформації та неймовірної складності агрегації даних.

Один з опитаних менеджерів зазначив, що Excel «не призначений для такого рівня оцінки», а сам процес міг залучати до 20 співробітників з різних департаментів і тривати до шести місяців. Така повільна процедура, яку проводили раз на два роки, не встигала за динамікою загроз і перетворювалася на формальність. Натомість Cyber Quant пропонує структуровану платформу зі стандартизованими опитувальниками та автоматизованим збором доказів. Завдяки цьому час на проведення оцінки скорочується на 50%, що дозволяє команді безпеки зосередитися на аналізі та стратегії, а не на механічній роботі з таблицями. За три роки економія робочого часу персоналу оцінюється у 148 000 доларів США з урахуванням ризиків та дисконтування. Більше того, компанії отримують змогу проводити оцінки частіше, реагуючи на нові вразливості майже в реальному часі, що робить процес справді динамічним інструментом управління, а не разовим звітом.

Другий напрямок фінансового впливу стосується реакції на результати зовнішніх аудитів та усунення виявлених недоліків. У минулому, коли аудитори надавали висновки, командам безпеки доводилося витрачати місяці на ручний пошук доказів, повторну перевірку контролів та підготовку відповідей. Cyber Quant значно спрощує цей процес, оскільки всі необхідні артефакти, контекст ризику та логіка пріоритезації вже зібрані та структуровані в системі. Це дозволяє скоротити час, необхідний для реагування на кожен висновок аудиту, на 55%. У композитній моделі це призводить до зменшення кількості висновків аудиту з 20 до 9, що вивільняє значний обсяг робочого часу висококваліфікованих фахівців. Загальна економія від цієї оптимізації за три роки оцінюється у 320 000 доларів США. Це дозволяє спрямувати зусилля команди безпеки на вирішення пріоритетних завдань і навіть на залучення до більш прибуткових проєктів, що, за словами одного з респондентів, підвищує маржинальність бізнесу та мотивацію персоналу.

Третій, хоч і менший за абсолютними цифрами, але надзвичайно важливий аспект – це вплив на інвестиційні рішення в сфері кібербезпеки. Традиційно компанії часто купували нові технології захисту під впливом маркетингу, регуляторного тиску або окремих, локальних інцидентів, не маючи чіткого розуміння, чи зменшать ці інвестиції загальний ризик підприємства. Cyber Quant виступає в ролі об'єктивного важеля для валідації таких рішень. Платформа дозволяє оцінити, чи дійсно запропонований інструмент або контроль суттєво вплине на рівень ризику з урахуванням специфіки бізнесу та регіону. В одному з наведених прикладів компанія відмовилася від запланованої покупки технології, оскільки аналіз Cyber Quant показав її неефективність у їхньому конкретному середовищі. Це дозволило уникнути зайвих витрат у розмірі 20 000 доларів лише за перший рік. Хоча ця сума може здаватися

невеликою порівняно з іншими статтями, вона символізує якісний зсув у мисленні: перехід від витрат на «гарантовану безпеку» до інвестицій у підтверджену ефективність, що є ознакою зрілості кіберстратегії.

Окрім прямих фінансових вигод, дослідження Forrester виокремлює важливі неформалізовані переваги, які, однак, мають критичне значення для довгострокового успіху бізнесу. Перш за все, це покращення комунікації між керівництвом та технічними спеціалістами. Мова фінансових втрат є універсальною для ради директорів. Cyber Quant надає змогу перекласти технічні дефіцити контролів на мову потенційного збитку від простоїв систем, втрати даних або репутаційних ризиків. Це кардинально змінює якість діалогу: замість суперечок щодо технічних налаштувань, обговорення фокусується на бізнес-пріоритетах. Вище керівництво починає розуміти необхідність інвестицій не як «примху спеціалістів», а як об'єктивну потребу для захисту виручки та стабільності компанії.

По-друге, це покращення пріоритезації контролів. Маючи об'єктивну картину ризиків у розрізі бізнес-одиниць та регіонів, команда безпеки може спрямовувати ресурси на найбільш критичні вразливості, ігноруючи менш суттєві, що підвищує ефективність захисних заходів.

Структура витрат на впровадження платформи є прозорою та прогнозованою. Дослідження враховує ліцензійні витрати, які для організації складають початковий внесок у розмірі 30 000 доларів за первинну оцінку та щорічну плату за ліцензію у 75 000 доларів. Після коригування на ризики, загальна трирічна вартість володіння оцінюється в 227 000 доларів США. Важливо підкреслити, що це модельна оцінка, а фактична ціна залежить від масштабу організації, кількості користувачів та специфіки ліцензійної угоди з Mastercard. Проте, з огляду на значний обсяг економії та підвищення ефективності, інвестиції виглядають більш ніж виправданими.

Висновки:

- **Автоматизація оцінки кібер-ризиків забезпечує високу рентабельність інвестицій.** Впровадження структурованих платформ для кількісної оцінки ризиків демонструє ROI понад 100% з окупністю менш ніж за пів року завдяки скороченню ручної праці та оптимізації процесів.
- **Ручні методи управління кібер-ризиками є прихованим джерелом збитків.** Робота з електронними таблицями та залучення зовнішніх консультантів призводять до втрати даних, дублювання зусиль і тривалих циклів оцінки, що створює ілюзію контролю замість реального управління загрозами.
- **Кількісне вираження ризику у фінансових термінах трансформує діалог з керівництвом.** Перехід від технічних звітів до моделювання потенційних збитків дозволяє узгоджувати пріоритети безпеки з бізнес-стратегією та отримувати обґрунтоване фінансування захисних заходів.
- **Об'єктивна оцінка ризиків запобігає неефективним капіталовкладенням у безпеку.** Можливість перевіряти реальний вплив запланованих технологічних рішень на загальний рівень ризику дозволяє уникати витрат на інструменти, які не відповідають актуальним загрозам та бізнес-контексту організації.

Підсумовуючи, варто зазначити, що Mastercard Cyber Quant є не просто програмним забезпеченням для управління ризиками, а прикладом комплексного рішення, яке змінює філософію кібербезпеки в організації. Воно усуває розрив між технічними деталями та стратегічним баченням бізнесу, перетворюючи кіберризик на керований бізнес-процес.

Однак справжня цінність платформи розкривається у її здатності надавати керівництву впевненість у завтрашньому дні, обґрунтовувати рішення про виділення бюджетів та будувати стійку, адаптивну систему захисту, здатну протистояти викликам сучасного цифрового світу. Для компаній, які прагнуть не просто виживати, а процвітати в умовах постійно зростаючих кіберзагроз, впровадження подібних платформ стає не питанням вибору, а стратегічною необхідністю.

Інші новини

Глинозем для російських ракет: економічний парадокс європейських санкцій [11]

Розслідування, опубліковане у березні 2026 року консорціумом журналістів OCCRP та його партнерами, викрило потенційно незручний зв'язок між найбільшим у Європі заводом з виробництва глинозему в Ірландії та російською військовою промисловістю. Це розслідування спричинило хвилю політичного резонансу, змусивши уряд Ірландії провести власне розслідування, результати якого, хоч і не були оприлюднені, потрапили до рук журналістів та викликали ще більше запитань, ніж відповідей.

Ситуація навколо заводу Aughinish Alumina стала яскравим прикладом складнощів, з якими стикається Європа, намагаючись збалансувати економічні інтереси, санкційну політику та моральні зобов'язання перед Україною.

У центрі скандалу опинився глинозем – білий порошок, який є ключовою сировиною для виробництва алюмінію. Цей матеріал, визнаний Європейським Союзом "критично важливою сировиною", має стратегічне значення для багатьох галузей, від енергетики до оборонної промисловості. Журналісти з’ясували, що продукція ірландського заводу Aughinish, що належить російському алюмінієвому гіганту Rusal, після потрапляння до росії опосередковано могла підживлювати російський військово-промисловий комплекс. Хоча відстежити шлях кожної конкретної партії глинозему після її переробки на алюміній виявилося неможливим через змішування сировини з різних джерел, журналісти отримали доступ до даних про транзакції, які проливають світло на цей ланцюг постачань.

Згідно з цими даними, російські алюмінієві заводи, які імпортували глинозем з Ірландії, продавали частину своєї готової продукції московському трейдеру Aluminum Sales Company (ASK). У період з початку повномасштабного вторгнення росії в Україну у 2022 році до квітня 2025 року ASK придбав у цих заводів алюміній на суму понад 640 мільйонів доларів. Своєю чергою, клієнтами ASK були 143 російські компанії, які виконували державні оборонні замовлення. Щонайменше 63 з цих компаній перебувають під санкціями Європейського Союзу, і 53 з них безпосередньо виробляють зброю, яка активно використовується росією у війні проти України. Серед них такі відомі підприємства, як "КамАЗ", Казанський вертолітний завод, "Курганмашзавод" та багато інших, що входять до ядра російського ВПК. Таким чином, розслідування продемонструвало, що європейська сировина, хоч і не безпосередньо, а через складну мережу посередників, сприяла виробництву озброєнь, які вбивають українців.

Реакція європейських політиків не змусила себе довго чекати. Лунали заклики запровадити повну заборону на експорт глинозему до росії, щоб завдати чергового удару по російській воєнній економіці. У липні 2026 року Європейський Парламент переважною більшістю голосів ухвалив необов'язкову резолюцію із закликом до такого кроку. Однак, що показово, Рада Європейського Союзу не включила глинозем до нового пакету санкцій, ухваленого того ж місяця, що свідчить про глибокі розбіжності та економічні вагання всередині блоку. Уряд Ірландії, зі свого боку, пообіцяв провести ретельне розслідування, і вже наприкінці липня оголосив, що його результати передано до Європейської комісії. Однак, як виявилося, це розслідування, проведене Департаментом підприємництва, туризму та зайнятості (DETE), викликало більше критики, ніж довіри.

Згідно з текстом, отриманим The Irish Times, ірландський урядовий звіт містить суперечливі висновки. З одного боку, в ньому стверджується, що "не було виявлено достатніх доказів", аби встановити, що глинозем з Aughinish використовується російськими військовими. Основою для такого висновку стала гарантія, надана заводом. Цю гарантію, підписану генеральним директором Rusal через два тижні після публікації розслідування OCCRP, було надано

[11] https://www.occrp.org/en/feature/faq-what-to-know-about-irelands-probe-into-our-reporting-on-its-alumina-exports-to-russia

ірландській владі. У ній стверджувалося, що жоден глинозем не використовується у військових цілях і що він використовується виключно для виробництва алюмінію на експорт. Також було надано документацію про те, що глинозем переробляється на окремих потужностях, призначених суто для експортного ринку. Щоб підкріпити ці запевнення, Rusal, за повідомленнями, найняв швейцарську інспекційну компанію для проведення незалежних аудитів на своїх російських заводах.

Проте звіт DETE містить і суттєві застереження. У ньому зазначено, що уряд не мав доступу до тих самих даних про транзакції, на яких ґрунтувалося розслідування OCCRP, а також не зміг отримати детальну інформацію про торгівлю компанії ASK. Без цих даних, як зазначено у звіті, не було "доказів, на основі яких Департамент міг би визначити, чи закуповує ASK матеріали, включно з алюмінієм, для військових підрядників, і якщо так, чи можна ці матеріали простежити до Aughinish". Визнаючи, що потрапляння глинозему до військового ланцюга постачань росії могло б становити порушення санкцій ЄС, звіт також наголошує на "відсутності перевірених внутрішніх торговельних даних у росії", що унеможливлює проведення повноцінного розслідування. Більше того, у звіті зазначається, що надані Rusal документи щодо кінцевих користувачів "не можуть бути задовільно перевірені або проаналізовані". Ця суперечливість – водночас і висновок про відсутність доказів, і визнання неможливості їх отримати та перевірити – викликала найбільше нарікань.

Найбільш спірним моментом є твердження Aughinish про те, що весь глинозем з Ірландії переробляється на алюміній виключно для експорту. Для цього російські заводи мали б підтримувати повністю окрему інфраструктуру, починаючи з величезних складів для зберігання та змішування сировини. Жодних доказів існування такого роздільного виробництва ні Aughinish, ні Rusal не надали. Більше того, витоки даних, якими володіє OCCRP, свідчать, що у 2025 році 27% алюмінію, виробленого на Красноярському заводі – одному з найбільших імпортерів ірландського глинозему, – було призначено для внутрішнього російського ринку. Цей факт безпосередньо суперечить заяві керівництва заводу.

Чимало критиків вказали на те, що урядова доповідь фактично відмовилася розглядати ключові докази, натомість покладаючись на гарантії, отримані від зацікавленої сторони. Міністр підприємництва Пітер Берк виправдовував рішення не публікувати звіт "комерційною чутливістю" та "юридичними причинами". Однак посольство України в Ірландії та уповноважений президента України з питань санкційної політики Владислав Власюк рішуче закликали оприлюднити результати, наголошуючи, що суспільний інтерес не дозволяє приховувати будь-які аспекти цього розслідування. Редакційна стаття The Irish Times підкреслила, що "розслідування, яке відмовляється вивчати докази, для перевірки яких воно було створене, не може стверджувати, що зняло з когось звинувачення". Експерти, зокрема професор Дублінського міського університету Доннаха О'Бічейн, звинуватили уряд у тому, що він діє як адвокат Rusal, а не як неупереджений слідчий.

Ситуація навколо Aughinish є лише верхівкою айсберга. Павло Шкуренко, дослідник санкцій у Київській школі економіки, зазначає, що проблема полягає не в пошуку "ірландських атомів у російській зброї", а в загальній структурній залежності Європи від російського ринку в алюмінієвому секторі. Він наголошує на необхідності "декаплінгу" – створення власних ринків для глинозему та його переробки в межах ЄС.

Подальший розвиток подій залежатиме від Європейської комісії, яка має вивчити звіт Ірландії та ухвалити рішення про можливе запровадження санкцій. Водночас, окреме розслідування шведських податкових органів щодо заводу Kubal, який також належить Rusal та імпортує глинозем з Aughinish, встановило, що компанія фактично контролюється підсанкційним російським олігархом Олегом Дерипаскою. Це призвело до замороження активів Rusal у Швеції, що створює додатковий тиск на компанію та може спонукати ЄС до більш жорстких дій.

Таким чином, історія з ірландським глиноземом стала не лише локальним скандалом, а й каталізатором для ширшої дискусії про ефективність європейських санкцій та межі економічного прагматизму у протистоянні з агресором.

Феномен «зворотньої» міграції: як Ла-Манш перетворюється на дзеркало міграційної політики [12]

Ситуація, що склалася навколо контрабанди людей через протоку Ла-Манш, протягом останніх років зазнала парадигмальних змін, які кардинально змінюють усталені уявлення про міграційні маршрути та механізми протидії нелегальній міграції.

Якщо протягом тривалого часу Ла-Манш розглядався виключно як бар'єр, який долають з європейського континенту до Великої Британії, то сьогодні ми стаємо свідками стрімкого зростання протилежного тренду – переправлення мігрантів з британських островів до континентальної Європи. Цей феномен, який отримав назву «зворотного» або «реверсивного» контрабандного трафіку, є не випадковим збоєм у системі, а прямим наслідком розбіжностей у візовій та імміграційній політиці між Сполученим Королівством та країнами Шенгенської зони, посилених наслідками Brexit та внутрішніми соціально-економічними чинниками, що діють у самій Великій Британії.

Матеріали, що лягли в основу цього аналізу, свідчать про системний характер явища. Показовою є справа, зафіксована ще в лютому 2023 року, коли французькі прикордонники в Кале виявили 58 осіб, захованих у вантажівці, яка прибула з Великої Британії. Це були громадяни Марокко, Тунісу та Алжиру, які на той момент вже перебували на території Сполученого Королівства на законних підставах за туристичними візами. Цей епізод виявився не поодиноким випадком, а лише верхівкою айсберга.

Розслідування викрило масштабну діяльність злочинних мереж, які організовували десятки таких рейсів у зворотному напрямку, стягуючи з мігрантів значні суми – близько 1200 фунтів стерлінгів з особи, що забезпечувало організаторам мільйонні прибутки. Так, Маджид Белабес, організатор алжирського походження, що базувався в Лондоні, отримав десять років тюремного ув'язнення за організацію 26 нелегальних рейсів, тоді як його спільник Азізе Бенаніба, який очолював паралельну мережу, забезпечив понад 20 перевезень з Дувра в Кале, заробивши близько 500 тисяч фунтів, а його угруповання, включаючи шістьох спільників, сукупно отримало 69 років позбавлення волі. Особливо жахливим є той факт, що під час одного з перевезень група, серед якої були діти віком від п'яти років, опинилася в герметичному рефрижераторі, що через затримку в Дуврі створило пряму загрозу їхньому життю.

Останні події, задокументовані у 2025 та 2026 роках, засвідчують, що цей процес не лише триває, але й набуває нових форм. Затримання в Дуврі двох румунських водіїв вантажівок, які перевозили 49 осіб, переважно громадян Бангладешу, а також операція з перехоплення 23 чоловіків, яких на таксі доставили з Лондона до терміналу порома, демонструють, що «зворотний» трафік став усталеним кримінальним бізнесом.

Примітно, що в усіх випадках ці мігранти мали законний статус у Великій Британії і згодом були звільнені, що підкреслює парадоксальність ситуації: люди, які вже отримали право перебувати в країні, свідомо обирають нелегальний спосіб залишити її, вдаючись до послуг контрабандистів.

Аналіз структури цих нових злочинних мереж виявляє їхню фундаментальну відмінність від усталених каналів контрабанди у напрямку з континенту до Великої Британії. Якщо на французькому узбережжі за десятиліття поліцейської протидії сформувалися високоорганізовані курдські угруповання, які монополізували контроль над запуском човнів і

[12] https://globalinitiative.net/analysis/migrants-reverse-smuggling-leave-uk/

жорстко конкурують за території, то ринок у Дуврі перебуває на ранній, «модульній» стадії розвитку. Він характеризується фрагментарністю, де різні функції – координація маршрутів, логістика, безпосереднє транспортування – виконуються різними, часто випадковими акторами: таксистами, водіями вантажівок, окремими організаторами з Алжиру, Румунії, Польщі, Литви та Південної Азії, які не утворюють єдиного центру управління.

Більше того, ця система є гнучкою – одні й ті самі водії та посередники залежно від попиту можуть перевозити людей як у Велику Британію, так і з неї, підлаштовуючись під кон'юнктуру. Цей неконсолідований ринок нагадує собою початковий етап формування контрабандного промислу, який у Кале спостерігався приблизно десять років тому, і він поки що не зазнав тих жорстких структурних змін, які відбуваються під впливом тривалого правового тиску.

Причини зростання «зворотної» контрабанди є багатошаровими та глибоко вкоріненими у політичних рішеннях останніх років. По-перше, ключову роль відіграє асиметрія у правилах легального в'їзду між Великою Британією та Шенгенською зоною. Після Brexit та посилення візової політики країнами Європейського Союзу, особливо Францією з вересня 2021 року, британська віза перестала бути автоматичним пропуском до континентальної Європи. Для багатьох національностей, зокрема з Північної Африки та Південної Азії, отримати туристичну чи навчальну візу до Сполученого Королівства стало легше, ніж до країн Шенгену. Таким чином, Лондон перетворився на своєрідний «вхідний портал» до Європи: мігранти легально потрапляють до Британії, а потім, інколи протягом кількох днів, звертаються до контрабандистів, щоб перетнути Ла-Манш у зворотному напрямку, оскільки подальша легальна подорож для них уже неможлива. Це не просто прогалина в законі, а структурна вада, яку неможливо усунути стандартними прикордонними заходами.

По-друге, потужним чинником виштовхування є сама імміграційна політика Великої Британії. Затяжні терміни розгляду заявок на надання притулку та інших імміграційних статусів, ризик опинитися без житла через обмеження системи підтримки, а також постійний тиск з боку імміграційних органів створюють для багатьох шукачів захисту та мігрантів нестерпні умови. За даними Міністерства внутрішніх справ, кількість випадків «організованої імміграційної злочинності» зросла майже на 50% за рік до березня 2026-го, що свідчить про активізацію як злочинців, так і правоохоронців. Водночас припинення публікації статистики про виїзд після 2020 року та неможливість оцінити чисельність осіб, які порушили візовий режим, робить цю категорію населення фактично «невидимою» для політиків, хоча саме вона має найсильніші стимули до виїзду та найбільшу поінформованість про послуги контрабандистів.

Третім важливим аспектом, який чітко проявляється в матеріалах, є здатність злочинних мереж миттєво реагувати на політичні сигнали та використовувати їх для створення штучного попиту. Яскравим прикладом є іспанська програма, запроваджена у квітні 2026 року, яка пропонувала право на проживання та роботу нелегальним мігрантам. Контрабандисти негайно розгорнули кампанію з реклами «переїзду до Іспанії через Британію», встановлюючи ціни від 980 до 1450 фунтів і націлюючись на студентів з Індійського регіону, які прострочили візи, хоча насправді умови програми вимагали доведеного перебування в Іспанії до 31 грудня 2025 року, що робило всіх перевезених протягом 2026 року автоматично невідповідними для участі. Цей випадок демонструє, що контрабанда людей – це не пасивне обслуговування існуючих міграційних потоків, а активна діяльність з формування ринку, де політичні новини стають маркетинговим інструментом, а мігранти вводяться в оману заради прибутку.

Перед політиками та правоохоронними органами постає складне завдання. Сьогодні прикордонні переходи з обох боків Ла-Маншу, особливо в Дуврі, залишаються слабко пристосованими до контролю виїзного трафіку. Законодавство надає обмежені підстави для втручання, коли люди намагаються покинути країну, навіть якщо є підозри, що вони виїжджають нелегально. Таким чином, більша частина ринку «зворотної» контрабанди є не стільки результатом ухилення від прикордонного контролю, скільки логічним наслідком конструкції самої імміграційної системи.

Вирішення проблеми неможливе виключно через посилення перевірок у Дуврі – це вимагає скоординованої політики між Великою Британією та Європейським Союзом, яка б усунула самі правові та процедурні розриви, якими користуються злочинці.

У ширшому сенсі, ситуація, що склалася, містить тривожні аналогії з минулим. Як колись Кале, який був відносно відкритим ринком для контрабанди, згодом трансформувався у зону, контрольовану невеликою кількістю потужних і безжальних угруповань, так само й Дувр зараз стоїть на порозі подібної еволюції. Якщо британська влада застосує до цього фрагментованого середовища жорсткий і тривалий тиск, то, ймовірно, це призведе не до зникнення контрабанди, а до її консолідації навколо найбільш стійких, добре фінансованих і готових до застосування насильства злочинних груп. Це означатиме, що замість розрізнених таксистів і випадкових водіїв виникнуть організовані синдикати, подібні до тих, що діють у Кале, зробивши проблему ще важчою для контролю.

Отже, визнання того факту, що контрабанда через Ла-Манш більше не є одностороннім явищем, а являє собою потік, який живиться неузгодженістю двох правових систем, є першим і необхідним кроком на шляху до вироблення адекватної, скоординованої та довгострокової відповіді як з боку Лондона, так і з боку Брюсселя. Ігнорування цієї реальності лише посилить хаос, збагатить злочинні мережі та наражатиме на смертельну небезпеку вразливих людей, які, з огляду на обставини, змушені обирати нелегальні шляхи пересування Європою.

Ваша думка важлива!

1. Чи потрібна Україні єдина наглядова платформа у сфері фінансового моніторингу, спільна для Держфінмоніторингу та секторальних регуляторів, чи достатньо міжвідомчого обміну даними?
2. Який рівень зрілості за шкалою чотирьох поколінь має інформаційна інфраструктура наглядових органів України у сфері ПВК/ФТ і що є найближчим досяжним кроком?
3. Які ризики для України можуть виникати через використання компаній із непрозорою структурою власності у схемах закупівлі товарів подвійного використання, і чи достатньо чинних механізмів перевірки бенефіціарних власників для їх виявлення?
4. Як в умовах війни та масової внутрішньої міграції, які суттєво збільшують вразливість населення до вживання заборонених речовин, Україна може вибудувати доступну систему комплексної допомоги, орієнтовану на зниження шкоди, психосоціальну підтримку та реінтеграцію?
5. Наскільки доцільним є створення в Україні спеціального податкового режиму для операцій з криптоактивами – чи має він будуватися на спрощенні чинних норм, чи потребує розробки принципово нового підходу?

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-2026-34

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.

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