Методологічний бюлетень

Серійний номер: МінФін-AML-2025-27

Липень 2025

“Секрет успіху в тому, щоб діяти!”

Данте Аліг’єрі

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.

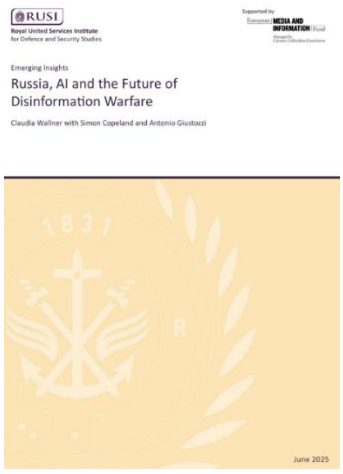
Містить актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

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.

АУДІОПЕРЕКАЗ

Звіти міжнародних організацій та окремих юрисдикцій

Інформаційна зброя нового покоління: як рф використовує AI для глобальної дезінформації [1]



Дослідження, підготовлене Королівським інститутом об’єднаних служб (RUSI) у червні 2025 року, присвячене аналізу того, як російські державні та проросійські діячі сприймають, використовують і інтегрують штучний інтелект (AI) у свої операції з ведення інформаційної війни та кампанії з дезінформації. Це дослідження є унікальним за фокусом на внутрішню комунікацію серед російських впливових спільнот і демонструє не лише практичне використання AI, але й те, як ця технологія стає інструментом побудови ідеології та стратегічного мислення.

У центрі дослідження знаходиться теза про те, що AI вже зараз перестав бути виключно інструментом майбутнього і активно використовується як ключовий компонент в інформаційних операціях росії. Автори зазначають, що російська стратегічна культура традиційно розглядає інформаційне протиборство як рівнозначне до звичайних та навіть ядерних форм збройного

[1] https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf

конфлікту. Інформаційна сфера в російській військово-політичній доктрині є критично важливим театром бойових дій. Відповідно, розвиток та застосування технологій AI стало логічним продовженням цього підходу, що поєднує класичні методи пропаганди, психологічного впливу та кібероперацій із новими цифровими інструментами.

Дослідження показує, що російська інформаційно-пропагандистська екосистема є глибоко фрагментованою і складається не лише з державних структур та спецслужб, але й з розгалуженої мережі проксі-діячів: хактивістських угруповань, афілійованих медіа, блогерів, онлайн-спільнот та напівофіційних каналів, серед яких Telegram є найпоширенішим. Ці діячі одночасно є як інструментами державної політики, так і відносно автономними суб'єктами, що часто діють у межах власних інтересів, проте в загальному руслі кремлівських наративів.

AI у цьому середовищі виступає багатофункціональним інструментом. По-перше, він використовується для автоматизації створення та розповсюдження контенту: фейкових новин, дезінформаційних відео, діпфейків, генерації фальшивих акаунтів та організації псевдодискусій. Прикладом цього стала операція «DoppelGänger», яка через генеровані за допомогою AI статті та фейкові новинні сайти імітувала легітимні західні ЗМІ, поширюючи прокремлівські меседжі серед європейської аудиторії. По-друге, AI активно застосовується у кіберопераціях – для посилення атак на критичну інфраструктуру, здійснення DDoS-атак, фішингових кампаній і проведення інформаційно-психологічних спецоперацій.

Особливу увагу дослідники приділяють тому, як російські діячі одночасно сприймають AI як стратегічний актив і джерело загроз. Внутрішній дискурс у проросійських каналах наповнений як гордістю за досягнення у використанні AI, так і глибокою тривогою щодо того, що західні країни, маючи технологічну перевагу, використовують аналогічні інструменти для дестабілізації самої росії. Особливо активно артикуються побоювання щодо потенційного використання західних моделей AI для впливу на громадську думку в росії, створення фальшивих аудіо та відеоматеріалів із компрометуючим змістом, а також загального когнітивного підриву російського суспільства. У цьому контексті Україна подається як полігон, на якому Захід нібито тестує свої інструменти інформаційної війни за допомогою AI, спрямовані проти росії.

Незважаючи на офіційний курс Кремля на цифровий суверенітет, у середовищі проросійських діячів спостерігається значне розчарування якістю вітчизняних AI-продуктів. Системи Sber GigaChat та YandexGPT регулярно критикуються за низьку якість відповідей, цензуру, небажання підтверджувати пропагандистські наративи, зокрема у питаннях територіальної належності Криму та інших окупованих регіонів України. Ці продукти звинувачують у наявності «ліберального» або «західного» впливу, а іноді навіть у прямій роботі на іноземні розвідки. Водночас іронічно, що, попри декларації про необхідність відмови від західних інструментів, більшість російських користувачів і надалі активно використовують саме західні платформи, такі як ChatGPT, Midjourney, Stable Diffusion та інші, визнаючи їхню технічну перевагу.

Кейси, розглянуті у дослідженні, особливо висвітлюють діяльність групи Вагнера та хактивістських угруповань, таких як NoName057(16), Cyber Army of Russia та інших. Вагнерівські канали демонструють високий рівень інституціоналізації підходу до інформаційної війни, включно з розробкою навчальних матеріалів для підготовки кадрів, використанням AI для моделювання інформаційних кампаній, управління бот-мережами та створення дипфейків. Водночас ці канали підкреслюють свою нібито вищу професійну якість і стратегічну компетентність у порівнянні з іншими російськими структурами, які критикуються за дилетантський підхід і неефективність. Своєю чергою, хактивістські групи використовують AI не лише для генерації контенту, але й для технічної підтримки кібератак, розробки інструментів автоматизації зламів, проведення DDoS-атак і репутаційного саботажу. Вони активно обмінюються технічними гайдами, інструкціями, базами даних і навіть створюють спеціалізовані продукти на основі AI для потреб кіберзлочинної діяльності.

Цінним аспектом дослідження є аналіз того, як самі ці групи рефлексують ризики, пов'язані з використанням AI. Вони визнають небезпеки діпфейків, що використовуються проти них, бояться можливості компрометації своїх лідерів через фальсифіковані аудіо чи відео, обговорюють загрози автономних систем на базі AI, які у майбутньому можуть вийти з-під контролю. Це створює унікальний феномен подвійної ролі AI як одночасно найпотужнішого ресурсу в сучасній гібридній війні та джерела екзистенційної загрози для самих його користувачів.

Дослідження підкреслює, що AI вже не просто інструмент для масштабування традиційних дезінформаційних кампаній, а фундаментально змінює механіку планування та реалізації інформаційних операцій. Водночас він посилює внутрішні суперечності в екосистемі російської пропаганди, де намагання досягти цифрового суверенітету вступає у конфлікт із технічною залежністю від західних технологій. Цей парадокс — ключовий фактор, який визначатиме подальший розвиток російських операцій інформаційного впливу, а також ефективність міжнародних стратегій протидії їм.

Висновки:

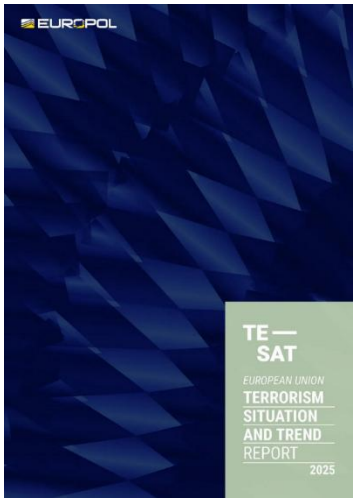
- **AI стає ядром російських інформаційних операцій:** Генеративний AI активно використовується для створення фейкового контенту, діпфейків, маніпулятивних текстів, бот-мереж і масованого поширення дезінформації. Окремі канали навіть формують спільноти спеціалістів із AI для участі в інформаційних кампаніях.
- **Високий рівень занепокоєння через технологічну залежність:** Російські діячі висловлюють глибоке невдоволення якістю власних AI-інструментів (Sber GigaChat, YandexGPT) та їх «недостатньою патріотичністю». Водночас вони змушені використовувати західні AI-сервіси, що суперечить політиці цифрового суверенітету.
- **AI використовується не лише для атаки, а й для захисту:** Поширені кампанії з медіаграмотності серед проросійських аудиторій із закликами ідентифікувати західні діпфейки, фейки та інформаційно-психологічні операції.
- **Децентралізована структура загрожує глобальній безпеці:** Поєднання державних структур, приватних військових компаній і напівсамостійних хактивістських угруповань, які активно використовують AI, створює стійку екосистему, здатну до автономної ескалації інформаційних атак у глобальному масштабі.

Терористичні загрози для Європи у 2025: тенденції, виклики, нові форми радикалізації [2]

Звіт є фундаментальним аналітичним документом, що надає комплексний огляд ситуації з тероризмом і насильницьким екстремізмом у країнах Європейського Союзу за 2024 рік. У документі підкреслюється, що терористична загроза в Європі залишається складною, багатогранною та динамічною. Вона безпосередньо пов'язана з глобальними геополітичними процесами, цифровою трансформацією суспільства і стрімким розвитком технологій. 2024 рік був роком, коли тероризм у ЄС посилився через вплив таких ключових факторів, як війна Ізраїлю з ХАМАС після атаки 7 жовтня 2023 року, триваюча російська агресія проти України та крах режиму Башара Асада в Сирії. Ці події не лише підігріли ідеологічні конфлікти в різних

[2] https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf

середовищах, але й стали каталізатором поширення радикальних наративів, радикалізації і мобілізації як у цифровому просторі, так і в реальному житті.



Загалом у 2024 році в ЄС було зафіксовано 58 терористичних атак, з яких 34 завершені, 5 невдалі та 19 попереджені. Найбільше атак зафіксовано в Італії (20) та Франції (14). Найнебезпечнішими залишаються джихадистські атаки — їхня кількість зросла з 14 у 2023 році до 24 у 2024-му. Вони виявилися найбільш летальними — 5 загиблих і 18 поранених. Значна частина атак скоєна одинаками, які не є формально пов'язаними з терористичними організаціями, однак діють під впливом радикальних ідеологій і онлайн-пропаганди. Поряд з цим суттєвим викликом стала надзвичайно висока частка залучення молоді та неповнолітніх до терористичної діяльності. З 449 затриманих за тероризм 133 були віком від 12 до 20 років, а наймолодшому затриманому було лише 12 років. Радикалізація цієї категорії відбувається майже виключно в цифровому просторі, де діти та молодь стають жертвами пропаганди, маніпуляцій та психологічного тиску з боку терористичних та екстремістських спільнот.

Феномен онлайн-радикалізації набув абсолютно нового виміру. Вперше фіксується масштабне злиття ідеологій: джихадизм, ультраправий екстремізм, прискоренство, сатанізм, окультизм і анархізм інтегруються у гібридні спільноти. Особливо небезпечним є розвиток так званих культових онлайн-мереж «764» або «Com», які залучають дітей віком від 8 років до виконання жорстоких дій — від самопошкоджень до вбивств, які потім записуються та поширюються всередині цих спільнот. Учасники цих мереж спеціалізуються на вербуванні вразливих осіб, зокрема дітей, використовуючи шантаж, погрози, залякування та обіцянки прийняття в «спільноту». Ці угруповання часто не мають чіткої ідеології, проте використовують елементи з джихадистської пропаганди, праворадикальних наративів, культу насильства та хаосу.

Геополітичні кризи суттєво підсилили дестабілізаційні фактори в Європі. Війна в Газі стала тригером для сплеску антисемітизму та пропаганди насильства серед усіх ідеологічних течій — від джихадистів до ліворадикалів і праворадикальних екстремістів. Війна росії проти України посприяла радикалізації обох сторін конфлікту — окремі праворадикальні бойовики долучаються як до українських, так і до російських формувань. Це породжує побоювання, що по завершенню війни ці особи з бойовим досвідом і психологічними травмами становитимуть підвищену загрозу для безпеки ЄС. Окремо наголошується, що війна створила сприятливі умови для розповсюдження нелегальної зброї, яка може опинитися в руках терористичних або кримінальних угруповань у Європі.

Колапс режиму Башара Асада в Сирії та встановлення контролю з боку угруповання Hay'at Tahrir al-Sham (HTS) викликає серйозні занепокоєння з точки зору регіональної та глобальної безпеки. Ситуація в Сирії підвищує ризик втечі з таборів для переміщених осіб бойовиків ІДІЛ, у тому числі громадян країн ЄС, що може призвести до нової хвилі терористичної активності в Європі. ІДІЛ продовжує зміцнювати свої позиції в Сирії та активно розширює свою присутність у регіонах Африки (Сахель, Мозамбік, Сомалі) та Афганістані, що створює загрозу нових хвиль терористичних атак проти європейських цілей.

Особливої уваги в звіті приділено технологічному аспекту тероризму. Активно використовуються генеративний штучний інтелект, діпфейки, моделі великих мовних систем (LLM), алгоритми маніпуляції, що дозволяють терористам створювати пропаганду високого рівня, уникати модерації контенту та прискорювати радикалізацію. Терористичні угруповання застосовують криптовалюти, NFT і цифрові версії системи хавала для забезпечення анонімного фінансування. Масштабно застосовуються дрони, 3D-друк зброї, моделювання атак у

віртуальних середовищах (у тому числі в метавсесвітах і на ігрових платформах), що дозволяє готувати виконавців атак без необхідності фізичної присутності на навчальних базах.

Зафіксовано збільшення арештів за терористичну діяльність: 449 осіб у 20 країнах ЄС, найбільше у Іспанії, Франції, Італії та Німеччині. Більшість арештів пов'язана з джихадизмом (289), далі йдуть правий тероризм (47), лівий і анархістський (28) та етнонаціоналістичний (27). Особливо тривожним є подвоєння кількості арештів за інші або неідентифіковані форми тероризму — 58 випадків. У судовій площині у 2024 році було винесено 485 рішень у справах про тероризм, з яких 427 — обвинувальні вироки. Середній термін ув'язнення — 6 років, але в ряді випадків застосовувалися довічні строки. Судові рішення охоплюють увесь спектр злочинів: від участі у терористичних організаціях до фінансування тероризму, пропаганди, планування та здійснення нападів, вербування, навчання і виготовлення вибухових пристроїв.

У звіті підкреслюється, що радикалізація в місцях позбавлення волі залишається серйозною проблемою для країн ЄС, як і повернення бойовиків з гарячих точок. Водночас дедалі більшою загрозою є саморадикалізовані одинаки, які не мають прямого зв'язку з терористичними структурами, але діють під впливом онлайн-пропаганди.

Ситуація з тероризмом у ЄС стає дедалі складнішою через злиття ідеологій, розмиття меж між терористичними та кримінальними групами, активне використання новітніх технологій і постійне залучення нових груп ризику, особливо молоді. Це потребує від правоохоронних і розвідувальних органів не лише зміни традиційних підходів, а й впровадження технологічно просунутих аналітичних інструментів, міжвідомчої координації, а також посилення міжнародної співпраці з акцентом на протидію цифровим формам радикалізації, терористичному фінансуванню та онлайн-пропаганді.

Висновки:

- **Зростання участі неповнолітніх і молоді в терористичній діяльності —** це виклик, який потребує негайного реагування шляхом посилення онлайн-моніторингу, програм профілактики та психосоціальної підтримки вразливих категорій населення, зокрема в шкільному середовищі.
- **Гібридизація терористичних ідеологій —** джихадизм, правий екстремізм, анархізм і окультизм зливаються в нові небезпечні форми радикалізації. Потрібно розробити оновлені методології оцінки ризиків та реагування, які враховують мультиідеологічну природу сучасного тероризму.
- **Активне використання новітніх технологій (AI, криптовалюти, метавсесвіт) —** створює новий клас загроз, які виходять за рамки класичних інструментів правоохоронних органів і вимагають інвестицій у кіберрозвідку, фінансову розвідку та розробку інноваційних контрзаходів.
- **Вплив міжнародних конфліктів (Газа, Сирія, війна рф проти України)** посилює радикалізацію, зростання антисемітизму, антизахідних настроїв і створює ризики повернення бойовиків та розповсюдження нелегальної зброї на території ЄС.

Секторальна оцінка ризиків сектору торгівлі предметами розкоші в Румунії [3]

Звіт є комплексним аналітичним дослідженням, мета якого — ідентифікувати, проаналізувати та зрозуміти специфічні ризики відмивання грошей та фінансування тероризму (ВК/ФТ), притаманні двом ключовим сегментам ринку предметів розкоші: торгівлі творами мистецтва та культурними цінностями, а також торгівлі дорогоцінними металами та камінням. Документ структуровано на три основні частини: вступна частина з методологією, та два великі розділи,

[3] https://www.onpcsb.ro/uploads/articole/attachments/68529d3fd49a1940566768.pdf

присвячені кожному сектору окремо. Методологія оцінки базується на міжнародних стандартах FATF, національному та європейському законодавстві, а також на даних, отриманих через анкетування суб'єктів звітності, аналізу статистичної інформації та звітів міжнародних організацій, таких як Europol, WCO, UNODC.

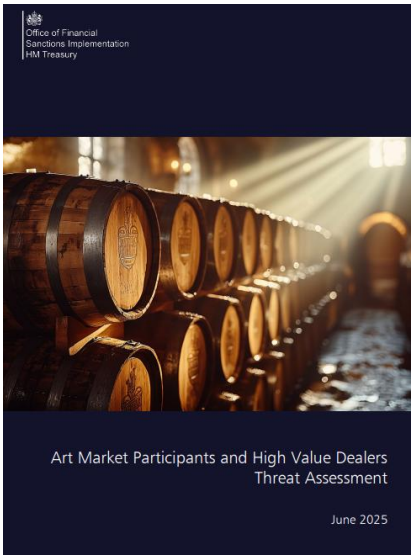
Перший аналітичний розділ присвячений сектору торгівлі творами мистецтва та рухомими культурними цінностями. Звіт підкреслює, що цей ринок є вразливим через низку притаманних йому характеристик: суб'єктивність оцінки вартості активів, конфіденційність транзакцій, висока мобільність предметів мистецтва та можливість використання готівкових розрахунків. У звіті детально розглядаються глобальні ризики, зокрема використання офшорних юрисдикцій та вільних зон для зберігання та продажу творів мистецтва без належного контролю. На національному рівні ризик сектору оцінено як "середній". Це обґрунтовано тим, що, попри зростання ринку та його інтеграцію у світову економіку (імпорт та експорт культурних товарів зростає), більшість транзакцій у Румунії мають відносно невеликі обсяги, а складні схеми з використанням компаній-прокладок чи юрисдикцій з високим ризиком не є поширеними. Проте, звіт виявляє суттєві прогалини у комплаєнс-культурі: неадекватні заходи KYC, слабка перевірка джерел походження коштів та статусу публічних діячів (PEP), а також повна відсутність звітів про підозрілі транзакції за період 2021-2024 років, що свідчить про низьку обізнаність учасників ринку щодо їхніх обов'язків у сфері ПВК/ФТ. У звіті наведено конкретні типології відмивання грошей, такі як заниження вартості творів мистецтва при перетині кордону, використання NFT для фіктивної торгівлі (wash-trading) та застосування фальшивих інвойсів для легалізації коштів.

Висновки:

- **Загальний рівень ризику обох секторів (мистецтво та дорогоцінні метали) оцінено як "середній".** Це означає, що, хоча системної загрози для фінансової системи Румунії наразі немає, існують значні вразливості, які можуть бути використані злочинцями. Для сектору мистецтва основна проблема — низька комплаєнс-культура та відсутність спеціального регулювання, тоді як для дорогоцінних металів ризики більше пов'язані з транскордонними операціями та високою ліквідністю самих активів.
- **Виявлено критичну прогалину у звітуванні про підозрілі транзакції.** За період з 2021 по 2024 рік від суб'єктів ринку мистецтва не надійшло жодного звіту про підозрілі транзакції. Це свідчить або про нерозуміння учасниками ринку своїх обов'язків, або про неефективність внутрішніх систем контролю. Рекомендовано терміново посилити навчання, нагляд та розробити чіткі індикатори підозрілої діяльності для цього сектору.
- **Необхідність створення окремого коду КВЕД (CAEN) для торговців мистецтвом є нагальною.** Наразі ці суб'єкти реєструються під загальними кодами, що унеможливлює точну ідентифікацію, оцінку розміру ринку та ефективний нагляд. Створення спеціального коду дозволить регулятору чітко визначити коло підзвітних осіб та застосовувати до них ризик-орієнтований підхід.
- **Транскордонні операції та міжнародні санкції становлять основну загрозу.** Звіт акцентує увагу на ризиках, пов'язаних з імпортом/експортом предметів розкоші, особливо у контексті співпраці з юрисдикціями зі слабким режимом ПВК/ФТ та ризиком обходу санкцій (зокрема, щодо російських алмазів). Учасникам ринку рекомендовано посилити перевірку географічного походження клієнтів, джерел їхніх статків та дотримуватися санкційних списків.

Другий аналітичний розділ зосереджений на секторі торгівлі дорогоцінними металами та камінням. Цей сектор, на відміну від ринку мистецтва, є більш регульованим у Румунії: діяльність вимагає отримання авторизації та щорічної візи від Національного агентства із захисту прав споживачів (ANPC), що включає перевірку на наявність судимостей. Сектор має значну економічну вагу, з імпортом на суму 470 мільйонів доларів та експортом на 351 мільйон доларів у 2023 році, де ключовим торговим партнером є Італія. Незважаючи на регулювання, ризики залишаються значними. Звіт визначає їхній рівень як "середній". Основні вразливості включають високу ліквідність та портативність активів (зокрема, золота та діамантів), можливість використання готівки (в межах встановлених лімітів), та складність відстеження походження каміння після його обробки та включення у ювелірні вироби. Особлива увага приділяється міжнародному контексту, зокрема Кімберлійському процесу сертифікації алмазів (у якому Румунія бере активну участь) та міжнародним санкціям проти російських алмазів, введеним G7, що створює ризики їх обходу. Аналіз клієнтської бази показав, що більшість клієнтів є румунськими фізичними особами, однак існують транзакції з високовартісними активами (понад 1 млн євро) з клієнтами з третіх країн, що створює підвищений географічний ризик. Звіт також наводить кейси, розслідувані правоохоронними органами, що демонструють використання коштовностей для відмивання доходів, отриманих від контрабанди, шахрайства та корупції.

Оцінка загрози для учасників арт-ринку та дилерів товарами високої вартості [4]



Цей документ є однією з серії галузевих оцінок, опублікованих OFSI, спрямованих на виявлення загроз дотриманню фінансових санкцій Сполученого Королівства та допомогу зацікавленим сторонам у розумінні та захисті від них, особливо після суттєвих змін у санкційному ландшафті, спричинених незаконним вторгненням росії в Україну у лютому 2022 року та подальшим запровадженням безпрецедентних фінансових санкцій. Основними суб'єктами цього оцінювання є учасники арт-ринку (AMPs) та дилери товарами високої вартості (HVDs), які з 14 травня 2025 року стали підзвітними суб'єктами та тепер підпадають під зобов'язання щодо звітування про фінансові санкції. AMPs визначаються як фірми або приватні підприємці, зареєстровані або зобов'язані зареєструватися в HMRC згідно з правилами боротьби з відмиванням грошей, які торгують або виступають посередниками у купівлі-продажу творів мистецтва вартістю від 10 000 євро, або зберігають твори мистецтва тієї ж вартості. HVDs – це фірми або приватні підприємці, які торгують товарами, отримуючи або здійснюючи готівкові платежі на суму не менше 10 000 євро за одну або кілька пов'язаних операцій, причому це стосується лише фізичної готівки. Обидва ці сектори працюють з дорогоцінними товарами (HVGs), визначення яких узгоджується з поняттям предметів розкоші, які є цінними, часто пов'язані з відомими брендами та можуть бути легко переміщені, включаючи картини, скульптури, ювелірні вироби, меблі, музичні інструменти, вина та інші предмети антикваріату.

Головним зобов'язанням для AMPs та HVDs є заморожування та звітність. Відповідні фірми повинні якомога швидше інформувати OFSI, якщо їм стало відомо або є достатні підстави підозрювати, що особа є підсанкційною (designated person - DP) або порушила регуляції

4 https://assets.publishing.service.gov.uk/media/6852a57c2b367fdd44c15e44/OFSI_Art_Market_Participants_and_High_Value_Dealers_Threat_Assessment.pdf

Сполученого Королівства. Це зобов'язання виникає, коли інформація надходить "у процесі ведення бізнесу". У повідомленні необхідно вказати інформацію, що є підставою для підозри, а також будь-які відомості для ідентифікації особи. Якщо підсанкційна особа є клієнтом, також необхідно повідомити про характер, суму чи кількість коштів або економічних ресурсів, що утримуються для цього клієнта. Дорогоцінні товари, що належать, утримуються або контролюються підсанкційною особою, є економічними ресурсами, які повинні бути заморожені відповідно до правил заморожування активів та про них необхідно повідомити OFSI. Угода з такими активами без відповідної ліцензії OFSI ризикує призвести до порушення фінансових санкцій Сполученого Королівства. Недотримання зобов'язань щодо звітності є правопорушенням, що карається ув'язненням до 6 місяців, штрафом або обома покараннями. OFSI має повноваження накладати грошові стягнення до 1 мільйона фунтів стерлінгів або 50% від оціночної вартості коштів чи ресурсів у разі порушень.

Оцінка OFSI базується на важливих висновках: по-перше, дуже ймовірно, що дорогі товари, які належать підсанкційним особам у Сполученому Королівстві, не були повідомлені OFSI. По-друге, ймовірно, що російські підсанкційні особи та їхні посередники здійснювали операції з дорогими товарами у Великій Британії в порушення заборон на заморожування активів. OFSI зауважило, що підсанкційні особи та їхні посередники, зіткнувшись з фінансовим тиском, намагаються використати властивості дорогих товарів, такі як їхня портативність, можливість володіння через складні корпоративні структури та здійснення непрозорих транзакцій (зокрема з готівкою та криптоактивами), для продажу або переміщення цих активів поза зоною дії санкцій. OFSI визначає посередника як будь-яку особу або організацію, що надає послуги або допомогу підсанкційним особам для порушення фінансових санкцій Сполученого Королівства. Такі посередники можуть бути професійними (з

Висновки:

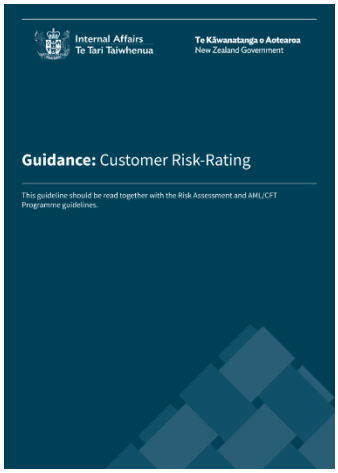
- **Обов'язкова та невідкладна звітність:** З 14 травня 2025 року AMPs та HVDs зобов'язані невідкладно заморожувати та повідомляти OFSI про всі дорогі товари, що належать, утримуються або контролюються підсанкційними особами, адже невиконання цього зобов'язання є правопорушенням і може призвести до значних штрафів або ув'язнення.
- **Посилена належна перевірка та пильність щодо "червоних прапорців":** Враховуючи високу ймовірність неврахованих дорогих товарів та активність російських підсанкційних осіб і їхніх посередників у порушенні санкцій, AMPs та HVDs повинні впровадити надійні процедури належної перевірки та особливу увагу приділяти "червоним прапорцям", таким як приховування зв'язків з підсанкційними юрисдикціями, незрозуміле походження коштів або власності, невідповідна ринковій ціна, а також будь-яка нетипова або поспішна поведінка контрагентів.
- **Подвійна відповідальність за звітність:** Зобов'язання повідомляти OFSI про підозри щодо фінансових санкцій є окремим та додатковим до обов'язку подавати SARs до NCA у разі підозри відмивання грошей або фінансування тероризму; необхідно забезпечити повне дотримання обох видів звітності, особливо враховуючи поточний низький рівень подачі SARs з боку сектору.
- **Глобальна дія санкцій та загроза з боку посередників:** Фінансові санкції Сполученого Королівства застосовуються до всіх осіб у Сполученому Королівстві та до всіх британських осіб по всьому світу, включаючи їхні філії. Тому AMPs та HVDs повинні бути особливо пильними щодо діяльності "посередників", тобто будь-яких осіб або організацій, які допомагають підсанкційним особам уникнути санкцій, оскільки вони становлять найбільш значну та постійну загрозу дотриманню правил.

умисною, необережною, неправомірною, недобросовісною або недбалою поведінкою) або непрофесійними (з тісними особистими зв'язками з підсанкційними особами, такими як члени родини, колишні дружини, партнери), які часто використовують менш складні методи для порушення санкцій. AMPs та HVDs повинні бути пильними щодо діяльності посередників та повідомляти про неї OFSI. Хоча російські санкції наразі є основною загрозою, важливо також бути обізнаними щодо загроз, що походять від інших підсанкційних режимів, таких як Лівія та КНДР.

Для зміцнення дотримання фінансових санкцій AMPs та HVDs повинні проводити надійну належну перевірку. Документ наводить ряд "червоних прапорців", які повинні викликати посилену перевірку та, за необхідності, звітування до OFSI. До них належать: зв'язки контрагентів із підсанкційними юрисдикціями (наприклад, росією) або спроби приховати такі зв'язки (наприклад, через "золотий паспорт"); збіг особистих даних контрагента зі зведеним списком фінансових санкцій OFSI; відмова контрагента надавати інформацію для перевірок KYC без поважних причин; намагання прискорити або затримати угоду, уникаючи перевірок KYC; купівля або продаж дорогоцінних товарів за ціною, суттєво вищою або нижчою за ринкову; незрозуміле походження коштів або історія володіння дорогоцінним товаром; спроби розбити загальну вартість на менші платежі, особливо нижче порогу в 10 000 євро; непідсанкційна особа, яка стверджує, що є початковим власником дорогоцінного товару, придбаного коштами підсанкційної особи; або домовленості про фізичне переміщення дорогоцінних товарів, що належать підсанкційній особі, після її включення до санкційного списку. Також важливо бути уважним до незвичайних або складних домовленостей про доставку, що включають проміжні юрисдикції, та до випадків, коли непідсанкційна особа здійснює платежі, пов'язані з дорогим товаром, які раніше здійснювала підсанкційна особа.

Окрім звітування до OFSI, якщо є підозра або обґрунтовані підстави підозрювати відмивання грошей або фінансування тероризму, фірми в регульованому секторі повинні подавати Повідомлення про підозрілу діяльність (SARs) до Національного агентства по боротьбі зі злочинністю (NCA). Ці зобов'язання є додатковими і не замінюють звітування до OFSI. Документ відзначає, що реєстрація AMPs та HVDs на SAR Portal є значно нижчою, ніж очікувалося, і лише невелика кількість SARs була подана цими секторами. OFSI наголошує на важливості дотримання AMPs та HVDs всіх розмірів як існуючих зобов'язань з боротьби з відмиванням грошей, так і нещодавно запроваджених зобов'язань щодо звітування про фінансові санкції.

Рекомендації щодо впровадження нової системи оцінювання ризику клієнтів [5]



Представлений посібник є офіційним роз'ясненням Міністерства внутрішніх справ Нової Зеландії, виданим відповідно до розділу 132(2) Закону про ПВК/ФТ 2009 року (the Act) , і всі підзвітні організації зобов'язані брати його до уваги при розробці або оновленні своїх програм комплаєнсу. Ключовим моментом, що червоною ниткою проходить через увесь документ, є формалізація вимоги щодо присвоєння рейтингу ризику кожному клієнту. Регулятор зазначає, що з 1 червня 2025 року ця вимога стає чітко прописаною частиною процедури належної перевірки клієнта (CDD). Водночас, у розділі "Погляд наглядового органу" (Supervisors' view) робиться важливе уточнення: Департамент вважає, що вимога рейтингувати клієнтів неявно існувала в Законі завжди, оскільки є основою для застосування ризик-орієнтованого підходу. Таким чином, нововведення не

[5] https://www.dia.govt.nz/AML-CFT-New-guidance-for-Customer-Risk-Rating

створює нову концепцію, а лише надає офіційного та обов'язкового статусу вже існуючій найкращій практиці.

Фундаментальна мета цього процесу — забезпечити, щоб підзвітні організації могли ефективно та раціонально розподіляти свої комплаєнс-ресурси. Правильно присвоєний рейтинг ризику дозволяє визначити інтенсивність та частоту заходів належної перевірки, постійного моніторингу та перегляду відносин з клієнтом. Це дозволяє зосередити максимальну увагу на клієнтах з високим ризиком, застосовуючи до них посилені заходи, і водночас не створювати надмірного навантаження при роботі з клієнтами, ризик яких оцінено як низький.

Посібник свідомо не пропонує єдиної універсальної моделі рейтингування, натомість наполягає на гнучкості та відповідності моделі до масштабу, характеру та складності бізнесу підзвітної організації. Для малих підприємств з невеликою кількістю клієнтів та простими продуктами, регулятор вважає достатнім впровадження простого, ручного процесу оцінки. Це може бути якісна оцінка за шкалою (наприклад, "низький", "середній", "високий") , яку співробітник робить на основі зібраної інформації та власної оцінки ризиків компанії. На противагу цьому, від великих та складних організацій, що мають широку клієнтську базу та комплексні продукти, очікується впровадження більш досконалих, часто автоматизованих, методологій. Це можуть бути бальні системи (scorecards) або матричні інструменти, що присвоюють питому вагу різним факторам ризику та розраховують підсумковий числовий або категорійний рейтинг. Важливою є вказівка на необхідність правильного налаштування моделі: якщо, наприклад, усі клієнти є резидентами Нової Зеландії, цей фактор має мати меншу вагу, щоб інші, більш значущі індикатори ризику, могли коректно ідентифікувати високоризикових клієнтів.

Процес присвоєння рейтингу має бути інтегрований у процедуру онбордингу клієнта. Супервізор пропонує такий підхід: спочатку визначається попередній рейтинг на основі початкової інформації, отриманої від клієнта, а потім, після завершення всіх кроків верифікації в рамках CDD, цей рейтинг підтверджується або коригується. Особлива увага приділяється кумулятивному ефекту: посібник застерігає, що наявність кількох індикаторів високого ризику не просто додає, а примножує загальний ризик.

Висновки:

- **Формалізація обов'язку з 1 червня 2025 року**. Рейтингування ризиків клієнтів перетворюється з рекомендованої практики на обов'язкову, чітко задокументовану вимогу. Це означає, що відсутність формалізованої та задокументованої процедури оцінки ризику клієнта після цієї дати буде прямим порушенням законодавства.
- **Масштабованість моделі оцінки ризиків є ключовою**. Посібник надає організаціям гнучкість, дозволяючи впроваджувати як прості якісні оцінки, так і складні бальні системи. Це знімає надмірне навантаження з малого бізнесу, але водночас встановлює високі стандарти для великих гравців.
- **Рейтинг ризику — це динамічний інструмент, а не статична мітка**. Документ рішуче зміщує акцент з одноразової оцінки під час онбордингу на постійний процес моніторингу та переоцінки. Ризик може змінюватися протягом циклу ділових відносин із клієнтом.
- **Документація — це ваш захист**. Регулятор вимагає не просто присвоювати рейтинг, а й документувати обґрунтування цього рішення. Саме ці записи слугуватимуть доказом того, чому до конкретного клієнта було застосовано стандартний, спрощений чи посилений рівень перевірки.

Одним із ключових меседжів документа є динамічність ризику. Присвоєний при онбордингу рейтинг не є остаточним. Він має систематично переглядатися в рамках постійної належної перевірки (ongoing CDD) та моніторингу рахунків. Ба більше, будь-яка суттєва зміна у транзакційній активності клієнта,

виявлена системою моніторингу (наприклад, нетипова операція), має слугувати тригером для негайного перегляду та, ймовірно, підвищення рейтингу ризику, незалежно від планового графіку перевірок. Цікавою є рекомендація регулятора поширити практику рейтингування і на існуючих клієнтів (залучених до 1 червня 2025 року), роблячи це поступово під час їх планового періодичного перегляду.

Вимоги до ведення записів також чітко визначені. Організації повинні зберігати не тільки сам рейтинг клієнта, а й дати його перегляду чи оновлення. Ці записи мають зберігатися щонайменше п'ять років після припинення ділових відносин (або завершення разової транзакції) і бути доступними для перевірки "негайно" (immediately accessible). Посібник наполегливо рекомендує документувати обґрунтування прийнятих рішень щодо рейтингу, оскільки це є доказовою базою правомірності застосованого рівня CDD. Нарешті, наглядовий орган вказує на необхідність періодичного тестування та перевірки самої моделі рейтингування, щоб переконатися в її ефективності та за необхідності вносити корективи.

Санкції

Сирія без санкцій: геополітичні наслідки рішення США [6]

У червні 2025 року Президент США Дональд Трамп підписав виконавчий указ, який передбачає офіційне скасування більшості санкцій, що діяли проти Сирії з 2004 року. Цей документ означає радикальний перегляд політики США щодо Сирії, орієнтований на підтримку її економічного відновлення, стимулювання гуманітарної допомоги та сприяння стабілізації регіону. Відповідно до положень указу скасовуються ключові санкційні режими, які були запроваджені попередніми адміністраціями, зокрема виконавчі укази E.O. 13338 від 2004 року, який блокував активи сирійських державних структур і забороняв експорт певних товарів; E.O. 13399 та E.O. 13460, які розширювали обмеження через загрозу національній безпеці США; а також E.O. 13572, E.O. 13573 і E.O. 13582, які були запроваджені у 2011 році у відповідь на порушення прав людини та насильство щодо цивільного населення під час громадянської війни. Згідно з цим рішенням розблоковуються активи понад 500 фізичних і юридичних осіб, включно з Центральним банком Сирії, а також скасовуються обмеження на транзакції, інвестиції та торгівлю, що відкриває шлях для американських і міжнародних компаній до повернення на сирійський ринок. Особливо це стосується секторів енергетики, будівництва, телекомунікацій та фінансів, які можуть стати основними драйверами економічного відновлення країни.

Водночас адміністрація США наголосила, що скасування загальних санкційних режимів не означає повної нормалізації відносин із Сирією. Зберігаються точкові обмеження проти окремих осіб і груп, пов’язаних із порушеннями прав людини, розповсюдженням хімічної зброї, торгівлею наркотиками, підтримкою терористичних організацій, зокрема ІДІЛ, а також іранських проксі-груп у регіоні. Ці обмеження надалі діють на підставі E.O. 13894 від 2019 року, який залишається чинним. Це означає, що будь-яка взаємодія з сирійськими контрагентами потребуватиме високого рівня перевірки на предмет відповідності залишковим санкційним обмеженням.

[6] https://www.whitehouse.gov/presidential-actions/2025/06/providing-for-the-revocation-of-syria-sanctions/

Ключовим політичним контекстом ухвалення цього рішення стала зміна політичної ситуації в Сирії після відставки Башара аль-Асада та приходу до влади нового уряду на чолі з Ахмедом аль-Шараа. Підписання указу відбулося після перемовин у Саудівській Аравії, де США узгодили позиції з ключовими регіональними діячами, зокрема Саудівською Аравією, Туреччиною та ОАЕ. Ці країни підтримали ідею скасування санкцій як інструменту зменшення впливу Ірану в регіоні та стимулювання політичної стабільності в Сирії. Адміністрація США також наголосила, що скасування санкцій сприятиме відновленню гуманітарних коридорів, розблокуванню поставок продовольства та медикаментів, а також відкриттю фінансових каналів для підтримки сирійського населення.

Разом з тим Білий дім наголосив, що бізнес та фінансові установи мають ретельно стежити за тим, щоб не співпрацювати з суб'єктами, які залишаються під цільовими обмеженнями. OFAC зобов'язався надати оновлені списки спеціальн визначених осіб та рекомендації щодо проведення санкційного скринінгу. Скасування широких санкцій супроводжувалося розробкою спеціальних ліцензій для гуманітарних організацій та компаній, що працюють у критично важливих секторах, пов'язаних із відновленням інфраструктури.

Міжнародна реакція на це рішення була неоднозначною. Частина європейських партнерів, зокрема Франція та Німеччина, висловили занепокоєння, вважаючи, що передчасне скасування санкцій може підірвати зусилля щодо досягнення довготривалого миру без чіткого виконання політичних реформ у Сирії. Водночас ОАЕ, Саудівська Аравія та Єгипет привітали рішення США, розглядаючи його як можливість для регіональної стабілізації та економічного відновлення. Цей крок також спрямований на обмеження впливу росії та Ірану, які традиційно підтримували режим Асада і мають значний економічний та військовий вплив у Сирії.

Висновки:

- **Відновлення економічної діяльності:** Скасування санкцій відкриває можливості для іноземних інвесторів та компаній, зацікавлених у відновленні сирійської інфраструктури та економіки.
- **Збереження цільових обмежень:** Незважаючи на загальне послаблення санкцій, зберігаються обмеження щодо осіб та організацій, пов'язаних із порушеннями прав людини та тероризмом, що вимагає ретельної перевірки контрагентів.
- **Міжнародна координація:** Необхідно враховувати, що інші країни, зокрема ЄС та Велика Британія, можуть мати власні санкційні режими щодо Сирії, що потребує координації дій на міжнародному рівні.
- **Гуманітарна підтримка:** Зняття обмежень на експорт продовольства та медикаментів створює можливості для надання гуманітарної допомоги населенню Сирії, що постраждало від багаторічного конфлікту.

Фактично цей указ демонструє стратегічний зсув у зовнішній політиці США, орієнтований не лише на політичний тиск, але й на створення економічних стимулів для відновлення Сирії. Проте ефективність цього кроку залежатиме від здатності нового сирійського уряду здійснити реальні демократичні перетворення, забезпечити дотримання прав людини та ліквідувати вплив терористичних груп і зовнішніх проксі-сил на території країни.

Звіти окремих інституцій та експертів

Від відкритого банкінгу до відкритих фінансів: Як змінюється фінансовий світ у 2025 році [7]

Документ є комплексним аналітичним дослідженням, яке висвітлює еволюцію концепції відкритого банкінгу на глобальному рівні та її перехід до моделі відкритих фінансів. У ньому детально розглядаються ключові драйвери, регуляторні трансформації, технологічні тренди, виклики та перспективи впровадження відкритих фінансових екосистем у різних регіонах світу. Автори відзначають, що відкритий банкінг більше не є вузько спеціалізованим підходом, як це було на початкових етапах його впровадження після прийняття Директиви PSD2 в Європейському Союзі. Сьогодні відкритий банкінг перетворився на повноцінний інструмент трансформації фінансового сектору, який сприяє розвитку інновацій, підвищенню ефективності та орієнтації фінансових послуг на потреби клієнтів. Основним фактором цього стало поєднання нормативних стимулів, технологічної зрілості та зростаючого попиту споживачів на персоналізовані, прозорі та зручні фінансові сервіси.

Документ підкреслює, що найуспішнішими прикладами впровадження відкритого банкінгу є Велика Британія, Австралія, Бразилія та Південна Корея, де ця модель стала не лише технічним стандартом, а й базою для створення нових бізнес-моделей, розвитку фінансових технологій і підвищення конкуренції. Тут фінансові установи, платформи та FinTech-компанії активно використовують API для інтеграції з третіми сторонами, розробки індивідуальних продуктів і масштабування своїх послуг. Проте глобальний розвиток відкритого банкінгу є нерівномірним. Наприклад, у США через відсутність єдиного обов'язкового регуляторного режиму цей процес є фрагментованим і ринково-орієнтованим, що обмежує масштабованість і універсальність підходів. У низці країн Азії та Африки розвиток відкритого банкінгу обмежується локальними ініціативами, тестовими проєктами або перебуває на початкових стадіях обговорення.

Автори акцентують увагу на тому, що наступним логічним етапом розвитку є перехід до відкритих фінансів — моделі, яка передбачає поширення принципів відкритого доступу до даних на всі сегменти фінансового сектору, включно зі страхуванням, інвестиціями, кредитами, пенсійним плануванням та іншими фінансовими продуктами. В основі цієї концепції лежить ідея створення єдиної інтегрованої фінансової екосистеми, де користувачі мають повний контроль над своїми фінансовими даними, а постачальники послуг можуть пропонувати комплексні, персоналізовані рішення. Водночас рівень готовності різних країн до впровадження відкритих фінансів істотно відрізняється. Якщо у Великій Британії, Бразилії та Австралії вже існують або впроваджуються відповідні нормативно-правові рамки, то в інших країнах ще тривають дискусії щодо підходів до регулювання, створення інфраструктури та забезпечення суспільної довіри до таких змін.

Документ також описує, як за останні кілька років розвиток відкритого банкінгу відбувався паралельно з іншими важливими трансформаціями у фінансовому секторі. Серед них особливо відзначаються стрімка цифровізація платежів, прискорена пандемією COVID-19, зростання

[7] https://media.licdn.com/dms/document/media/v2/D4E1FAQG8a1vrPyskVQ/feedshare-document-pdf-analyzed/B4EZfAsx97HsAY-/0/1751284677241?e=1752710400&v=beta&t=MDcmW9oCY6c8jrilBiMurdh3A8OgvFrKMtnOeEz0kcQ

популярності безконтактних оплат, цифрових гаманців і моделей Buy Now, Pay Later (BNPL), а також значне посилення ролі технологічних гігантів, таких як Apple і Google, у сфері платежів. У період з 2020 по 2021 роки ринок FinTech пережив справжній бум інвестицій, з появою фінансових «супераппів» на кшталт Revolut або Nubank. Однак із 2022 року спостерігається фаза консолідації: скорочення персоналу, зниження оцінок компаній, хвиля злиттів і поглинань, що свідчить про стабілізацію ринку після періоду надшвидкого зростання.

Особливу увагу документ приділяє впливу регуляторних змін і технологічних інновацій на подальший розвиток галузі. Зокрема, у 2023 році в кількох країнах були впроваджені цифрові валюти центральних банків (CBDC), а в Європейському Союзі розпочалася імплементація нових регуляторних актів — PSD3, Payment Services Regulation (PSR), Instant Payments Regulation (IPR) і Financial Data Access (FiDA). Ці акти покликані посилити вимоги до прозорості, безпеки та доступності фінансових даних, зробити платіжні послуги швидшими й надійнішими та забезпечити споживачам більший контроль над їхніми фінансовими потоками. Паралельно значно посилюється регулювання у сферах криптовалют, захисту персональних даних і сталого фінансування (ESG).

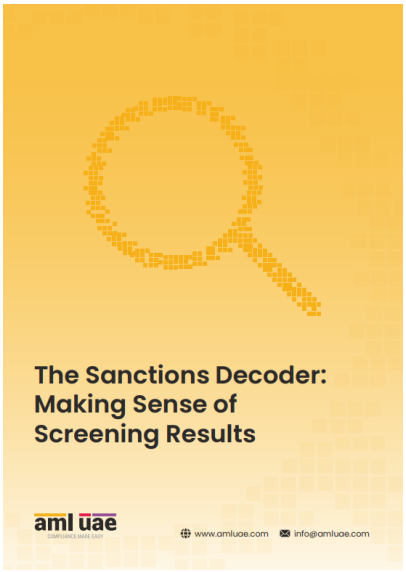
Висновки:

- **Перехід від відкритого банкінгу до відкритих фінансів є глобальним трендом.** Фінансовим установам та регуляторам рекомендується адаптувати свої стратегії до розширеного доступу до даних не лише по платіжних рахунках, а й у сферах інвестицій, страхування та кредитування.
- **Регуляторний ландшафт стає більш комплексним і жорстким.** Європейські ініціативи PSD3, PSR, IPR та FiDA є прикладами тенденції до гармонізації правил, яка стане викликом для країн, які ще не впровадили повноцінні регуляторні рамки для відкритого банкінгу.
- **Штучний інтелект стає ключовим елементом фінансових послуг.** Організаціям необхідно розробити політики управління ризиками, пов'язаними з використанням AI, включаючи питання етичності, прозорості та захисту даних, особливо в сферах скорингу, ПВК/ФТ та протидії фінансовим шахрайством.
- **Нерівномірність розвитку відкритого банкінгу створює ризики регуляторного арбітражу.** Для країн без єдиного нормативного поля (як-от США або окремі держави Азії та Африки) існує ризик формування тіньових ринків даних і недобросовісних практик.

Ще одним суттєвим трендом, який відображає цей документ, є зростаюче використання штучного інтелекту у фінансових послугах. Генеративні моделі, такі як ChatGPT, уже активно застосовуються у сферах кредитного скорингу, управління ризиками, виявлення шахрайських операцій і покращення клієнтського сервісу. Це водночас створює нові можливості для автоматизації, персоналізації послуг і підвищення ефективності, але також піднімає питання етики, управління ризиками та захисту даних.

Загалом документ демонструє, що відкритий банкінг і відкрите фінансування більше не є виключно регуляторною вимогою чи технологічним трендом, а стають ключовими складовими майбутньої фінансової інфраструктури. Водночас він чітко вказує, що для досягнення повного потенціалу відкритих фінансових екосистем необхідно вирішити низку викликів, пов'язаних із довірою користувачів, стандартизацією даних, розвитком технічної інфраструктури, правовими гарантіями та кібезахистом.

Санкційний комплаєнс на практиці в ОАЕ: як уникнути помилок у скринінгу та відповідати вимогам регулятора [8]



Документ глибоко розкриває багатогранність підходу до процесу санкційного скринінгу, роблячи акцент на необхідності не лише технічного, а й методологічно вивіреного аналізу отриманих результатів. Автори наголошують, що санкційний скринінг не є виключно технічним процесом, обмеженим простим зіставленням імен чи інших параметрів клієнтів із даними санкційних списків. Це складний, багаторівневий процес, що потребує високого рівня професіоналізму, методичної точності, застосування ризик-орієнтованого підходу та бездоганного розуміння як нормативних вимог, так і практичних аспектів ПВК/ФТ та TFS.

В основу документа покладено концепцію того, що результати санкційного скринінгу повинні бути інтерпретовані виключно з урахуванням повного контексту ідентифікаційних даних клієнта, характеристик санкційної інформації та параметрів самої скринінгової системи. Неправильне або поверхове трактування результатів може не лише створити ризик порушення нормативних вимог, але й призвести до фінансових втрат, штрафів або кримінальної відповідальності для компанії, яка не виконає обов'язків щодо замороження активів або своєчасного подання повідомлень до фінансової розвідки.

Дуже детально автори розглядають побудову внутрішнього процесу санкційного скринінгу. Процедура починається із обов'язкової підписки на актуальні санкційні списки, зокрема локальні списки терористів ОАЕ, списки ООН згідно з резолюціями Ради Безпеки ООН (зокрема 1718 та 2231) та інші міжнародні санкційні бази даних. Регульовані суб'єкти повинні забезпечити безперервний моніторинг змін у цих списках і їх своєчасне відображення в скринінгових системах.

Наступним кроком є правильне збирання і введення ідентифікаційних даних про клієнтів. Для фізичних осіб це повне ім'я, всі можливі псевдоніми та альтернативні написання, дата народження, громадянство, реквізити документів (паспорт, ID-карта тощо) та остання відома адреса. Для юридичних осіб — повна назва, усі можливі варіанти скорочень, адреси головного офісу та філій, реєстраційний номер, а також обов'язково дані кінцевих бенефіціарних власників (КБВ), які перевіряються за тими ж критеріями, що й фізичні особи.

Особлива увага приділена опису самого механізму скринінгу. Автори наголошують, що більшість регуляторних вимог не встановлюють технічних параметрів скринінгу, однак саме налаштування програмного забезпечення, обраний рівень допустимої подібності, логіка побудови алгоритмів та здатність інструменту обробляти мовні, транскрипційні та культурні відмінності суттєво впливають на точність результатів.

Усі результати скринінгу класифікуються на чотири категорії: повний збіг, частковий збіг, хибний збіг і відсутність збігу. Документ надзвичайно ретельно описує кожен із цих сценаріїв, наводячи детальні матриці співставлення ідентифікаційних параметрів, які дозволяють візуально зрозуміти процес прийняття рішень щодо визначення типу збігу. При цьому особлива увага приділяється тому, що навіть при наявності високоякісного програмного забезпечення

[8] https://amluae.com/wp-content/uploads/2025/02/The-Sanctions-Decoder_-Making-Sense-of-Screening-Results-N.pdf

остаточне рішення завжди приймає людина, а отже якість підготовки аналітиків комплаєнсу стає критично важливим фактором.

Окремим великим блоком описано процес розв'язання часткового збігу — однієї з найбільш проблемних і ризикових категорій. Тут підкреслено, що часткові збіги найчастіше виникають у ситуаціях недостатності даних, коли або відсутні документи клієнта, або їх якість не дозволяє провести чітку ідентифікацію (наприклад, сумнівні копії документів, підроблені дані або відсутність критичних параметрів у відкритих джерелах). Ці кейси вимагають негайної зупинки всіх операцій і подання PNMR, але також вимагають особливої обережності недопущення розкриття клієнту факту здійснення санкційної перквірки або подання відповідного повідомлення.

Висновки:

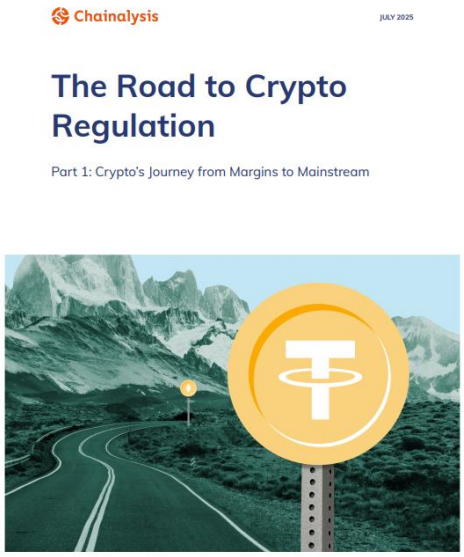
- **Необхідність швидкого реагування на повний збіг:** У разі повного збігу компанія зобов'язана заморозити активи клієнта протягом 24 годин та подати звіт про замороження активів (FFR) через портал goAML не пізніше 5 календарних днів.
- **Правильна обробка часткового збігу є критичною:** Частковий збіг вимагає негайного призупинення операцій і подання PNMR. Недостатня увага до таких випадків може призвести до санкцій з боку регуляторів.
- **Оптимізація процесів для зниження хибних збігів:** Потрібно регулярно налаштовувати параметри санкційного скринінгу, обирати якісні провайдери санкційних списків та уникати надмірної чутливості фільтрів, яка призводить до зайвих хибних спрацювань.
- **Документування та архівування процесів — обов'язкове:** Усі дії, включно з аналізом збігів, рішеннями, поданими звітами та застосованими заходами, мають бути ретельно задокументовані й збережені відповідно до вимог регуляторів.

Не менш важливим є опис хибних збігів, які стають великою проблемою для компаній, що мають великий обсяг клієнтської бази, особливо у мультикультурних регіонах або при роботі з іноземними клієнтами. Автори підкреслюють, що систематично високий рівень хибних спрацювань є сигналом до негайного аудиту якості даних, параметрів скринінгового програмного забезпечення та правильності підключення до санкційних джерел. Ігнорування цієї проблеми може призвести до затримок в обслуговуванні клієнтів, збільшення операційних витрат і, зрештою, до втрати конкурентоспроможності.

Документ також надає надзвичайно важливу методологію роботи з кейсами, де отримано відсутність збігу. Автори нагадують, що навіть у випадку відсутності збігу обов'язковим залишається проведення стандартної процедури належної перевірки (CDD), а для окремих категорій клієнтів — застосування посиленої перевірки (EDD) у рамках ризик-орієнтованого підходу.

На завершення підкреслюється, що санкційний комплаєнс — це не просто набір технічних процедур, а елемент корпоративної культури управління ризиками, що включає комплекс заходів: постійне оновлення політик і процедур, регулярне навчання персоналу, тестування систем скринінгу, внутрішній аудит і моніторинг ефективності, а також належна співпраця з регуляторами та фінансовою розвідкою. Документ формулює чітке розуміння того, що відсутність або недосконаліть санкційної програми у сучасному середовищі є не лише регуляторним ризиком, але й реальним бізнес-ризиком, який здатен зруйнувати фінансову стійкість і репутацію будь-якої організації незалежно від її розміру та сфери діяльності.

Глобальне регулювання крипто: виклики, прогалини та нові стандарти [9]



Документ від Chainalysis представляє комплексний огляд глобального розвитку регулювання криптовалют та цифрових активів, відображаючи шлях трансформації криптоіндустрії від маргінального явища до системної складової світової фінансової екосистеми. Основна ідея документа полягає в тому, що криптовалюти стали настільки значущими для глобальної фінансової системи, що більше не можуть існувати поза рамками державного регулювання, оскільки обсяг ринку вже перевищує 3 трильйони доларів, а використання криптоактивів тісно інтегрується з традиційним фінансовим сектором. Водночас виклики, пов'язані з природою криптоактивів, залишаються значними, адже вони не підпадають чітко під жодну з традиційних фінансових категорій — цінні папери, товари, валюти чи платіжні інструменти, що змушує регуляторів усього світу шукати нові підходи. Суттєвим є також питання про те, чи мають юрисдикції створювати окреме законодавство для криптоактивів, чи достатньо розширити існуючі фінансові рамки на цей сектор. Документ досліджує стан регулювання у 25 провідних юрисдикціях, які разом охоплюють 73% світової активності у сфері криптовалют, з акцентом на три ключові напрями: фінансова цілісність, захист споживачів і ринкова доброчесність.

В частині фінансової цілісності, яка в першу чергу пов'язана з протидією відмиванню коштів та фінансуванню тероризму, основним міжнародним стандартом є Рекомендація 15 FATF, яка була оновлена у 2018 році та визначає вимоги до віртуальних активів (VAs) і постачальників послуг, пов'язаних з віртуальними активами (VASPs). Її виконання включає оцінку ризиків ВК/ФТ, обов'язкову реєстрацію та ліцензування VASP, впровадження KYC, моніторинг транзакцій, дотримання Travel Rule, а також обов'язок виявлення та повідомлення про підозрілі операції. Згідно зі звітом FATF середини 2024 року, близько 75% юрисдикцій залишаються або частково сумісними, або зовсім не виконують ці стандарти, що створює глобальні ризики для фінансової системи. ЄС значно просунувся в гармонізації цього напряму через впровадження пакетів MiCA, AMLR і TFR, які охоплюють всі аспекти ПВК/ФТ для криптосектору. Водночас залишаються юрисдикції, такі як В'єтнам чи Австралія, які досі не запровадили або лише частково впровадили відповідні правила. Зазначається, що навіть наявність законодавчих рамок не гарантує ефективного нагляду та правозастосування — це значно складніший процес, особливо для країн із обмеженими ресурсами та недостатнім досвідом у регулюванні криптотехнологій. Важливим чинником залишається впровадження інструментів on-chain аналітики, які суттєво розширюють можливості як регуляторів, так і приватних компаній у виявленні підозрілої активності, відслідковуванні потоків коштів та ідентифікації незаконних транзакцій у реальному часі.

Другим ключовим напрямом є захист споживачів, який значно менш гармонізований порівняно з регулюванням у сфері ПВК. Тут національні підходи сильно різняться, що обумовлено різними рівнями ризик-апетиту регуляторів. Документ наголошує на кількох базових інструментах захисту споживачів, серед яких обов'язкові розкриття інформації, прозорість маркетингових матеріалів, вимоги до публікації whitepaper із зазначенням усіх ризиків, заборони або обмеження реклами для роздрібних клієнтів (як у Сінгапурі), проведення тестів на придатність

[9] https://www.chainalysis.com/wp-content/uploads/2025/06/the-road-to-crypto-regulation-part-release.pdf?mkt_tok=NTAzLUZBUC0wNzQAAAGbT3F8xz_5iNBIUAktYD7jFm3SWM5CQTM20MF41wtqKM0L59-0nT8V5A2LIwNbIxyLjR8xHIxCM0BWf_I-Oq7qp6MlwLRJZ2ZeBWqk-AhmKbsN

і відповідність клієнтів, обмеження на використання кредитних коштів для купівлі криптоактивів або заборона участі роздрібних інвесторів у стейкінгу (Сінгапур, частково — Велика Британія). Важливим трендом стало посилення вимог до зберігання клієнтських активів: багато юрисдикцій запроваджують обов'язкове холодне зберігання до 98% активів (Гонконг), 95% (Австралія) або 90% (Сінгапур), а також створення страхових фондів або резервів для покриття втрат клієнтів у випадку злому чи банкрутства біржі. Документ також зазначає, що зростання обсягів шахрайства та кібершахрайства, орієнтованого на роздрібних інвесторів, змушує регуляторів впроваджувати нові підходи, такі як використання інструментів попереднього виявлення шахрайських структур і блокування шахраїв ще до здійснення ними атак. У цьому контексті Chainalysis пропонує рішення Alterya та Hexagate, які дозволяють виявляти загрози ще на стадії їх підготовки завдяки аналізу поведінкових і on-chain патернів.

Найбільш проблемною залишається сфера ринкової доброчесності. Більшість юрисдикцій взагалі не мають окремого законодавства щодо запобігання маніпуляціям ринком у криптоіндустрії. У США, Великій Британії, Індії, Бразилії та Україні взагалі відсутні спеціальні норми, що прямо забороняють інсайдерську торгівлю, імітаційну торгівлю чи pump-and-dump схеми (схема, при якій група осіб ціну активу через дезінформацію, фейкові новини або скоординовані покупки (pump), щоб потім продавати акти за завищеною ціною та обвалювати ринок (dump), завдаючи збитків іншим інвесторам. Натомість органи влади змушені застосовувати традиційні кримінальні статті, такі як шахрайство, або поширювати правила щодо цінних паперів чи товарів, якщо актив визнається таким. Лише окремі юрисдикції, такі як ЄС, Південна Корея, Канада, Гонконг та частково Туреччина, мають повноцінні правила ринкової доброчесності. При цьому регулятори стикаються з серйозними практичними проблемами у моніторингу

Висновки:

- **Лише ЄС та декілька азійських юрисдикцій забезпечили повну відповідність стандартам FATF щодо ПВК/ФТ у сфері VASP.**

  Практична дія: інші країни мають якнайшвидше завершити впровадження 15 Рекомендації FATF — зокрема ліцензування VASP, виконання Travel Rule та нагляд за їхнім ризик-менеджментом. FATF у 2025 році перевірятиме не лише нормативну базу, а й фактичне виконання.

- **У 80% проаналізованих країн відсутнє ефективне регулювання ринкової доброчесності крипторинків.**

  Рекомендація: країни повинні впровадити норми, які забороняють інсайдерську торгівлю, маніпуляції (імітаційну торгівлю, pump-and-dump) та зобов'язують платформи до торгового моніторингу. ЄС (MiCA Title VI), Канада, Південна Корея і Гонконг вже реалізували такі вимоги.

- **Існує критична фрагментованість у регулюванні захисту споживачів, що створює регуляторні прогалини.**

  Практичний наслідок: лише окремі юрисдикції (наприклад, Сінгапур, Гонконг, Південна Корея) запровадили вимоги до холодного зберігання, резервів або заборони на рекламу. Іншим країнам слід прийняти мінімальні стандарти зберігання, компенсації втрат і маркетингових обмежень.

- **Ончейн-аналітика та інструменти постійного моніторингу (Alterya, Hexagate) — ключ до ефективного регулювання.**

  Конкретний результат: використання відкритих блокчейн-даних дозволяє виявляти підозрілу активність у реальному часі, включно з обхідниками Travel Rule, шахраями, маніпуляціями та інсайдерськими операціями. Рекомендовано державним регуляторам та платформам інтегрувати такі інструменти в наглядові процеси.

ринку: висока волатильність, перехресні лістинги активів на різних платформах (централізованих і децентралізованих), складність визначення моменту, коли інформація стає публічною у DAO-проєктах, де голосування відбуваються у відкритому блокчейні. Також традиційні підходи до моніторингу не працюють належним чином у криптосекторі, де значна частина маніпуляцій відбувається через DEX або міжмережеві переміщення коштів.

У фінальній частині документ наголошує, що розвиток регулювання відбуватиметься не лише у сфері централізованих бірж, брокерів і кастодіальних сервісів, а поступово поширюватиметься на DeFi-сервіси, геймінгові платформи, метавсесвіти та інші сфери Web3, де межі між фінансовими й нефінансовими послугами розмиті. Водночас зростатиме напруженість між національними законодавствами і глобальними моделями бізнесу, які оперують у декількох юрисдикціях одночасно. Приклади таких фрикцій вже помітні у різних підходах до Travel Rule, вимогах до локального зберігання приватних ключів (як у Гонконзі) чи різних порогах для обов'язкового KYC. Окремо наголошується, що наступний розділ серії буде присвячений регулюванню стейблкоїнів, їх ролі в екосистемі та пов'язаним з ними регуляторним викликам. Підсумовуючи, документ підкреслює, що побудова довіри до блокчейнів можлива лише за умови ефективного регулювання, яке поєднує інновації, захист споживачів, фінансову безпеку та прозорість ринку.

Оперативна незалежність та автономія ПФР [10]

У статті опублікованій Томмазо Ді Руцца (K2 Integrity), розкривається критично важливе значення операційної незалежності та автономії підрозділів фінансової розвідки (ПФР) як системоутворювальної передумови ефективної архітектури протидії відмиванню коштів та фінансуванню тероризму.

Автор починає з тези, що дотримання технічних стандартів FATF і досягнення ефективності можуть бути лише поверхневими, якщо не закладені фундаментальні умови — серед яких провідною є незалежність і автономність ПФР. Посилаючись на Рекомендацію 29 FATF та її тлумачення, а також на позиції Егмонтської Групи, автор підкреслює, що незалежність ПФР не є бажаною опцією, а є безумовною вимогою. Вона забезпечує не лише доброчесність аналітичної роботи та захист конфіденційної інформації, а й довіру як усередині країни, так і з боку міжнародних партнерів.

Незалежно від моделі ПФР (адміністративна, правоохоронна, судова, гібридна), вони мають бути захищені від політичного, урядового чи приватного втручання. Але на практиці багато ПФР у різних юрисдикціях страждають від слабкої інституційної інтегрованості, організаційної невизначеності, недостатніх ресурсів і навіть порушень — таких як залучення співробітників ПФР до судових процесів як свідків або примусові обшуки, що ставлять під загрозу безперервність операцій і конфіденційність.

Особливо небезпечним є те, що навіть такі кричущі випадки не були вчасно виявлені FATF чи регіональними органами типу FSRB, що вказує на структурну сліпу пляму в існуючій методології оцінювання. Автор стверджує, що це не винятки, а системна проблема: ПФР, як порівняно молоді інституції, не мають достатньої ваги й чіткого статусу, на відміну від органів нагляду чи правоохоронців.

[10] https://www.linkedin.com/pulse/operational-independence-autonomy-fiu-foundational-tommaso-di-ruzza-kjyof/?trackingId=Pze2ENKaTPu%2BVRR5rXlBog%3D%3D

Окремо автор акцентує на тому, що у контексті публічно-приватного партнерства (PPP), яке набуває дедалі більшого значення в боротьбі з ПВК/ФТ, ПФР водночас мають зберігати свою виключну компетенцію й довіру. Без організаційної автономії неможливо досягнути якісної взаємодії з приватним сектором, оскільки вона є гарантом як функціональної незалежності, так і стабільності довіри.

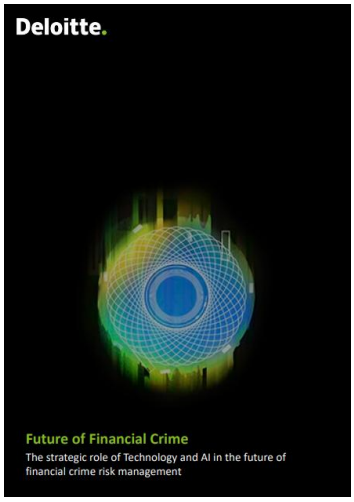
Висновки:

- **Операційна незалежність ПФР є не просто вимогою FATF, а системною умовою ефективності ПВК/ФТ**, що має забезпечуватись незалежно від інституційного розміщення ПФР у державному апараті.
- **Наявні оцінювальні механізми FATF/FSRB мають сліпу зону щодо реальної автономії ПФР**, що дозволяє толерувати глибокі порушення без належної уваги — цю прогалину потрібно виправити у рамках п'ятого раунду оцінок.
- **ПФР мають бути захищені як від формального втручання, так і від структурної залежності (кадрової, бюджетної, IT-інфраструктурної).** Інакше — навіть за наявності ресурсів — неможливо гнучко реагувати на ризики та зміни у технологічному середовищі.
- **Егмонтська Група повинна стати форумом, який дозволяє ПФР безпечно сигналізувати про ризики їх автономії**, не побоюючись репутаційних втрат для своєї держави — лише така відкритість забезпечить довгострокову стійкість міжнародної системи фінансової розвідки.

Надзвичайно важливим сигналом є пропозиція посилити оцінку в рамках п'ятого раунду взаємних оцінок FATF/FSRB: не лише перевіряти, як використовуються фінансові розвіддані (Безпосередній Результат 6), але й оцінювати фактичні умови функціонування ПФР. При цьому автор наголошує на існуючому парадоксі: країни можуть замовчувати проблеми автономності, побоюючись зниження рейтингу під час оцінки, тим самим знецінюючи процес заснований на результатах.

Насамкінець, підкреслюється роль Егмонтської Групи як потенційного каталізатора змін. Вона має створити безпечний простір для обміну інформацією між ПФР і зміцнення системної ефективності глобальної архітектури фінансової розвідки.

Стратегічна роль технологій та штучного інтелекту в майбутньому управлінні ризиками фінансових злочинів [11]



Аналітичний документ, підготовлений Deloitte, окреслює фундаментальну трансформацію у сфері управління ризиками фінансових злочинів, що базується на новітніх технологіях, штучному інтелекті (AI) та переосмисленні функцій підрозділів фінансової безпеки. Автори пропонують стратегічне бачення майбутнього, де традиційна реактивна модель поступається місцем інтелектуально керованій, цифрово орієнтованій і ризик-фокусованій системі, з інтегрованим моніторингом ризиків і вдосконаленою аналітикою на основі даних.Документ наголошує на суттєвому ускладненні загроз: кіберзлочинці активно використовують генеративний AI для створення дипфейків, фальсифікації ідентифікаційних документів, маніпуляцій доказами, а також для вербування фінансових «мулів». Це створює виклик для

[11] https://www.deloitte.com/uk/en/services/consulting-financial/blogs/2025/the-strategic-role-of-technology-and-ai-in-the-future-of-financial-crime-risk-management.html

фінансових установ, які, з одного боку, зіштовхуються з високими витратами на відповідність вимогам регуляторів, а з іншого — змушені керувати неефективними системами виявлення з великою кількістю хибнопозитивних спрацювань.

Нинішні IT-системи фінансових установ часто застарілі, фрагментовані, працюють в ізольованому режимі і не дозволяють інтегрувати нові джерела даних чи масштабувати функціонал. У таких умовах ефективна протидія фінансовим злочинам стає майже неможливою. Водночас, наголошується на зростанні обсягу внутрішніх та зовнішніх даних, включаючи відкриті джерела й ініціативи з обміну інформацією, як-от ODIN у Данії або Стаття 75 в новому AML-пакеті ЄС, що передбачає міжнародний обмін аналітикою.

Регулятори (Wolfsberg Group, DFSA, Данський нацбанк) дедалі активніше підтримують застосування AI в управлінні ризиками фінансових злочинів, визнаючи його потенціал у боротьбі з шахрайством, ПВК/ФТ і кіберзагрозами. Водночас вони підкреслюють важливість відповідального використання технологій, у тому числі в рамках пілотних програм, sandbox-платформ та лабораторій фінансових інновацій.

У практичній площині Deloitte виділяє п’ять ключових технологічних векторів трансформації:

1. Холістичний збір та інтеграція даних – цифровізація всіх процесів, підвищення якості даних, збагачення відкритими та комерційними джерелами, що дозволяє будувати 360-градусне бачення клієнта та його ризиків.
2. Виявлення через AI – поступовий відхід від статичних правил і перехід до динамічних моделей, що аналізують поведінкові патерни та знижують кількість хибних спрацювань (на 30–40% у кращих практиках).
3. Єдиний ризиковий профіль клієнта – об’єднання всіх сигналів у єдиний індикатор, що динамічно оновлюється відповідно до змін у поведінці клієнта.
4. Інтегрований моніторинг – злиття раніше розділених функцій KYC, TM, Fraud та Trade Surveillance для досягнення синергії в управлінні ризиками.
5. Аналітик нового покоління – посилення команди спеціалістами з data science, автоматизація рутинних завдань і впровадження AI-асистентів (AI copilots), що навчаються на основі практики найкращих аналітиків.

Також у документі висвітлюється необхідність стратегічного «зміщення парадигми»: фінансові установи повинні розбудовувати модульну, адаптивну IT-архітектуру,

Висновки:

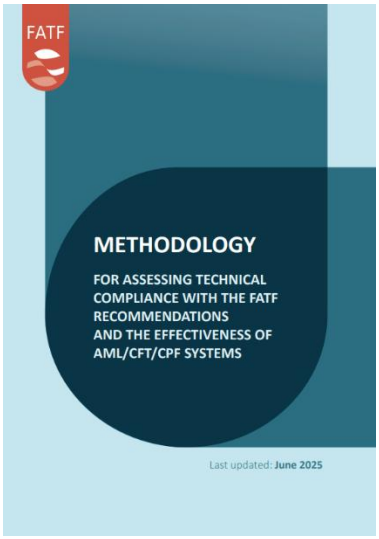
- **Фінансові установи мають відмовитись від фрагментованих систем та перейти до єдиної інтегрованої моделі ризику, яка охоплює всі функції (KYC, TM, Fraud, Sanctions, Cyber)** — це дозволяє суттєво підвищити ефективність виявлення серйозних загроз і зменшити дублювання зусиль.
- **Впровадження AI-моделей замість традиційних правил дозволяє знизити кількість хибнопозитивних сигналів на 30–40% та забезпечує більш точне виявлення поведінкових аномалій**, які є характерними для фінансових злочинів.
- **Побудова 360-градусного ризикового профілю клієнта на основі збагачених внутрішніх і зовнішніх даних** стає базовим елементом для виявлення складних схем, особливо у транснаціональних мережах.
- **Організаційна трансформація команд у менші, мультидисциплінарні підрозділи з автоматизованими процесами та AI-підтримкою** дозволяє оптимізувати ресурси та підвищити якість рішень — при збереженні фокусу на найвищі ризики.

яка дозволить швидко інтегрувати нові інструменти, відповідати на зміну регуляторних вимог і координуватися з Chief Technology/Data Officers на рівні установи. Це потребує створення кросфункціональних команд, які працюватимуть над повною трансформацією моделі управління ризиками фінансових злочинів — від структури до процесів.

Наприкінці Deloitte підкреслює, що ізольоване впровадження технологій неможливе — ефективність боротьби з фінансовими злочинами у XXI столітті можлива лише через партнерство між приватним сектором, регуляторами та технологічними компаніями, з урахуванням безпрецедентного темпу змін у сфері AI, даних та кіберзлочинності.

Для загального розвитку

FATF оновлює Методологію[12]



3 червня 2025 року світова спільнота отримала оновлену версію Методології FATF — ключового інструменту, за яким оцінюють країни на відповідність стандартам протидії відмиванню коштів, фінансуванню тероризму та розповсюдженням зброї масового знищення (ПВК/ФТ/ФР). Ці зміни стали не просто черговим технічним апгрейдом: вони значною мірою переформатовують підхід до оцінювання ризиків, визначаючи нові орієнтири для фінансових установ, державних органів і бізнесу.

Найважливішим сигналом із оновлень є безкомпромісне підсилення ризик-орієнтованого підходу. FATF остаточно закріпила за країнами обов'язок забезпечувати, щоб заходи протидії відмиванню коштів були пропорційні рівню встановленого ризику, причому як для високих, так і для низьких його проявів. Це означає, що більше не буде виправдань для формального виконання процедур: якщо у сфері виявлено високі ризики відмивання або фінансування тероризму, заходи мають бути посилені; натомість там, де ризики низькі, допускаються спрощені процедури, проте із суворим дотриманням фінансових санкцій, передбачених Рекомендацією 7. Також FATF прямо забороняє застосування спрощених процедур у разі наявності підозри на ПВК/ФТ чи при підвищених ризиках, навіть якщо бізнес загалом виглядає «безпечним». Таким чином, ризик-орієнтований підхід із декларативного стає справді робочим інструментом.

Нововведення також деталізують вимоги до фінансових установ і ВНУП (суб'єктів первинного фінмоніторингу, які не є фінансовими установами, наприклад, юристи, бухгалтери, ріелтори). Тепер вони повинні мати затверджені на рівні вищого керівництва політики й процедури з управління ризиками, що враховують як національні вимоги, так і власні оцінки ризиків. Ці оцінки ризиків відтепер мають бути документовані, постійно актуалізовані та передані на запит до компетентних органів чи саморегулівних організацій. Зокрема, пункт 1.15 прямо вимагає від фінансових установ і ВНУП не лише проводити, а й тримати в актуальному стані оцінки ризиків ФР — ризиків, пов'язаних із фінансуванням розповсюдження зброї масового знищення. Це безпрецедентно підвищує увагу до ФР у порівнянні з попередніми версіями методології.

Ще одним важливим акцентом стало глибоке допрацювання положень, що стосуються віртуальних активів і постачальників послуг з віртуальних активів (VASPs). FATF тепер прямо зазначає, що країни повинні визнавати віртуальні активи як «майно», «фонди» чи їх еквіваленти

[12] https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF-Assessment-Methodology-2022.pdf.coredownload.inline.pdf

у правовому полі, навіть якщо це не прописано окремо в законі, за умови, що практика чи судова інтерпретація дозволяє трактувати їх таким чином. У разі відсутності такого правового підходу країна одразу отримує дефіцит у відповідності до рекомендацій FATF. Крім того, VASP визначаються як повноцінні джерела інформації про бенефіціарів для цілей Рекомендацій 24 і 25. Це критично важливо, оскільки світовий обіг віртуальних активів дедалі більше використовується для нелегальних фінансових операцій, а FATF своїм оновленням визнає їх такою ж частиною фінансової системи, як і традиційні банки чи небанківські установи.

Оновлені Безпосерені результати (IO 3 та IO 4) докорінно переглядають питання оцінки ефективності нагляду над фінансовими установами, ВНУП та VASP. FATF переформатувала та перенумерувала десятки питань, додавши до них вимоги до пропорційності перевірок і нагляду до рівня ризику. Країни тепер мають не просто проводити перевірки, а підтверджувати, що їхня частота, інтенсивність і охоплення відповідають реальному ризику. Наприклад, наглядові органи повинні не допускати необґрунтованого «масового де-рискінгу», коли сектори чи клієнти відрізаються від фінансових послуг через загальні підозри, а не на основі конкретних ризиків. Водночас країни мають активно стимулювати застосування спрощених заходів для суб'єктів із низьким рівнем ризику та демонструвати ефективність взаємодії між регуляторами, приватним сектором і фінансовою розвідкою.

Особливо показовою є деталізація IO 3 та IO 4, яка робить оцінку не лише технічної відповідності, а й реальної ефективності заходів, що впливають на протидію відмиванню коштів та фінансуванню тероризму. FATF прямо прописує, що оцінювачі мають перевіряти, як швидко та якісно фінансові установи надають дані за запитами регуляторів, скільки рахунків відмовлено через неповні CDD, як тренди з моніторингу операцій корелюють із національною оцінкою ризиків і чи адаптують суб'єкти фінансового моніторингу свої внутрішні політики до актуальних ризиків. Усе це суттєво підвищує планку відповідальності як для держав, так і для приватного сектору.

Оновлення торкнулися й Глосарію: додано нові визначення, що стосуються фінансової інклюзії, уточнено поняття ризиків фінансування розповсюдження та підсилено опис категорій, пов'язаних з VASP та віртуальними активами. Крім того, оновлено додатки до Методології, зокрема список супровідних документів FATF, де з'явилися нові рекомендації щодо балансування між ПВК/ФТ і фінансовою інклюзією. Зміни в розділі «Вступ» підсилюють акцент на тому, що розуміння національного контексту, матеріальності та структурних факторів тепер обов'язково має включати аналіз бар'єрів до фінансової інклюзії як невід'ємної частини системи управління ризиками.

Таким чином, червневе оновлення Методології FATF у 2025 році не лише робить оцінювання більш технічно

Висновки:

- **Інтеграція фінансової інклюзії у ПВК/ФТ-системи.** Оцінка ефективності тепер напряму враховує, чи не створюють ПВК/ФТ-заходи бар'єри для легального доступу населення до фінансових послуг. Країнам рекомендовано впроваджувати пропорційні заходи з урахуванням соціального контексту.
- **Посилення вимог до ризик-орієнтованого підходу.** Країни мають продемонструвати, що їхні національні оцінки ризиків охоплюють як загрози ВК/ФТ/ФР, так і ризики, пов'язані з виключенням з фінансових послуг.
- **Актуалізація підходів до віртуальних активів та VASP.** Внесені уточнення до оцінки VASP як джерела інформації про бенефіціарних власників, а також до їхнього регулювання в контексті Рекомендації 15 та інших рекомендацій.
- **Глибша інтеграція питань санкцій та фінансування розповсюдження.** У IO.11 уточнені приклади специфічних факторів, що дозволяють краще оцінити ефективність заходів з протидії обходу санкцій та ФР.

глибоким, а й переводить міжнародні стандарти у площину практичного ризик-орієнтованого управління, де кожна країна зобов’язана не просто створювати формальні процедури, а доводити їхню ефективність у реальному запобіганні відмиванню коштів, фінансуванню тероризму та розповсюдженню зброї масового знищення.

Ваша думка важлива!

1. Як, на вашу думку, фінансовим установам знайти баланс між впровадженням інноваційних AI-рішень для ПВК/ФТ та одночасним створенням захисту від загроз, які генерує сам штучний інтелект?
2. Яким чином штучний інтелект у поєднанні з відкритим доступом до фінансових даних може впливати на ризики фінансових злочинів, зокрема ВК/ФТ, і як має трансформуватися система фінансового моніторингу для ефективного реагування?
3. Як змінюються підходи до санкційного скринінгу в умовах використання новітніх технологій, включно з штучним інтелектом, машинним навчанням та блокчейн-рішеннями, і наскільки готова Україна до їх повноцінного впровадження у сфері ПВК/ФТ та санкційного комплаєнсу?
4. Якою мірою розвиток генеративного штучного інтелекту, криптовалют і цифрових платформ сприяє радикалізації, фінансуванню тероризму та підготовці атак, і чи достатньо ефективно Україна інтегрує ці ризики у свою національну систему ПВК/ФТ? Як має трансформуватися фінансова розвідка і кіберрозвідка в цих умовах?
5. Секторальна оцінка ринку предметів розкоші в Румунії та звіт OFSI для Сполученого Королівства вказують на критично низький рівень звітування про підозрілі операції у високоризикових секторах. Чи не є ідеї про «партнерство» та «розбудову культури» ілюзією, коли мова йде про сектори, які історично звикли працювати в умовах конфіденційності та мінімального втручання? Можливо, єдиним дієвим механізмом для таких ринків є саме жорсткий нагляд і невідворотність покарання, а справжня культура комплаєнсу — це вже наслідок, який формується роками після встановлення «жорсткої руки» регулятора, а не причина позитивних змін?
6. Які, з вашого досвіду, існують найбільш значущі, але непублічні фактори тиску (політичного, відомчого, ресурсного) на підрозділ фінансової розвідки? І які практичні механізми, окрім законодавчих гарантій, могли б забезпечити його реальну операційну незалежність в українських реаліях?
7. Оновлена Методологія FATF вперше робить такий сильний акцент на необхідності забезпечити фінансову інклюзію, застерігаючи від невиправданого "де-рискінгу". З якими найбільшими труднощами стикаються українські фінансові установи, намагаючись збалансувати вимоги ПВК/ФТ та принцип доступності фінансових послуг?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-27

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

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