Методологічний бюлетень

Серійний номер: МінФін-AML-2025-49

Грудень 2025

“Або ви керуєте вашим днем, або день управляє вами”

Джим Рон

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

Стратегічне рішення ЄК: Внесення Росії до списку високоризикових юрисдикцій [1]

У грудні 2025 року Європейська Комісія (ЄК) прийняла безпрецедентне рішення, яке докорінно змінює архітектуру фінансових відносин з Російською Федерацією. Прийняття делегованого регламенту щодо включення Росії до списку третіх країн з високим ризиком (high-risk third countries) є кульмінацією тривалого процесу оцінки стратегічних недоліків у російській системі ПВК/ФТ. Це рішення виходить далеко за межі традиційної санкційної політики, переносячи Росію в категорію юрисдикцій, що становлять структурну загрозу цілісності фінансової системи Європейського Союзу.

Правова природа та механізм прийняття рішення

Рішення базується на повноваженнях, наданих Комісії статтею 9(2) Директиви (ЄС) 2015/849 (4-та Директива AMLD). Традиційно Європейський Союз синхронізував свій список

[1] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_2910/IP_25_2910_EN.pdf

високоризикових країн з рішеннями Групи з розробки фінансових заходів боротьби з відмиванням коштів (FATF). Однак, ситуація з Росією створила унікальний прецедент. Членство Росії у FATF було призупинено, що унеможливило проведення стандартних процедур взаємної оцінки цією організацією.

Враховуючи цей вакуум та зобов'язання, взяті на себе в рамках Делегованого Регламенту (ЄС) 2025/1393 від 8 липня 2025 року, Європейська Комісія провела власну автономну оцінку. Методологія цієї оцінки була комплексною і включала аналіз інформації з відкритих джерел, даних компетентних органів країн-членів ЄС, Європейської служби зовнішніх справ (EEAS) та розвідувальних даних.

Оцінка підтвердила, що Росія має стратегічні недоліки у своїх режимах ПВК/ФТ, які не лише не виправляються, а й поглиблюються через державну політику сприяння обходу санкцій, фінансування агресивної війни проти України та підтримку терористичних проксі-груп. Комісар з фінансових послуг Maria Luís Albuquerque підкреслила: "Ми виконали своє зобов'язання оцінити країни, членство яких у FATF призупинено. Це демонструє нашу рішучість захистити фінансову систему ЄС".

Операційні наслідки для "підзвітних суб'єктів"

Включення Росії до "чорного списку" ЄС має пряму дію після набрання чинності регламентом і активує статтю 18a Директиви 4AMLD. Це фундаментально змінює підхід європейських банків та інших підзвітних суб'єктів (аудиторів, юристів, нотаріусів, крипто-провайдерів) до роботи з російськими клієнтами.

Тип заходу	Деталізація вимог	Практична імплементація
Посилена перевірка (EDD)	Обов'язкове застосування заходів посиленої належної перевірки до *всіх* ділових відносин та транзакцій, що залучають високоризикові треті країни.	Банки не можуть застосовувати спрощену або стандартну перевірку. Кожна транзакція з РФ розглядається як апріорі підозріла.
Джерела статків (SoW/SoF)	Вимога отримання додаткової інформації про клієнта, бенефіціарного власника та *походження коштів і статків*.	Клієнти з російським корінням мусять надати документальні докази легальності капіталу за весь період його формування (історична ретроспектива).
Схвалення керівництва	Встановлення або продовження ділових відносин потребує схвалення старшого керівництва (Senior Management Approval).	Рішення про обслуговування російських клієнтів піднімається з рівня комплаєнс-офіцера на рівень правління, що збільшує персональну відповідальність директорів.
Посилений моніторинг	Вимога проведення посиленого моніторингу ділових відносин шляхом збільшення кількості та частоти перевірок.	Перехід від періодичного перегляду до моніторингу в режимі реального часу та запиту пояснень щодо економічної доцільності кожної операції.

На відміну від санкцій, які часто є адресними (блокування конкретних осіб чи секторів), статус країни з високим ризиком є *структурним* і *всеохоплюючим*. Він стосується всієї юрисдикції. Це

створює ефект "токсичності", коли вартість комплаєнсу для обслуговування транзакцій з Росією стає настільки високою, що фінансові установи обирають стратегію повного де-ризкінгу — тобто розриву відносин.

Геополітичний вимір та вплив на Україну

Міністерство фінансів України відіграло ключову роль у адвокації цього рішення. Міністр фінансів Сергій Марченко назвав це "історичним рішенням", яке допоможе протидіяти російським загрозам, включаючи фінансування тероризму та ухилення від санкцій.

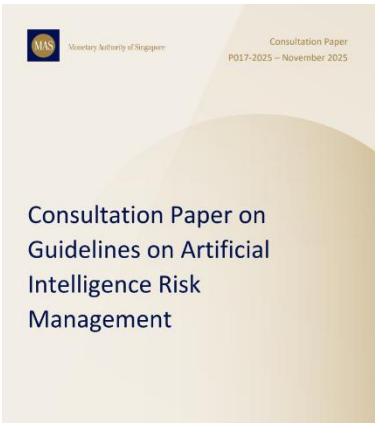
Включення до списку ЄС має екстериторіальний ефект. Європейські банки будуть вимагати від своїх банків-кореспондентів у третіх країнах (наприклад, у Туреччині, ОАЕ, Казахстані, Китаї) застосовувати аналогічні заходи перевірки до російських платежів, якщо ці платежі проходять через євро. Це звужує можливості Росії використовувати "дружні юрисдикції" як шлюзи для доступу до європейського ринку.

Висновки:

- **Тотальна "токсичність" юрисдикції:** Рішення ЄК перетворює Росію на фінансового вигнанця не лише через політичні санкції, а й через технічні стандарти фінансової безпеки. Будь-яка транзакція з РФ тепер автоматично класифікується як операція з підвищеним ризиком ВК, що робить її проведення через європейську банківську систему практично неможливим.
- **Ефект "доміно" для третіх країн:** Банки у нейтральних юрисдикціях (ОАЕ, Центральна Азія) опиняться під подвійним тиском: з одного боку, санкції США (вторинні санкції), з іншого — AML-вимоги ЄС. Це змусить їх обирати між збереженням доступу до ринків долара/євро та обслуговуванням російського капіталу.
- **Інструмент для конфіскації:** Статус високого ризику створює потужне правове підґрунтя для арешту та подальшої конфіскації російських активів у Європі, оскільки презумпція легальності походження коштів з такої юрисдикції фактично скасовується.

Крім того, це рішення посилює позицію України у питаннях конфіскації активів. У європейських судах статус "високоризикової юрисдикції" значно спрощує доведення незаконного походження коштів російських олігархів, фактично перекладаючи тягар доведення (burden of proof) на власника активів.

Від принципів до жорстких процесів: Глибокий аналіз Керівних принципів MAS щодо управління ризиками AI [2]



Грошово-кредитне управління Сінгапуру (MAS) зробило вирішальний крок у трансформації наглядового ландшафту технологій, опублікувавши у листопаді 2025 року консультативний документ щодо "Керівних принципів управління ризиками штучного інтелекту". Цей документ знаменує собою фундаментальний зсув парадигми від декларативного слідування етичним нормам до впровадження жорстко регламентованих операційних процедур. Якщо раніше сінгапурський регуляторний підхід базувався на добровільних принципах FEAT (Fairness, Ethics, Accountability, Transparency — Справедливість, Етика, Підзвітність, Прозорість), запроваджених у 2018 році, то запропоновані Керівні принципи перетворюють ці концепції на обов'язкові елементи системи внутрішнього контролю

[2] https://www.mas.gov.sg/-/media/mas-media-library/publications/consultations/bd/2025/final_consultation_paper_on_guidelines_on_ai_risk_management_forrelease.pdf

фінансових установ. Документ чітко артикулює, що відповідальність за управління ризиками AI більше не може бути локалізована в межах IT-департаментів або підрозділів аналітики даних; вона безальтернативно піднімається на рівень Ради директорів та вищого керівництва (Board and Senior Management). Саме керівні органи зобов'язані не просто бути поінформованими про впровадження технологій, а активно затверджувати стратегію управління даними, визначати апетит до ризику щодо використання AI та забезпечувати наявність ресурсів для ефективного нагляду.

Запропонована архітектура управління ризиками базується на вимозі створення комплексного інвентарю (AI Inventory) всіх систем штучного інтелекту, що використовуються в установі, включаючи ті, що знаходяться на стадії розробки, тестування або експлуатації. Це є прямою відповіддю на загрозу "тіньового AI" (Shadow AI), коли окремі бізнес-підрозділи можуть впроваджувати алгоритмічні рішення без централізованого погодження, створюючи приховані вразливості. Для кожного елемента в цьому реєстрі фінансова установа зобов'язана проводити формалізовану оцінку суттєвості ризику. Методологія такої оцінки, згідно з баченням MAS, має бути багатовимірною і враховувати щонайменше три ключові параметри: вплив (Impact) на клієнтів та фінансову стабільність установи у разі збою, складність (Complexity) використовуваних моделей та ступінь покладання (Reliance) на результати роботи алгоритму. Такий підхід вимагає від банків перегляду існуючих карт ризиків і інтеграції специфічних метрик AI в загальну систему управління операційними ризиками. Критично важливо, що регулятор вимагає застосування цих стандартів не лише до власних розробок (in-house), але й до рішень, придбаних у зовнішніх постачальників (Third-Party AI), що фактично поширює наглядовий периметр на технологічних торговців через механізми договірної відповідальності та належної перевірки.

Особливий акцент у документі зроблено на специфічних викликах, пов'язаних із Генеративним AI та Великими мовними моделями (LLMs). MAS визнає, що ці технології вносять нові вектори загроз, які не були характерні для традиційного машинного навчання, зокрема "галюцинації" (генерація правдоподібної, але хибної інформації), непередбачувану поведінку (emergent behavior) та вразливість до атак через маніпуляцію вхідними даними (prompt injection attacks). У відповідь на це регулятор пропонує впровадження спеціалізованих контролів життєвого циклу (AI Life Cycle Controls). У сфері управління даними це означає забезпечення репрезентативності навчальних вибірок для уникнення

Висновки:

- **Обов'язкова інвентаризація та класифікація:** Фінансові установи повинні створити централізований реєстр усіх систем AI (включаючи GenAI та моделі третіх сторін) та класифікувати їх за матрицею матеріальності ризику, що стане фундаментом для визначення необхідного рівня контролю.
- **Персональна відповідальність Ради директорів:** Управління ризиками AI виводиться з площини суто технічних завдань; Рада директорів зобов'язана затвердити структуру управління, яка гарантує відповідність використання AI затвердженому апетиту до ризику та етичним принципам FEAT.
- **Специфічні контролі для GenAI:** Визнання унікальних ризиків генеративного AI (галюцинації, маніпуляції даними) вимагає впровадження додаткових шарів захисту, включаючи спеціалізоване тестування на стійкість (adversarial testing) та моніторинг дрейфу моделей (model drift) в режимі реального часу.
- **Контроль ланцюга постачання:** Використання сторонніх рішень не звільняє установу від відповідальності; банки повинні інтегрувати вимоги щодо прозорості та тестування моделей у процеси закупівель та контрактні зобов'язання торговців.

упередженості, що є технічною реалізацією принципу Справедливості з FEAT. У сфері прозорості (Transparency) та пояснюваності (Explainability) MAS демонструє прагматичний підхід: визнаючи, що повна інтерпретація "чорних скриньок" (Black Box models) може бути технічно неможливою, регулятор вимагає забезпечення "пост-фактум пояснюваності" — здатності установи пояснити логіку прийняття конкретного рішення клієнту або аудитору, а також забезпечення відтворюваності результатів.

Крім того, документ інституціоналізує вимогу "людського нагляду" (Human-in-the-loop), інтенсивність якого має прямо корелювати з рівнем матеріальності ризику. Для процесів, що мають високий вплив на права та фінансове становище клієнтів (наприклад, кредитний скоринг або виявлення підозрілих транзакцій), повна автоматизація без участі людини визнається неприйнятною. Фінансові установи повинні розробити механізми, які дозволяють операторам перехоплювати управління або ветувати рішення AI у випадку виявлення аномалій. Це вимагає від банків інвестицій не лише в технології, а й у навчання персоналу, здатного критично оцінювати рекомендації алгоритмів. Взаємодія з національними ініціативами, такими як Project MindForge та Veritas, підкреслює намір Сінгапуру створити екосистему, де регуляторні вимоги підкріплюються практичними інструментами тестування та валідації моделей, що робить цей документ глобальним бенчмарком для регулювання AI у фінансовому секторі.

Реформа системи звітування про підозрілу діяльність (SARs) у Великій Британії: Аналіз оновлених настанов UKFIU [3] [4] [5]

У листопаді 2025 року Підрозділ фінансової розвідки Великої Британії (UKFIU), що діє у структурі Національного агентства по боротьбі зі злочинністю (NCA), завершив масштабне оновлення методологічної бази системи звітування про підозрілу діяльність (SARs), опублікувавши три нові розділи Керівництва. Цей крок є відповіддю на довготривалу критику системи за надмірну кількість "захисних" звітів низької якості та технічну застарілість інфраструктури. Оновлені документи формують єдину екосистему вимог, яка зміщує фокус з формального виконання регуляторних норм на надання правоохоронним органам дієвої розвідувальної інформації. Реформа підкріплюється впровадженням нового Порталу SAR, який замінює застарілу систему SAR Online, вимагаючи від суб'єктів моніторингу адаптації своїх операційних процесів до нових технічних та змістовних стандартів.

Документ "Chapter 1: Using the SAR Portal" фокусується на технічній архітектурі взаємодії. Ключовою новацією є суворі вимоги до ідентифікації та реєстрації користувачів, спрямовані на забезпечення цілісності даних та безпеки каналів зв'язку. UKFIU наголошує на критичній важливості актуальності контактних даних у профілі організації. Це не бюрократична вимога, а операційна необхідність: у випадку подання запиту на Захист від відмивання коштів (DAML), будь-яка затримка у комунікації через невірні контакти може призвести до спливу термінів, що поставить установу перед вибором між блокуванням коштів клієнта без правових підстав або здійсненням транзакції з ризиком вчинення злочину. Інструкція деталізує процеси делегування прав доступу, що дозволяє великим фінансовим групам налаштувати гнучку систему

[3] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/774-ukfiu-chapter-1-using-the-sar-portal/file
[4] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/775-ukfiu-chapter-2-submitting-a-sar/file
[5] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/776-ukfiu-chapter-3-understanding-damls-and-datfs/file

внутрішнього погодження звітів перед їх відправкою, забезпечуючи додатковий рівень контролю якості на стороні підзвітного суб'єкта.

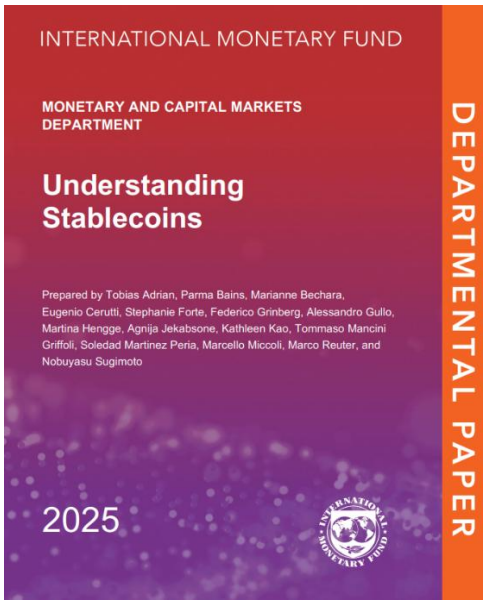
"Chapter 2: Submitting a SAR" є методологічним ядром реформи, яке встановлює нові стандарти якості звітування. UKFIU прямо засуджує практику "захисного звітування" (defensive reporting) — подання малозмістовних звітів виключно для уникнення регуляторних санкцій. Натомість вимагається чітка структуризація "Причини підозри" (Reason for Suspicion), яка повинна відповідати на питання "хто, що, де, коли, чому і як", уникаючи надмірного використання професійного жаргону, але надаючи конкретні фактичні дані. Найважливішим елементом стає обов'язкове та коректне використання кодів глосарію (Glossary Codes). Це інструмент автоматизованого сортування, який дозволяє правоохоронцям миттєво виявляти пріоритетні загрози серед сотень тисяч звітів. Наприклад, коди на кшталт "XXSNEXX" (пов'язані з санкціями) або коди, що стосуються фінансування тероризму, автоматично ескалюють звіт до відповідних підрозділів. Неправильне кодування фактично робить звіт "невидимим" для аналітиків, нівелюючи зусилля комплаєнс-офіцера. Документ також чітко розмежовує повідомлення про злочин (яке має спрямовуватися в поліцію) та фінансову розвідку, вимагаючи від суб'єктів розуміння різниці між цими процесами.

"Chapter 3: Understanding DAMLs and DATFs" містить найбільш суттєві юридичні зміни. Відбувся остаточний перехід від термінології "Згода" (Consent) до "Захист" (Defence against Money Laundering - DAML). Це фундаментальна зміна парадигми: UKFIU підкреслює, що регулятор не "дозволяє" проведення транзакції і не підтверджує законність коштів, а лише надає підзвітному суб'єкту статутний захист (defence) від кримінального переслідування за конкретну дію з конкретним майном, яка в іншому випадку вважалася б злочином. Документ встановлює жорсткі критерії для подання DAML: такий запит може бути поданий лише за наявності чітко ідентифікованого майна та наміру здійснити конкретну дію. Запити "на всяк випадок" або для отримання "комфорту" щодо клієнта будуть відхилятися. Окрему увагу приділено ризику розголошення (tipping off) відповідно до розділу 333A POCA. У період очікування рішення (7 робочих днів плюс можливий мораторій до 31 дня і більше), установам заборонено розкривати клієнту факт розслідування. Настанова надає рекомендації щодо комунікації з клієнтами в цей період, щоб уникнути як порушення закону, так і конфлікту з клієнтом через затримку платежів. Також згадується підвищення порогу для DAML до £3000, що має зменшити кількість звітів про дрібні транзакції.

Висновки:

- **Юридична точність DAML:** Зміна терміну на "Захист" (Defence) вимагає від комплаєнс-офіцерів розуміння того, що отримання DAML не легітимізує клієнта чи його кошти загалом, а лише захищає співробітників банку від кримінальної відповідальності за конкретну транзакцію.
- **Імператив якості даних:** Використання кодів глосарію (Glossary Codes) стає критичним елементом валідності звіту; помилки в кодуванні або відсутність структурованої наративної частини можуть призвести до того, що звіт буде вважатися таким, що не надає корисної розвідінформації.
- **Управління ризиком Tipping Off:** Фінансові установи повинні розробити чіткі скрипти та протоколи комунікації з клієнтами на період очікування рішення по DAML, щоб пояснити затримки без розкриття факту подання SAR, що є кримінальним злочином.
- **Технічна готовність:** Перехід на новий Портал та вимоги до актуалізації даних вимагають перегляду внутрішніх процедур адміністрування доступу до систем фінмоніторингу, щоб уникнути операційних ризиків при поданні термінових запитів.

Аналіз документа МВФ "Розуміння стейблкоїнів" (2025): Загрози монетарному суверенітету та виклики фінансовій цілісності [6]



Опублікований у грудні 2025 року документ МВФ пропонує всебічний аналіз феномену стейблкоїнів, виходячи за межі їх сприйняття як інструменту для обслуговування крипторинку та розглядаючи їх як системний фактор глобальної економіки. Автори звіту (Tobias Adrian та ін.) констатують, що стейблкоїни, капіталізація яких стрімко зросла, а 98% вартості прив'язано до долара США, створюють безпрецедентні виклики для макрофінансової стабільності, особливо в країнах з ринками, що розвиваються (Emerging Markets and Developing Economies — EMDEs).

Ключовим макроекономічним ризиком, виділеним у звіті, є загроза "валютного заміщення" (currency substitution) або "криптоізації" (cryptoization). У країнах зі слабкими інституціями, високою інфляцією та волатильними національними валютами доларові стейблкоїни можуть швидко витіснити місцеву валюту як засіб заощадження та платежу. Це призводить до втрати "монетарного суверенітету": національні центральні банки втрачають важелі впливу на економіку, оскільки зміни процентних ставок або грошової маси не впливають на сектор, що оперує в іноземній цифровій валюті. МВФ попереджає, що цей процес може бути незворотним і призвести до відтоку капіталу, послаблення фінансового посередництва локальних банків та підвищення вразливості до зовнішніх шоків.

Висновки:

- **Загроза монетарному суверенітету:** Поширення доларових стейблкоїнів у країнах, що розвиваються, загрожує повною "доларизацією" економік та втратою здатності національних урядів проводити незалежну монетарну політику.
- **Системна інтеграція ризиків:** Тісний зв'язок резервів стейблкоїнів з ринком державного боргу США створює канал передачі кризових явищ з крипторинку в традиційну фінансову систему, що вимагає жорсткого пруденційного нагляду.
- **Прогалини в AML/CFT:** Технологічні особливості та регуляторна фрагментація роблять стейблкоїни ефективним інструментом для обходу санкцій; МВФ закликає до глобальної координації та уніфікації стандартів (зокрема, імплементації Travel Rule).
- **Вимога банківських стандартів:** Для пом’якшення ризиків емітенти стейблкоїнів повинні підлягати регулюванню, еквівалентному банківському, з акцентом на захист прав споживачів та гарантування погашення (redemption rights).

З точки зору фінансової цілісності та ПВК/ФТ, документ вказує на структурні прогалини в існуючій архітектурі нагляду. Стейблкоїни, завдяки своїй технологічній природі (можливість піринговых P2P переказів в обхід посередників, використання некастодіальних гаманців/unhosted wallets), створюють ідеальне середовище для обходу міжнародних санкцій та відмивання коштів. МВФ наголошує на проблемі фрагментації регулювання: різні юрисдикції застосовують різні підходи (від MiCA в ЄС до Clarity for Payment Stablecoins Act у США та специфічних режимів в Азії), що створює можливості для регуляторного

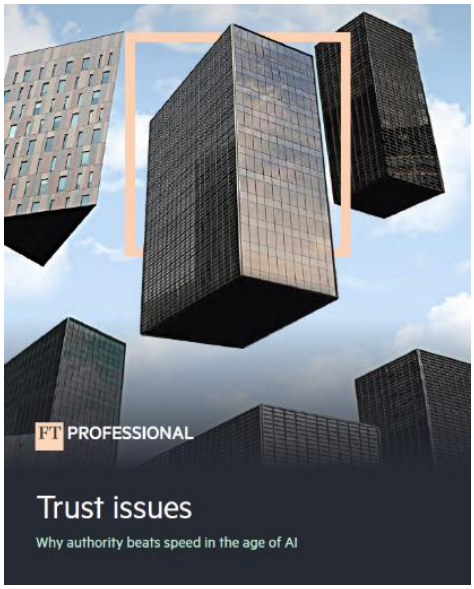
[6] https://www.imf.org/-/media/files/publications/dp/2025/english/usea.pdf

арбітражу. Емітенти можуть обирати юрисдикції з найслабшим наглядом, продовжуючи надавати послуги глобально.

Окремий блок аналізу присвячено структурі резервів. Найбільші стейблкоїни (USDT, USDC) акумулюють значні обсяги короткострокових казначейських зобов'язань США (US Treasuries), стаючи вагомими гравцями на ринку традиційного боргу. МВФ попереджає про ризик зворотного зв'язку: паніка на ринку криптоактивів ("run on stablecoin") може змусити емітентів екстрено розпродавати казначейські облігації, що спровокує волатильність і підвищення ставок на традиційних фінансових ринках. У зв'язку з цим МВФ наполягає на застосуванні принципу "однакова діяльність, однаковий ризик, однакове регулювання", рекомендуючи застосовувати до емітентів стейблкоїнів пруденційні вимоги, аналогічні банківським: високі стандарти ліквідності, сегрегація активів клієнтів, прозорість резервів та обов'язковий аудит.

Звіти окремих інституцій та експертів

Штучний Інтелект та Криза Довіри: Звіт FT Professional про Трансформацію Послуг [7]



Звіт комплексно досліджує зміну парадигми довіри, цінності та професійних компетенцій у світі, де штучний інтелект (AI) проникає в усі види інтелектуальної праці. Головна ідея документа полягає в тому, що вік швидкості, який приніс AI, не замінює — а навпаки посилює потребу в авторитетності, відповідальності та надійності. Для надавачів професійних послуг (юридичних фірм, консалтингу, фінансового сектору тощо) AI стає каталізатором структурних змін у бізнес-моделях, процесах і вимогах до персоналу.

На початку звіту підкреслюється, що питання “чи використовувати AI” більше не існує; стоїть лише питання **як** його використовувати відповідально. Водночас існує значний глобальний дефіцит довіри: половина респондентів у дослідженні KPMG не довіряють AI. На цьому тлі компанії зростаючими темпами інвестують у технології, розуміючи їх конкурентну важливість — 65% опитаних FT Professional вказують AI як один із ключових інвестиційних пріоритетів. Окрема увага приділяється напрузі між необхідністю оперативно експериментувати з новими інструментами та потребою підтримувати належне управління й безпеку даних.

Звіт детально демонструє, як AI трансформує традиційні механізми створення вартості. Яскравим прикладом є юриспруденція, де рутинна робота молодших юристів — аналіз документів, e-discovery, узагальнення матеріалів — тепер виконується за лічені хвилини за допомогою AI. Це, з одного боку, полегшує робочий тиск і дає змогу юристам зосередитися на аналітичній роботі; з іншого — підриває саму концепцію billable hour, роблячи її застарілою як метод вимірювання вартості. Клієнти очікують швидше отримувати продукти та більше стратегічної цінності за ті ж кошти. Виникають альтернативні моделі плати: фіксовані тарифи, підписка, оплата за підсумковий результат, а не за витрачений час. Компанії дедалі більше орієнтуються на фінансові наслідки використання AI, а не на кількість годин, що потребує нових підходів до оцінки продуктивності та внеску.

[7] https://www.ragan.com/white-papers/trust-issues-why-authority-beats-speed-in-the-age-of-ai/

Водночас AI стимулює створення нових напрямів діяльності: половина компаній уже відкрили окремі бізнес-підрозділи, що надають AI-підсилені послуги. За прикладами з юридних фірм, AI навіть розширює спектр завдань, які клієнти передають юристам — наприклад, аналіз податкових декларацій, створення внутрішніх рекомендацій щодо оптимізації, що раніше виконували сторонні фінансові спеціалісти.

Наступний великий блок звіту присвячено відповідальному використанню AI. Значна частина компаній вважає, що обмеження щодо конфіденційності клієнтів завжди стримуватимуть впровадження AI — 45% респондентів прямо вказали на це. Тому в юридичній галузі з'явився чіткий підхід, заснований на **трьох принципах: згода, компетентність, конфіденційність**. Практики виділяють численні ризики: від некоректної сегрегації клієнтських даних до неконтрольованих «галюцинацій» AI. Юридичні фірми створюють жорсткі інфраструктурні "етичні стіни" між клієнтами та інвестують у освіту персоналу, адже без правильної компетенції використання інструментів може становити загрозу. Звіт підкреслює, що управління ризиками AI неможливе без культури грамотного використання інструментів і постійного навчання.

Далі документ показує, що в епоху інформаційного перенасичення та зростання кількості помилкових даних ключовим ресурсом стає не швидкість, а авторитетність джерела. Навіть за наявності найпотужніших LLM, компанії вказують, що для прийняття стратегічних рішень людська оцінка важливіша за AI: 64% вважають людський інтелект ціннішим у критичному аналізі, хоча для макроринкової аналітики бізнес частіше покладається на AI. Саме тому конкурувати в майбутньому будуть не за доступ до AI, а за якість власних, унікальних баз даних, довготривалу репутацію та контрольовані канали знань.

Звіт також зауважує, що правові та репутаційні ризики навколо використання стороннього контенту для тренування моделей стають дедалі гострішими. Справи проти компаній, що незаконно використовують авторські матеріали, змусили найбільших гравців, таких як OpenAI, укладати офіційні ліцензійні угоди з видавцями (Financial Times, NYT, Washington Post). Це формує нову ринкову динаміку: високоякісні дані стають стратегічним активом, спонукаючи корпорації до купівлі технологічних компаній (угоди Salesforce—Informatica, IBM—DataStax), аби зміцнити доступ до структурованих і неструктурованих даних.

У блоці про бар'єри виділено три основні проблеми, що ускладнюють поєднання AI-інсайтів із

Висновки:

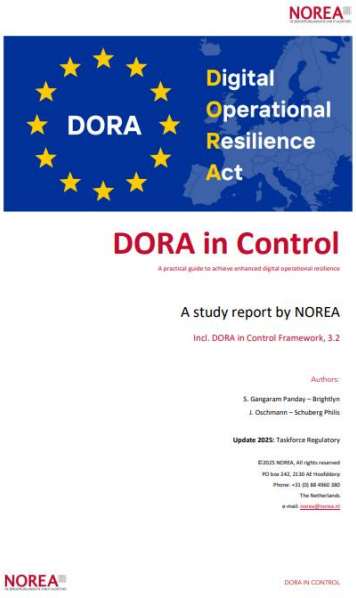
- **Бізнес-моделі професійних послуг змінюються: billable hour стає застарілою.** Компаніям необхідно перейти до моделей, що відображають створену цінність, а не часові витрати. Рекомендація: вже зараз адаптувати системи оцінювання ефективності та розробити альтернативні схеми оплати (фіксовані тарифи, підписки, outcome-based fee).
- **Авторитетні дані стають стратегічною конкурентною перевагою.** Компанії повинні інвестувати у власні, юридично чисті, високоякісні масиви даних і розвивати захищені AI-інфраструктури. Це також передбачає регулярне очищення, ліцензування та аудит даних.
- **Відповідальне впровадження AI неможливе без системної AI-грамотності та управління ризиками.** Необхідно впровадити обов'язкове навчання персоналу, створювати етичні протоколи, формалізувати підходи до конфіденційності та розмежування даних клієнтів, а також впроваджувати централізовані моделі governance.
- **Людські навички — критичне мислення, стратегічний контекст, інтерпретація — визначатимуть успіх.** Організації повинні розвивати компетенції, що доповнюють, а не дублюють можливості AI: постановка задач, контекстуальний аналіз, робота з клієнтами, інтеграція AI у бізнес-стратегію.

традиційними джерелами інформації:
• **організаційні та технологічні**, особливо у фінансових установах;
• **низька якість метрик AI**, що ускладнює перевірку достовірності інформації;
• **низький рівень AI-грамотності персоналу**, включно з керівництвом.

Важливою темою стає трансформація компетенцій: у середовищі, де agentic AI здатний автономно приймати частину рішень, людські навички — критичне мислення, інтерпретація, соціальна взаємодія, лідерство — стають ціннішими. Парадоксально, але попит на "м'які" навички зростає сильніше, ніж попит на суто технічні вміння. Компанії активно розбудовують компетенції з prompt engineering, розпізнавання патернів та стратегічного розуміння AI. Одночасно працівники очікують, що компанія забезпечить доступ до сучасних інструментів, і 40% бізнесів уже хвилюються щодо нерівності доступу до AI всередині організації.

Фінальна частина містить практичні поради від експертів. Їх головний меседж: **AI не замінює людей — він посилює тих, хто вміє працювати із даними, ставити правильні запитання та забезпечувати стратегічний контекст**. У центрі професійних послуг майбутнього лежатимуть:
• стратегічне мислення,
• високий рівень обізнаності у специфіці сектору,
• здатність перевіряти й удосконалювати результати AI,
• здатність інтегрувати технологію у вже ефективні робочі процеси.

Аналітичний огляд практичної імплементації DORA та її операційної рамки контролю [8]



Документ *"DORA in Control"* є комплексним методичним орієнтиром, створеним NOREA, що виконує роль мосту між нормативною базою Регламенту (ЄС) 2022/2554 (DORA) та реальними процесами управління ІКТ-ризиками у фінансових установах. Він має на меті ліквідувати прогалину між суто юридичним формулюванням вимог та практикою їх застосування. Уже у вступних положеннях автори наголошують на тому, що цифрова стійкість сьогодні — це не окрема функція, а фундаментальна умова сталого функціонування фінансового сектора, з огляду на зростання технологічної залежності, ризику каскадних ефектів збоїв і загальну складність ландшафту кіберзагроз.

Основна логіка документа складається з трьох великих блоків: контекст та обґрунтування DORA, інтерпретація принципів регулювання, а також практичний інструментарій — DORA in Control Framework. У частині, присвяченій контексту, підкреслюється еволюція європейського регулювання від фокусу на кібербезпеці до набагато ширшого поняття *операційної стійкості*. DORA позиціонується не як черговий комплаєнс-акт, а як рамка для забезпечення життєздатності критичних функцій у всіх сценаріях цифрових інцидентів. Окрема увага приділяється взаємозв'язку з NIS2, де DORA оголошена *lex specialis*, що фактично робить її більш деталізованою і жорсткою нормою для фінансової сфери. Наголошується, що, хоча багато організацій підпадають одночасно під дію NIS2 і DORA, саме

[8] https://media.licdn.com/dms/document/media/v2/D4D1FAQHLdfhjVdmuEw/feedshare-document-pdf-analyzed/B4DZrUu094IAAY-/0/1764505645528?e=1766016000&v=beta&t=h1iR-1sHoBIs-7RyK8K3fd1hiVTIY3fbRX7MNcRGVck

DORA задає чіткий технічний каркас, який може слугувати основою і для виконання вимог NIS2, які є значно загальнішими.

Важливо, що автори пояснюють сутність принципового підходу, який є стрижнем DORA. На відміну від суто приписного регулювання, DORA вимагає від установ сформувати власні механізми управління ризиками, пропорційні масштабам, складності та критичності їхніх послуг. У документі демонструється, що така гнучкість одночасно є і перевагою, і складністю: фахівці з права, IT та бізнесу інтерпретують вимоги по-різному, ускладнюючи формування єдиного підходу. Звідси виникає потреба в інструменті, який би стандартизував переклад нормативних вимог у набір контрольних дій. Саме цю прогалину й покликаний заповнити DORA in Control Framework.

Найбільш змістовну частину звіту становить опис створення та структури фреймворка, що складається з 8 доменів, 28 піддоменів та 95 конкретних контролів, кожен з яких має прямі посилання на статті DORA та відповідні RTS/ITS. Фреймворк розроблено шляхом глибокої декомпозиції вимог DORA та об'єднання повторюваних або споріднених положень у логічні контрольні одиниці. Це дозволяє фінансовим установам не лише виконувати gap-аналіз, але й отримати одразу готову операційну модель впровадження. Додатковою перевагою є інтеграція моделі зрілості ЦБ Нідерландів та візуальних інструментів прогресу, що спрощує комунікацію з правлінням, аудитом і регулятором.

Зміст доменів охоплює весь життєвий цикл ICT-ризиків: від управління та стратегічної відповідальності менеджменту, до технічних аспектів шифрування, тестування стійкості, управління інцидентами, політик розвитку ПЗ, безперервності бізнесу та критично важливих третіх сторін. Документ докладно описує, що саме повинні містити політики, які параметри мають контролюватися, як вести реєстри постачальників, якими критеріями класифікувати інциденти тощо. Це перетворює DORA з декларативного нормативного акту на практичний план дій для фінансової установи.

Особливо цінним є включення інженерного підходу до побудови контролів. Автори пропонують застосовувати метод 5W/1H (what, who, where, when, why, how) для фіксації логіки кожного рішення. Такий підхід спрямований на усунення кореневих причин, а не лише

Висновки:

- **Фінансовим установам необхідно терміново перейти від реактивного підходу до операційної стійкості до структурованої моделі, де всі процеси управління ICT-ризиками формалізовані, задокументовані й регулярно переглядаються.** DORA вимагає не просто наявності політик, а їх практичної ефективності та відповідності ризиковому профілю установи.
- **Створення деталізованого реєстру критичних функцій, активів та третіх сторін - фундаментальний елемент усієї відповідності DORA.** Без чіткої інвентаризації неможливо виконати вимоги щодо оцінки ризиків, тестування, забезпечення безперервності та класифікації інцидентів.
- **Управління взаємодією з ICT-постачальниками - один із найслабших та найризикованіших компонентів установ, і DORA робить цю сферу повністю прозорою для регулятора.** Практичне завдання - переглянути всі контракти, додати вимоги щодо аудиту, тестування, експортності даних, сценаріїв відмови та субпідрядників.
- **Фінансовим установам потрібно запровадити постійний цикл тестування стійкості та критичний аналіз інцидентів, інтегруючи їх у стратегічне управління.** Це означає щорічні тестування плану безперервності бізнесу та відновлення після катастрофи, TLPT (Threat-Led Penetration Testing) за потреби, регулярну перевірку планів відновлення, тренування кризових команд та включення результатів у стратегічну звітність для менеджменту.

відповідність вимогам. Він переводить DORA-імплементацію з рівня формального комплаєнсу до рівня системного підсилення операційної стійкості інституції.

Документ завершується докладним розкладанням кожного контролю: поясненнями, вимогами до процедур, класифікаційних підходів, фіксації відповідальності та вимог до внутрішнього аудиту. Ключовою ідеєю фінальної частини є те, що стійкість - це циклічний процес: тестування, аналіз інцидентів, постійне оновлення політик і процедур, аудит та адаптація. Фреймворк розглядається як «живий інструмент», який має еволюціонувати разом із цифровим ландшафтом та змінами у регулюванні.

Таким чином, документ не просто описує DORA — він формує практичну, структуровану, інженерно обґрунтовану методологію її реалізації, яка може використовуватися як основа для програми цифрової стійкості фінансової організації будь-якого масштабу.

Як стейблкоїни змінюють банківську інфраструктуру Європи [9]

Документ представляє собою комплексне дослідження того, як провідні європейські банки формують власні стратегічні, інфраструктурні та регуляторно-відповідні моделі використання та випуску стейблкоїнів в умовах швидкого переходу глобальних фінансових ринків до токенізованої економіки. Звіт фіксує центральну тезу: стейблкоїни перестали бути лише криптовалютним інструментом — вони трансформуються у критичний компонент банківської інфраструктури та основу майбутніх моделей руху грошей, розрахунків та цифрових активів. У вступній частині підкреслюється, що стабільне зростання інституційного інтересу та поява конкуруючих моделей емісії (банківської, консорціумної, ліцензованої під MiCA) позбавляють банки можливості залишатися осторонь, оскільки невключення до нових мереж розрахунків ризикує призвести до ерозії депозитної бази та зменшення клієнтської цінності.

Аналітична частина, що описує стан європейського ринку стейблкоїнів, демонструє різке розширення емісії єврових токенів у 2024–2025 роках (загальна капіталізація €489.7 млн станом на жовтень 2025 року), а також появу широкої палітри моделей випуску: від банківських емітентів (Banking Circle, ODDO BHF, SG-FORGE) до транснаціональних консорціумів (ING, UniCredit, SEB, Danske, KBC та ін.). Стабільний та структурний висхідний тренд ринку протягом двох років, що підтверджує дозрівання попиту й інституційної довіри. Документ підкреслює, що MiCA створив чіткий регуляторний контур, який стимулював банки переходити від експериментів до реальних продуктів, спрямованих на інтеграцію стейблкоїнів у платіжні, казначейські та інвестиційні операції клієнтів.

У виконавчому резюме наведено ключові стратегічні висновки європейських фінансових установ. По-перше, стейблкоїни починають виконувати роль нового "ліквідного та розрахункового шару" банківської інфраструктури — основу для програмованих платежів, токенізованих цінних паперів, 24/7-розрахунків. З іншого боку, банки ще не виявили сталих моделей монетизації: доходи від емісії є мінімальними, а реальне джерело прибутку — розвиток сервісів на базі токенізованих грошей: FX-конверсія, комерційні розрахунки,

[9] https://docsend.com/view/njjq9kdm9bcxw6jf

автоматизована ліквідність, корпоративні казначейські рішення. Третім важливим аспектом є баланс між масштабованістю та регуляторною відповідністю: консорціумні моделі (наприклад, ING та RBI) успішно забезпечують ліквідність і поширення, але позбавляють банк вигод від фракційного резервування. Документ наголошує, що головний бар'єр сьогодні — не технологія, а операційна перебудова банківських процесів під режим 24/7 та автоматизований AML/KYC у реальному часі, що вимагає як зміни внутрішніх процедур, так і залучення фахівців нового профілю.

У розділі Inside the Stablecoin Strategies, який охоплює інтерв'ю з ключовими банками, детально розкрито відмінності підходів:

- **Banking Circle** створив EURI як "технологічно нейтральний" банк-емітент із моделлю 1:1 резервування, роблячи акцент на ролі банку як сервісного провайдера та кастодіана для інших емітентів. Фокус — міжнародні платежі, корпоративна ліквідність та інтеграція з фінтех-сектором.
- **ING та RBI**, як члени європейського консорціуму, обґрунтовують модель спільної емісії як єдиний шлях до масштабування й усунення фрагментації. Банки підкреслюють важливість уніфікації комплаєнсу, операційних стандартів та міжбанківської взаємодії.
- **BBVA** будує власний MiCA-сумісний токен у партнерстві з Visa, орієнтуючись на ринки з високою інфляцією та пілотні програми токенізованих ринків капіталу в ЄС.
- **Delubac & Cie** позиціонує себе як нішевий "кореспондентський банк 3.0", який використовує стейблкоїни для прискорення міжнародних розрахунків і пропонує корпоративним клієнтам інноваційні послуги токенізованих інструментів ліквідності.
- **ODDO BHF** продемонстрував модель прямої емісії EUROD із розміщенням резервів на балансі банку, що підвищує довіру та ліквідність. Цей підхід є рідкісним серед європейських банків і демонструє повноцінне інтегрування стейблкоїну у внутрішню фінансову архітектуру.
- **SG-FORGE** реалізувала найбільш технологічно просунутий кейс: стабільні токени EURCV та USDCV, які використовуються не лише у корпоративних розрахунках та капітальних ринках, а й у

Висновки:

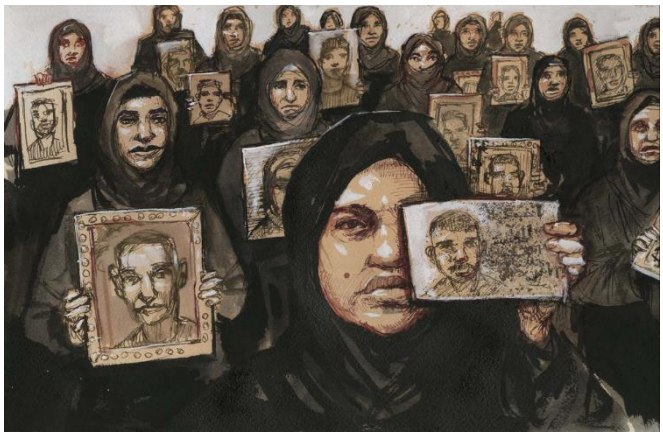
- **Європейські банки переходять від експериментів до реальної інтеграції стейблкоїнів у платіжну та казначейську інфраструктуру.**
  Практична дія: банкам необхідно створювати 24/7-сумісні розрахункові моделі, автоматизувати AML/KYC-процеси та впроваджувати програмовані грошові інструменти для корпоративних клієнтів.
- **Консорціумні моделі стають ключем до масштабування, але банки повинні узгодити операційні стандарти, процедури комплаєнсу та управління ризиками.**
  Практична дія: розробка спільних AML-правил, протоколів взаємодії, стандартизованих SLA для емісії та викупу стейблкоїнів.
- **Участь банків у DeFi через ліцензовані токени (як у кейсі SG-FORGE) формує новий клас регульованої onchain-ліквідності.**
  Практична дія: установам слід розглядати DeFi-інтеграцію через permissioned vaults, де забезпечується вбудований KYC та контроль ризиків.
- **Європі необхідні масштабні єврові стейблкоїни для збереження конкурентоспроможності проти домінування долара в ончейн-економіці.**
  Практична дія: урядам і регуляторам слід стимулювати розвиток інфраструктури та сприяти гармонізації MiCA у межах всього ЄС.

DeFi. Показовим є кейс інтеграції з Morpho та Uniswap, що робить Société Générale першим глобальним системно важливим банком (G-SIB), який вивів стейблкоїн у децентралізоване середовище. Також наведено схему, яка ілюструє інтеграцію через permissioned vaults, демонструючи повну відповідність ризик-мандатам та AML-вимогам, при цьому забезпечуючи участь банку у глобальній onchain-ліквідності.

Розділ про тематичний кейс Morpho демонструє, як децентралізовані кредитні протоколи стимулюють реальний попит на стейблкоїни, створюючи механізми позики, генерації прибутку, ізольованих ризикових сегментів, повної прозорості та програмованої ліквідності. Діаграма на сторінці 13 чітко показує, як Morpho виступає “ліквіднісним шаром” для стейблкоїнів, забезпечуючи високий обсяг операцій та інституційний рівень управління ризиками. У цьому контексті інтеграція SG-FORGE стала новим етапом зближення традиційного банкінгу та DeFi, оскільки відкриває можливість для корпоративних та казначейських клієнтів використовувати програмовані onchain-операції з повним збереженням регуляторної відповідності.

Фінальний розділ із "голосами індустрії" представляє стратегічне бачення учасників ринку: формування майбутнього олігополії єврових стейблкоїнів, перехід до універсальної токенізації фінансових потоків, технологічні зрушення у сфері RWA та DeFi, а також потребу у взаємодії традиційних та токенізованих систем до моменту, коли фінансова інфраструктура стане повністю ончейн. Експертні цитати підкреслюють, що стейблкоїни — не тимчасовий тренд, а ключовий елемент глобальної конкуренції між ЄС і США за майбутню архітектуру цифрових валют.

Правда, похована у архівах: що відкриває світові Damascus Dossier [10]



Damascus Dossier — це масштабне транскордонне розслідування, яке розкриває цілісну картину того, як сирійський режим Башара Асада створив і підтримував одну з найбільш брутальних державних «машин убивств» XXI століття, а також як ця система була опосередковано підживлена міжнародними фінансовими потоками та недостатнім контролем з боку міжнародних організацій. В основі розслідування — понад 134 000 файлів (приблизно 243 ГБ даних) із сирійських спецслужб за більш ніж три десятиліття, від середини 1990-х до грудня 2024 року, включно з документами Повітряної розвідки, Головного управління розвідки та інших силових структур. Ці матеріали, отримані німецьким мовником NDR і передані ICIJ та 24 медіапартнерам, містять внутрішні доповідні, службове листування, оперативні звіти, списки затриманих і загиблих, медичну документацію, а також понад 33 000 високоякісних фотографій тіл загиблих, що документують смерті щонайменше понад 10 200 в’язнів режиму, переважно у 2015–2024 роках. Сукупно вони демонструють не хаотичні злочини на тлі війни, а системну політику масових арештів, тортур і вбивств, бюрократично оформлених через мережу спецслужб, військових госпіталів та «офіційної» документації, покликаної приховати масштаби насильства.

Документи і фотодокази показують, як арешти та страти набули індустріального, майже конвеєрного характеру. Фотографії, зроблені військовими фотографами, фіксують тіла виснажених, закатованих людей, іноді — по кілька десятків знімків однієї жертви, позначеної

[10] https://www.icij.org/investigations/damascus-dossier/

лише номером; серед жертв є навіть немовлята. Це не випадкові «витоки» окремих злочинів, а внутрішній архів держави: найбільша колекція зображень убитих сирійських в'язнів, коли-небудь отримана журналістами. За даними ICIJ, знімки передавалися до військових судів, де судді своїми підписами «легалізували» смерті як юридичний факт, фактично забезпечуючи виконавцям судовий імунітет. Паралельно з цим працював паперовий конвеєр: військові госпіталі Харрастаў та Тішрін оформлювали медичні свідоцтва про смерть, де причиною майже завжди зазначалася «кардіореспіраторна» або «серцева зупинка», тобто «натуральна» смерть, що приховувало реальні причини — голод, тортури, побиття, інші форми нелюдського поводження. Один із колишніх лікарів свідчить, що бланки довідок готувалися наперед і їх просто «підписували», не маючи жодного стосунку до реальної судово-медичної оцінки. Аналіз репрезентативної вибірки фотографій показав: приблизно три чверті тіл мають ознаки голодування, майже дві третини — ознаки фізичного насильства, майже половина — повністю оголені. При цьому, за оцінками Syrian Network for Human Rights, режим Асада зник безвісти понад 160 000 людей, тобто навіть ця колосальна маса матеріалів охоплює лише фрагмент загального масштабу злочинів.

Окремий вимір Damascus Dossier — це людський вимір «пошуку правди» сім'ями зниклих. Після падіння режиму в грудні 2024 року тисячі людей кинулися до тюрем, моргів, масових поховань, переглядали архіви, написи на стінах камер, останки в братських могилах, намагаючись знайти бодай натяк на долю рідних. У статті про Тхайєра аль-Наджара із ICIJ показано, як одна роздрукована фотографія знімка свідоцтва про смерть брата, виданого одним із відділень служб безпеки, стає для родини першим офіційним підтвердженням загибелі після 13 років невідомості. Для інших сімей витік документів дає бодай мінімальний фрагмент істини — ім'я в рукописному списку розстріляних, запис у внутрішньому реєстрі, фото тіла. Водночас ті ж матеріали оголюють масштабну вторинну травму: відкриття архівів, короткий період, коли людям дозволили фотографувати документи, а потім знову їх закриття новою владою, глибокі конфлікти між офіційною «комісією з розшуку зниклих» та низовими ініціативами, такими як рух «Намети правди», де родини публічно вимагають повної відкритості архівів і доступу до інформації. Цей пласт показує не лише злочини минулого, а й сучасну боротьбу за право на пам'ять, правду і справедливість, що прямо корелює з майбутніми процесами перехідного правосуддя, кримінального переслідування та розробки політик репарацій.

Ще один критично важливий аспект дослідження — виявлення міжнародних фінансових і інституційних зв'язків, які опосередковано підтримували репресивну систему. Матеріали щодо компанії Shorouk for Protection, Guarding and Security Services демонструють, що ООН протягом більш ніж десятиліття заплатила цій структурі щонайменше 11 млн доларів США в рамках понад 130 контрактів за охорону офісів і об'єктів агенцій ООН у Дамаску, зокрема штаб-квартири у готелі Four Seasons та спільних приміщень для кількох агенцій. Витік внутрішніх меморандумів показує, що Shorouk де-факто була «володіємою та контрольованою» Головним управлінням розвідки — одним з найжорстокіших репресивних органів, причетних до тортур, сексуального насильства та позасудових страт. У документах фіксуються перекази «частки прибутку» компанії на рахунки спецслужби, а також листування, де сирійські посадовці, включно з міністром закордонних справ Фейсалом Мекдадом, обговорюють необхідність збереження контрактів з ООН, бо персонал Shorouk використовувався для стеження за співробітниками ООН і контролю над їхньою діяльністю. Попри попередження правозахисних організацій у 2022 році щодо зв'язків Shorouk із розвідкою, ООН продовжувала працювати з компанією ще два роки, посилаючись на формальну відповідність процедур закупівель і відсутність «офіційних» доказів власності з боку спецслужб. У результаті гуманітарні кошти фактично перерозподілялися на користь апарату, який паралельно катував і вбивав десятки тисяч громадян.

Узагальнююча стаття «About the Damascus Dossier» підсумовує, що витік не лише документує злочини, а й демонструє повну логіку функціонування «машини зникнення»: централізований контроль над мережею спецслужб, координація з союзниками (зокрема Росією та Іраном), систематичне використання медичних закладів та бюрократичної звітності для маскування вбивств, а також критично важливі зв'язки з міжнародними інституціями, через які режим отримував легітимацію та ресурси. Журналісти з понад 20 країн, працюючи над масивом документів понад вісім місяців, не лише реконструювали ланцюг командування й механіку вбивств, а й перенесли фокус на право жертв і їхніх родин на правду, ідентифікацію тіл, доступ до свідоцтв про смерть, фіксацію винних і забезпечення того, щоб ці дані були використані в кримінальних справах, процесах універсальної юрисдикції, санкційній та фінансовій політиці. Сама структура Dossier (документи спецслужб + фотодокази + фінансова та контрактна документація) створює фундамент для подальших дій: від цільових санкцій і замороження активів причетних до відмивання коштів і контрактних схем до посилення due diligence в ООН та інших міжнародних організаціях, які працюють у середовищах з високим ризиком масових порушень прав людини.

Висновки:

- **Damascus Dossier створює безпрецедентну доказову базу для кримінальних переслідувань і санкційної політики.**
- Необхідні кроки: системна передача структурованих даних (імена жертв, підписантів, командирів, служб, дат та місць) до органів, що здійснюють провадження за принципом універсальної юрисдикції, а також до органів, відповідальних за санкції та фінансовий моніторинг, з метою індивідуальних санкцій, замороження активів і включення до списків високого ризику.
- **Документи та фотодокази демонструють повністю бюрократизовану модель масових убивств, де медична та судова документація системно використовувалися для приховування злочинів.**
- Необхідні кроки: включити аналіз «офіційних» документів режиму (свідоцтв про смерть, внутрішніх медичних записів, реєстрів в'язниць) у стандартні методики розслідування злочинів проти людяності; використовувати ці паттерни для оцінки ризиків у поточних конфліктах, де аналогічні практики можуть маскуватися під формальну законність.
- **Розслідування виявило системну інституційну уразливість ООН та інших міжнародних організацій до проникнення з боку репресивних режимів через контракти, закупівлі й безпекові послуги.**
- Необхідні кроки: радикально посилити процедури належної перевірки для постачальників, особливо у сфері безпеки в країнах із високим ризиком масових порушень прав людини; запровадити обов'язкову перевірку бенефіціарної власності контрагентів на предмет зв'язків із спецслужбами й силовими структурами, підкріплену незалежними зовнішніми аудитами та прозорою публічною звітністю.
- **Для сімей зниклих витік матеріалів став одночасно джерелом правди і нової травми, а питання доступу до архівів перетворилося на ядро майбутнього перехідного правосуддя в Сирії.**
- Необхідні кроки: створити незалежний, захищений механізм управління архівами (із участю постраждалих, неурядових організацій та міжнародних партнерів), який забезпечить безпечний доступ родин до інформації про долю зниклих, поєднуючи це з програмами психологічної підтримки, юридичної допомоги та чітким планом використання цих даних у національних і міжнародних процедурах правосуддя.

Рекомендовані матеріали та заходи

Європейський саміт з боротьби з фінансовими злочинами 2026 [11]

Дата: 29 квітня 2026 року

Місце: RDS Convention Centre, Дублін, Ірландія

Організатор: AML Intelligence

Цей захід, анонсований як одна з головних подій року у сфері фінансової безпеки, має стратегічне значення для професійної спільноти у 2026 році. Його актуальність зумовлена завершенням формування нової архітектури фінансового моніторингу в Європейському Союзі, зокрема повноцінним запуском AMLA (Anti-Money Laundering Authority) у Франкфурті. Саміт стане платформою, де будуть визначені практичні аспекти взаємодії між новим наднаціональним регулятором та національними наглядовими органами.

Основні тематики: Програма заходу сфокусована на найбільш гострих викликах, що стоять перед індустрією:

- **Нова ера нагляду ЄС:** Детальний розбір механізмів прямого нагляду AMLA за найбільш ризиковими транскордонними фінансовими установами.
- **Геополітика та Санкції:** Аналіз впливу глобальної нестабільності на режими санкцій, методи виявлення схем обходу через треті юрисдикції та роль вторинних санкцій.
- **Технологічні інновації:** Практичне застосування AI в транзакційному моніторингу, боротьба з шахрайством, що використовує діпфейки (AI-enabled fraud), та регулювання криптоактивів в рамках MiCA.
- **Людський фактор та злочинність:** Роль фінансових установ у виявленні ознак торгівлі людьми та сучасного рабства через аналіз фінансових потоків.

Ключові спікери: Склад доповідачів підтверджує високий статус заходу, залучаючи осіб, що безпосередньо впливають на формування політики:

- **Bruna Szego:** Голова AMLA. Її виступ очікується як програмний, що визначить пріоритети європейського нагляду на найближчі роки.
- **Claude Bocqueraz:** Заступник голови підрозділу з боротьби з фінансовими злочинами Європейської Комісії (DG FISMA), ключова фігура у розробці законодавства ЄС.
- **Philippe Vollot:** Член правління Rabobank, екс-CCO Danske Bank, визнаний експерт з антикризового управління та трансформації комплаєнс-культури.
- **Ilze Znotina:** Колишня директорка ПФР Латвії, відома своєю безкомпромісною боротьбою з відмиванням коштів через балтійську фінансову систему.

Для кого це корисно: Участь у саміті є важливою для керівників департаментів фінансового моніторингу українських банків, що підтримують кореспондентські відносини з європейськими установами, працівників з санкційного комплаєнсу, а також представників регуляторів, які працюють над гармонізацією українського законодавства з нормами ЄС. Це унікальна

[11] https://www.amlintelligence.com/asp-products/european-anti-financial-crime-summit-2026/

можливість зрозуміти очікування європейських партнерів "з перших вуст" та адаптувати власні стратегії ризиків.

Навчальні кейси UKFIU [12]

Ця всеосяжна серія навчальних матеріалів, що складається із 14 відео, є цінним ресурсом, спрямованим на поглиблене розуміння та практичне виявлення фінансових злочинів. Основна корисність цього циклу, присвяченого тематичним дослідженням Звітів про підозрілу діяльність (SARs) UKFIU, полягає у трансформації теоретичних знань у конкретні навички ідентифікації складних злочинних схем.

Відео охоплюють кілька критично важливих типологій злочинів, надаючи спеціалістам з фінансового моніторингу та відповідним органам практичні приклади:

1. Відмивання коштів. Серія приділяє значну увагу загальним механізмам відмивання коштів, як це ілюструють тематичні дослідження Case Study 3 та Case Study 4. Ці приклади мають на меті продемонструвати базові та просунуті методи легалізації незаконно отриманих доходів. Вивчення цих кейсів є фундаментальним для розуміння того, як злочинці маскують джерела коштів, та для встановлення характерних ознак, які мають викликати підозру у фінансових установах.

2. Шахрайство. Серія детально розкриває різні аспекти шахрайської діяльності. Загальні випадки шахрайства, представлені, наприклад, у Case Study 13, дозволяють аналізувати типові стратегії, які використовуються для обману з метою фінансової вигоди. Розуміння цих стратегій дозволяє спеціалістам оперативно ідентифікувати підозрілі транзакції та схеми, які можуть бути ознаками шахрайства.

3. Захист вразливих осіб. Однією з найбільш важливих типологій, висвітлених у серії, є шахрайство, спрямоване на вразливих осіб, зокрема Case Study 6. Цей аспект є життєво необхідним, оскільки він акцентує увагу не лише на фінансових втратах, але й на етичних та соціальних наслідках злочинів. Цей конкретний кейс зосереджується на специфічних індикаторах ризику, які сигналізують про те, що клієнт може стати жертвою експлуатації, допомагаючи фінансовим установам виконувати свій обов'язок щодо захисту найбільш незахищених клієнтів.

Загалом, ця серія відео є практичним навчальним інструментом, який значно підвищує пильність та компетентність фахівців. Кожне тематичне дослідження надає деталі, необхідні для ефективного складання Звітів про підозрілу діяльність (SARs), що є ключовим елементом у національній та міжнародній системі боротьби з відмиванням коштів та фінансуванням тероризму. Таким чином, серія сприяє глибокому розумінню механізмів фінансової злочинності, що дозволяє установам не лише реагувати на злочини, але й активно їм запобігати.

[12] https://www.youtube.com/watch?v=WgdAPAFIwUU&list=PLvYg7_Lx5KSqb82JBdrTrUG6VRqV93QCF

Інші новини

"Кібер-Захисники" та еволюція соціальної інженерії: Аналіз нових превентивних ініціатив Європолу [13]

Європол розпочав реалізацію нової стратегії боротьби з кіберзлочинністю, яка зміщує акцент з виключно правоохоронних заходів на масштабну превенцію та освіту. Ключовим елементом цієї стратегії стала кампанія "Cyber Defenders", яка включає запуск інтерактивної гри на платформі Roblox. Цей крок свідчить про глибоке розуміння демографії сучасної кіберзлочинності: правоохоронці намагаються "перехопити" молодь (віком 12+), яка часто стає об'єктом вербування кримінальними групами (наприклад, для ролі "грошових мулів" або виконання DDoS-атак), ще до моменту вчинення ними правопорушень. Гра симулює роботу кіберполіцейських, навчаючи гравців розпізнавати шахрайство, захищати цифрову ідентичність та розуміти наслідки злочинних дій.

Паралельно з ігровою ініціативою, Європол опублікував пакет аналітичних матеріалів та настанов, які детально описують механіку сучасних схем **соціальної інженерії**. Звіти, зокрема IOCTA (Internet Organised Crime Threat Assessment), підкреслюють, що злочинці все частіше відмовляються від складних технічних зламів на користь маніпуляції людською психологією.

Особливу увагу приділено таким типологіям:

1. **"Pig Butchering" та Романтичні афери:** Це гібридна форма злочину, що поєднує емоційну маніпуляцію з інвестиційним шахрайством. Злочинці місяцями вибудовують довірливі відносини з жертвою, перш ніж переконати її інвестувати значні кошти у фальшиві криптовалютні платформи. Європол надає детальні індикатори: пропозиції надвисоких прибутків, відмова від відеозустрічей, тиск щодо терміновості інвестицій.
2. **Безпека в онлайн-іграх:** Публікація "10 правил безпечного онлайн-геймінгу" спрямована на протидію грумінгу (психологічній підготовці дітей до експлуатації) та крадіжці акаунтів. Документ закликає до анонімізації профілів та категоричної відмови від переходу в приватні месенджери з незнайомцями.
3. **Використання AI в шахрайстві:** Європол попереджає про зростання якості фішингових атак завдяки Generative AI. Злочинці використовують LLM для створення бездоганних текстів та діпфейків для обходу біометричної верифікації або імітації голосу керівників компаній (CEO Fraud).

Ці матеріали підкреслюють, що в епоху AI "людський фаєрвол" — критичне мислення та обізнаність користувачів — стає останньою лінією оборони, яку неможливо замінити суто технічними засобами захисту.

[13] https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/cyber-defenders

Ліквідація мережі шахрайства з криптовалютою, яка відмила понад 700 мільйонів євро [14]

Europol оголосив про успішне розгортання завершальної стадії масштабної міжнародної операції з викриття і руйнування великої мережі криптовалютного шахрайства та відмивання коштів — мережі, яка за даними слідства, відмила понад €700 мільйонів.

Зловмисники працювали через підроблені криптовалютні інвестиційні та торгові платформи, створені для імітації легітимних бірж або інвестиційних сервісів. Ці платформи приваблювали довірливих користувачів обіцянками надзвичайно високих, «гарантованих» доходів. Потенційних жертв заманювали через ретельно сплановані рекламні кампанії — в тому числі із застосуванням deepfake-технологій: у рекламі використовували підроблені відео або фото відомих осіб чи «експертів», щоб створити ефект довіри й авторитету.

Після реєстрації на таких ресурсах жертвам демонстрували вигадані інтерфейси — панелі з нібито «напрацьованим прибутком», графіками росту, що створювало ілюзію реальної торгівлі або інвестування. Коли ж люди намагалися вивести кошти, їм починали надходити дзвінки або повідомлення з високим тиском — купою приводів для додаткових інвестицій або оплати «комісій», «податків», «розблокування виграшу» тощо. Ці тактики соціальної інженерії та психологічного тиску спрацьовували на жадібність і недосвідченість жертв.

Як тільки кошти надходили — зловмисники переводили їх у криптовалюту (або приймали вже як криптоактиви), а потім лавірували через численні гаманці, різні криптобіржі, блокчейн-мікшери або інші методи для ускладнення відстеження. Таким чином вони ховали походження коштів, створюючи складну, міжнародну, розпорошену систему відмивання.

Розслідування та затримання проводилися поетапно і охопили багато країн: перша хвиля рейдів відбулась 27 жовтня 2025 року — з обшуками у Кіпрі, Німеччині і Іспанії, за результатами яких було затримано дев’ять підозрюваних, а також вилучено значні активи: частину коштів на банківських рахунках, криптовалюту, готівку, цифрові носії та «розкішні» предмети — годинники тощо. Друга хвиля пройшла 25–26 листопада 2025 року з акцентом на інфраструктуру, що забезпечувала шахрайські кампанії — зокрема call-центри, афілійовані рекламні мережі, фірми, що створювали й поширювали підроблену рекламу та залучали нових «інвесторів». Рейди провели у країнах, серед яких — Бельгія, Болгарія, Німеччина, Ізраїль та інші.

За оцінками правоохоронців, зловмисницька мережа не була хаотичною групою хакерів або рядових шахраїв — це була добре структурована організація, яка фактично діяла як бізнес: з відділами маркетингу, продажів (call-центри), техпідтримки, фінансових потоків, відмивання. Такий рівень організації і масштабу ставить її серед наймасштабніших онлайнових схем шахрайства з криптовалютами в Європі.

Хоча вилучені активи (готівка, криптоактиви, цифрові пристрої тощо) зазвичай значно менші за загальну суму про відмивання — що пояснюється тим, що більша частина коштів вже переведена, розподілена або виведена — ця операція є важливим сигналом для злочинних угруповань: навіть найскладніші схеми вже не гарантують безкарності.

[14] https://www.europol.europa.eu/media-press/newsroom/news/international-takedown-of-cryptocurrency-fraud-network-laundering-over-eur-700-million

Цей випадок демонструє, наскільки кримінальні групи еволюціонували, адаптуючи класичні фінансові шахрайства під нові технології та цифрові активи: вони використовували інтернет-рекламу, афілійований маркетинг, кол-центри, маніпуляції через соціальну інженерію, deepfake-технології та можливості блокчейну, аби створити переконливі ілюзії «легальних», «прибуткових» проектів. Одночасно — вони експлуатували слабкі сторони сучасної регуляторики, недостатню увагу до контролю за рекламою, афілійованими мережами, криптовалютними обмінами та KYC/AML-процедурами.

Підсумовуючи, ця операція — не просто чергове затримання шахраїв, а демонстрація: масштаб, організація й технологічна складність таких схем можуть досягати рівня «промислового виробництва». І лише через скоординовані зусилля між країнами, з використанням сучасних методів цифрової криміналістики, аналізу блокчейну та співпраці правоохоронців можна добитися реального удару по таким мережам лише за умови рішучості, швидкості та міжнародної співпраці.

Ваша думка важлива!

1. Які додаткові інструменти для конфіскації активів режиму РФ може активувати статус країни високого ризику і як їх краще застосувати Україні?
2. Чи готові фінансові установи впроваджувати інвентаризацію AI-систем і оцінку ризиковості моделей так само системно, як вони роблять це для ICT-ризиків?
3. Чи можна вважати shadow AI одним з найсерйозніших нових джерел операційних ризиків у банківській системі? Як інституції мають його усувати?
4. Як може вплинути вимога до структурування Reason for Suspicion на якість SAR у довгостроковій перспективі та чи може застосування Glossary Codes стати стандартом для інших юрисдикцій, включно з Україною, з метою підвищення ефективності аналізу SAR?
5. Чи зможуть банківські стейблкоїни стати реальним конкурентом CBDC, чи їхня роль залишиться інфраструктурною?
6. Що має робити міжнародна фінансова система, щоб запобігати використанню банківських каналів для підтримки репресивних державних режимів, як це показано у Damascus Dossier?

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-2025-49

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].