Методологічний бюлетень

Серійний номер: МінФін-AML-2025-19

Травень 2025

“Маленькі справи, зроблені наполегливо, сильніші за великі задуми без дій”

Пітер Маршалл

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

Онлайн-гемблінг: червоні прапорці та типології ВК/ФТ/ФР [1]

Документ підготовлено Підрозділом фінансової розвідки Острова Мен з метою виконання зобов’язань відповідно до Рекомендації 29 FATF та сприяння галузям, які підпадають під фінансовий моніторинг, у виявленні типових схем зловживань в індустрії онлайн-гемблінгу. Документ подає систематизований аналіз можливих механізмів використання онлайн-гемблінгових платформ для ВК/ФТ/ФР. Представлені у документі сценарії є вигаданими, але засновані на даних, отриманих та проаналізованих ПФР Острова Мен, і покликані підвищити обізнаність про новітні загрози та вектори фінансової злочинності в цифровому середовищі.

Онлайн-гемблінг становить приблизно 14% ВВП Острова Мен і є складовою розвиненої екосистеми професійних послуг, що

[1] https://www.fiu.im/media/1245/online-gambling-typology-2025.pdf

включає юридичні, IT, бухгалтерські та корпоративні послуги. Регулювання сектору здійснюється відповідно до закону OGRA 2001 через наглядову комісію з азартних ігор (GSC), яка видає п’ять типів ліцензій (повна, субліцензія, мережева, постачальника ПЗ, токенізована/блокчейн-ліцензія). Залежно від типу ліцензії змінюється й розподіл обов’язків щодо належної перевірки клієнтів: власники повної або субліцензії проводять перевірку самостійно, а мережеві ліцензіати можуть покладатися на перевірку, здійснену їхніми партнерами. Усі оператори мають звітувати до ПФР про підозрілі дії згідно з Кодексом з ПВК/ФТ 2019 року.

У документі окрема увага приділяється тому, як гемблінгові рахунки використовуються для переміщення коштів, уникнення нагляду, структуризації та переведення активів через мікротранзакції. Вказано на типові ознаки, які можуть сигналізувати про ВК/ФТ/ФР, зокрема:

- аномальна структура депозитів/виведення коштів;
- реєстрація кількох акаунтів з однієї IP-адреси;
- використання VPN, анонімайзерів, криптовалют;
- низький рівень ігрової активності при значному русі коштів.

Особливо ризиковими визнано бізнес-моделі "білої етикетки" (white label), де одна компанія надає платформу іншій компанії, яка володіє доступом до клієнтів. Це створює прогалини в належній перевірці клієнтів і підвищує ризики для ПВК.

У розділі про бенефіціарну власність акцентується на використанні складних корпоративних структур (у тому числі за участю VASP та компаній-оболонок) для маскування реальних власників ігрових платформ, а також для створення фіктивного "респектабельного іміджу" в юрисдикціях з високими регуляторними вимогами. Наведено приклади використання офшорів, номінальних директорів, трастів та інших посередників для утруднення ідентифікації кінцевих бенефіціарних власників.

Також розглянуто випадки кіберзлочинності: злам акаунтів, викрадення персональних даних гравців і використання внутрішньої ігрової валюти для обігу коштів між злочинцями. У деяких сценаріях платформи використовуються для переведення криптоактивів, отриманих внаслідок хакерських атак, у фіатні кошти.

Висновки:

- **Юридичні лазівки та структура ліцензування створюють прогалини в перевірці клієнтів, особливо при використанні мережевих або white label** моделей, де обов’язки з CDD можуть бути делеговані стороннім операторам без належного контролю з боку платформи або регулятора.
- **Варто запровадити поглиблений моніторинг структур корпоративної власності ігрових платформ**, з акцентом на виявлення прихованих бенефіціарів у юрисдикціях із слабким регулюванням або в зонах конфлікту.
- **Від ПФР потребується більше уваги у гемблінговому секторі**, зокрема шляхом аналізу походження коштів у криптовалютах та транзакцій, пов’язаних з компаніями, що можуть бути пов’язані з програмами розробки ЗМЗ або підсанкційними особами.
- **Підзвітним установам слід інтегрувати індикатори у свої процедури моніторингу**, зокрема аномальні ігрові шаблони, однотипні акаунти, активність у позаробочий час, часті виведення коштів одразу після поповнення, та відсутність ігрової активності при високих обертах транзакцій.

Європейська блокчейн-пісочниця: Звіт про найкращі практики [2]

Документ є виконавчим резюме другого звіту про найкращі практики Європейської блокчейн-пісочниці (European Blockchain Sandbox), ініціативи Європейської Комісії, спрямованої на створення безпечного, конфіденційного та конструктивного середовища для діалогу між інноваторами у сфері технологій розподіленого реєстру (DLT/blockchain) та національними й європейськими регуляторами. Основна мета пісочниці — сприяти юридичній визначеності шляхом взаємного навчання: інноватори здобувають розуміння нормативно-правових вимог, а регулятори — знання про нові технології.

Другий цикл діалогів, який тривав з вересня 2024 по березень 2025 року, продовжив роботу першого раунду, розширивши тематику обговорення й залучивши нові сторони. Було відібрано 20 проєктів із різних секторів, які базуються на різних блокчейн-інфраструктурах, включаючи приватні, публічні, консорціумні та гібридні варіанти. Ці проєкти охоплюють широкий спектр тем, зокрема: цифрову ідентичність, токенізацію активів, ESG-звітування, NFT, децентралізовані фінанси (DeFi), електронне голосування, страхування, міжнародну торгівлю, розумні контракти та ін.

Ключовим елементом пісочниці є регуляторні діалоги, які проводяться в режимі конфіденційного обговорення між інноваторами та відповідними регуляторами. У межах другого раунду було залучено близько 80 представників регуляторів та органів нагляду з понад 20 юрисдикцій. Важливо, що ці діалоги не обмежувались лише фінансовим сектором — були охоплені також питання захисту даних, кібербезпеки, боротьби з відмиванням коштів, цифрових підписів, захисту прав споживачів та інші напрями.

Кожен з проєктів був відповідно зіставлений з релевантними національними та європейськими органами регулювання, що дозволило провести глибокі фахові діалоги у сфері регуляторної відповідності, інноваційного застосування технологій та нормативної оцінки потенційних ризиків. У процесі діалогу регулятори отримували попередні технічні брифінги про особливості DLT, що були підготовлені командою Bird & Bird / OXYGY. Важливою новацією стала поява форматів «тільки для регуляторів» між першим і другим діалоговими раундами, які дали можливість учасникам спільно осмислити перші враження, уточнити позиції та сформулювати додаткові запитання до розробників.

У структурному плані діалоги охоплювали три типи підходів:

1. Оцінка регуляторної відповідності технологій та кейсів;
2. Використання DLT як інструменту для підвищення ефективності відповідності законодавству (compliance by design);
3. Обговорення можливості адаптації чи створення регуляторних інструментів, що базуються на DLT (наприклад, впровадження електронних гаманців EUDI відповідно до eIDAS 2, або сертифікація смарт-контрактів).

У документі детально висвітлено специфіку правових рамок, у межах яких відбувалися діалоги, зокрема:

[2] https://blockchain-observatory.ec.europa.eu/system/files/2025-04/Best%20practices%20report%20-%20Abstract%20%20Executive%20summary%20EN%20%28final%2025.04.2025%29.pdf

- **Захист персональних даних відповідно до GDPR, особливо у контексті відкритих блокчейнів.** Питання, чи дані, записані у блокчейні, є персональними в розумінні GDPR (Регламент 2016/679), залишалося центральним у діалогах. Якщо інформація у ланцюгу блоку є персональними даними, це накладає обов'язок на операторів забезпечити дотримання принципів правомірності, мінімізації, цільового обмеження та прав суб'єкта даних. Особливий виклик становить незворотність і незмінність записів у відкритих блокчейнах. Обговорювалися способи мінімізації ризиків, зокрема шляхом зберігання персональних даних поза ланцюгом (off-chain), використання хеш-функцій або псевдонімізації.
- **Роль регламенту eIDAS 2 та впровадження європейського цифрового гаманця (EUDI Wallet) для ідентифікації та електронного підпису в контексті DLT**. Нова редакція регламенту eIDAS (eIDAS 2 – Регламент (ЄС) 2024/1183) передбачає створення Європейського цифрового гаманця (EUDI Wallet) і розширює перелік довірчих послуг. В діалогах розглядалося, як DLT-рішення можуть інтегрувати ці цифрові засоби ідентифікації та забезпечувати надійні й юридично значимі транзакції. Вивчався потенціал взаємодії між eIDAS 2 та AML-законодавством, Company Law та IoT-середовищем — зокрема, питання сертифікації, електронного підпису, електронного атрибута та електронної печатки в контексті DLT.
- **Взаємодія блокчейн-рішень з регламентом AI Act**. Застосування DLT для забезпечення надійності штучного інтелекту — одна з нових тем другого раунду. Обговорювались питання відповідності змішаних рішень вимогам AI Act, зокрема щодо прозорості, відстежуваності, управління даними, збереження записів. Було висвітлено особливості відкритого коду як спільного знаменника для AI та DLT, що має вплив на застосування спеціального режиму для open-source AI, передбаченого AI Act.
- **Правовий статус DAO та можливість застосування юридичних форм на зразок SCE як "обгортки" для DAO**. DAO (децентралізовані автономні організації) як структура без юридичної особи та централізованого управління становлять виклик для регуляторів. Обговорювались ризики персональної відповідальності учасників DAO, проблеми виконання контрактних зобов'язань і відповідності GDPR, зокрема коли DAO працює на permissionless блокчейнах. Аналізувався потенціал використання Європейської кооперативної структури (SCE) як "обгортки" для легалізації DAO.
- **DLT-рішення для електронного голосування, зокрема в корпоративному управлінні**. Оскільки законодавство ЄС не гармонізує e-voting, кожна держава-член має власні правила. Обговорювалась можливість використання DLT для проведення виборів, зокрема у приватному секторі (напр., загальні збори акціонерів). Визначено, що eIDAS 2 може бути регуляторним каталізатором, зокрема через EUDI Wallet для верифікації особи виборця. Приклади країн — Естонія, Румунія, Греція.
- **Застосування блокчейну для автоматизації та прозорості ESG/CSRD/EUDR-звітування**. CSRD (Corporate Sustainability Reporting Directive) та EUDR (Regulation on Deforestation-free Products) передбачають вимоги до надійності, достовірності та повноти даних про сталий розвиток. DLT було визнано придатним для забезпечення незмінності, прозорості та контрольованого доступу до таких даних. Додатково розглядалося використання DLT для цифрових паспортів продукції (Battery Passports, DPPs), які відповідають новим нормам ESPR (Regulation on Ecodesign for Sustainable Products).
- **Підвищення ефективності дотримання санкційного режиму за допомогою прозорих DLT-логів**. Обговорювались рішення, які забезпечують відстеження санкційних списків і уніфіковані аудиторські сліди, доступні як для внутрішнього контролю, так і для наглядачів, майже в реальному часі. Такі системи можуть значно підвищити ефективність виконання санкцій у великих транснаціональних групах.

- **Використання смарт-контрактів і DLT у контексті DORA, включаючи оцінку ризиків інформаційно-комунікаційних технологій (ICT).** Регламент DORA (про цифрову операційну стійкість) стосується фінансових установ і ICT-постачальників. DLT-провайдери, які надають послуги фінансовим установам, можуть підпадати під DORA, особливо якщо мають статус «ICT third-party service provider». Обговорювалась потреба в оцінці ризиків, пов'язаних із смарт-контрактами, які розглядаються як ICT-актив, та контрактне регулювання таких відносин.
- **Регуляторні виклики AMM (автоматизованих маркетмейкерів) у DeFi, та потреба у майбутньому регулюванні з боку ESMA**. Розглядалося регулювання AMM, які працюють на смарт-контрактах та використовують пул ліквідності замість книг заявок. Попри наявність базового регулювання у MiCAR, AMM не охоплені прямо ні MiFID, ні DLT Pilot Regime. Учасники запропонували взяти MiCAR як модель для подальшого регулювання AMM, зокрема для прозорості, та рекомендували розробити настанови від ESMA.

Доповідь фіксує практичні висновки, виклики та моделі взаємодії, виявлені під час діалогів, а також напрацьовані найкращі практики та рекомендації для інноваторів і регуляторів. Зокрема, виявлено необхідність кращого узгодження міжгалузевих підходів до класифікації активів, регуляторної співпраці між юрисдикціями, а також забезпечення технічної нейтральності регулювання. Визнається потенціал sandbox-механізму як інструменту для моделювання політики на практиці, особливо у випадках із транснаціональним виміром застосування технологій.

Висновки:

- **Необхідно покращити міжсекторальну й транснаціональну координацію регуляторів**. Регулятори з різних юрисдикцій та секторів мають різне бачення щодо класифікації технологій, активів і відповідних ризиків, що створює фрагментоване середовище для інноваторів.
- **Потрібно адаптувати регулювання до гнучких і технологічно нейтральних моделей**. Застосування блокчейн-технологій у нефінансових секторах вимагає регуляторного підходу, що орієнтується не на конкретну технологію, а на функціональні характеристики послуги.
- **Sandbox-формат є ефективним інструментом для навчання регуляторів**. Безпечне середовище діалогу дозволяє регуляторам глибше розуміти нові технології без тиску прийняття регуляторних рішень негайно.
- **Інноваторам слід заздалегідь враховувати регуляторні обмеження**. Раннє залучення до діалогу з регуляторами (наприклад, через пісочницю) дозволяє уникнути витратних помилок у дизайні продукту або бізнес-моделі.

Результати другого циклу показали високу зацікавленість з боку як інноваторів, так і регуляторів, у продовженні таких форматів обміну. Також підкреслюється, що Європейська блокчейн-пісочниця може бути прикладом для інших ініціатив у межах цифрового переходу та розробки політик у сфері новітніх технологій, а формат конфіденційного міжвідомчого діалогу може бути масштабований і адаптований до інших технологій (AI, IoT тощо).

У розділі висновків звіт відзначає якісне зростання участі регуляторів — у середньому 8 регуляторів на кожен діалог (проти 4 у першому раунді), а також глибину обговорень. Відгуки з боку обох сторін були переважно позитивними. Регулятори високо оцінили можливість краще зрозуміти нові технології, а учасники — отримати доступ до фахового правового аналізу та рекомендацій без страху негайного регуляторного втручання.

У 3-му циклі очікується акцент на поєднанні DLT із AI, IoT, хмарними технологіями, а також глибше занурення в сектори енергетики та охорони здоров'я. Оскільки більшість регуляторів виявили бажання повторно брати участь, змін до формату діалогу не планується.

Регулювання

Керівні принципи щодо обробки персональних даних за допомогою технологій блокчейн [3]

Документ підготовлений Європейською радою із захисту даних (EDPB), є нормативно-методичним орієнтиром для суб'єктів, які планують або вже здійснюють обробку персональних даних із використанням технологій блокчейн або DLT. Його мета — забезпечити відповідність такої обробки вимогам Загального регламенту про захист даних (GDPR) в умовах високої технічної складності, розподіленого характеру систем і невизначеності щодо ролей та відповідальності учасників.

Документ починається з окреслення ключових властивостей блокчейн-систем: децентралізація, відсутність посередників, незмінність записів, прозорість та криптографічна перевірка транзакцій. Проте саме ці властивості створюють структурні труднощі щодо дотримання принципів GDPR — зокрема, принципу мінімізації, обмеження строків зберігання, права на стирання, виправлення та заперечення обробки. Наприклад, у більшості блокчейн-рішень дані не піддаються коригуванню після запису, що суперечить вимогам GDPR про можливість видалення або виправлення персональних даних.

EDPB наголошує, що з технічної складності не випливає правова безвідповідальність: незалежно від особливостей технології, необхідно дотримуватись усіх вимог GDPR. У цьому контексті особливу увагу приділено структурі DPIA (оцінці впливу на захист даних), яка має стати інструментом для обґрунтування застосування блокчейн-рішень. DPIA повинна охоплювати детальний опис архітектури блокчейну, юридичних ролей (контролерів, процесорів), механізмів консенсусу, типів даних (включаючи метадані та payload), схеми доступу, моделі управління, а також розгляд можливостей реалізації прав суб'єктів даних.

Описано переваги та ризики різних типів блокчейнів (публічні/приватні, з відкритим або обмеженим доступом), зокрема наголошено, що моделі обмеженого доступу з централізованим управлінням дозволяють чіткіше розподілити відповідальність і є більш бажаними для проєктів із обробкою персональних даних. Рекомендовано уникати зберігання персональних даних напряму у відкритому блокчейні. Натомість, можливі такі технічні засоби як: зберігання off-chain, використання хешів, шифрування, або механізмів доказу існування.

В окремому розділі розглядається відповідність принципам обробки даних з GDPR (стаття 5): законність, прозорість, цільове обмеження, мінімізація, точність, обмеження зберігання, цілісність та конфіденційність. Кожен принцип оцінюється в контексті блокчейн-рішень, з урахуванням властивостей таких систем. Наприклад, принцип точності особливо важливий перед записом даних у блокчейн, адже подальше виправлення практично неможливе. Зберігання зашифрованих або хешованих даних не знімає зобов'язань щодо захисту, адже вони все одно залишаються персональними даними за змістом GDPR.

[3] https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en

У питанні законності обробки даних наголошено, що необхідно обґрунтувати кожну правову підставу (стаття 6 GDPR), а також обмеження прав (стаття 23), якщо блокчейн використовується, наприклад, для цілей ПВК або державних реєстрів. Такі обмеження мають бути передбачені законом та пропорційними.

Особлива увага приділяється міжнародним передачам даних (глава V GDPR), що часто супроводжують блокчейн-рішення. Рекомендовано забезпечувати відповідність стандартним контрактним положенням і закладати ці механізми ще на етапі проєктування системи. Також наведено інструменти оцінки ризиків та архітектурних рішень, які дозволяють впровадити підхід «захист даних за замовчуванням і за дизайном» (стаття 25).

Розділ про безпеку обробки описує ризики компрометації алгоритмів (наприклад, через появу квантових обчислень), атаки типу 51%, помилки в управлінні ключами, та необхідність створення процедур виявлення і реагування на інциденти. Зокрема, підкреслюється необхідність періодичного оновлення безпекових практик та включення процедур виявлення уразливостей і реагування на них до системного управління.

Права суб'єктів даних (розділ 5) також є фокусом документа. Оскільки повноцінне видалення чи виправлення даних у блокчейні є технічно складним або неможливим, рекомендується реалізовувати права через проєктні рішення — наприклад, зберігання посилань замість даних, а в разі запиту на видалення — знищення офчейн-даних, які дають змогу ідентифікувати особу. Також описано шляхи реалізації прав на доступ, портативність, заперечення та обмеження автоматизованого прийняття рішень.

У додатку А надано 16 конкретних рекомендацій — від вибору типу блокчейну, вимог до прозорості та мінімізації, до технічного забезпечення безпеки, дотримання періодів зберігання та реалізації прав суб'єктів даних. Наприклад, прямо зазначено, що якщо неможливо реалізувати стирання або анонімізацію даних у межах встановленого строку зберігання, такі дані не слід записувати на блокчейн взагалі.

Висновки:

- **Зберігання персональних даних на блокчейні має бути винятком**: Якщо реалізація прав суб'єкта (на стирання, виправлення) є неможливою або технічно не гарантована, такі дані слід зберігати лише off-chain.
- **Тип блокчейну має бути обґрунтований DPIA**: Використання публічного блокчейну з відкритим доступом вимагає глибокої оцінки ризиків і виправданої необхідності — за відсутності таких умов слід використовувати блокчейн із обмеженим доступом або приватні архітектури.
- **Технічні засоби не звільняють від відповідальності**: Використання шифрування, хешування або криптографічних комітментів не усуває обов'язків згідно з GDPR — такі дані залишаються персональними і потребують додаткових заходів захисту.
- **Гарантована реалізація прав суб'єкта — обов'язкова умова**: Жоден технічний вибір (включно зі смарт-контрактами або незмінністю записів) не може бути виправданням невиконання запиту суб'єкта даних відповідно до статей 15–22 GDPR.

Документ є значним внеском у гармонізацію підходів до захисту персональних даних у блокчейн-середовищі й демонструє системний, технологічно глибокий і нормативно чіткий підхід до поєднання інновацій та захисту прав людини в цифрову епоху.

Нова ера регулювання криптоактивів у Великій Британії: аналіз проєкту нормативного акту 2025 року [4]

Політична записка, опублікована Міністерством фінансів Великої Британії (HM Treasury), є ключовим аналітичним документом, який супроводжує проєкт нормативного акту (Statutory Instrument, SI), спрямованого на інтеграцію криптоактивів у правове поле британської фінансової системи. Цей документ деталізує підходи до регулювання діяльності з криптоактивами в межах системи Financial Services and Markets Act 2000 (FSMA), зосереджуючи увагу на створенні чітких визначень, периметрів регулювання, нових категорій діяльності, а також уточненні пов'язаних змін до чинного законодавства, включаючи нормативи з ПВК/ФТ.

У вступі окреслюється політичний контекст ініціативи: після публікації консультацій у 2023 році та підтвердження у 2024-му уряд вирішив запровадити новий режим регулювання криптоактивів, зокрема стейблкоїнів, із незначними змінами. Основна ціль — інтеграція діяльності з криптоактивами до вже існуючої регуляторної інфраструктури фінансових послуг Великої Британії, а також створення системи дозволів та нагляду, яка забезпечить фінансову стабільність, прозорість ринку та захист споживачів. Пропоноване регулювання не поширюється на включення стейблкоїнів до платіжного регуляторного периметра (Payments Services Regulations 2017), однак передбачає, що в перспективі уряд може повернутися до цього питання у відповідь на розвиток ринку.

Ключовим є створення нових категорій активів — «qualifying cryptoassets» та «qualifying stablecoins». Перші визначаються як цифрові активи, що є взаємозамінними, передаваними, не є традиційними фінансовими інструментами (тобто не прирівнюються до облігацій, акцій, тощо), і не включають токенізовану електронну валюту або депозити. «Qualifying stablecoin» — це стейблкоїн, прив'язаний до фіатних валют із забезпеченням у вигляді фіатів або їх комбінації з іншими активами, призначений для підтримки стабільної вартості. Окрему категорію становлять так звані «specified investment cryptoassets» — токенізовані форми традиційних фінансових інструментів (наприклад, акцій або облігацій), що підпадають як під визначення криптоактивів, так і під статус «specified investments» за FSMA, для яких зберігається чинний регуляторний підхід із адаптацією до цифрових технологій. Ці визначення встановлюють чітку законодавчу рамку для відмежування різних форм цифрових активів.

Проєкт нормативного акту створює нові регульовані види діяльності відповідно до FSMA/RAO: емісію стейблкоїнів (із включенням функцій пропозиції, викупу та управління стабільністю вартості); зберігання (кастодіальне обслуговування) криптоактивів; операції з ними як головною стороною або агентом; організацію угод; операції криптовалютної торговельної платформи; та надання послуг стейкінгу. При цьому враховується необхідність виключення деяких випадків — наприклад, тимчасове зберігання активів для цілей клірингу та розрахунків не визнається кастодіальною діяльністю. У сфері стейкінгу додатково враховано розповсюдження моделей liquid staking, із розмежуванням відповідної діяльності за окремими регуляторними категоріями.

4 https://assets.publishing.service.gov.uk/media/680f6397b0d43971b07f5bfd/20250428_RAO_SI_draft_policy_note.pdf

Важливою складовою є визначення географічного периметра регулювання. Документ чітко встановлює, що будь-яка діяльність, яка прямо або опосередковано орієнтована на роздрібного споживача з Великої Британії, підлягає авторизації FCA, незалежно від місця розташування компанії. Разом з тим, дозволено обслуговування інституційних клієнтів без авторизації за умови, що ці клієнти не є посередниками між нерезидентною фірмою і роздрібним споживачем у Великій Британії. Також визначено, що емітенти стейблкоїнів повинні отримати дозвіл лише в разі ведення відповідної діяльності з території Сполученого Королівства.

У сфері ПВК/ФТ документ передбачає істотне спрощення: компанії, які отримають авторизацію за новим режимом, більше не зобов'язані реєструватися окремо як постачальники криптовалютних послуг відповідно до MLRs 2017. Проте вимоги ПВК залишаються чинними у повному обсязі, окрім вимоги реєстрації. Це відображає прагнення до уникнення дублювання зобов'язань без зниження стандартів контролю за ризиками ВК/ФТ.

Значну увагу також приділено правовому розмежуванню між криптоактивами та іншими фінансовими інструментами. Внесено зміни до законодавства, щоб виключити кваліфіковані стейблкоїни та їх забезпечення з-під дії правил про колективні інвестиційні схеми (CIS), альтернативні інвестиційні фонди (AIF), а також електронні гроші. Це дозволяє чітко визначити правовий статус нових цифрових інструментів і уникнути регуляторної плутанини.

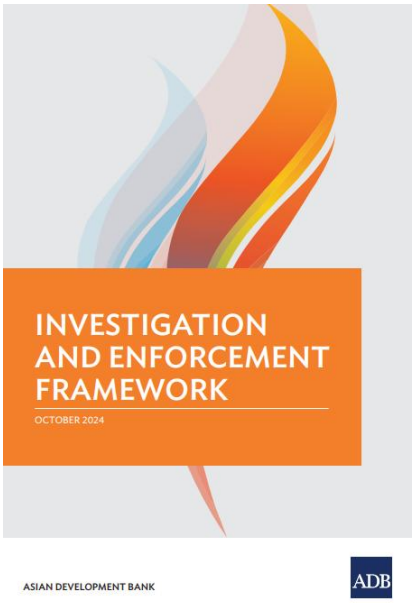
Висновки:

- **Усі постачальники послуг із криптоактивами, орієнтовані на британських роздрібних клієнтів, мають бути авторизовані FCA.** Платформи, кастодіальні сервіси, емітенти стейблкоїнів повинні почати готувати документи на авторизацію.
- **Уніфікація нормативного поля: нові види регульованої діяльності інтегруються у вже існуючу інфраструктуру FSMA, RAO, FPO та MLRs.** Фірми отримають єдиний канал відповідності замість подвійного регулювання (наприклад, не потрібно окремо реєструватися згідно з MLRs, якщо вже є авторизація за FSMA).
- **DeFi-проєкти не охоплені спеціальним регулюванням, однак можуть підпадати під вимоги, якщо існує «контролююча сторона».** Учасникам DeFi слід оцінити ступінь централізації/контролю в проєкті з точки зору потенційного регуляторного охоплення.

Документ також встановлює перехідний режим, який дозволяє компаніям, що вже надають послуги з криптоактивами, подати заявки на авторизацію до FCA у визначений період. У разі відмови такі фірми не вважаються такими, що порушують режим, однак повинні припинити укладення нових угод і здійснити впорядковане згортання бізнесу на території Великої Британії впродовж не більше ніж двох років. FCA також отримує повноваження для прискорення або скорочення періоду такого згортання в окремих випадках.

Документ свідчить про перехід Великої Британії до повноцінного режиму фінансового регулювання криптоактивів, у якому ці активи розглядаються як новий клас фінансових інструментів, що потребує відповідного нагляду, ліцензування та нормативної чіткості. Він закладає основу для інтеграції криптосектору в мейнстрим фінансової системи країни, при цьому забезпечуючи узгодженість з вимогами щодо боротьби з ВК/ФТ, захисту прав споживачів і фінансової стабільності.

Механізми доброчесності в дії: аналіз Investigation and Enforcement Framework Азійського банку розвитку (2024) [5]



Документ, опублікований Азійським банком розвитку (ADB) у жовтні 2024 року, є фундаментальним адміністративним актом, що регламентує порядок розслідування порушень доброчесності у зв'язку з діяльністю, пов'язаною з проєктами, які фінансує, адмініструє або підтримує ADB. Він замінює попередні версії Integrity Guidelines (2006, 2012, 2015) і складається з двох взаємопов'язаних частин: «Investigation Guidelines» (Правила розслідування) та «Enforcement Guidelines» (Правила примусового впливу). Документ створений відповідно до стандартів міжнародних фінансових інституцій, зокрема Світового банку, ЄБРР, Африканського та Міжамериканського банківського розвитку, і гармонізує понятійно-правову базу щодо порушень доброчесності на рівні міждержавного адміністрування.

Правила розслідування визначають повноваження та обов'язки Офісу з антикорупційної діяльності та доброчесності (Office of Anticorruption and Integrity, OAI), який функціонує як незалежний структурний підрозділ із виключною юрисдикцією щодо оцінки повідомлень про зловживання, корупцію, шахрайство, змову, тиск, конфлікт інтересів, перешкоджання розслідуванню, відплату викривачам, а також інші порушення Антикорупційної політики ADB. Зазначено чіткі визначення integrity violations, які охоплюють не лише класичні форми неправомірної поведінки, але й інституційні зловживання, такі як несанкціоновані контрактні модифікації під час відсторонення, а також порушення умов доброчесності з боку пов'язаних осіб чи суб'єктів. Ключовим є те, що ADB застосовує адміністративну процедуру, а не судовий розгляд, що дозволяє оперативно вживати обмежувальні заходи, зберігаючи при цьому основні гарантії процесуальної справедливості.

Після отримання повідомлення OAI проводить первинну оцінку достовірності, суттєвості та перевірюваності скарги. У разі наявності підстав розпочинається повноцінне розслідування, що передбачає збір і аналіз документів, електронних матеріалів, свідчень, а також технічних та фінансових даних. Всі матеріали зберігаються в системі OAI з дотриманням стандартів конфіденційності та доступу. Розслідування завершується або закриттям справи у разі відсутності доказів, або підготовкою висновку з проєктом «show cause letter» – офіційного повідомлення особі або суб'єкту про наявність підстав для санкцій. Далі справа переходить до Integrity Enforcement Committee (IEC), що складається переважно з незалежних (зовнішніх) членів, які ухвалюють рішення щодо санкцій на основі балансу ймовірностей.

Правила примусового впливу детально описують можливі санкції, які включають публічну догану, обмежувальні умови, тимчасове або безстрокове відсторонення, з можливістю повернення після виконання умов, а також фінансові відшкодування. Базова санкція за доведене порушення — трирічне відсторонення з можливістю коригування терміну з урахуванням обтяжуючих або пом'якшуючих обставин. При цьому ADB залишає за собою право застосовувати тимчасове відсторонення навіть на стадії розслідування, якщо ризики підтвердження порушення високі. У документі детально визначено перелік факторів, які враховуються при призначенні санкції, включаючи тяжкість порушення, участь керівництва компанії, співпрацю з розслідуванням, історію попередніх порушень, а також наявність комплаєнс-систем або програм добровільного розкриття.

[5] https://www.adb.org/sites/default/files/institutional-document/1001456/investigation-enforcement-framework.pdf

Окрему увагу приділено механізму апеляцій — Enforcement Appeals Committee (EAC), який має незалежний мандат та ухвалює рішення за письмовими матеріалами без участі сторін. Також описано механізм публічного розкриття санкцій: перше порушення, як правило, не розголошується, якщо немає обтяжуючих обставин, однак повторні порушення або відмова від співпраці — публікуються у відкритому реєстрі на вебсайті ADB. Важливим є положення про взаємне визнання санкцій між МФІ в рамках Угоди про взаємне визнання відсторонень (AMEDD), що посилює транскордонний контроль за зловживаннями.

Висновки:

- **Запровадження чітко розмежованої моделі**, у якій одна інституція відповідає за розслідування (OAI), а інша — за ухвалення санкційних рішень (IEC), забезпечує належний баланс повноважень, процедурну справедливість та захист від конфлікту інтересів.
- **Інтеграція обов'язку співпраці з розслідуванням до договірних зобов'язань учасників проєктів** дозволяє ефективно збирати докази, захищати інтереси інституції та запобігати ухиленню від відповідальності.
- **Застосування превентивних заходів**, таких як тимчасове відсторонення або врегулювання шляхом добровільного визнання (Proposed Resolution Agreements), дозволяє оперативно реагувати на ризики та знижувати потенційну шкоду ще до завершення повного розслідування.
- **Визнання та застосування механізму взаємного відсторонення** між багатосторонніми фінансовими інституціями у межах AMEDD посилює транскордонний контроль за порушеннями доброчесності та створює спільну відповідальність учасників ринку за дотримання єдиних стандартів етики.

Таким чином, IEF ADB створює модельну систему дотримання доброчесності у міжнародних проєктах розвитку, поєднуючи процедурну чіткість, стандартизованість визначень, гнучкість у реагуванні та захист прав сторін. Документ є цінним джерелом для розробки національних механізмів антикорупційного реагування в частині взаємодії з донорами, кредиторами, а також для адаптації принципів адміністративної відповідальності у сфері

Звіти окремих інституцій та експертів

Як стати непрямим учасником SEPA [6]

Документ є докладним професійним посібником, який розкриває комплексну дорожню карту для фінансових установ — зокрема платіжних установ (ПУ) та установ електронних грошей (EMI) — що мають намір стати непрямими учасниками SEPA (Single Euro Payments Area). Його підготувала команда Numeral, технологічної компанії, яка спеціалізується на автоматизації платежів та інтеграції з банками через API. Посібник має на меті ліквідувати інформаційні прогалини, які зазвичай супроводжують процес виходу на рівень SEPA-учасника, особливо для нефінансових установ або нових гравців на фінансовому ринку.

[6] https://www.numeral.io/guides/becoming-sepa-participant

Документ починається з пояснення загальних засад функціонування SEPA: її зони охоплення (36 країн), платіжних схем (SCT, SCT Inst, SDD Core, SDD B2B), ролі платіжних провайдерів (PSP) і механізмів клірингу та розрахунків (CSM), які здійснюють маршрутизацію і розрахунки між установами. Пояснено чотиристоронню модель транзакцій у SEPA та специфіку роботи PSP — від кредитних установ (банків) до ліцензованих фінтехів.

У центрі уваги гайду — непряма участь у SEPA, яка є єдиною доступною моделлю для ПУ/EMI, оскільки пряма участь вимагає наявності рахунку в ЄЦБ і статусу банку. У моделі непрямої участі фінансова установа підключається до SEPA через спонсор-банк, який є прямим учасником SEPA та забезпечує взаємодію з CSM.

Посібник детально описує вигоди непрямої участі, серед яких:

- Отримання власних IBAN і BIC, що сприяє підвищенню довіри користувачів до бренду, уникненню дискримінації за IBAN (особливо у випадках з транскордонними клієнтами) та зменшенню залежності від постачальників BaaS (модель фінансових послуг, за якої технологічні компанії надають банківські послуги через API, використовуючи ліцензію банку або платіжної установи-партнера);
- Покращення контролю над транзакціями — включно з можливістю самостійно обробляти R-транзакції (спеціальні повідомлення у платіжній системі SEPA, які використовуються для обробки помилок, винятків та повернень під час здійснення платежів) та побудовою внутрішніх сценаріїв реагування;
- Підвищення швидкості обробки платежів завдяки скороченню кількості посередників у ланцюгу платежу (залежність лише від спонсор-банку та CSM, а не від внутрішніх процесів великих банків або BaaS-платформ);
- Економія витрат, зокрема на транзакції, обробку помилок, а також усунення плати за створення віртуальних IBAN, яку зазвичай стягують банки.

Особливо цінною є частина, що описує типові сценарії переходу до статусу SEPA-учасника, зокрема:

- трансформація з корпоративного клієнта банку у SEPA-учасника;
- перехід з моделі агентства BaaS до повноцінної ліцензованої ПУ/EMI з участю в SEPA;
- вихід на ринок нової ПУ/EMI одразу як SEPA-учасника.

Виділено три ключові напрями підготовки до входу в SEPA як непрямого учасника:

1. Регуляторно-адміністративний блок: отримання BIC від SWIFT, повідомлення місцевого регулятора, реєстрація BIC у

Висновки:

- **Фінансовим установам слід стратегічно розглянути модель участі в SEPA**, оскільки непряма участь забезпечує ключові переваги: власні IBAN/BIC, контроль над платежами, гнучкість та зниження вартості обробки транзакцій.
- **Перед початком проєкту з SEPA-участі потрібно підготувати три напрями паралельно**: (1) виконання регуляторних завдань (отримання BIC, реєстрація у EPC), (2) вибір і підписання угоди зі спонсор-банком, (3) технічна інтеграція.
- **Операційна готовність SEPA-учасника потребує автоматизації всіх ключових процесів**, включно з моніторингом транзакцій, управлінням винятками (R-транзакціями), розмежуванням коштів між settlement і safeguarding рахунками згідно з регуляторними вимогами.
- **Вибір спонсор-банку має стратегічне значення**, оскільки він впливає на швидкість, гнучкість, ціноутворення, доступні SEPA-схеми, а також підтримку інтеграції й операційну стійкість. Рекомендується оцінювати не лише тарифи, а й глибину підтримки та додаткові сервіси.

Європейській платіжній раді (EPC), вибір CSM, а також формальне включення у таблиці маршрутизації.

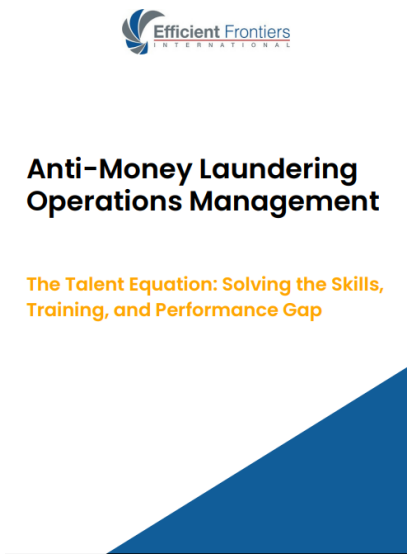
2. Комунікація зі спонсор-банком: вибір банку з урахуванням покриття SEPA-схем, моделей ціноутворення, досвіду обслуговування інших непрямих учасників, відкриття рахунків (settlement і safeguarding), обговорення моделей обліку та дебетування комісій.
3. Технічна інтеграція: побудова або адаптація систем обміну повідомленнями (API, SFTP, message brokers), налаштування мапінгу форматів (ISO 20022: pacs, pain, camt), проходження тестування і сертифікації з боку банку.

Окремий блок присвячено операційному функціонуванню SEPA-учасника, з акцентом на вимоги до обробки вхідних/вихідних SCT/SCT Inst/SDD платежів, підтримку R-транзакцій, облік у settlement та safeguarding рахунках. Підкреслено, що відповідність регуляторним вимогам передбачає щоденне очищення settlement-рахунку і своєчасне переведення коштів на рахунок захисту коштів клієнтів (safeguarding account).

Важливим є також розділ про необхідну технічну інфраструктуру. Представлено ролі core banking system (наприклад, Tuum), платформи з автоматизації платежів (Numeral), модулів верифікації транзакцій (Hawk.ai, Salv, Feedzai) та сценарії використання API. Пояснено, як саме Numeral бере на себе функції інтеграції, обробки помилок, моніторингу та ручного втручання в проблемні транзакції.

Таким чином, документ виступає як вичерпне методичне керівництво для фінансових установ, що хочуть оптимізувати свої платіжні процеси, стати менш залежними від банківських посередників і зміцнити регуляторну відповідність та довіру з боку клієнтів.

Рівняння таланту: вирішення проблеми розриву між навичками, навчанням та продуктивністю [7]



Документ є аналітичним документом підготовленим компанією EFI (Efficiency For Industry) — постачальником послуг у сфері ПВК, що зосереджується на CDD, моніторингу транзакцій, скринінгу та навчанні аналітиків. Звіт ґрунтується на глибокому аналізі системних проблем у сфері підготовки, відбору, оцінки й управління аналітиками фінансового моніторингу, зокрема у контексті ПВК/ФТ.

Ключовою проблемою, яка визначає тон усього документа, є дисбаланс між попитом і пропозицією на ринку кадрів у сфері фінансової безпеки. Попри формальну наявність великого глобального пулу спеціалістів, більшість організацій діють у рамках локалізованого підходу — обмежуючи себе вимогами щодо юрисдикції або досвіду роботи в конкретному регіоні. Автори наполягають на тому, що основні вимоги у сфері ПВК/ФТ часто є стандартизованими (напр., через стандарти FATF) і мають значно менше локальних відмінностей, ніж вважається. У той же час переоцінювання "локального досвіду" зменшує доступ до глобальних ресурсів, ускладнює масштабування та сприяє підвищенню витрат на персонал. Це особливо критично у проектах з ліквідації відставання або при реалізації великих програм моніторингу.

[7] https://3d646725-c68f-471d-b12e-03834568caef.usrfiles.com/ugd/3d6467_a43f63181b1b478cb7991e0329f33a4b.pdf

Звіт жорстко критикує поточні практики найму, де перевага надається досвіду (рокам роботи) як проксі-показнику компетентності. Такий підхід, на думку авторів, не витримує емпіричної перевірки: аналітики з меншим досвідом часто демонструють кращі результати, якщо проходять належне навчання і працюють у структурованому середовищі. Структури найму, орієнтовані на перегляд CV та фільтрацію за ключовими словами, упускають кандидатів з високим потенціалом, але нетиповим профілем, або тих, хто не володіє локальним "контекстним досвідом", хоча має належні навички.

Окремо розглядається проблема так званого "contractor conundrum" — системна залежність від короткострокових контрактів у сфері ПВК, зокрема у проектах банків і консалтингових фірм. Така модель орієнтується на гнучкість і масштабованість, але часто не дає змоги вкладатися в навчання персоналу, призводить до стагнації навичок і підтримує замкнене коло "міграції середніх спеціалістів". Підрядники рідко проходять оновлення знань або валідацію навичок, а бізнес-моделі на кшталт "time & materials" мотивують виконавців на збільшення обсягу, а не якості.

Автори пропонують альтернативний підхід — перехід до аутсорсингових моделей, орієнтованих на результат (outcome-based models). У таких моделях компенсація аналітиків прив’язана до якості й швидкості виконання справ, а не до часу перебування в проєкті. Цей підхід стимулює високу продуктивність, самонавчання та підтримує стабільність якості. Він також вимагає наявності системи валідації навичок, постійного навчання та моніторингу результатів роботи.

Висновки:

- **Досвід ≠ компетентність**: відбір аналітиків має базуватися на практичних навичках і потенціалі, а не на роках роботи; впровадження тестів на здібності (aptitude tests) та симуляцій дозволяє виявити справжній потенціал кандидатів.
- **Результат-орієнтоване ціноутворення мотивує**: моделі, де винагорода аналітика залежить від якості й швидкості рішень, забезпечують кращу продуктивність, ніж моделі з оплатою за час (day rate).
- **Навчання має бути безперервним і персоналізованим**: ефективне підвищення кваліфікації аналітиків потребує регулярних симуляцій, оцінки слабких місць та використання QC як зворотного навчального механізму.
- **Фокус на адаптивності, а не на "локалізації"**: глобальний підхід до управління персоналом дозволяє скоротити витрати, масштабуватися швидше та формувати більш різноманітні та компетентні команди.

У контексті професійної кваліфікації звіт ставить під сумнів ефективність наявних сертифікаційних програм, які зосереджуються на теоретичних знаннях, а не на практичних навичках. Наприклад, знання про FATF або вимоги AMLD ще не свідчать про здатність аналітика ефективно працювати з кейсами, вирішувати конфлікти з фронт-офісом або коректно будувати аргументацію. Альтернативою можуть бути сценарні симуляції (case simulators) або інші методи оцінки, засновані на реальних робочих ситуаціях.

Рекомендовано системно використовувати оціночні тести на здібності (aptitude testing) як перший етап відбору — особливо для молодших аналітиків. Досвід роботи не завжди свідчить про ефективність, а натомість такі якості як допитливість, увага до деталей, стресостійкість і здатність до навчання часто є кращими індикаторами потенціалу. Оцінка повинна враховувати не лише технічні знання, а й м’які навички — комунікацію, уміння аргументувати, аналізувати та адаптуватися до змін.

Ключову роль у формуванні високоефективної команди аналітиків має структуроване навчання, що базується на індивідуальних прогалинах знань, стилях навчання, симуляціях

реальних ситуацій і зворотному зв'язку з QC. Валідоване навчання не повинно завершуватись на етапі онбордингу — воно має бути безперервним. Особливо підкреслюється важливість постійного навчання в умовах, коли злочинці також постійно вдосконалюються: вони тестують системи, адаптуються, і тому організаціям необхідно навчатись швидше за своїх опонентів.

Розглядається також механізм зворотного зв'язку як навчальної платформи — тобто використання результатів QC (quality control) не лише для перевірки якості, а й як мікронавчальних сегментів. Це дозволяє аналітикам закріплювати знання у контексті реальних помилок і формувати сталі навички через повторення та емоційне включення.

В останньому розділі аналізується проблема хронічної недостатньої продуктивності. Автори наполягають, що перед тим як оцінювати окремого виконавця, слід перевірити, чи створено для нього необхідні умови (наставництво, чіткі інструкції, доступ до ресурсів, підтримка керівництва). Після цього слід чітко розрізняти дефіцит знань (що вирішується навчанням) та дефіцит здібностей (що може потребувати переведення в іншу роль або припинення співпраці).

Документ завершується закликом до індустріального підходу до управління талантами у сфері ПВК/ФТ — через впровадження моделей із чіткою перевіркою навичок, результативним управлінням ефективністю, безперервним навчанням і стратегічною роботою з глобальними командами.

ШІ у фінансах: оцінка ефективності, ризиків і стандартів впровадження GenAI у банківській системі [8]

Аналітичний звіт розкриває стратегічну, технологічну та регуляторну складову впровадження генеративного штучного інтелекту (GenAI) у банківському секторі, пропонуючи структуровану рамку для його ефективної та безпечної інтеграції. Автори звіту — експерти Kodex AI та Deutsche Bank — розглядають GenAI як технологію з високим трансформаційним потенціалом, здатну радикально змінити підходи до комплаєнсу, управління ризиками, обслуговування клієнтів і внутрішніх бізнес-процесів. У центрі дослідження — ідея, що для досягнення стійкої вигоди від GenAI необхідна не лише інноваційність, але й глибока технічна, регуляторна та організаційна підготовленість.

Документ окреслює триетапний підхід до впровадження GenAI. Перший етап — застосування базових можливостей обробки природної мови: генерація текстів, автоматизоване складання звітів, резюмування юридичних чи регуляторних документів. Другий етап — так звані «chat-to-agent» рішення, де мовна модель інтегрується з іншими інструментами, наприклад Python-агентами, для виконання аналітичних або кодових запитів. На третьому етапі організація може впроваджувати автономні GenAI-системи, здатні самостійно приймати рішення, здійснювати складні дії і виконувати повноцінну функціональну заміну в рутинних і аналітичних процесах.

Ключова увага приділена визначенню факторів якості GenAI-систем. До них віднесено якість та обсяг тренувальних даних, здатність моделі до адаптації (через PEFT, LoRA, RAG), архітектурні особливості, здатність до пояснюваності результатів, а також питання інформаційної безпеки та захисту конфіденційності. Особливо підкреслюється, що без належної підготовки даних — у т.ч. із використанням синтетичних та анонімізованих джерел — високоякісні результати від GenAI неможливі. Ризик «галюцинацій» (здатність моделі створювати переконливі, але фактично

[8] https://corporatebank.db.com/files/documents/publications/whitepaper-Adopting-Generative-AI-in-Banking.pdf

хибні, неточні або вигадані відповіді, які не відповідають реальним даним, логіці чи контексту завдання) розглядається як серйозний, але технічно керований, за умови використання відповідної архітектури, перевірки результатів людьми та встановлення механізмів зворотного зв'язку (human-in-the-loop).

Значну частину звіту присвячено регуляторному та етичному контексту. Автори вказують на складність адаптації GenAI до багатошарових нормативних вимог, зокрема щодо захисту даних, трансграничної передачі інформації, відповідальності за автоматизовані рішення, авторських прав на навчальні дані, а також на необхідність створення галузевих «пісочниць» (ШІ-«пісочниці») і відкритих стандартів для прозорості. Також порушено тему нерівності доступу до якісних даних через IP-обмеження — зокрема парадокс, коли публічна інформація (наприклад, регуляторні новини) не може бути використана у комерційних GenAI-рішеннях. Це обмежує потенціал систем і загрожує домінуванням великих технологічних гравців над дрібнішими інноваційними компаніями.

Звіт наголошує на важливості врахування людського чинника. Інтеграція GenAI повинна супроводжуватись програмами перенавчання, зміною корпоративної культури та залученням персоналу до адаптації систем. Автори підкреслюють, що основна цінність GenAI — не в заміні працівників, а в масштабуванні їх можливостей та звільненні від рутинних завдань. Для досягнення цього необхідно впроваджувати політики пояснення результатів моделей, створювати аудиторські сліди (audit trails), забезпечувати відповідність етичним нормам та прозоро оцінювати продуктивність рішень.

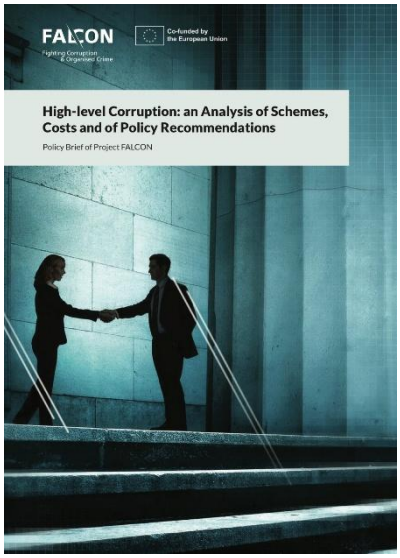
Окрему увагу приділено викликам у неангломовних ринках. Автори закликають до створення локальних benchmarks і навчальних наборів, адаптованих до національної термінології та культурного контексту. Вони попереджають, що без таких заходів компанії з неангломовних країн ризикують як у якості результатів, так і в дотриманні нормативних вимог, що може викликати юридичні наслідки чи втрату репутації.

Загалом, документ є комплексним стратегічним орієнтиром для банківських і фінансових установ, які прагнуть інтегрувати GenAI у свою діяльність. Його цінність полягає у збалансованому підході: одночасному розгляді технічної архітектури, бізнес-вигод, регуляторних викликів та соціальних аспектів впровадження інновацій.

Висновки:

- **Поступове впровадження GenAI — критичний шлях до успіху:** Рекомендовано реалізовувати GenAI-проєкти поетапно: від автоматизації рутинних текстових завдань до агентних і автономних рішень. Це дозволяє уникати операційних, правових і репутаційних ризиків та поступово вибудовувати внутрішню довіру до систем.
- **Запровадити інституційні ШІ-«пісочниці» та стандартизовані тестові дані:** Створення регульованих середовищ для експериментування (ШІ-«пісочниці») і доступ до анонімізованих, високоякісних фінансових баз даних дозволить фінансовим установам безпечно тестувати GenAI-рішення без порушення нормативних вимог.
- **Активне управління ризиками «галюцинацій» і викривлень даних:** Необхідно впроваджувати RAG-архітектуру, використання SPIN/PEFT-технологій, залучати галузевих експертів до оптимізації моделей і застосовувати фільтрацію контенту на вході/виході.
- **Формування національних критеріїв якості і розробка власних LLM-моделей — ключ до ефективного масштабування:** Країни з неангломовними ринками повинні розвивати локальні тестові набори і LLM з урахуванням галузевої термінології, щоб зменшити ризики помилкових результатів, непорозумінь або регуляторних санкцій.

Високорівнева корупція у цифрах і схемах: глобальні ризики, наслідки та політичні рішення[9]



Документ, підготовлений в рамках проєкту FALCON, є комплексним аналітичним дослідженням високорівневої корупції, яке охоплює чотири основні домени: корупцію у сфері публічних закупівель, ухилення від санкцій з боку клептократів і олігархів, прикордонну корупцію та інші випадки високорівневої корупції, що не належать до зазначених категорій. Документ базується на міждисциплінарному підході, який поєднує аналіз 63 кейсів з понад 40 країн, опрацювання відкритих судових документів, ЗМІ, експертних інтерв'ю, а також аналітичну роботу з великими масивами адміністративних і корпоративних даних. Автори фокусуються на схемах, інструментах, фінансових потоках, транскордонному характері корупції та її наслідках, із метою виявлення ефективних способів протидії та запобігання.

У частині аналізу схем і методів реалізації корупції дослідження демонструє, що найпоширенішими злочинними практиками є хабарництво, розтрата державних коштів, шахрайство, підробка документів та незаконне переведення активів. Різні форми корупції часто поєднуються між собою та охоплюють складні багаторівневі схеми із залученням юридичних осіб, підставних осіб, професійних посередників та фінансових інструментів. Готівка є головною формою обміну в прикордонній корупції, тоді як у сфері публічних закупівель і санкційних схем домінують банківські перекази, використання корпоративних структур і офшорних юрисдикцій. Майже в половині кейсів спостерігається використання високоризикових або третіх юрисдикцій, а у понад третині випадків – залучення членів сім'ї або довірених осіб для приховування бенефіціарів. Найбільш активно використовуваними «юрисдикціями-посередниками» є Велика Британія, США, ОАЕ, Швейцарія, Британські Віргінські Острови, що підкреслює роль економічно розвинених країн з високим рівнем корпоративної конфіденційності як посередників у схемах легалізації корупційних доходів.

Документ також пропонує новітній підхід до виявлення корупційних ризиків шляхом використання якісних адміністративних даних і цифрових індикаторів. Такі індикатори формуються на основі аномалій у процесах закупівель (наприклад, занадто короткий термін публікації тендерів, висока частка неконкурентних процедур), корпоративних структурах (наявність офшорних власників, фіктивних директорів, зв'язків із PEP), а також у прикордонній діяльності (часті перетини кордону, коротка тривалість перебування, використання фальшивих документів). У документі проілюстровано конкретні кейси, серед яких постачання медичних товарів за завищеними цінами під час пандемії COVID-19 у Великій Британії, контрабанда сигарет через білорусько-литовський кордон, а також придбання нерухомості в США російським олігархом через офшори для обходу санкцій.

Щодо наслідків, дослідження підкреслює системний характер впливу корупції на суспільство та економіку. Зокрема, вона викривляє розподіл бюджетних ресурсів, знижує якість державних послуг, зменшує довіру до інститутів, відштовхує іноземні інвестиції та породжує широку соціальну несправедливість. В окремих секторах це має конкретно вимірювані наслідки — наприклад, в Хорватії укладення контрактів із високими корупційними ризиками призвело до перевитрат у розмірі понад 50 млн євро. У прикордонному контексті наслідки проявляються у

[9] https://baselgovernance.org/sites/default/files/2025-04/2025_03_10-FALCON-Policy-Brief_final.pdf

вигляді бюджетних втрат, ускладнення законної торгівлі, підтримки тіньової економіки та послаблення безпеки.

У завершальній частині документ пропонує двокомпонентну політику протидії: покращення якості даних та зміцнення законодавчого середовища. У сфері даних рекомендується запровадження уніфікованих ідентифікаторів для зв'язку між наборами (ідентифікатори податків, закупівель, юридичних осіб), стандартизація форматів, розвиток інструментів анонімізації та поліпшення доступу до даних для громадянського суспільства та міжнародних партнерів. В частині правового регулювання наголошується на необхідності обмеження процедур, вразливих до зловживань (зокрема, неконкурентних тендерів), цифровізації митних процесів, гармонізації стандартів управління санкціями між країнами ЄС, вдосконалення інструментів виявлення конфлікту інтересів та е-декларування. Увага також приділяється проблемам імплементації: нестача ресурсів, неефективна координація між відомствами, дублювання функцій і відсутність інституційної спроможності є критичними перешкодами для ефективної реалізації навіть найкращих нормативно-правових рішень.

Висновки:

- **Корупція має транснаціональний характер та часто оперує через стабільні «юрисдикції-посередники» юрисдикції, що забезпечують високий рівень конфіденційності й легальності обігу активів.**
  Рекомендація: Створити міжнародні реєстри та угоди щодо прозорості бенефіціарів, обміну інформацією та контролю за офшорами.
- **Найвищі ризики корупції виявляються у неконкурентних закупівлях, із залученням PEP, та в умовах надзвичайних ситуацій (наприклад, COVID-19).**
  Рекомендація: Встановити чіткі межі та прозорість застосування виняткових процедур.
- **Недоступність і несумісність адміністративних даних (особливо у сфері COI, власності, публічних контрактів) суттєво обмежує виявлення корупційних схем.**
  Рекомендація: Впровадити стандартизовані, машинозчитувані формати з єдиними ідентифікаторами та міжвідомчий обмін.
- **Фактичне впровадження законів залежить не лише від їх якості, але й від спроможності виконавчих органів: кадри, технічне оснащення, координація.**
  Рекомендація: Інвестувати в інституційну спроможність і чіткий розподіл повноважень між органами влади.

Узагальнюючи, цей Policy Brief не лише викриває глобальні схеми високорівневої корупції, але й закладає конкретний методологічний фундамент для їхнього виявлення і профілактики через дані, цифрові інструменти та міжсекторальну взаємодію.

Протидія відмиванню коштів у 2025: нова ера санкцій, обміну інформацією та технологічної трансформації [10]

NICE Actimize
Know more. Risk less.

У блозі, опублікованому аналітиками компанії NICE Actimize, висвітлено ключові очікувані тенденції у сфері протидії відмиванню коштів (ПВК) на глобальному рівні у 2025 році. Документ фокусується на п'яти критичних напрямках розвитку: активізація санкційного режиму,

[10] https://www.niceactimize.com/blog/aml-predictions-information-sharing-increased-sanctions-and-regulatory-landscape-prioritized-for-2025/?utm.com

посилення міжорганізаційного обміну інформацією, зростання регуляторної уваги до нефінансових бізнесів, вплив геополітичної поляризації на ПВК-інфраструктуру та модернізація технологічних підходів до виявлення фінансових злочинів.

На тлі зростання міжнародної нестабільності, санкції залишаються одним з основних інструментів політичного та економічного тиску, а їх обхід — дедалі більш витонченим. У 2025 році очікується подальше розширення санкційних списків, особливо в частині «вторинних санкцій», що стосуватимуться осіб і компаній, які допомагають ухилятися від існуючих обмежень. Це, у свою чергу, зумовлює потребу в глибшій перевірці транзакцій, багатоступеневому моніторингу ланцюгів платежів та впровадженні більш складних систем ризик-аналізу.

Другим визначальним трендом є міжінституційний обмін інформацією, як відповідь на зростаючий рівень складності фінансових схем і роль транснаціональних злочинних мереж. Автори наголошують, що традиційно слабка комунікація між фінансовими установами, з одного боку, і органами влади та іншими суб'єктами — з іншого, створює простір для зловживань. Як приклад успішних ініціатив наводиться платформа COSMIC (Collaborative Sharing of ML/TF Information) у Сінгапурі, що дозволяє банкам спільно ідентифікувати клієнтів високого ризику на ранніх етапах. У публікації підкреслюється, що у 2025 році все більше юрисдикцій ухвалюватимуть закони, що легітимізують та стимулюють такий обмін інформацією.

Окрему увагу автори приділяють визначеним нефінансовим установам та професіям (ВНУП), які залишаються недостатньо охопленими регулюванням, попри високий ризик залучення до схем відмивання коштів. Йдеться про юристів, бухгалтерів, агентів з нерухомості та інших суб'єктів, які можуть виступати фінансовими посередниками або сприяти ухиленню від контролю. Згідно з очікуваннями, у 2025 році регуляторна політика буде активно спрямована на розширення обов'язків ВНУП щодо ідентифікації клієнтів, ведення документації та повідомлення про підозрілі транзакції.

Глобальний геополітичний ландшафт також суттєво впливає на майбутнє ПВК-середовища. Посилення блокового протистояння, відсторонення окремих країн від участі в міжнародних структурах (зокрема, FATF), зростаюча роль альтернативних міждержавних альянсів, таких як BRICS, — усе це ускладнює уніфікацію підходів до протидії фінансовим злочинам. Водночас Європейський Союз демонструє прагнення зміцнити внутрішню ПВК-архітектуру через створення єдиного наглядового органу (AMLA), гармонізацію законодавства та імплементацію регуляторного пакета шостої директиви (AMLD6).

Фінальним і, можливо, найтрансформаційнішим напрямом, який висвітлюється в публікації, є технологічна еволюція у сфері ПВК. Сучасні програми забезпечення відповідності часто є надмірно витратними, повільними та малоефективними. У відповідь на ці проблеми організації вдаватимуться до широкомасштабного впровадження інновацій — генеративного штучного інтелекту, машинного навчання, графових аналітичних моделей та автоматизованих систем виявлення аномалій. Автори підкреслюють, що 2025 рік стане критичним у визначенні того, чи зможуть фінансові установи використати технології не лише як інструмент автоматизації, а як платформу для стратегічного аналізу ризиків і проактивного реагування на загрози.

Таким чином, блог NICE Actimize окреслює майбутнє ПВК як динамічну, багатовекторну систему, що вимагає від учасників фінансового ринку готовності до адаптації, високої технологічної гнучкості, залучення до міжнародних ініціатив та готовності працювати у все складнішому нормативному полі. Публікація не лише ідентифікує ключові виклики 2025 року, але й задає рамки для формування стратегій стійкості та ефективності у глобальній боротьбі з фінансовими злочинами.

Рекомендовані матеріали та події

Розкриваючи темні гроші: серія фільмів від HBO “The Dark Money Game” [11]

Серія документальних фільмів HBO The Dark Money Game, що складається з двох частин — Ohio Confidential та Wealth of the Wicked, створена під керівництвом лауреата премії Оскар, режисера Алекса Гібні. Натхненна книгою Джейн Маєр Dark Money: The Hidden History of the Billionaires Behind the Rise of the Radical Right, серія досліджує приховані фінансові мережі, які дозволяють багатим особам і корпораціям впливати на політичні процеси в США через непрозорі канали, такі як некомерційні організації та суперкомітети політичних дій (super PACs). Ці фільми розкривають, як "темні гроші" — невідстежувані кошти — підривають демократичні принципи, сприяючи корупції та маніпуляціям у політиці.

Документальний фільм Ohio Confidential зосереджується на найбільшому корупційному скандалі в історії Огайо, пов’язаному з законопроєктом HB6 та хабарницькою схемою на суму 61 мільйон доларів, організованою енергетичною компанією FirstEnergy. Ця схема мала на меті забезпечити ухвалення у 2019 році суперечливого закону про енергетичну підтримку, який приносив вигоду компанії, одночасно накладаючи фінансові зобов’язання на платників податків Огайо. Центральною фігурою скандалу став спікер Палати представників Огайо Ларрі Хаусхолдер, який використав незаконні кошти для зміцнення своєї політичної влади. Фільм починається з трагічного епізоду — очевидного самогубства лобіста Ніла Кларка, смерть якого стала ключем до розкриття складної змови. Хаусхолдер, засуджений у 2023 році, відбуває 20-річний термін у федеральній в’язниці FCI Elkton в Лісабоні, штат Огайо.

Ohio Confidential використовує інтерв’ю з ключовими учасниками, зокрема авторкою Джейн Маєр, колишньою головною суддею Верховного суду Огайо Морін О’Коннор, журналісткою Columbus Dispatch Лорою А. Бішофф, а також федеральними прокурорами та слідчими. Ці свідчення розкривають механізми функціонування "темних грошей" та їхній вплив на законодавчий процес. Фільм демонструє, як корпоративні інтереси, підкріплені значними фінансовими ресурсами, можуть купувати політичний вплив, підриваючи довіру громадськості до державних інституцій. Сюжет підкреслює зраду інтересів виборців, адже HB6 не лише збагатив політичних і корпоративних еліт, але й завдав шкоди пересічним мешканцям Огайо, змусивши їх оплачувати підтримку збиткових енергетичних об’єктів.

Другий фільм серії, Wealth of the Wicked, розширює перспективу, аналізуючи історію фінансування політичних кампаній у США, починаючи від створення Федеральної виборчої комісії (FEC) у 1974 році й закінчуючи революційним рішенням Верховного суду у справі Citizens United проти FEC у 2010 році. Цей документальний фільм досліджує, як суперкомітети політичних дій, релігійні організації та інші групи спеціальних інтересів використовують юридичні лазівки для прихованого впливу на вибори та державну політику. Особливу увагу приділено тонкій межі між законними політичними пожертвами та хабарництвом, що вказує на системні слабкості в регулюванні фінансування кампаній. Фільм ілюструє, як необмежений

[11] https://www.hbo.com/the-dark-money-game/season-1/1-the-dark-money-game-ohio-confidential

фінансовий вплив сприяє політичній поляризації та послаблює демократичну систему, наголошуючи на необхідності реформ для відновлення прозорості.

Обидва фільми об'єднує спільна тема — руйнівний вплив "темних грошей" на демократію. Вони показують, як фінансова непрозорість породжує корупцію та підриває довіру до уряду. Режисерський підхід Гібні поєднує ґрунтовне розслідування з захопливим оповіданням, використовуючи інтерв'ю, архівні кадри та наративні реконструкції для залучення глядачів. Виробництво фільмів вирізняється участю авторитетних експертів, таких як Джейн Маєр, та досвідом Гібні у викритті системної корупції. Поєднання локального фокусу на скандалі в Огайо з ширшою національною перспективою робить серію актуальною як для місцевої аудиторії, так і для тих, хто стурбований станом демократії в США.

Прем'єра подкасту Launder This: Кріс Файстл про знищення каліфорнійського картелю та фінансові злочини[12]

Прем'єрний епізод подкасту Launder This, який веде визнаний експерт із фінансових злочинів Дев Одедра, присвяченій аналізу фінансових злочинів і комплаєнсу.

Епізод отримав назву «Після Ескобара: Кріс Файстл. Справжні наркобарони». У центрі цього дебютного випуску — глибока й захоплююча розмова з Крісом Файстлом, колишнім агентом Управління з боротьби з наркотиками США (DEA), який відіграв ключову роль у ліквідації одного з найпотужніших наркокартелів в історії — каліфорнійського картелю в Колумбії. Цей епізод не лише занурює слухачів у напружений світ боротьби з наркоторгівлею, але й розкриває складні фінансові механізми, які забезпечували діяльність картелю, що ідеально вписується в тематику подкасту, присвячену фінансовим злочинам.

Файстл ділиться детальними спогадами про свої операції в Колумбії, де він діяв у самому серці боротьби з каліфорнійським картелем. Його розповідь переносить слухачів у небезпечне середовище, де кожен день був сповнений ризику, а стратегії правоохоронців вимагали неабиякої винахідливості та мужності.

Він описує, як каліфорнійський картель, на відміну від більш хаотичного картелю Медельїна, очолюваного Пабло Ескобаром, діяв із вражаючою бізнесовою дисципліною, використовуючи структури, подібні до корпорацій, для управління своєю глобальною мережею наркоторгівлі. Ця організація прославилася своєю здатністю інтегруватися у легальні економічні системи, що робило її особливо складною мішенню для правоохоронних органів.

Важливою частиною епізоду є акцент на фінансових аспектах діяльності картелю. Каліфорнійський картель славився не лише масштабами наркоторгівлі, але й витонченими методами відмивання грошей, включаючи використання підставних компаній, офшорних банківських рахунків і складних схем переказу коштів через міжнародні фінансові системи. Одедра, як експерт із фінансових злочинів, майстерно пов'язує розповідь Файстла із сучасними методами боротьби з відмиванням грошей, демонструючи, як уроки, отримані під час операцій проти каліфорнійського картелю, залишаються актуальними для нинішніх зусиль у протидії фінансовій злочинності. Ця дискусія підкреслює, як наркокартелі використовують глобалізовану

[12] https://open.spotify.com/episode/5Q362dn7NlcwVtVkt3NGE0?go=1&sp_cid=a696145bd3af49bedf15cd1ff35344b7&utm_source=embed_player_p&utm_medium=desktop&nd=1&dlsi=b68d444d8dab4922

фінансову систему для маскування своїх доходів, і як правоохоронні органи адаптуються до цих викликів.

Значну увагу в епізоді приділено книзі Файстла «Після Ескобара: Знищення сумнозвісних каліфорнійських хрещених батьків та найбільшого наркокартелю в історії», написаній у співавторстві з Дейвом Мітчеллом і Джессікою Балбоні. Книга, є детальним описом зусиль DEA щодо знищення каліфорнійського картелю та аналізує ширші наслідки цієї перемоги для глобальної боротьби з наркоторгівлею.

Зміна ДНК злочинності [13]

Останній епізод подкасту Європолу під назвою «Зміна ДНК злочинності» відкриває перед слухачами важливу і водночас тривожну дискусію про те, як стрімкий розвиток технологій, глобалізація і цифровізація змінюють саму природу організованої злочинності. Випуск є глибоким аналітичним зануренням у сучасну злочинну екосистему Європи та світу, й базується на висновках одного з найважливіших стратегічних звітів Європолу — Оцінки загроз організованої злочинності у ЄС (EU SOCTA 2024). Цей звіт, який публікується кожні чотири роки, визначає пріоритети для правоохоронних органів усіх країн-членів ЄС, і цей епізод є його аудіовідлунням — стислою, але насиченою інтерпретацією ключових тенденцій, викликів і прогнозів.

У подкасті виступають одразу кілька фахівців з Європолу, зокрема Ендрю Райт, керівник підрозділу стратегічного аналізу, який разом із модераторкою розповідає про зміни в структурах організованої злочинності, методах її дій та взаємозв'язок із законною економікою. Один з основних меседжів епізоду — організована злочинність перестала бути виключно насильницькою вуличною діяльністю. Вона стала високотехнологічною, адаптивною та системно інтегрованою у глобальну економіку. Сучасні злочинні групи, за словами Ендрю Райта, дедалі частіше функціонують як гібридні бізнеси, які використовують ті ж самі цифрові технології, що й легальний приватний сектор: від соціальних мереж до криптовалют, від алгоритмічного таргетингу до транснаціональних логістичних ланцюгів.

Однією з головних загроз, які обговорюються у випуску, є технологічна еволюція злочинних методів — кіберзлочинність, зловживання штучним інтелектом, використання deepfakes, шифрування, даркнет і криптовалюти створюють новий рівень складності для правоохоронних структур. При цьому, як зазначається, злочинці дедалі частіше використовують правові прогалини, слабкості регуляторного нагляду в окремих юрисдикціях та можливості, які відкривають глобальні фінансові інструменти. Усе це формує те, що Європол окреслює як "нову ДНК злочинності" — злочинний ландшафт, що змінюється на клітинному рівні.

У дискусії підкреслюється, що межа між онлайн і офлайн злочинністю розмита. Традиційні види злочинів — торгівля людьми, контрабанда наркотиків, шахрайство — усе частіше мають цифровий компонент: комунікація між членами груп відбувається через зашифровані канали, реклама незаконних послуг — у Telegram чи WhatsApp, а фінансові операції — у криптоактивах.

[13] https://www.europol.europa.eu/media-press/europol-podcast/episode-18-changing-dna-of-crime?mtm_campaign=publications/documents-just-published-20250506&utm_term=publications/documents-just-published&mtm_source=newsletter&mtm_medium=email&mtm_content=title&mtm_group=document

Ставка на інноваційність стала основною ознакою злочинного мислення, що вимагає такої ж інноваційності у протидії.

Важливо, що в подкасті звучить акцент не лише на виклики, але й на відповідь правоохоронної системи. Європол закликає до міжвідомчої співпраці, обміну аналітичними даними, використання штучного інтелекту для передбачення ризиків, а також до спільної побудови цифрової стійкості. Прозвучали приклади того, як завдяки координації вдається виявляти нелегальні лабораторії з виробництва наркотиків, запобігати масштабним кіберзлочинам і відстежувати транскордонні фінансові потоки, які стоять за торгівлею людьми та зброєю.

Особливо цікавою є згадка про появу нових профілів злочинців. Якщо раніше уявлення про злочинця було пов'язане з конкретною географією чи приналежністю до кримінальних кланів, то сьогодні це може бути технологічно підкована особа будь-якого віку, національності чи бекґраунду, яка діє в онлайн-середовищі, уникає фізичних контактів, і використовує псевдоніми та VPN. Це ускладнює профілювання, вимагає нових підходів до аналітики та потребує швидшого прийняття інновацій у сфері кримінального аналізу.

Загалом, епізод 18 подкасту Європолу — це глибока, стратегічно важлива розмова про еволюцію злочинності в епоху цифрового прориву. Він не тільки інформує, але й спонукає до переосмислення парадигми боротьби зі злочинністю, підкреслюючи необхідність адаптації як інституційних структур, так і законодавства. Подкаст буде особливо цінним для аналітиків, кримінологів, розробників політик, фахівців з фінансового моніторингу, кібербезпеки та всіх, хто працює на перетині технологій і безпеки. Його основний висновок звучить як заклик до дії: щоб ефективно боротися із сучасною злочинністю, ми маємо змінити не лише інструменти, але й мислення — так само, як змінилася ДНК злочинного середовища.

Регулювання штучного інтелекту та майбутнє ПВК [14]

Вже в середу, 14 травня 2025 року відбудеться вебінар, який організовує компанія ComplyAdvantage, присвячений регулюванню штучного інтелекту (ШІ) та його впливу на системи ПВК/ФТ/ФР. Цей захід є надзвичайно актуальним у контексті набуття чинності Закону про ШІ в ЄС (EU AI Act), який передбачає жорсткі вимоги до використання ШІ, включаючи високі штрафи за недотримання — до 35 мільйонів євро або 7% світового річного обороту компанії.

Вебінар спрямований на обговорення ключових аспектів нового регуляторного середовища, зокрема необхідності забезпечення «AI-грамотності» персоналу, ідентифікації та моніторингу використання ШІ в організаціях, а також управління ризиками, пов'язаними з «тіньовим ШІ» — використанням несанкціонованих або вбудованих ШІ-рішень без належного контролю. Особлива увага приділяється високоризиковим застосуванням ШІ, таким як автоматизоване прийняття рішень у фінансовому моніторингу, що вимагає прозорості, пояснюваності та відповідності етичним стандартам.

[14] https://get.complyadvantage.com/insights/ai-regulation-webinar?utm_campaign=10992215-CA0081%20%7C%20AI%20Regulation%20webinar%20%7C%20May%202025%20%7C%20EMEA%20%7C%20AMER&utm_medium=email&_hsenc=p2ANqtz-9tAhUjBqBDRdpVzAU-rB79SXrHjLpX3IoKhLqiSz5PItIMrrMBdh6sSrbj8qDxSnVMwxQa-4raS3UBJXcVUGqXLcpJEw&_hsmi=360526877&utm_content=360534309&utm_source=hs_email

Для фахівців у сфері ПВК/ФТ/ФР цей вебінар є надзвичайно корисним, оскільки ШІ вже активно використовується для виявлення підозрілих транзакцій, моніторингу клієнтів та аналізу ризиків. Однак, з огляду на нові регуляторні вимоги, організаціям необхідно переглянути свої підходи до впровадження ШІ, забезпечити відповідність новим стандартам та уникнути потенційних правових наслідків. Захід також надає можливість ознайомитися з найкращими практиками управління ШІ-ризиками та інтеграції етичних принципів у процеси ПВК/ФТ/ФР.

Інші новини

Викриття тіньового флоту [15]

Стаття опублікована Danwatch, є ґрунтовним журналістським розслідуванням, яке викриває складну шахрайську схему, пов'язану з діяльністю російського тіньового флоту. Цей флот, що складається з суден, які використовуються для обходу міжнародних санкцій, зокрема тих, що стосуються експорту російської нафти, став об'єктом уваги через махінації з фальшивими страховими документами.

Стаття детально описує, як норвезька підставна компанія Ro Marine стала ключовим елементом цієї схеми, видаючи підроблені сертифікати, що дозволяло суднам уникати перевірок і продовжувати незаконну діяльність. Викриття цієї афери спричинило значний міжнародний резонанс, змусивши держави, які надають суднам право плавати під їхніми прапорами, відкликати свої дозволи для цієї компанії, що суттєво обмежило її операційну спроможність.

Стаття розкриває ширший контекст проблеми тіньового флоту, який діє в умовах правової невизначеності, використовуючи прогалини в міжнародних регуляціях для транспортування підсанкційних товарів. Норвезька компанія, яка опинилася в центрі скандалу, використовувалася як інструмент для створення видимості легітимності, надаючи суднам фальшиві страхові документи, що є обов'язковими для проходження перевірок у портах. Розслідування, проведене Danwatch, пролило світло на цю схему, підкресливши її масштаби та системний характер. Воно стало каталізатором для дій з боку міжнародної спільноти, зокрема держав, які оперативно відреагували, внісши Ro Marine до чорних списків і скасувавши її акредитацію. Це рішення не лише ускладнило діяльність самої компанії, але й стало сигналом для інших учасників подібних схем про посилення контролю.

Міжнародна реакція, підкреслює важливість скоординованих зусиль у боротьбі з тіньовим флотом. Чорні списки, до яких потрапила норвезька компанія, є ефективним інструментом, що обмежує можливості шахрайських організацій вести бізнес, оскільки держави та приватні компанії уникають співпраці з такими суб'єктами. Стаття наголошує на необхідності вдосконалення систем перевірки страхових документів, вказуючи на вразливості в чинних механізмах морського регулювання. Вона також звертає увагу на економічні та політичні наслідки діяльності тіньового флоту, який дозволяє Росії обходити санкції, підтримуючи свій нафтовий експорт. Обмеження таких операцій може мати значний вплив на економіку країни-агресора, послаблюючи її фінансові можливості.

[15] https://danwatch.dk/en/russian-shadow-fleet-fraudster-blacklisted-across-the-globe/

Стаття також підкреслює роль журналістських розслідувань у боротьбі з глобальними проблемами. Danwatch, як організація, що спеціалізується на дослідженні порушень у сфері міжнародної торгівлі та прав людини, демонструє свою здатність впливати на політику та регулювання. Викриття шахрайської схеми стало не лише інформаційним проривом, але й практичним поштовхом для дій, спрямованих на припинення незаконної діяльності. Це розслідування є прикладом того, як журналістика може сприяти прозорості та підзвітності, змушуючи уряди та міжнародні організації реагувати на виявлені проблеми.

Цифрові пастки: Як екстремісти радикалізують підлітків [16]

Стаття Associated Press присвячена тривожній тенденції радикалізації підлітків екстремістськими групами через онлайн-платформи, де використовуються ультранасильницький контент, соціальні мережі, ігрові сервіси та зашифровані месенджери. Центральною історією є випадок у Франції з 12-річним хлопчиком, який, за словами його матері, проводив години у своїй кімнаті, нібито граючи у відеоігри чи виконуючи домашні завдання, але насправді збирав величезну бібліотеку джихадистської пропаганди, включно з відео обезголовлення та інструкціями зі створення вибухівки. Цей випадок є прикладом ширшої глобальної проблеми, коли дуже молоді люди стають жертвами цифрової маніпуляції, що перетворює їх на потенційних терористів, часто без відома батьків чи правоохоронних органів, аж поки не стає занадто пізно.

Подорож хлопчика у темні глибини інтернету почалася з невинних пошуків інформації про іслам після того, як тітка подарувала йому Коран. Ці пошуки, підживлені алгоритмами, які спрямовують користувачів до дедалі радикальнішого контенту, та цікавістю дитини, привели його до зашифрованих чатів і ультранасильницької пропаганди, яку поширюють бойовики Ісламської держави та інші екстремістські угруповання. Французький прокурор Поль-Едуард Лаллуа, який домігся засудження хлопчика за двома звинуваченнями, пов’язаними з тероризмом, у серпні 2024 року, підкреслив, що перегляд тисяч зображень і відео настільки спотворив світогляд дитини, що для відновлення нормального сприйняття реальності знадобляться роки психологічної роботи. Прокурор застеріг, що без втручання хлопчик міг би стати "повністю дегуманізованою зброєю", здатною вчинити жахливі злочини навіть із простим ножем.

Стаття підкреслює глобальний масштаб проблеми, зазначаючи, що контртерористичні служби по всьому світу фіксують дедалі молодших підозрюваних. У Франції національний прокурор з питань боротьби з тероризмом Олів’є Крістен повідомив про різке зростання кількості неповнолітніх, звинувачених у терористичних злочинах: з двох у 2022 році до 19 у 2024 році, причому деякі з них були лише 15-річними. Мережа розвідувальних служб "П’ять очей" (США, Велика Британія, Канада, Австралія, Нова Зеландія) у грудні 2024 року оприлюднила рідкісне публічне попередження, наголосивши, що радикалізовані неповнолітні становлять таку ж серйозну терористичну загрозу, як і дорослі. Приклади з Австрії, де 14-річний підліток планував

[16] https://apnews.com/article/technology-parenting-terror-islamic-state-police-security-attacks-4888bab2d10502edadf787d419d45b5b

атаку на вокзалі у Відні, та Бельгії, де третина підозрюваних у плануванні атак у 2022–2024 роках були неповнолітніми, включно з 13-річним, ілюструють цю тенденцію.

Процес радикалізації описується як швидкий, часто він займає лише кілька місяців, і полегшується легким доступом до екстремістського контенту на платформах, які підлітки вже активно використовують. Стаття пояснює, як деякі діти, починаючи з перегляду насильницької порнографії чи кривавих зображень, поступово переходять до джихадистської пропаганди через алгоритмічні рекомендації та взаємодію в зашифрованих чатах. Ці цифрові простори дозволяють екстремістам діяти анонімно, що ускладнює втручання правоохоронців порівняно з попередніми поколіннями бойовиків, які взаємодіяли у фізичному світі. Стаття також зазначає, що радикалізовані підлітки походять із різних соціальних верств, і не лише з тих, хто має поведінкові проблеми, що ускладнює профілактичні заходи.

Випадок із 12-річним хлопчиком підкреслює виклики для батьків, які часто не підозрюють про онлайн-діяльність своїх дітей. Його мати вважала, що він займається невинними справами, а адвокат родини, Камель Айссауї, стверджував, що хлопчик став жертвою маніпулятивних цифрових платформ. Після засудження дитину помістили до спеціалізованого закладу без доступу до соціальних мереж, під наглядом педагогів і з регулярними відвідинами батьків, що підкреслює необхідність інтенсивної реабілітації. Стаття завершується роздумами прокурора, який описав колекцію хлопчика з 1739 джихадистських відео як таку, що "перевершує будь-яке розуміння", наголошуючи на масштабах і жорстокості контенту, який підживлює цю кризу.

Перші результати порушення санкцій Великої Британії: справа Овсяннікова[17]

Прес-реліз Національного агентства із боротьби зі злочинністю Великої Британії (NCA), описує перші в історії країни судові вироки за порушення санкцій, запроваджених відповідно до Положення про санкції проти Росії 2019 року.

Обвинуваченими у справі є Дмитро Овсянніков, колишній губернатор Севастополя, призначений Росією в незаконно анексованому Криму, та його брат Олексій Овсянніков. Ця справа підкреслює рішучість Великої Британії забезпечувати виконання санкцій, спрямованих проти осіб, пов’язаних із діями Росії в Україні, особливо після повномасштабного вторгнення 2022 року.

Дмитро Овсянніков обіймав посаду губернатора Севастополя з 2016 по 2019 рік за призначенням президента Росії Володимира Путіна. У 2017 році він потрапив під санкції Європейського Союзу, а після виходу Великої Британії з ЄС аналогічні фінансові обмеження були запроваджені відповідно до національного законодавства. Незважаючи на ці санкції, Овсянніков у січні 2023 року отримав британський паспорт завдяки британському громадянству свого батька. 1 лютого 2023 року він прибув до Великої Британії, де приєднався до своєї дружини та двох дітей, які вже проживали в будинку його брата Олексія в районі Клепем, Лондон.

Основні порушення санкційного режиму полягали в спробах обійти фінансові обмеження. У лютому 2023 року Дмитро Овсянніков відкрив банківський рахунок у Великій Британії, на який його дружина перерахувала 76 000 фунтів стерлінгів. Ці кошти були використані для внесення застави за автомобіль Mercedes Benz GLC 300 SUV. Однак банк незабаром виявив, що

[17] https://www.nationalcrimeagency.gov.uk/news/nca-secures-first-convictions-for-breach-of-uk-sanctions

Овсянніков перебуває в санкційному списку, і заморозив рахунок. Після цього Олексій Овсянников придбав зазначений автомобіль і застрахував його на ім'я Дмитра, що дозволило останньому отримати доступ до транспортного засобу, попри санкційні обмеження. Крім того, у травні 2024 року Олексій сплатив понад 40 000 фунтів за навчання двох молодших дітей Дмитра, що стало ще одним порушенням санкцій, оскільки це вважалося наданням економічних ресурсів особі під санкціями.

Овсянніков був цілком обізнаний про свій санкційний статус, оскільки раніше звертався до Міністерства закордонних справ, Співдружності та розвитку (FCDO) з проханням зняти з нього обмеження. Його навмисні дії з обходу санкцій за підтримки брата призвели до їхнього арешту та засудження. У січні 2024 року Дмитра заарештували, а Олексій добровільно дав свідчення щодо своєї ролі у сприянні ухиленню від санкцій. Дмитра визнали винним у порушенні санкційного режиму та відмиванні грошей, пов'язаних із переказом 76 000 фунтів і заставою за автомобіль. Олексія засудили за надання економічних ресурсів особі під санкціями, зокрема за купівлю автомобіля та оплату шкільних зборів. Ці вироки стали першими в історії Великої Британії за сприяння особі, яка перебуває під санкціями.

Прокуратура Корони (CPS) планує розпочати процедуру повернення незаконно отриманих коштів і активів у рамках провадження щодо доходів від злочинної діяльності. Генеральний директор NCA Грем Біґґар зазначив, що ці вироки демонструють увагу агентства не лише до осіб під санкціями, а й до тих, хто сприяє порушенню санкційних правил. Він підкреслив внесок Підрозділу NCA, який із початку вторгнення Росії в Україну здійснив понад 180 операцій із нейтралізації загроз від еліт, пов'язаних із Путіним, та їхніх пособників. Уповноважений із питань санкцій FCDO Стівен Дауті наголосив на рішучості уряду посилювати тиск на Росію та її поплічників, а також на вдосконаленні інструментів правоохоронних органів для ефективного виконання санкцій. Прокурор CPS Джуліус Капон підкреслив, що санкції спрямовані на обмеження фінансових можливостей ключових фігур, щоб змусити Росію припинити військові дії, і ці вироки мають стати чітким сигналом для інших порушників.

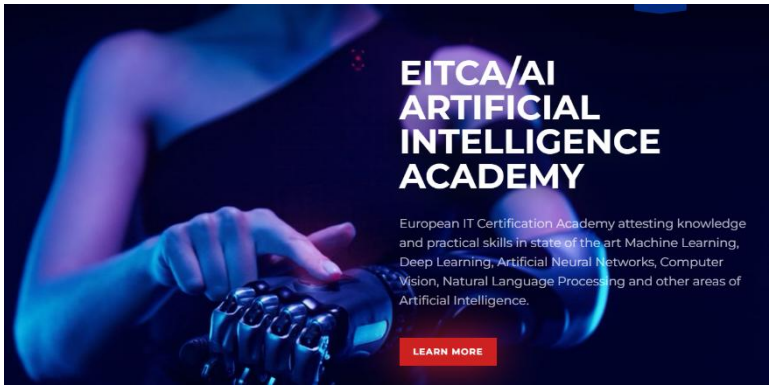
Оголошена 9 квітня 2025 року справа відображає посилення зусиль Великої Британії у боротьбі з ухиленням від санкцій на тлі війни Росії проти України. Документ також згадує ширшу діяльність NCA, зокрема цілодобову лінію для звернень, систему повідомлень про підозрілу діяльність і такі ініціативи, як операція Stovewood, хоча вони не стосуються безпосередньо цієї справи. Успіх цієї операції підкреслює важливість скоординованих дій між NCA, CPS та іншими урядовими структурами для забезпечення ефективного виконання санкцій і притягнення до відповідальності всіх причетних до їх порушення.

Для загального розвитку

ШІ Академія [18]

EITCA/AI Artificial Intelligence Academy — це повноцінна міжнародна програма професійної сертифікації у сфері штучного інтелекту, розроблена Європейським інститутом сертифікації інформаційних технологій (EITCI), що базується у Брюсселі. Ця академія має на меті надати учасникам не лише фундаментальні теоретичні знання, але й практичні навички, необхідні для ефективної роботи в одному з найдинамічніших та найперспективніших напрямів сучасної цифрової економіки — штучному інтелекті. Програма побудована на системі сертифікаційних модулів EITC (European Information Technologies Certification), які разом формують повноцінну

[18] https://eitca.org/eitca-ai-artificial-intelligence-academy/?ch=r3v9xg



академічну траєкторію сертифікації EITCA. Завдяки онлайн-формату навчання, відсутності вимог до фізичної присутності, гнучкому розкладу та доступності для широкого кола учасників, EITCA/AI є однією з найбільш демократичних та масштабованих освітніх ініціатив у галузі цифрових технологій. Навчальна програма складається з 12 модулів, кожен з яких зосереджений на певному аспекті ШІ — від базових основ Python, необхідних для подальшого програмування алгоритмів, до спеціалізованих технологій, таких як глибоке навчання з TensorFlow та PyTorch, використання Google Cloud Platform для машинного навчання, а також концептуально складніші напрямки, як-от квантове машинне навчання. Структура навчання побудована так, щоб поступово ускладнювати матеріал, забезпечуючи при цьому логічну послідовність між модулями. Кожен модуль оцінюється за допомогою онлайн-іспиту — тестування, що містить 15 запитань з варіантами відповідей, який необхідно пройти за 15 хвилин. Прохідний бал становить 60%, і учасники мають можливість безкоштовного повторного складання у разі невдачі. Після успішного завершення кожного модуля учасник отримує сертифікат EITC, а після проходження всіх 12 модулів — комплексний сертифікат EITCA/AI, який підтверджує професійну компетентність у сфері штучного інтелекту на рівні, що відповідає міжнародним стандартам.

Навчальні матеріали програми створені англійською мовою і включають відеолекції, інтерактивні вправи, презентації та текстові файли, доступні для завантаження у форматі PDF. Навчання є повністю асинхронним, що дозволяє учасникам обирати власний темп і режим занять. За потреби можна звертатися до технічної або методичної підтримки через електронну систему. Загальний обсяг навчального навантаження орієнтовно становить 180 годин, що робить програму інтенсивною, але цілком здійсненною навіть для зайнятих фахівців.

Сертифікати, видані EITCI, мають цифрове підтвердження, що дає змогу перевірити їхню справжність онлайн і легко додавати до резюме чи профілю на LinkedIn. Хоча сам інститут не є офіційною структурою Європейського Союзу, він діє відповідно до принципів цифрової політики ЄС щодо розвитку цифрових компетентностей громадян. Програма EITCA/AI була розроблена також як частина ініціативи з підвищення кваліфікації у сфері цифрових навичок у межах цифрової трансформації, що особливо важливо для фахівців з країн, які мають обмежений доступ до високоякісної IT-освіти.

Ваша думка важлива!

1. Як Україна може посилити свою роль у міжнародній боротьбі з російським тіньовим флотом, враховуючи її стратегічне розташування на Чорному морі та вплив санкцій на економіку Росії?
2. Які конкретні кроки можуть зробити українські школи, батьки та громади, щоб підвищити цифрову грамотність і захистити дітей від впливу екстремістського контенту в інтернеті, особливо в умовах зростання психологічної вразливості через воєнний стрес?
3. Чи достатньо нинішніх західних санкцій, щоб зупинити фінансування російської військової машини, і як Україна може лобіювати їх посилення?
4. Яким чином має бути врегульований статус стейблкоїнів в Україні?
5. Яку роль відіграють політично значущі особи (PEP) у формуванні корупційних практик в Україні, і чи достатньо дієвим є нинішній інструментарій для виявлення їхнього впливу на публічні закупівлі?
6. Чи повинні регулятори розглядати можливість заборони або суттєвого обмеження "white label" моделей у гемблінгу як надмірно ризикованих для ПВК/ФТ-середовища?
7. Чи варто в Україні створити національну sandbox-платформу для регуляторного діалогу з DLT-інноваторами, за прикладом ЄС? Які тематики мають бути в центрі першого пілоту?
8. Чи готові українські небанківські установи до інтеграції в SEPA як непрямі учасники? Які бар'єри вважаєте найважчими — технічні, регуляторні чи бізнес-моделі?

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-2025-19

Бюлетень є волонтерською 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].