Методологічний бюлетень

Серійний номер: МінФін-AML-2026-07

Лютий 2026

“Знати недостатньо – потрібно діяти”

Йоганн Ґете

Мета

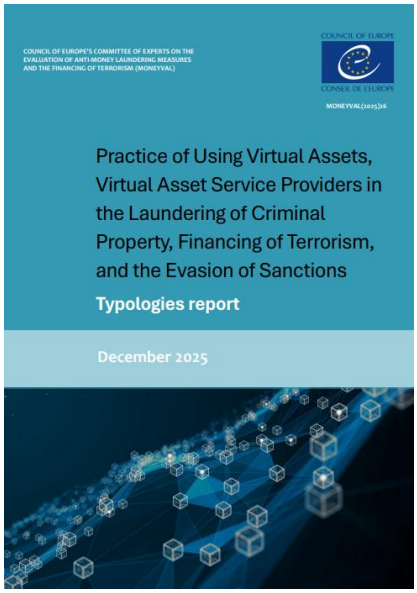
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено 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

Віртуальні активи між новими стандартами ЄС та реальністю "тіньових" потоків [1]



Цей звіт, затверджений на 70-му пленарному засіданні MONEYVAL у грудні 2025 року, є фундаментальним документом, що фіксує еволюцію регуляторного ландшафту та типологій злочинності у сфері віртуальних активів серед 25 юрисдикцій-членів. На відміну від попереднього звіту 2023 року, фокус цього дослідження змістився з базової імплементації стандартів FATF на складні питання ухилення від цільових фінансових санкцій (ЦФС), операційні виклики імплементації "Travel Rule" та інституційну спроможність регуляторів в умовах переходу на стандарти MiCA. Документ викриває критичний розрив між *de jure* наявністю законодавчої бази та *de facto* ефективністю нагляду, особливо в контексті транскордонних потоків та децентралізованих протоколів.

Звіт фіксує тектонічний зсув у регулюванні, спричинений імплементацією регламентів ЄС 2023/1114 (MiCA) та 2023/1113

[1] https://rm.coe.int/moneyval-2025-26-typologies/48802a9b30

(TFR). Для країн-членів ЄС це означає перехід від національних режимів реєстрації до уніфікованого ліцензування з високими пруденційними вимогами. Статистика свідчить, що 81% юрисдикцій MONEYVAL вже вимагають ліцензування або реєстрації VASP, однак перехідні періоди створюють значні адміністративні "пляшкові горлечка". Показовим є кейс Чехії, де національний регулятор (CNB) зіткнувся з необхідністю переоцінки 188 існуючих суб'єктів у стислі терміни. Станом на кінець жовтня 2025 року, з 236 заявок не було видано жодної нової ліцензії CASP, 79 заявок було відхилено, а 13 визнано юридично недійсними. Це демонструє різке підвищення бар'єру входу на ринок: багато гравців, що діяли в режимі "легкої реєстрації", не здатні відповідати стандартам корпоративного управління, захисту активів клієнтів та AML-контролю, передбаченим MiCA. У країнах, що не входять до ЄС (наприклад, Андорра, Гернсі, Острів Мен), спостерігається тенденція до добровільного наближення законодавства до стандартів ЄС, особливо в частині класифікації стейблкоїнів (розподіл на EMT та ART) та вимог до емітентів,.

Незважаючи на те, що понад 90% юрисдикцій призначили органи нагляду (здебільшого це фінансові регулятори або ПФР), методологія оцінки ризиків залишається нерівномірною. Багато національних оцінок ризиків (НОР) базуються на застарілих даних або теоретичних моделях, ігноруючи специфічні загрози фінансування розповсюдження зброї масового знищення та ухилення від санкцій. Критичною проблемою є відсутність верифікованих даних про транскордонні потоки: регулятори часто покладаються на самозвітування VASP, не використовуючи інструменти блокчейн-аналітики для незалежної верифікації. Це створює "сліпі зони", де регулятор не бачить взаємодії піднаглядних суб'єктів з неліцензованими біржами, міксерами або підсанкційними адресами. Звіт підкреслює, що відсутність зареєстрованих VASP у юрисдикції часто помилково трактується як низький ризик, хоча населення може активно використовувати офшорні платформи. Ефективною практикою визнано підхід Гібралтару (GFSC), який інтегрував блокчейн-аналітику в наглядові процеси, що дозволяє виявляти розбіжності між звітністю VASP та реальним рухом коштів on-chain.

Впровадження Travel Rule залишається найбільш проблемною зоною: лише 46% юрисдикцій фактично імплементували цю вимогу. Основні перешкоди – технічна несумісність протоколів обміну даними, "проблема сходу сонця" (sunrise issue), коли контрагенти в інших юрисдикціях ще не зобов'язані передавати дані, та використання некастодіальних гаманців. Звіт зазначає, що в ЄС TFR вирішує проблему гармонізації, але для третіх країн ситуація залишається складною. Відсутність автоматизованого обміну даними про бенефіціарів транзакцій перетворює Travel Rule на формальність, де VASP проводять перевірку ex-post, а не в режимі реального часу, що нівелює превентивну функцію правила.

Документ також детально аналізує використання ВА для обходу санкцій, що стало домінуючою типологією. Естонський ПФР ідентифікував три ключові схеми: прямі P2P транзакції, використання ланцюгів посередників та ескроу-сервіси. Особливу загрозу становлять стейблкоїни (зокрема USDT), які використовуються для розрахунків у міжнародній торгівлі в обхід банківської системи. Кейс України демонструє масштаб проблеми: виявлено переказ понад $140 млн між підсанкційними криптобіржами, пов'язаними з РФ та Іраном, та darknet-платформами. Також висвітлено нові гібридні загрози, такі як використання ВА у схемах нелегальної міграції (кейс Молдови, де оплата за транзит здійснювалася виключно в USDT для конспірації), та використання онлайн-гемблінгу для відмивання коштів (кейс Острова Мен, де виявлено зв'язок гральних акаунтів з гаманцями, залученими до поширення матеріалів з насильством над дітьми).

Звіт критично оцінює якість STR. Спостерігається феномен "захисного звітування" та автоматичної генерації STR на основі спрацювання тригерів блокчейн-аналітики без належного аналізу. Це призводить до перевантаження ПФР низькоякісною інформацією. Водночас, зростає роль державно-приватних партнерств (PPP): лише 40% юрисдикцій мають активні PPP, але там,

де вони діють (наприклад, Мальта, Гібралтар), якість розвідданих значно вища. Щодо конфіскації активів, ключовим викликом залишається технічне зберігання вилучених активів. Юрисдикції переходять від ad-hoc рішень до створення державних кастодіальних гаманців з мультипідписом (multi-sig). Проблемою залишається взаємодія з DeFi-протоколами та міксерами, де відсутній централізований адміністратор, якому можна пред'явити ордер на замороження, що вимагає від правоохоронців розвитку навичок on-chain розслідувань та отримання приватних ключів.

Висновки:

- **Перехід до On-Chain нагляду:** Регулятори повинні відмовитися від пасивного нагляду (аналіз звітності) на користь активного використання інструментів блокчейн-аналітики. Це дозволить верифікувати обсяги транзакцій, виявляти взаємодію з неліцензованими VASP та міксерами, а також валідувати ефективність систем моніторингу суб'єктів. Відсутність власних аналітичних інструментів у регулятора прирівнюється до нездатності здійснювати ефективний нагляд.
- **Операціоналізація Travel Rule:** VASP та банки повинні терміново впровадити технічні протоколи для обміну даними (наприклад, TRP, OpenVASP) для відповідності вимогам TFR/FATF. Фахівці з комплаєнсу мають розробити процедури для обробки транзакцій з некастодіальними гаманцями, включаючи методику підтвердження володіння гаманцем, оскільки проста відмова від таких транзакцій може бути комерційно неприйнятною.
- **Фокус на якості STR та аналізі санкцій:** СПФМ повинні відійти від автоматичного звітування про всі "підозрілі" транзакції, виявлені аналітичним ПЗ. Необхідно додати етап людського аналізу для відсіювання хибних спрацювань. У контексті санкцій, скринінг імен клієнтів є недостатнім; критично важливим є скринінг адрес гаманців на предмет зв'язків (прямих та опосередкованих) з підсанкційними кластерами та сервісами мікшування.
- **Інтеграція секторів з високим ризиком:** Регулятори та комплаєнс-підрозділи повинні звертати особливу увагу на перетин VASP з індустріями онлайн-гемблінгу та нерухомості. Як показують кейси Острова Мен та Андорри, ці сектори використовуються як шлюзи для введення нелегальних криптоактивів у легальний обіг, тому належна перевірка має включати перевірку джерела походження віртуальних активів (Source of Wealth/Funds).

Від фрагментації до централізації: стратегія AMLA у побудові нової системи ПВК/ФТ ЄС [2]

Документ Європейського органу з протидії відмиванню коштів та фінансуванню тероризму (AMLA) є комплексною стратегічною та операційною програмою становлення цього органу як центрального елементу нової європейської системи ПВК/ФТ. Він відображає перехід AMLA від початкової інституційної фази до повноцінної регуляторної, наглядової та аналітичної діяльності в масштабах усього Європейського Союзу та закріплює її роль як ключового координатора між національними регуляторами, фінансовими розвідками, правоохоронними органами та приватним сектором.

У вступній частині документа підкреслюється, що запуск AMLA у 2025 році став відповіддю на системну фрагментацію європейського нагляду у сфері ПВК/ФТ, яка тривалий час дозволяла

[2] https://www.amla.europa.eu/document/download/27549516-d110-4e91-b1ed-d3552b8f9661_en?filename=AMLA%20SPD%202026-2028.pdf

злочинним мережам використовувати різницю у правозастосуванні між державами-членами. Створення єдиного органу розглядається як інституційний фундамент для реалізації AML Package 2024 року та побудови уніфікованого правового простору у сфері запобігання ВК/ФТ. Документ позиціонує AMLA не лише як регулятора, а як центр формування політики, методології та практики фінансового моніторингу в ЄС.

Місія AMLA формулюється як забезпечення цілісності внутрішнього ринку ЄС шляхом впровадження єдиного, ризик-орієнтованого та технологічно розвиненого підходу до протидії фінансовим злочинам. Візія органу спрямована на перехід від реактивної моделі до проактивного виявлення, запобігання та системного стримування незаконних фінансових потоків. AMLA прагне стати центром експертизи та глобальним орієнтиром у сфері ПВК/ФТ, поєднуючи регуляторну жорсткість із підтримкою інновацій та розвитку фінансового сектору.

Стратегічний блок документа вибудовує діяльність AMLA навколо п’яти взаємопов’язаних напрямів: уніфікації та пропорційності регулювання, посилення координації між органами влади та приватним сектором, розвитком цифрових технологій та аналітики, забезпечення високих стандартів доброчесності й підзвітності, а також формування глобального лідерства ЄС у сфері ПВК/ФТ. Ці напрями не розглядаються ізольовано, а інтегруються у всі операційні процеси органу.

Центральне місце в документі займає формування Єдиного зводу правил у сфері ПВК/ФТ, який має усунути різночитання законодавства та практик між державами-членами. AMLA визначає розробку регуляторних технічних стандартів, імплементаційних стандартів і керівних настанов як ключовий інструмент гармонізації. Особлива увага приділяється належній перевірці клієнтів, груповим політикам, бізнес-оцінці ризиків, постійному моніторингу та взаємодії з третіми країнами. Документ наголошує, що регулювання має бути водночас жорстким щодо високоризикових операцій і пропорційним щодо низькоризикових сегментів, щоб не створювати надмірного тиску на легальний бізнес.

Важливим елементом стратегії є цифрова трансформація AMLA. Документ передбачає створення масштабної інформаційно-аналітичної екосистеми, що об’єднує Центральну базу даних у сфері ПВК/ФТ, модернізовані платформи EuReCA та FIU.net, інструменти машинного навчання, системи прогнозування ризиків і візуалізації даних. AMLA прагне інтегрувати штучний інтелект у всі ключові процеси, включно з аналізом транзакцій, виявленням аномалій і підтримкою наглядових рішень. Водночас документ передбачає створення системи управління ризиками AI для запобігання упередженості, помилковим висновкам і порушенням прав людини.

Окремий розділ присвячений побудові власної системи ризик-аналізу AMLA. Орган розробляє інтегровану модель оцінки загроз, яка охоплює фінансові, нефінансові, технологічні та транскордонні ризики. Передбачається регулярна підготовка секторних і тематичних оцінок ризиків, аналітичних висновків і рекомендацій для суб’єктів фінансового моніторингу та регуляторів. Ця система має стати основою для відбору установ для прямого нагляду, планування перевірок і формування пріоритетів ПФР.

Документ детально описує поетапне формування механізму прямого нагляду AMLA за найбільшими та найризикованішими фінансовими установами ЄС. До 2028 року мають бути створені спільні наглядові команди, уніфіковані процедури виїзних і дистанційних перевірок,

системи обміну даними з національними регуляторами та централізований механізм застосування санкцій. Паралельно вибудовується модель непрямого нагляду, яка передбачає регулярні оцінки діяльності національних органів, взаємні перевірки, навчальні програми та можливість втручання у разі системних порушень.

Значна увага приділяється інтеграції нефінансового сектору у загальноєвропейську систему ПВК/ФТ. Документ визнає, що ВНУП історично залишалися слабкою ланкою, і передбачає створення єдиних методик, колегій нагляду, програм підвищення обізнаності та механізмів контролю для адвокатів, нотаріусів, рієлторів, трастових провайдерів та інших професійних груп.

Формування та практичне впровадження діяльності підрозділу фінансових розвідок AMLA розглядається як ключовий елемент аналітичної складової системи. Документ передбачає перехід від простого обміну інформацією до системної спільної аналітичної роботи, стандартизацію форматів STR, розвиток спільних розслідувань, регулярні оцінки спроможності національних ПФР та створення механізмів медіації. AMLA позиціонується як центральний хаб фінансової розвідки ЄС.

Висновки:

- **AMLA формується як головний центр управління системою ПВК/ФТ в ЄС.** До 2028 року AMLA отримає повноваження прямого нагляду за найбільшими та найризикованішими фінансовими установами, централізованого застосування наглядових заходів і санкцій, а також координації діяльності національних регуляторів, що фактично завершує етап фрагментованої моделі ПВК/ФТ у ЄС.
- **Система протидії ВК/ФТ у ЄС переходить до цифрової, дата-орієнтованої та аналітичної моделі нагляду.** AMLA вибудовує єдину інформаційно-аналітичну екосистему з використанням централізованих баз даних, автоматизованого аналізу транзакцій і алгоритмічної оцінки ризиків, що істотно підвищує вимоги до технологічної зрілості суб'єктів фінансового моніторингу.
- **ПФР інтегруються у спільний європейський аналітичний простір.** Роль ПФР трансформується від обміну інформацією до системної спільної аналітичної роботи на основі уніфікованих форматів повідомлень, спільних аналітичних продуктів і регулярних взаємних оцінок, що підвищує якість транскордонних фінансових розслідувань.
- **Нефінансовий сектор остаточно включається до жорстко регламентованої системи нагляду у сфері ПВК.** ВНУП охоплюються уніфікованими методологіями оцінки ризиків, наглядовими механізмами та санкційними інструментами на рівні ЄС, що усуває структурні прогалини у системі ПВК/ФТ.

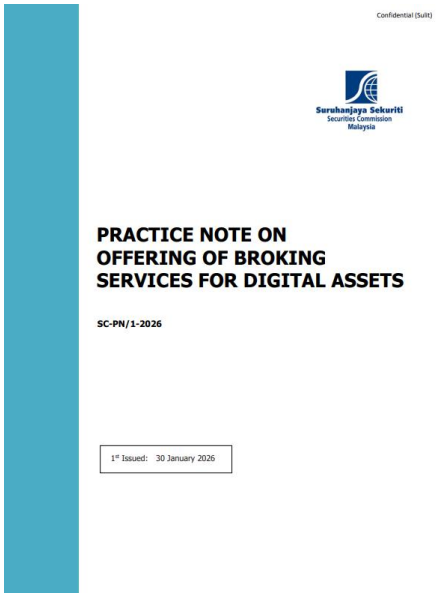
Фінансово-ресурсний блок демонструє масштабне інституційне зростання органу, із поступовим збільшенням штату до понад 400 осіб і переходом до моделі фінансування через наглядові збори. Велика увага приділяється кадровій політиці, навчанню, доброчесності, гендерному балансу та формуванню стійкої організаційної культури.

Окремо документ регламентує внутрішні механізми контролю, захисту персональних даних, боротьби з корупцією, захисту викривачів та забезпечення дотримання фундаментальних прав. Передбачається призначення спеціального уповноваженого з дотримання прав людини та посилення ролі внутрішнього аудиту. Це формує модель регулятора, орієнтованого не лише на ефективність, а й на легітимність та суспільну довіру.

У цілому документ відображає прагнення Європейського Союзу побудувати високотехнологічну, централізовану та аналітично орієнтовану систему протидії відмиванню коштів і фінансуванню

тероризму, в якій AMLA виступає як стратегічний, наглядовий і координаційний центр. Документ демонструє, що боротьба з фінансовими злочинами розглядається як елемент економічної безпеки, стабільності внутрішнього ринку та міжнародного впливу ЄС, а діяльність AMLA — як довгострокова інвестиція у стійкість європейської фінансової системи.

Як держава «вбудовує» криптоактиви у фінансову систему: досвід Малайзії та уроки для регуляторів [3]



Документ, виданий Комісією з цінних паперів Малайзії, являє собою комплексний нормативно-методологічний інструмент, спрямований на інституційну інтеграцію ринку цифрових активів у традиційну систему регулювання ринків капіталу та фінансових послуг, з урахуванням сучасних ризиків фінансової злочинності, технологічної вразливості та транскордонного характеру віртуальних фінансових операцій.

Документ побудований на принципі, що цифрові валюти та цифрові токени, які відповідають установленим критеріям, визнаються різновидом цінних паперів, а отже підлягають повному регуляторному режиму, передбаченому законодавством про ринки капіталу. Це означає відмову від підходу до криптоактивів як до «паралельного» або «альтернативного» фінансового сектору та їх включення до єдиного правового поля з банківськими, інвестиційними та брокерськими послугами.

Концептуально документ відображає прагнення регулятора створити контрольовану, прозору та стабільну екосистему цифрових активів, у якій ключову роль відіграє не лише технологія, а передусім інституційна спроможність учасників ринку дотримуватися стандартів доброчесності, фінансової дисципліни та відповідності міжнародним вимогам у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. У цьому сенсі документ фактично транслює підхід, близький до стандартів FATF щодо постачальників послуг з віртуальними активами, адаптуючи його до контексту ринків капіталу.

Важливою структурною особливістю документа є закріплення превентивної моделі регулювання. Ліцензіат не може розпочати надання брокерських послуг щодо цифрових активів у режимі «постфактум-контролю», а зобов'язаний пройти попередню процедуру інформування регулятора та підтвердження готовності своєї організаційної, технологічної та комплаєнс-інфраструктури. Обов'язковість зовнішньої валідації внутрішніх політик незалежним аудитором формує додатковий рівень інституційної відповідальності та створює механізм багаторівневого контролю, у межах якого зменшується ризик формального або імітаційного впровадження вимог.

Таким чином, документ закладає модель, за якої доступ до ринку цифрових активів отримують лише ті суб'єкти, які досягли достатнього рівня організаційної зрілості, мають розбудовані системи управління ризиками, внутрішнього контролю та фінансового моніторингу, а також спроможні продемонструвати реальну, а не декларативну відповідність стандартам регулятора. Це суттєво підвищує бар'єр входу на ринок і сприяє його професіоналізації.

[3] https://www.sc.com.my/api/documentms/download.ashx?id=3229facc-55f0-4021-a32c-d076ea575ff5

Окремий фундаментальний блок документа присвячений формуванню контрольованого ланцюга походження цифрових активів. Регулятор чітко обмежує перелік допустимих джерел, з яких брокери можуть отримувати доступ до цифрових активів, дозволяючи співпрацю лише з локально зареєстрованими біржами або з іноземними платформами, що підлягають реальному нагляду у своїх юрисдикціях. При цьому наголошується, що формальна наявність реєстрації або ліцензії не є достатньою підставою для співпраці. Ліцензіат зобов'язаний оцінювати ефективність систем ПВК/ФТ/ФР, рівень регуляторного контролю, практику нагляду та санкційне середовище відповідної юрисдикції.

Фактично документ перекладає на брокера функцію первинного регуляторного фільтра, який має запобігати проникненню в національну фінансову систему ризикових або непрозорих іноземних платформ. Це відповідає сучасному міжнародному підходу до транскордонного нагляду, коли приватні фінансові установи виконують роль «першої лінії оборони» у сфері фінансової безпеки.

Регулювання операційної діяльності брокерів у сфері цифрових активів у документі побудоване на принципі максимального зниження системних і поведінкових ризиків. Заборона маржинального фінансування, кредитування та дискреційного управління спрямована на нейтралізацію механізмів надмірного ризикування, спекулятивних бульбашок і масових втрат інвесторів, характерних для нерегульованих крипторинків. Обов'язковість торгівлі на умовах повної передоплати мінімізує кредитний ризик і ризик неплатоспроможності клієнтів.

Обмеження щодо переліку дозволених до торгівлі цифрових активів формують централізований механізм контролю за фінансовими інструментами, які допускаються до обігу. Це дозволяє регулятору оцінювати не лише юридичний статус активів, а й їхню економічну доцільність, технологічну надійність, ризик маніпулювання та потенціал для зловживань.

Питання захисту клієнтських активів у документі розглядається як один із ключових елементів регуляторної архітектури. Вимога повної сегрегації активів створює правові та операційні бар'єри для їх неправомірного використання, особливо у випадках фінансових труднощів, банкрутства або шахрайських дій з боку брокера. Використання виключно регульованих кастодіанів додатково знижує ризики втрати активів унаслідок кібератак, внутрішніх зловживань або технічних збоїв.

Регулювання питання доходів від цифрових активів демонструє прагнення

Висновки:

- **Вхід на ринок брокерських послуг щодо цифрових активів можливий лише за умови попереднього регуляторного контролю та зовнішньої валідації комплаєнсу,** що робить неможливим запуск таких послуг без зрілої внутрішньої системи управління ризиками та ПВК/ФТ/ФР.
- **Відповідальність за перевірку іноземних платформ цифрових активів покладається безпосередньо на ліцензіата,** включно з оцінкою реального регуляторного нагляду та ефективності систем ПВК/ФТ/ФР, а не лише формальної наявності ліцензії.
- **Регулятор свідомо виключає найбільш спекулятивні та ризикові моделі торгівлі цифровими активами,** забороняючи маржинальне фінансування, кредитування та дискреційне управління, що суттєво знижує системні та поведінкові ризики.
- **Захист клієнтських активів і прозорість поводження з доходами від цифрових активів є центральним елементом регуляторної логіки,** що вимагає повної сегрегації активів, використання регульованих кастодіанів і чітко задокументованої згоди клієнта на будь-які відступи від базового принципу належності доходів клієнту.

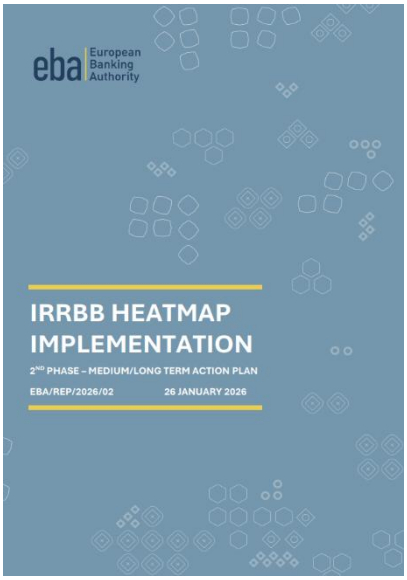
забезпечити економічну справедливість та прозорість відносин між брокером і клієнтом. Принцип, за яким усі вигоди належать клієнту, якщо інше прямо не погоджено письмово, мінімізує можливості прихованого перерозподілу доходів і зловживань з боку посередника.

Блок вимог щодо розкриття інформації та прозорості діяльності спрямований на формування культури усвідомленого інвестування. Регулятор вимагає не лише формального інформування, а надання інформації у формі, доступній для розуміння пересічним клієнтом. Особливий акцент робиться на специфічних технологічних подіях, таких як хардфорки, ейрдропи, збої блокчейн-мереж, які можуть істотно впливати на вартість і правовий статус активів. Це дозволяє зменшити інформаційну асиметрію між професійними учасниками ринку та інвесторами.

Вимоги до управління ризиками та кадрового потенціалу свідчать про те, що регулятор розглядає цифрові активи як високоспеціалізовану сферу, яка не допускає поверхневого підходу. Очікується наявність експертних знань у сфері блокчейн-технологій, кібербезпеки, правового регулювання, фінансового моніторингу та транскордонного комплаєнсу. Таким чином, документ стимулює формування професійного середовища, орієнтованого на довгострокову стабільність, а не на короткострокові спекулятивні вигоди.

У підсумку документ формує цілісну, багаторівневу систему регулювання, у якій цифрові активи розглядаються не як виняток із фінансової системи, а як її складова частина, що потребує посиленого нагляду, підвищених стандартів доброчесності та інституційної відповідальності. Документ поєднує елементи ринкового регулювання, фінансового моніторингу, захисту прав інвесторів і технологічного ризик-менеджменту в єдину модель, спрямовану на забезпечення фінансової стабільності, репутаційної надійності юрисдикції та відповідності міжнародним стандартам у сфері ПВК/ФТ/ФР. У цьому контексті він може розглядатися як приклад системного, стратегічно орієнтованого підходу до державного управління ринком цифрових фінансових інструментів.

Процентний ризик після епохи низьких ставок: нова наглядова парадигма Європейського банківського органу [4]



Документ, підготовлений Європейським банківським органом, є комплексним аналітичним і методологічним матеріалом, спрямованим на системне поглиблення регуляторного та наглядового підходу до управління процентним ризиком у банківській книзі та ризиком кредитного спреду в умовах трансформації європейського фінансового середовища після періоду тривалих ультранизьких ставок. Він продовжує послідовну лінію документів EBA, започатковану після ухвалення у 2022 році оновлених керівних настанов щодо процентного ризику у банківській книзі (IRRBB) і ризику кредитного спреду в банківській книзі (CSRBB), та відображає перехід від фази первинного впровадження нових стандартів до етапу їх глибокої інституціоналізації в системах управління ризиками банків.

У звіті чітко простежується логіка наглядового навчання на основі даних. EBA не обмежується нормативними деклараціями, а вибудовує свої висновки на багаторічному масиві емпіричної інформації, отриманої через ITS-звітність, кількісні

[4] https://www.eba.europa.eu/sites/default/files/2026-01/9addc5b3-7578-4002-9a8d-1f7473220a2e/Report%20on%20IRRBB%20heatmap%20implementation.pdf

дослідження впливу, аналіз внутрішніх моделей та результатів інспекцій. Такий підхід демонструє еволюцію європейського нагляду від формального контролю відповідності до ризик-орієнтованого аналізу поведінки установ у реальному економічному середовищі. Документ фактично виступає як «метазвіт» про те, як банки реагують на регуляторні стимули, які моделі вони обирають і які стратегічні компроміси формуються між прибутковістю, стабільністю та регуляторними очікуваннями.

Загальний аналіз результатів подається не лише як статистичний огляд, а як індикатор зрілості систем управління активами і пасивами. Зниження частки банків з аномальними значеннями показників економічної вартості капіталу інтерпретується як наслідок активнішого використання деривативів, перегляду структури балансу, скорочення середньозваженого строку чутливості активів і пасивів до процентних ставок та підвищення якості внутрішнього моделювання. Водночас EBA підкреслює, що така стабілізація має частково «механічний» характер, пов'язаний із загальним підвищенням ставок, яке саме по собі зменшує чутливість вартості до шоків. Це означає, що зниження ризику не завжди є результатом стратегічної трансформації, а може маскувати структурні слабкості, які проявляться у фазі нового зниження ставок.

Особлива увага приділяється дисбалансу між управлінням ризиком економічної вартості та ризиком доходності. Документ показує, що більшість банків історично будували свої системи IRRBB навколо захисту капіталу і регуляторних коефіцієнтів, тоді як волатильність чистого процентного доходу часто розглядалася як другорядна проблема. У новому середовищі це створює загрозу стратегічної нестабільності, оскільки навіть за формальної капітальної стійкості банки можуть втрачати здатність генерувати стабільний фінансовий результат. Таким чином, звіт опосередковано стимулює переосмислення ролі ПВК як інструменту не лише регуляторної відповідності, а й бізнес-стійкості.

Аналіз п'ятирічного обмеження для безстрокових депозитів у документі виходить за межі технічної дискусії про строки репрайсингу. EBA розглядає цей ліміт як інституційний механізм боротьби з когнітивними викривленнями у моделюванні, коли банки схильні переоцінювати лояльність клієнтів і стабільність ресурсної бази. У звіті простежується ідея, що регуляторне обмеження виконує роль «якоря», який стримує надмірно оптимістичні очікування менеджменту. Водночас визнається, що універсальне правило не може однаково ефективно працювати для всіх бізнес-моделей, особливо для кооперативних банків, регіональних установ або банків зі спеціалізованими клієнтськими сегментами. Тому EBA просуває модель контрольованої гнучкості, де винятки можливі, але лише в рамках формалізованого наглядового діалогу та на основі доказів.

Підхід до моделювання комерційної маржі у звіті відображає прагнення регулятора зберегти баланс між економічною реалістичністю та регуляторною порівнянністю. Документ визнає, що поведінка клієнтів щодо безстрокових депозитів є складною, асиметричною та залежною від макроекономічного контексту, тому жорстке застосування фіксованого спреду може спотворювати ризикову картину. Водночас поширення таких гнучких підходів на інші продукти розглядається як потенційний шлях до «м'якого регуляторного арбітражу», коли банки через моделювання штучно згладжують негативні сценарії. Таким чином, рекомендації EBA спрямовані на стримування цього ризику шляхом чіткого розмежування між поведінковими і неповедінковими інструментами.

Розділ, присвячений CSRBB, має системне значення для всієї архітектури ризик-менеджменту. EBA фактично констатує, що ризик кредитного спреду досі не інтегрований у внутрішні системи багатьох банків на рівні, порівнянному з кредитним чи процентним ризиком. Обмеження периметру CSRBB інструментами за справедливою вартістю відображає не лише технічні складнощі, а й культурну інерцію, за якої ризики, не відображені безпосередньо в бухгалтерській звітності, недооцінюються. Документ наполягає на необхідності переходу до

економічної логіки оцінки ризиків, де ключовим критерієм є чутливість до ринкових факторів, а не облікова форма.

Окремо підкреслюється значення інтеграції CSRBB у процес ICAAP, що фактично означає визнання цього ризику як потенційно системного для капітальної адекватності. Таким чином, ЕВА формує передумови для того, щоб у майбутньому кредитні спреди розглядалися не як другорядний ринковий фактор, а як повноцінний елемент внутрішнього капітального планування.

Аналіз хеджування у звіті демонструє амбівалентність сучасних практик. З одного боку, широке використання процентних свопів свідчить про високий рівень технічної зрілості ринку. З іншого боку, залежність від бухгалтерського хеджування та обмежене використання економічних портфельних моделей вказують на те, що багато банків продовжують будувати свої стратегії навколо облікових правил, а не економічної сутності ризику. ЕВА розглядає це як структурне обмеження, яке може знижувати адаптивність банків у кризових умовах.

Важливим концептуальним елементом документа є прагнення до узгодження трьох вимірів управління ризиками: регуляторного, бухгалтерського та економічного. Участь ЕВА у проєкті IASB з динамічного управління ризиками розглядається як інструмент подолання фрагментації між цими сферами. Фактично звіт закладає основу для майбутньої інтегрованої моделі, у якій внутрішні системи банків одночасно задовольнятимуть вимоги нагляду, фінансової звітності та стратегічного управління.

У стратегічному вимірі документ відображає трансформацію ролі наглядових органів. ЕВА дедалі більше позиціонує себе не лише як нормотворця, а як аналітичний центр, який формує знання про поведінку банківської системи, поширює «кращі практики» та стимулює організаційне навчання в секторі. Застосовуючи підхід, заснований на систематизованій карті ризиків, регулятор вибудовує механізм безперервного зворотного зв'язку між аналітичними даними, нормотворчою діяльністю та практикою нагляду.

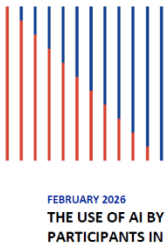
У підсумку звіт постає як комплексний стратегічний документ, що відображає перехід європейського банківського нагляду від епохи стандартизованих формальних вимог до моделі, заснованої на глибокому аналізі поведінки, якості управління та здатності банків інтегрувати ризик-менеджмент у свою бізнес-стратегію. Він закладає основу для

Висновки:

- **П'ятирічне обмеження для безстрокових депозитів має залишатися базовим стандартом.** Банкам необхідно інтегрувати цей ліміт у внутрішні моделі, політики у сфері ПВК та хеджування, а будь-які відхилення погоджувати з регулятором на основі документованих поведінкових досліджень.
- **Моделювання маржі повинно бути стандартизованим для більшості продуктів.** Установам слід забезпечити застосування постійного спреду для всіх неповедінкових інструментів та переглянути внутрішні наглядові тести на виявлення істотних відхилень з метою усунення необґрунтованої гнучкості.
- **Сфера охоплення CSRBB потребує суттєвого розширення та методологічного узгодження на рівні всієї банківської системи.** Банки мають провести повну інвентаризацію активів і зобов'язань та включити до оцінки всі позиції, чутливі до кредитних спредів, незалежно від бухгалтерського обліку.
- **Хеджування повинно еволюціонувати від захисту капіталу до комплексного управління доходністю.** Підрозділам з управління ризиками доцільно розширити стратегії з урахуванням впливу на чистий процентний дохід, посилити економічне страхування ризику та формалізувати його взаємозв'язок із загальною стратегією розвитку банку.

формування більш стійкої, прозорої та аналітично зрілої фінансової системи, у якій управління процентним ризиком і ризиком кредитного спреду розглядається не як ізольована технічна функція, а як центральний елемент корпоративного управління та фінансової стабільності.

Впровадження штучного інтелекту на фінансових ринках: досвід Франції та регуляторні уроки для Європи [5]



У звіті здійснено комплексне емпіричне та аналітичне дослідження реального стану використання штучного інтелекту (AI) фінансовими учасниками у Франції, яке ґрунтується на опитуванні ста респондентів із числа піднаглядних фінансових установ, публічних компаній, юридичних та аудиторських фірм, а також на даних інвесторського барометра. Метою дослідження є не лише фіксація рівня технологічного впровадження, а й оцінка інституційної зрілості сектору, ступеня інтеграції AI у бізнес-процеси, якості внутрішнього управління ризиками та готовності системи фінансового нагляду до нових технологічних викликів.

У вступній частині звіту підкреслюється, що сучасний етап розвитку штучного інтелекту, особливо генеративних моделей, суттєво змінив характер взаємодії людини з інформаційними системами, зробивши аналітичні та обробні інструменти доступними для широкого кола користувачів. Це спричинило глибоку трансформацію професійних практик у фінансовому секторі, де AI дедалі активніше використовується для оптимізації процесів, підвищення якості управління ризиками, автоматизації документообігу та персоналізації клієнтських сервісів. Водночас регулятор наголошує, що таке прискорене впровадження супроводжується ризиками, пов’язаними з якістю даних, прозорістю моделей, залежністю від зовнішніх постачальників та потенційним ослабленням людського контролю.

Методологічна основа дослідження побудована на трьох окремих анкетуваннях, спрямованих на різні категорії учасників ринку, що дозволило сформувати міжсекторну картину використання AI. Аналіз охоплює як кількісні показники рівня впровадження та інвестицій, так і якісні аспекти внутрішнього управління, політик безпеки, навчання персоналу та процедур валідації. Такий підхід дає змогу розглядати використання штучного інтелекту не як окрему IT-функцію, а як елемент загальної системи корпоративного управління та контролю.

Центральним висновком першого розділу є фіксація дуже високого рівня поширення AI серед фінансових установ. Переважна більшість респондентів уже використовує відповідні технології або планує їх запровадження у найближчій перспективі, при цьому значна частина рішень перебуває на стадії повноцінної експлуатації. Водночас простежується чітка залежність між масштабом організації та рівнем цифрової зрілості: великі фінансові групи демонструють значно вищу спроможність до системної інтеграції AI, тоді як малі та мікропідприємства залишаються на початкових етапах або обмежуються окремими інструментами. Інвестиційні прогнози підтверджують сталість цього тренду, оскільки більшість великих гравців планує подальше нарощування витрат на відповідні технології.

[5] https://www.amf-france.org/sites/institutionnel/files/private/2026-02/202602-rapport-amf-ia-et-acteurs-des-marches-financiers-en.pdf

Аналіз практичних кейсів показує, що використання штучного інтелекту має переважно внутрішньоорганізаційний характер. Основний масив застосувань спрямований на автоматизацію підготовки текстів, перекладів і резюме, створення внутрішніх асистентів, очищення та обробку даних, підтримку IT-розробки та базову клієнтську комунікацію. Інструменти, безпосередньо пов'язані з наданням інвестиційних послуг або прийняттям фінансових рішень, залишаються у меншості, що свідчить про обережне ставлення установ до делегування критично важливих функцій алгоритмам. У сфері ПВК/ФТ та комплаєнсу AI застосовується передусім для підтримки транзакційного моніторингу, виявлення аномалій і первинної аналітики, але не як автономний інструмент ухвалення рішень.

З технологічного погляду домінуюче місце посідають генеративні моделі та інструменти обробки природної мови, що пояснюється їх універсальністю та відносною простотою інтеграції. Переважна більшість установ використовує готові комерційні рішення, а власна розробка залишається обмеженою. Це супроводжується високою концентрацією залежності від кількох глобальних постачальників, переважно неєвропейського походження, що формує довгострокові ризики технологічної та даної залежності. Інфраструктурно найбільш поширеною є гібридна модель, яка поєднує власні ресурси з хмарними сервісами.

У розділі, присвяченому перевагам і ризикам, звіт демонструє прагматичне бачення фінансового сектору. Основні вигоди пов'язуються з підвищенням продуктивності, скороченням витрат, оптимізацією процесів та покращенням якості аналітики. Разом із тим респонденти чітко усвідомлюють ризики, серед яких домінують питання захисту даних, кібербезпеки, надмірної автоматизації, нестачі кваліфікованих кадрів та можливого дрейфу моделей. Особливу увагу приділено проблемі надмірної залежності від технологій без належного людського контролю, що може призводити до помилкових або некоректних рішень у чутливих сферах.

У відповідь на ці виклики більшість організацій запровадила базові механізми управління, головним із яких є принцип обов'язкової участі людини у перевірці результатів роботи систем. Широко застосовуються процедури контролю якості даних, трасування джерел інформації та валідації результатів. Значна частина установ має формалізовані політики використання AI, які охоплюють питання етики, прозорості, захисту інформації та відповідальності. Водночас рівень обізнаності персоналу щодо принципів роботи моделей залишається низьким, а навчальні програми часто мають фрагментарний характер, що стримує подальший розвиток.

Окремі розділи звіту присвячені галузевим особливостям використання

Висновки:

- **Фінансовим установам необхідно переходити від «пілотних проєктів» до системного управління AI,** інтегруючи його у загальну модель ризик-менеджменту, ПВК/ФТ-контролю та внутрішнього аудиту, з обов'язковим документуванням життєвого циклу моделей.
- **Залежність від обмеженого кола неєвропейських постачальників є стратегічним ризиком,** тому доцільно розвивати багатохмарні стратегії, локальні рішення та плани виходу у разі припинення співпраці з постачальниками послуг.
- **Принцип «участі людини в процесі прийняття рішень» має бути формалізований у внутрішніх нормативних документах** із чітким визначенням відповідальності за помилки AI у сферах комплаєнсу, ПВК/ФТ, інвестиційного консультування та фінансової звітності.
- **Без системних програм підготовки кадрів масштабування AI неможливе,** тому установам слід інвестувати в багаторівневе навчання (керівний склад — управлінський рівень — операційний персонал), орієнтоване на управління ризиками, а не лише на технічні навички.

AI. Керуючі компанії зосереджуються на аналітиці та комплаєнсі, інвестиційні фірми — на автоматизації та підтримці клієнтів, ринкові інфраструктури — на моніторингу зловживань і кіберризиків, фінтех-компанії — на інформаційних сервісах, публічні компанії — на фінансовій комунікації, юридичні фірми — на аналізі контрактів і належній перевірці, а аудиторські компанії — на перевірці транзакцій та ризик-аналізі. У юридичному та консалтинговому секторі фіксуються найбільш відчутні прямі вигоди у вигляді економії часу та підвищення якості документів, однак і тут ключову роль відіграє постійний людський контроль.

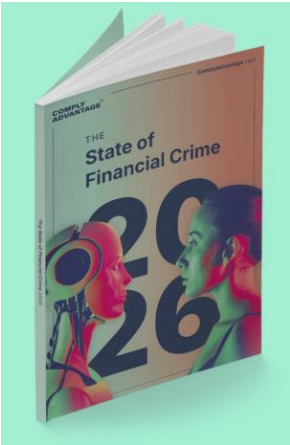
Значну увагу в документі приділено власному досвіду Управління фінансових ринків Франції (AMF) у впровадженні штучного інтелекту в наглядову діяльність. Регулятор використовує технології штучного інтелекту для виявлення шахрайства, аналізу звітності, контролю розкриття інформації щодо екологічних, соціальних та управлінських чинників, обробки звернень та моніторингу ринкових зловживань. Розвиток наглядових технологічних рішень розглядається як необхідна умова ефективного фінансового нагляду в умовах зростаючої складності фінансових ринків. При цьому AMF інвестує у підвищення кваліфікації персоналу, експериментальні проєкти та забезпечення суверенності даних.

У завершальній частині звіту використання AI розглядається в ширшому європейському та міжнародному контексті через призму позицій ESMA та IOSCO. Підкреслюється, що застосування алгоритмів не знімає відповідальності з керівних органів фінансових установ, не замінює вимоги до належного управління та не послаблює обов’язок діяти в інтересах клієнтів. Особлива увага приділяється ризикам для роздрібних інвесторів, які дедалі частіше користуються автоматизованими системами інвестиційного консультування та чат-ботами без належного розуміння їхніх обмежень.

У підсумку звіт формує цілісну картину поступового переходу фінансового сектору від експериментального використання штучного інтелекту до стадії системної інтеграції, яка супроводжується зростанням регуляторних, організаційних та етичних вимог. AI постає не як автономний замінник професійного судження, а як інструмент підтримки, ефективність і безпечність якого визначається якістю корпоративного управління, рівнем підготовки персоналу та здатністю організацій інтегрувати технології у свої системи управління ризиками, комплаєнсу та відповідальності.

Звіти окремих інституцій та експертів

Стратегічний горизонт 2026: Конвергенція Агентного ШІ, інституціоналізація MLaaS та геополітика санкційного ухилення [6]



Цей документ являє собою фундаментальне стратегічне дослідження, що моделює ландшафт фінансових злочинів та регуляторного середовища на горизонті 2026 року. Звіт базується на опитуванні 600 керівників вищої ланки та фахівців з комплаєнсу у ключових юрисдикціях (США, Канада, Великобританія, Франція, Сінгапур, Австралія) та аналізує конвергенцію технологічних загроз, геополітичної фрагментації та еволюції злочинних методологій. Центральною тезою документа є перехід від ізольованих ризиків до системних, гібридних загроз, де межі між кіберзлочинністю, шахрайством, відмиванням коштів та фінансуванням тероризму остаточно стираються, вимагаючи від регуляторів та суб'єктів первинного фінансового моніторингу (СПФМ) докорінної зміни архітектури контролю.

[6] https://get.complyadvantage.com/insights/the-state-of-financial-crime-2026

Документ фіксує критичний зсув у використанні штучного інтелекту. Якщо поточний фокус зосереджено на генеративному AI (GenAI) для створення діпфейків та синтетичних ідентичностей, то головним викликом 2026 року стає «Агентний AI» (Agentic AI). Це автономні системи, здатні не лише генерувати контент, а й планувати, міркувати та виконувати багатоетапні завдання без втручання людини. Для сфери ПВК це означає появу автоматизованих злочинних систем, здатних самостійно проходити процедури KYC, реагувати на запити комплаєнсу та керувати мережами «мулів» (money mules) у промислових масштабах. Звіт вказує на розрив між очікуваннями та реальністю: 99% організацій мають бюджети на AI, проте реальне впровадження агентних рішень для скринінгу та моніторингу становить лише близько 33%. Зростання шахрайства, зокрема схем pig butchering, що генерують мільярдні збитки та базуються в Південно-Східній Азії, демонструє інтеграцію соціальної інженерії, криптоактивів та торгівлі людьми. Звіт підкреслює, що 61% респондентів стурбовані можливостями моніторингу в реальному часі в умовах миттєвих платежів, що вимагає переходу від статичних правил до поведінкової аналітики.

Особливу увагу приділено концепції «Відмивання грошей як послуга» (Money Laundering-as-a-Service, MLaaS). Звіт деконструює структуру цього ринку, виділяючи п'ять кластерів провайдерів: від незалежних агентів до спеціалізованих підрозділів організованих злочинних груп та професійних посередників. Найбільш загрозливим трендом визначено діяльність Китайських мереж відмивання грошей (CMLN), які обслуговують мексиканські картелі та інші злочинні угруповання. Методологія CMLN базується на дзеркальних транзакціях («літаючі гроші» або fei ch'ien), що дозволяє здійснювати розрахунки майже миттєво без транскордонного переміщення коштів через банківську систему SWIFT, використовуючи взаємозалік торговельних операцій та продаж валюти китайським громадянам в обхід капітальних обмежень КНР. Це створює замкнений цикл, невидимий для традиційних TMS (Transaction Monitoring Systems). Окремо аналізується кейс операції "Destabilize", що викрила мережу, яка використовувала стейблкоїни (USDT) для обслуговування російських еліт та

Висновки:

- **Перехід до динамічного моніторингу на основі AI:** Традиційні системи, що базуються на статичних правилах, визнаються неефективними проти CMLN та Агентного AI. Фінансовим установам необхідно терміново впроваджувати поведінкову аналітику та AI-моделі для виявлення складних, нелінійних паттернів у реальному часі, інтегруючи дані про пристрої, IP-адреси та поведінку користувачів у єдиний профіль ризику.
- **Інтеграція геополітичного аналізу в комплаєнс:** В умовах SEaaS та дивергенції санкційних режимів (США vs ЄС), банки повинні посилити перевірку ланцюгів постачання та кінцевих користувачів, особливо щодо товарів подвійного призначення. Необхідно враховувати ризики «непрямого» зв'язку через хаби у третіх країнах (ОАЕ, Туреччина, Центральна Азія) та переходити від формального скринінгу до глибокого розслідування торговельних потоків.
- **Регулювання криптоактивів як стандарт:** Врахування ризиків стейблкоїнів та DeFi більше не є опцією, а стає обов'язковим стандартом. Це вимагає впровадження інструментів он-чейн аналітики, забезпечення дотримання Travel Rule та перегляду ризик-апетиту щодо клієнтів, які взаємодіють з VASP, особливо в юрисдикціях з високим ризиком.
- **Стратегічне управління даними:** Успішна протидія MLaaS вимагає руйнування фрагментацій між підрозділами кібербезпеки, шахрайства та AML. Створення єдиного шару даних та участь у зовнішніх державно-приватних партнерствах (PPP) для обміну інформацією є критичними умовами для виявлення мережевих загроз, які невидимі для однієї інституції.

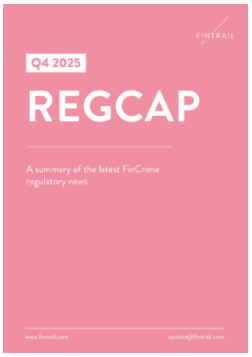
кіберзлочинців, поєднуючи готівкові кур'єрські мережі в Лондоні з крипто-траншами в Москві та Дубаї.

Аналіз геополітичного ландшафту вказує на формування стійкої осі ухилення «Росія-Іран-КНДР-Китай». Вводиться поняття «Ухилення від санкцій як послуга» (Sanctions Evasion-as-a-Service, SEaaS), де треті країни та спеціалізовані фірми надають логістичні та фінансові шлюзи. Звіт деталізує використання «тіньового флоту» танкерів (понад 550 суден під санкціями ЄС/Великобританії), маніпуляції з кодами HS для товарів подвійного призначення та використання стейблкоїнів для транскордонних розрахунків в обхід доларової системи. Важливим є прогноз щодо дивергенції (розбіжності) регуляторних підходів у 2026 році. Очікується, що США гіпотетично за адміністрації Трампа можуть перейти до дерегуляції та використання тарифів як інструменту тиску, тоді як ЄС посилюватиме централізацію через новостворений орган AMLA (Anti-Money Laundering Authority), який розпочне прямий нагляд у 2028 році. Це створює ризик регуляторного арбітражу та ускладнює комплаєнс для транснаціональних банків.

Звіт констатує інтеграцію криптоактивів у мейнстрім фінансових злочинів. Стейблкоїни (ринкова капіталізація понад $300 млрд) стають основним інструментом розрахунків для злочинних мереж через їх ліквідність та стабільність ціни. Виділено специфічні загрози: використання «ланцюгових стрибків» (chain hopping) та нерегульованих мостів (bridges) для розриву сліду транзакцій, а також зростання ролі DeFi. Регуляторна відповідь включає імплементацію MiCA в ЄС, законодавчі ініціативи в США (GENIUS Act) та жорсткі вимоги до VASP у Гонконгу та ОАЕ. Розширення периметра AML також стосується нефінансових посередників: в Австралії та Канаді посилюються вимоги до рієлторів, юристів та торговців дорогоцінними металами, тоді як у США спостерігається тенденція до звуження вимог щодо бенефіціарної власності (Corporate Transparency Act) через судові оскарження та політику дерегуляції,.

Документ аналізує трансформацію фінансування тероризму, зокрема використання краудфандингу в крипті групами ХАМАС та ІДІЛ. Акцент робиться на політизації відмивання коштів: професійні ландромати обслуговують не лише кримінал, а й державні розвідки (зокрема РФ) для фінансування диверсійних операцій у Європі («гібридна війна»), що вимагає від комплаєнс-офіцерів перегляду матриць ризиків: клієнт з високим ризиком відмивання стає загрозою нацбезпеці. Також висвітлюється проблема торгівлі людьми як фінансового злочину, що генерує $150 млрд щорічно, з акцентом на необхідності інтеграції показників торгівлі людьми у системи моніторингу.

Регуляторний зріз Q4 2025: Реформа Companies House, імплементація DORA та автономія ЄС у санкціях проти РФ [7]



Цей документ є комплексним регуляторним зрізом за четвертий квартал 2025 року, який фіксує кульмінацію кількох довгострокових трендів у глобальній архітектурі боротьби з фінансовими злочинами: перехід від нормотворчості до агресивного правозастосування, інституціоналізація нагляду за новими технологіями (зокрема AI та криптоактивами) та остаточна геополітична фрагментація санкційних режимів. Звіт, що охоплює юрисдикції Сполученого Королівства, ЄС, США, Канади, Сінгапуру та ОАЕ, демонструє, що регулятори більше не толерують «паперовий комплаєнс»: штрафи стають рекордними не лише за фактом відмивання, а й за системні

[7] https://fintrail.com/regcap-content/q4-2025

вразливості контролів, навіть якщо вони не призвели до безпосереднього використання системи злочинцями.

У Сполученому Королівстві 4-й квартал 2025 року ознаменувався фундаментальною централізацією наглядових функцій. Рішення призначити Financial Conduct Authority (FCA) єдиним органом нагляду за сектором професійних послуг (юристи, бухгалтери, TCSP) свідчить про провал моделі саморегулювання через професійні асоціації (PBS), які роками демонстрували конфлікт інтересів та недостатню жорсткість. Це супроводжується імплементацією нових вимог щодо осіб зі значним контролем (PSC), де запроваджено обов'язкову верифікацію особи через Companies House. Скасування вимоги вести локальні реєстри PSC на користь централізованої бази даних змінює логіку перевірок: тепер первинним джерелом істини стає державний реєстр, якість даних у якому історично була низькою, що створює нові операційні ризики для банків при розбіжностях даних. Оновлення вказівок NCA щодо звітів про підозрілу діяльність (SAR) та захист від відмивання коштів (DAML) вказує на намагання регулятора зменшити захисне звітування, яке перевантажує фінансову розвідку, вимагаючи від суб'єктів моніторингу глибшого попереднього аналізу перед подачею звіту.

Аналіз штрафів за Q4 2025 виявляє зміну парадигми дій з правозастосування. Кейс Nationwide Building Society (£44 млн штрафу) є хрестоматійним прикладом провалу моніторингу рахунків подвійного призначення. Банк дозволив використовувати персональні рахунки для бізнес-цілей, пропустивши транзакції на £27.3 млн шахрайських коштів з фондів підтримки під час пандемії (Covid furlough schemes). Регулятор чітко дав зрозуміти: знання про використання персонального рахунку для бізнесу без переведення клієнта на відповідний тариф та застосування відповідних контролів є системним порушенням. Ще більш показовим є штраф Центрального банку Ірландії (CBI) для Coinbase Europe (€21.4 млн). Цей прецедент встановлює новий стандарт відповідальності для фінтех-сектору та VASP. Проблема полягала не у відсутності системи моніторингу, а в її неправильній конфігурації та IT-збоях, внаслідок яких 31% транзакцій (обсягом €176 млрд) залишилися неперевіреними. Вимога проведення ретроспективного моніторингу (lookback review), який зайняв три роки і виявив тисячі пропущених STR, демонструє, що технологічні збої більше не розглядаються як пом'якшувальна обставина. Регулятори вимагають абсолютної стійкості IT-інфраструктури як базового елементу ліцензійних вимог.

Ключовою подією в ЄС стало офіційне внесення Росії до списку високоризикових третіх країн Єврокомісії, що є прямим відхиленням від позиції FATF (яка призупинила членство РФ, але не внесла її до чорного списку). Це створює юридичну колізію для міжнародних банківських груп: транзакції, пов'язані з РФ, тепер автоматично підпадають під вимоги посиленої належної перевірки (EDD) в межах ЄС, незалежно від санкційного статусу конкретних контрагентів. Паралельно відбувається передача повноважень від EBA до новоствореного органу AMLA, який розпочне роботу наприкінці 2025 року. EBA вже підготувала технічні стандарти (RTS) для оцінки ризиків, які стануть основою Єдиного зводу правил (Single Rulebook). Впровадження DORA виходить на фінішну пряму з публікацією списку критичних ICT-провайдерів (Amazon, Google, Microsoft), що фактично вводить Big Tech у периметр фінансового нагляду, визнаючи хмарні сервіси системно важливими для фінансової стабільності.

Звіт також деталізує складні схеми ухилення від санкцій, зокрема через іранський тіньовий банкінг ($9 млрд потоків через кореспондентські рахунки США). FinCEN викрив використання підставних компаній у Гонконгу та ОАЕ, які, не маючи реальної діяльності, забезпечують розрахунки за нафту та нафтопродукти. Окремої уваги заслуговує «Бурштинове попередження» (Amber Alert) від NCA щодо «тіньового флоту». Це мережа сотень застарілих суден з непрозорою власністю, які використовуються Росією, Іраном та КНДР для експорту енергоносіїв. Для фахівців з комплаєнсу це означає необхідність інтеграції даних морського трекінгу (AIS) та аналізу супутникових знімків у процедури торговельного фінансування, оскільки традиційної

документарної перевірки вже недостатньо для виявлення ship-to-ship transfers (STS) та маніпуляцій з прапорами. Також висвітлено зростання шахрайства з push-платежами (APP scams), де регулятор Сполученого Королівства запровадив механізм обов'язкового відшкодування збитків жертвам, перекладаючи фінансовий тягар на платіжні системи та банки, що змушує їх інвестувати в превентивні моделі AI.

Висновки:

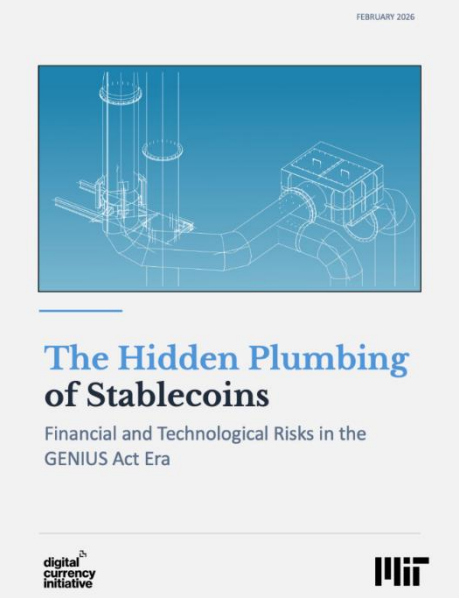
- **Технологічна стійкість як основа ліцензії:** Технічні збої в системах моніторингу транзакцій (TMS) тепер прирівнюються до відсутності контролю. Фінансові установи повинні впровадити безперервне тестування цілісності даних та регулярні аудити конфігурацій сценаріїв моніторингу. Аргумент "системної помилки" більше не приймається регуляторами як виправдання, а призводить до вимог ретроспективного перегляду всіх транзакцій за роки збоїв.
- **Операціоналізація геополітичних ризиків:** Внесення Росії до списку високоризикових країн ЄС вимагає від міжнародних груп перегляду матриць ризиків. Навіть якщо транзакція дозволена санкційним режимом (наприклад, гуманітарна допомога або "energy carve-outs"), вона автоматично вимагає EDD та схвалення вищим керівництвом, якщо вона проходить через юрисдикцію ЄС. Це створює додаткове навантаження на підрозділи першої лінії захисту.
- **Інтеграція нефінансових даних у моніторинг:** Попередження про "тіньовий флот" та іранський тіньовий банкінг демонструють, що транзакційний моніторинг без контекстуальних даних є сліпим. Банки, залучені до торговельного фінансування, повинні інтегрувати зовнішні джерела даних (морський трафік, реєстри корпоративної прозорості третіх країн, дані про IP-адреси) для виявлення складних мереж ухилення, які маскуються під легальну торгівлю.

FATF та МВФ синхронно наголошують на подвійній природі штучного інтелекту. З одного боку, це загроза (діпфейки, автоматизоване шахрайство), з іншого — необхідний інструмент для наглядових органів (SupTech). Сінгапур (MAS) випустив детальні інструкції щодо управління ризиками AI, вимагаючи від банків пояснюваності (explainability) алгоритмів та людського нагляду за рішеннями AI. Канада йде шляхом інституційних реформ, створюючи Агентство з фінансових злочинів (Financial Crimes Agency) за зразком британського NCA, щоб подолати фрагментацію між розвідкою та поліцією. ОАЕ, прийнявши Федеральний декрет-закон № 10, повністю синхронізують своє законодавство зі стандартами FATF, особливо в частині віртуальних активів, намагаючись закріпити статус глобального крипто-хабу з «білим» регулюванням.

Між резервами та кризою ліквідності: системні ризики стейблкоїнів у новій регуляторній моделі США [8]

Документ присвячений комплексному аналізу фінансових, ринкових, технологічних і регуляторних ризиків стейблкоїнів у контексті впровадження GENIUS Act у США у 2025 році. Автори виходять із того, що новий закон уперше створює єдину федеральну рамку для регулювання емісії, резервного забезпечення та нагляду за доларовими стейблкоїнами, однак водночас закладає спрощене уявлення про стабільність цих інструментів як суто балансову проблему, яку можна вирішити через вимоги до складу резервів і прозорість. У роботі

8 https://static1.squarespace.com/static/6675a0d5fc9e317c60db9b37/t/6982abb3c5cfd2209a98da90/1770171315639/The+Hidden+Plumbing+of+Stablecoins_+vShare.pdf



наголошується, що реальна здатність стейблкоїнів підтримувати паритет 1:1 залежить не лише від якості активів, а й від функціонування ринку державних облігацій, пропускної здатності брокерсько-дилерської системи та надійності блокчейн-інфраструктури

У вступній частині автори розміщують стейблкоїни в ієрархії грошової системи, показуючи, що вони займають нижчий рівень порівняно з банківськими депозитами, оскільки їх погашення зазвичай здійснюється через комерційні банки та ринкову ліквідацію цінних паперів. Це означає, що стабільність стейблкоїнів опосередкована приватною фінансовою інфраструктурою і не має прямої опори на баланс центрального банку. Така конструкція робить їх особливо вразливими до криз ліквідності, оскільки формальна платоспроможність емітента не гарантує можливості оперативного виконання зобов'язань у стресових умовах.

Значна частина документа присвячена аналізу механіки емісії та погашення стейблкоїнів. Автори детально описують, що в разі використання казначейських облігацій як резервів процес викупу включає продаж цінних паперів, конвертацію отриманих коштів у банківські депозити та подальший переказ користувачу. Така багатоступенева процедура створює часові затримки, залежність від клірингових систем і ризик втрат вартості у разі нестабільності ринку. Особливо підкреслюється, що в умовах масового погашення навіть короткострокові збої в обробці операцій можуть підірвати довіру до стейблкоїна.

У розділі про ризики неплатоспроможності автори показують, що вимога резервного забезпечення 1:1 без обов'язкових капітальних буферів створює «ножову межу» платоспроможності, за якої будь-які втрати вартості активів одразу ставлять під загрозу виконання зобов'язань. Аналіз публічної звітності великих емітентів свідчить, що більшість із них мають надзвичайно низькі показники власного капіталу, які були б неприйнятними за банківськими стандартами. Хоча використання короткострокових інструментів і зворотних репо знижує процентний ризик, ці механізми не забезпечують захисту від масштабних ринкових або операційних шоків.

Порівнюючи балансну структуру стейблкоїн-емітентів із банками та фондами грошового ринку, автори доходять висновку, що перші поєднують у собі найуразливіші риси обох моделей. Майже всі їхні зобов'язання підлягають негайному погашенню, як у банківських депозитів, але при цьому вони не мають доступу до страхування вкладів і стандартних механізмів підтримки ліквідності з боку центрального банку. Водночас, подібно до фондів грошового ринку, вони інвестують у короткострокові інструменти, однак не мають ефективних інструментів стримування «набігів», таких як комісії або тимчасові обмеження на погашення.

Центральним елементом дослідження є аналіз вразливості ринку казначейських облігацій США. На прикладі криз 2019 і 2020 років автори показують, що навіть відносно невеликі обсяги продажу можуть призвести до серйозних збоїв у ліквідності та ціноутворенні. Обмеження балансу банків, зумовлені нормативом додаткового коефіцієнта співвідношення капіталу до активів, зменшують здатність брокерів масштабувати посередництво в кризових умовах. Унаслідок цього виникає двосторонній механізм поширення ризику: масові погашення стейблкоїнів тиснуть на ринок облігацій, а ринкові збої, своєю чергою, стимулюють подальші погашення.

Окремий розділ присвячений технологічним і операційним ризикам. Автори підкреслюють, що блокчейн-інфраструктура, на якій функціонують стейблкоїни, має власні джерела вразливості, пов'язані зі смарт-контрактами, мостами між мережами, оракулами, механізмами консенсусу та управлінням ключами. Помилки в коді, кібератаки або збої мережі можуть тимчасово або повністю заблокувати перекази й погашення навіть за повного резервного забезпечення. Таким чином, технічні проблеми здатні трансформуватися у фінансову нестабільність через втрату довіри та різке зростання попиту на викуп

У фінальній частині роботи оцінюється ефективність GENIUS Act як регуляторної основи. Автори визнають, що закон суттєво посилив вимоги до якості резервів, прозорості та нагляду, зокрема через заборону повторного використання активів і регулярні публічні розкриття. Водночас він залишає відкритими ключові питання щодо капітальних вимог, механізмів управління ліквідністю та доступу до ресурсів Федеральної резервної системи. Особливо наголошується на нерозв'язаній дилемі: надання емітентам доступу до центрального банку могло б підвищити стійкість, але водночас створило б ризики для трансмісії монетарної політики та ролі банківського сектору

У підсумку автори доходять висновку, що довгострокова стабільність стейблкоїнів не може бути забезпечена лише через формальні вимоги до резервів. Вона потребує інтегрованого підходу, який охоплює регулювання фінансових ринків, розвиток інфраструктури ліквідності, встановлення адекватних капітальних стандартів і системне управління технологічними ризиками. Без такої комплексної моделі навіть GENIUS-сумісні стейблкоїни залишатимуться потенційним джерелом фінансової нестабільності в умовах масштабного використання.

Висновки:

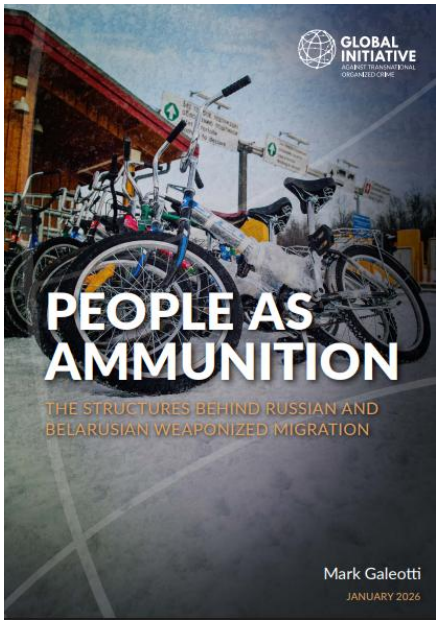
- **GENIUS Act підвищує якість резервів стейблкоїнів, але не гарантує стабільності паритету в умовах ринкового стресу.** Підтримання обміну 1:1 залежить від роботи ринку казначейських облігацій і посередників. У разі перевантаження цієї інфраструктури можливі затримки або відхилення від паритету.
- **Більшість великих емітентів мають дуже низький рівень власного капіталу навіть за наявності високоякісних активів.** За банківськими стандартами вони були б недокапіталізованими. Це підвищує ризик неплатоспроможності у разі шоків.
- **Масові погашення стейблкоїнів можуть спричинити дестабілізацію ринку державних облігацій США.** Навіть відносно невеликі обсяги продажу здатні перевищити можливості брокерів. Це створює взаємне посилення ринкових і ліквідних ризиків.
- **Технічні збої блокчейн-інфраструктури можуть порушити обіг і погашення стейблкоїнів навіть за повного резервного забезпечення.** Проблеми смарт-контрактів, мостів або консенсусу напряму впливають на довіру користувачів. Технологічний ризик є рівнозначним фінансовому.

Міграція як зброя: анатомія гібридної війни кремля [9]

У сучасному світі, де пряме військове зіткнення між ядерними державами залишається малоймовірним сценарієм через загрозу взаємного знищення, на перший план виходять інструменти так званої «гібридної» або «асиметричної» війни. Це поняття охоплює надзвичайно широкий спектр явищ — від кібератак на енергетичні мережі та виборчі системи до масованих

[9] https://globalinitiative.net/wp-content/uploads/2026/01/Mark-Galeotti-People-as-ammunition-The-structures-behind-Russian-and-Belarusian-weaponized-migration-GI-TOC-January-2026.pdf

дезінформаційних кампаній у соціальних мережах, від економічного тиску за допомогою енергоресурсів до підривної діяльності через підконтрольні неурядові організації. Однак, мабуть, найцинічнішим і водночас найефективнішим проявом такої війни є перетворення людського горя, відчаю та прагнення до кращого життя на інструмент політичного шантажу.



Документ, опублікований Глобальною ініціативою проти транскордонної організованої злочинності, є не просто черговим звітом про міграційну кризу. Це найґрунтовніше на сьогодні дослідження феномену, який у дипломатичних кабінетах Брюсселя, Варшави та Гельсінкі делікатно називають «інструменталізацією міграції», тоді як у кремлі його вже давно внесли до переліку стандартних оперативних процедур.

Ключова теза дослідження, яку автор наполегливо розвиває від розділу до розділу, полягає в тому, що москва та мінськ діяли не ізольовано один від одного і не спонтанно. Між 2015 і 2023 роками відбулася стрімка еволюція тактики, взаємне навчання та адаптація успішних практик. Те, що починалося як експериментальний, майже імпровізований інструмент, перетворилося на відлагоджений конвеєр.

Перші ластівки з'явилися ще у 2015 році на стику кордонів росії та Норвегії. Тоді сотні мігрантів, переважно із охопленої війною Сирії, почали використовувати воістину абсурдний, на перший погляд, юридичний лайфхак, який отримав назву «велосипедний маршрут». Суть його полягала у геніальній простоті: російське законодавство забороняло перетин кордону пішки, тоді як норвезьке вимагало наявності в'їзної візи для автомобілів. Про велосипеди не згадував жоден нормативний акт. Мігранти купували квитки в Дамаску чи Бейруті, летіли до москви, долали 38-годинний залізничний маршрут до Мурманська, автобусом до кордону, де на них уже чекали заповзятливі місцеві ділки, готові за п'ятсот доларів продати старий, не раз перефарбований велосипед.

У той момент це виглядало як суто стихійна «підприємницька ініціатива», наслідок недосконалості національних законодавств. Однак автор, спираючись на інтерв'ю з колишніми норвезькими та фінськими дипломатами, розбиває цю ілюзію вщент. Він звертає увагу на ключову деталь: Мурманська область — це не просто північний регіон. Це зона стратегічної відповідальності Північного флоту, район базування атомних підводних човнів. В'їзд туди для іноземців суворо лімітований і контролюється ФСБ. Той факт, що сотні сирійців, афганців та індійців раптово отримали можливість безперешкодно дістатися до прикордонної смуги, не може бути випадковістю. Більше того, сам фінський міністр Петтері Орпо зізнався, що під час закритих зустрічей російські офіційні особи дали зрозуміти: у них є інструмент, який працює, і вони готові його використати. Найкращим доказом наявності «кнопки» стало те, що потік мігрантів зупинився майже миттєво, щойно норвежці погодилися на переговори. Це була не стихія, а демонстрація сили.

Наступний етап, білорусько-польський кордон 2021 року, став якісним стрибком не лише в масштабах, які сягнули десятків тисяч людей, але й у рівні жорстокості та цинізму. Олександр Лукашенко, який сам у минулому очолював прикордонні війська, опинився в стані тотальної міжнародної ізоляції після фальсифікованих виборів 2020 року. Він реалізував свою давню, ще з 2002 року, погрозу «залити Європу мігрантами та наркотиками». На відміну від 2015 року, мова вже не йшла про те, що прикордонники просто «заплющують очі» або беруть дрібні хабарі. Білоруський КДБ під керівництвом взяв на себе пряме оперативне управління всім

процесом. Державний авіаперевізник «Белавіа» та підконтрольні спецслужбам туроператори на кшталт «Центр Курорт» почали активно рекламувати «туристичні пакети» до мінська з Багдада, Дамаска, Єревану, Стамбула. Вартість такого пакету коливалася від двох до п'яти тисяч євро і включала не лише переліт, а й чіткі інструкції: куди їхати, які речі мати з собою, що говорити при затриманні, де шукати кусачки для дроту. Коли під тиском Євросоюзу іракські авіалінії припинили польоти до мінська, на заміну миттєво прийшли сирійські авіакомпанії, зокрема Cham Wings, яка запустила щоденні рейси. КДБ не просто дозволив контрабандистам працювати — він створив для них сприятливе ринкове середовище з нульовим ризиком. Курдські та сирійські злочинні угруповання, які раніше спеціалізувалися на торгівлі наркотиками, швидко перекваліфікувалися на експертів з людського трафіку. Це явище автор дослідження називає «девіантною публічно-приватною співпрацею», де держава виступає генеральним підрядником, що гарантує безпеку угоди, а організована злочинність — субпідрядником, що забезпечує логістику на місцях.

Операції 2021 року призвели до загибелі понад двадцяти людей від переохолодження в пущі, спричинили гуманітарну катастрофу, зруйнували тисячі життів. Але автор пропонує подивитися на ситуацію очима кремлівського стратега, для якого категорії «добра» і «зла» є похідними від категорій «корисності» та «ефективності». З точки зору інструментальної раціональності кремля, який вимірює успіх не кількістю врятованих, а обсягами створеного хаосу, виснаженням ресурсів противника та глибиною поляризації європейських суспільств.

Росія та білорусь навчилися віртуозно використовувати внутрішні суперечності Європейського Союзу. Коли Польща відповідала на провокації зведенням стіни та відмовою пропускати мігрантів, Брюссель критикував Варшаву за порушення права на притулок. Коли Німеччина, не витримавши навантаження, повертала мігрантів до Польщі, Варшава звинувачувала Берлін у егоїзмі. Таким чином, агресор досягає класичного ефекту «подвійного удару». По-перше, він створює фізичне, матеріальне навантаження на інфраструктуру: Польща щороку витрачає близько 600 мільйонів євро на утримання кордону та прийом мігрантів. По-друге, і це важливіше, він перетворює прикордонні держави на «поганих поліцейських» в очах ліберальної Європи. Різка реакція польських силовиків стала предметом гострої критики з боку Управління Верховного комісара ООН з прав людини, що дозволило білоруській пропаганді годинами крутити сюжети про «звірства» польських військових.

Автор дослідження окреслює п'ять потенційних сценаріїв розвитку подій, кожен з яких базується на реальних геополітичних та кримінальних трендах, зафіксованих розвідками країн ЄС. Найбільш тривожним, майже апокаліптичним за своїми масштабами, виглядає так званий «лівійський сценарій». Росія вже більше п'яти років має суттєвий військово-політичний вплив у східній Лівії через ПВК «Вагнер» та її наступників, які діють під крилом командувача Халіфи Хафтара. Лівія історично була і залишається головним «відправним пунктом» для міграційного потоку до Італії та Мальти. Автор пропонує сценарій, за яким москва, отримавши контроль над лівійським узбережжям або здатність впливати на місцеві збройні угруповання, отримує у своє розпорядження велетенський «кран», здатний затопити південну Європу.

Іншим, не менш небезпечним інструментом є «врегульована порада». Фізичне переміщення мільйонів людей через кордони — це надзвичайно складна логістична операція, яка потребує великих коштів, інфраструктури та часу. Натомість росія може просто активізувати дезінформаційні кампанії в соціальних мережах, месенджерах та закритих чатах, поширюючи чутки про те, що певний кордон раптово став «прозорим», або що Німеччина відновила політику «відкритих дверей». Це найдешевший, найшвидший і найважчий для блокування спосіб гібридного впливу. Він не потребує залучення ФСБ чи КДБ на місцях, достатньо лише кількох бото-ферм та тролів, які працюють на арабську аудиторію.

Не оминає автор і гострого кута внутрішньоєвропейських ризиків, зокрема неоднозначної ролі Угорщини. Він обережно, але наполегливо припускає, що Віктор Орбан, який уже у 2015 році віртуозно використав міграційну кризу для зміцнення власної влади та просування антибрюссельської риторики, теоретично міг би спровокувати нову хвилю напруги, щоб остаточно продемонструвати «неспроможність» ліберальних еліт ЄС. У цьому контексті мова вже навіть не стільки про прямий російський вплив, скільки про фатальний збіг інтересів націоналістичних сил всередині Євросоюзу та зовнішніх гравців, які прагнуть його дезінтеграції.

Хоча ФСБ є безпосереднім інструментом виконання на кордоні, вона не має інституційних повноважень наказувати Міністерству закордонних справ спростити візовий режим для громадян Ємену, або Міністерству внутрішніх справ — ігнорувати перевірку документів у мігрантів. Дослідник доходить однозначного висновку, що всі подібні міжвідомчі операції координуються єдиним центром — Адміністрацією Президента Російської Федерації. Він називає її «тіньовим урядом», структурою, яка перетворює розрізнені, часто конкуруючі між собою відомства на єдиний, добре відлажений механізм. Цей рівень централізації, на думку автора, є найкращим доказом того, що міграційна зброя більше не є імпровізацією місцевих командирів ФСБ у Мурманську чи прикордонників у Пскові. Вона офіційно внесена до стратегічного арсеналу кремля, поруч із кібератаками та енергетичним шантажем. Це усвідомлення має кардинально змінити підходи до протидії. Недостатньо просто посилювати контроль на кордоні; потрібно розуміти, хто саме і в який спосіб віддає накази про відкриття та закриття міграційних коридорів.

Висновки:

- **Інструменталізація міграції — це свідома державна політика.** Росія та білорусь діють за єдиним централізованим задумом: координують міжвідомчу взаємодію, а «кран» відкривається і закривається за політичним рішенням.
- **Ключ — симбіоз держави та організованої злочинності.** Спецслужби створюють безпечне середовище для кримінальних мереж, які забезпечують логістику.
- **Москва вважає цю зброю ефективною, бо вона сіє хаос.** Навіть якщо довгострокові результати сумнівні, короткострокові цілі досягаються: виснаження ресурсів, поляризація суспільств, сварки між країнами ЄС.
- **Європа залишається вразливою, загрози зміщуються на південь.** Польща і Фінляндія посилили кордони, тому москва шукає нові плацдарми: Лівія, Балкани, Туреччина.

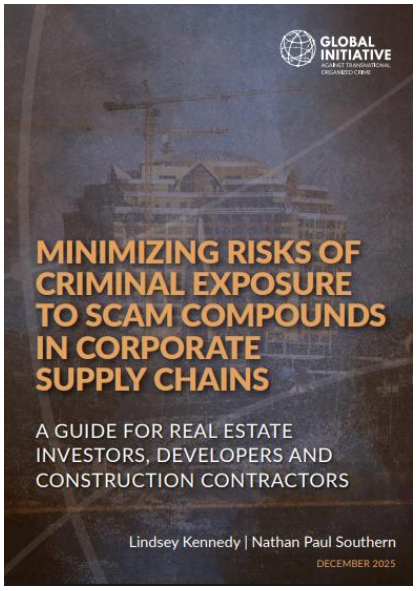
Підсумовуючи автор не лише констатує проблему, а й пропонує чіткі, структуровані рамки для ефективної відповіді. Він категорично застерігає від двох фатальних крайнощів. Перша крайність — це паніка та надмірна, неконтрольована сек'юритизація. Будівництво стін, мілітаризація кордонів, виділення десятків мільярдів євро виключно на загороджувальні заходи — це пастка, в яку агресор і прагне загнати Європу. Це веде до «фортеці Європа», де військові бюджети з'їдають соціальні, де права людини приносяться в жертву ілюзії безпеки, де ЄС втрачає свою ідентичність як простір свободи та демократії.

Друга крайність — це заперечення та інфантилізм, коли кожен новий спалах міграційної активності вперто списують виключно на «економічні причини» чи «кліматичні зміни», ігноруючи очевидну, задокументовану роль спецслужб.

Автор також наголошує на надзвичайній важливості діалогу з країнами походження мігрантів. Досвід 2021 року з Іраком є вкрай показовим. Багдад не отримав жодної вигоди від того, що його громадяни мерзнуть у білоруських лісах, витрачають останні заощадження на сумнівних контрабандистів і гинуть на кордоні. Навпаки, це створило для іракського уряду серйозні репутаційні втрати та фінансові витрати на репатріацію тіл загиблих. Створення широких міжнародних коаліцій країн, які спільно та публічно засуджують практику інструменталізації,

може позбавити москву та мінськ важливого політичного камуфляжу та перетворити їхню «зброю» на токсичний актив.

Як легітимний бізнес допомагає будувати кримінальну економіку Південно-Східної Азії [10]



Глобальна індустрія онлайн-шахрайства, яка за оцінками експертів щорічно генерує понад трильйон доларів збитків, вже давно перестала бути виключно справою хакерів-одинаків, вірусних розсилок чи підпільних кол-центрів, орендованих на місяць. Сьогодні це повноцінна транснаціональна кримінальна економіка, яка за масштабами та складністю організації наближається до нарко-картелів або незаконного видобутку корисних копалин, але з однією суттєвою відмінністю: вона має власну капіталомістку інфраструктуру, багаторівневу логістику та, що найважливіше, відкриту й системну участь приватного сектору, який часто навіть не вважає свою діяльність чимось протиправним.

Звіт, підготовлений GI-TOC свідомо зміщує фокус уваги з безпосередніх виконавців злочинів — операторів скам-центрів, вербувальників та місцевих корумпованих чиновників — на їхніх «мирних», «легітимних» і часто публічних співучасників.

Автори звіту пропонують поглянути на проблему крізь призму так званої «пре-операційної фази». Це критично важливий часовий проміжок, коли шахрайський комплекс існує ще лише на папері, у вигляді інвестиційної пропозиції, містобудівного плану або напів-зведених конструкцій. На цьому етапі він ще не викрав жодної людини, не утримував жодного раба, не відмив жодного долара. Але саме на цьому етапі він отримує землю, юридичну адресу, будівельні дозволи, генерального підрядника, субпідрядників, а також, що особливо показово, — позитивне висвітлення в міжнародних ділових ЗМІ. І саме на цьому етапі легітимний бізнес має найбільше важелів впливу: можна відмовитися від контракту, зажадати розкриття бенефіціарів, повідомити у відповідні органи. Однак, як демонструє звіт, у переважній більшості випадків бізнес цього не робить. І це мовчання, ця пасивність, це «незнання» мають свою ціну.

Одним із найцінніших аналітичних інструментів, запропонованих дослідниками, є концепція «спектру співучасті». Це не бінарна класифікація «винний — невинний», а прагматичний інструмент для оцінки ризиків та визначення стратегій втручання. На одному полюсі цього спектру розташована «ненавмисна співучасть». Йдеться про компанії, які стали жертвами цілеспрямованої дезінформації. Їм показали глянцеві буклети про «екологічні міста майбутнього», «туристичні гавані» або «інноваційні технопарки». Вони провели формальну перевірку, не натрапили на свіжі кримінальні справи і підписали контракт. Однак відсутність кримінального минулого не дорівнює відсутності кримінального сьогодення. Часто засновники таких проєктів є рецидивістами, але їхні попередні злочини скоєні в інших юрисдикціях, під іншими іменами, або ж були «залагоджені» на рівні місцевих еліт.

Далі за спектром — «неохоча співучасть». Це компанії, які починають підозрювати недобре, коли проєкт вже запущено, коли підписано незворотні зобов'язання, коли вихід із контракту загрожує судовими позовами або, що ще гірше, фізичною безпекою представників компанії в

[10] https://globalinitiative.net/wp-content/uploads/2025/12/Lindsey-Kennedy-Nathan-Paul-Southern-Minimizing-risks-of-criminal-exposure-to-scam-compounds-in-corporate-supply-chains-GI-TOC-December-2025.pdf

країні перебування. Саме ця категорія найчастіше звертається по допомогу, але, як правило, із запізненням.

«Пасивна співучасть» — це царина байдужості. Компанії бачать червоні прапорці, але свідомо вирішують їх ігнорувати. Вони не ставлять запитань, коли замовник просить прибрати вікна з перших поверхів або збільшити кількість ліжкомісць до щільності, характерної для казарм. Вони не реагують, коли в місцевій пресі з'являються статті про протести громади проти забудовника. Вони списують це на «специфіку регіону».

Нарешті, на протилежному полюсі перебувають «активна співучасть» та «прямі учасники». Активна співучасть — це ситуація, коли підрядник чітко розуміє призначення об'єкта і навіть спеціалізується на таких замовленнях. Його портфоліо включає як звичайні житлові комплекси, так і об'єкти з характерними ознаками скам-комплексів: антисуїцидні сітки, затемнені кімнати, багаторівневі системи контролю доступу. Такі компанії не є кримінальними у правовому сенсі, але вони є критично важливим елементом кримінальної екосистеми. Вони — місток між світом «брудних» грошей та світом «чистої» архітектури.

Найвищий рівень — «прямі учасники». Це компанії, створені безпосередньо кримінальними авторитетами для управління активами, відмивання коштів та легалізації статусу. Їхня небезпека полягає в тому, що вони навмисно диверсифікують портфель: вони можуть будувати шахрайські центри на одній ділянці, а на сусідній — фінансувати будівництво школи або лікарні. Вони спонсорують спортивні змагання, публікують звіти про корпоративну соціальну відповідальність, запрошують на відкриття об'єктів дипломатів та політиків. Це робить їх практично невразливими для звичайної комплаєнс-перевірки: потенційний партнер бачить солідний бізнес і не усвідомлює, що він фінансує ланцюг постачання торгівлі людьми.

Найбільш промовистою і водночас трагічною ілюстрацією такої взаємодії є кейс з бетоном. У листопаді 2024 року незалежні дослідники, перебуваючи в районі Мей Сот на кордоні Тайланду і М'янми, зафіксували колону вантажівок-бетонозмішувачів із брендуванням «KK Concrete», які прямували в бік KK Park — одного з найбільш одіозних шахрайських комплексів М'янми, відомого систематичними тортурами та примусовим утриманням іноземців. Сама по собі поставка бетону — це абсолютно законна господарська операція. Однак сукупність обставин: назва компанії, що збігається з назвою кримінального об'єкта, напрямок руху, географічна близькість — створюють нерозривний контекст. Після того, як дослідники оприлюднили цю інформацію, завод на території Таїланду був демонтований. Але проблема не зникла. Бетонний завод просто перемістився — фізично, через річку, на територію М'янми, де юрисдикція тайської поліції не діє, а влада або безсила, або співучасна. Це ідеальна метафора всієї системи: коли легітимний бізнес стикається з репутаційною загрозою, він не припиняє співпрацю з криміналом, а змінює логістику, роблячи її менш прозорою.

Окремий і надзвичайно складний пласт проблеми стосується ролі міжнародних фінансових інституцій та ініціативи «Один пояс — один шлях» (BRI). Автори звіту уникають спрощених звинувачень на адресу Китаю, натомість пропонують системний аналіз уразливостей. Ініціатива BRI, яка є наймасштабнішою інфраструктурною програмою сучасності, стала жертвою власного успіху. Відсутність централізованого реєстру проєктів, децентралізована модель ухвалення рішень та величезна кількість субпідрядників різних рівнів створюють ідеальне середовище для маніпуляцій. Фраза «активно відповідаємо ініціативі Один пояс — один шлях» перетворилася на універсальний маркер легітимності, який не потребує підтвердження. Дослідники наводять показовий приклад Шве Кокко — мегапроєкту на кордоні М'янми, який публічно позиціонувався як частина BRI, доки посольство Китаю в Янгоні не виступило з офіційною заявою, заперечуючи будь-який зв'язок. Проблема в тому, що така спростовна заява з'явилася вже після того, як було залучено інвестиції, розпочато будівництво та сформовано позитивний інформаційний фон.

Ще гіршою є ситуація з Dara Sakor у Камбоджі. Цей об'єкт, який перебуває під санкціями США, неодноразово фігурував у звітах правозахисних організацій як хаб для шахрайських операцій. Попри це, він був включений до офіційного звіту BRI, а його девелопери отримували фінансування від Банку розвитку Китаю. Для західного інвестора, який проводить перевірку, згадка про зв'язок з BRI та китайським державним банком є потужним сигналом безпеки. Він сприймає це як гарантію того, що проєкт пройшов багаторівневу перевірку. Насправді ж цей сигнал виявляється хибним. Це створює ефект «інформаційної пастки»: чим більше легітимних інституцій взаємодіє з проєктом на ранніх стадіях, тим складніше пізніше переконати нових партнерів у його кримінальному характері.

Не менш гострою є критика на адресу багатосторонніх банків розвитку, зокрема Азійського банку розвитку. Формально АБР та Світовий банк мають розвинені системи комплаєнсу, включаючи механізми внесення недобросовісних підрядників до «чорних списків». Однак ефективність цих механізмів зводиться нанівець двома факторами. По-перше, АБР часто не публікує обґрунтування своїх рішень. Інвестор бачить назву компанії в списку, але не знає, чи була вона покарана за технічну помилку в тендерній документації, чи за систематичні хабарі, чи за зв'язки з організованою злочинністю. По-друге, після закінчення терміну компанія зникає з публічних реєстрів, і сліди її правопорушень губляться. Це дозволяє рецидивістам вільно повертатися на ринок. Більше того, сам АБР опинився під вогнем критики за схвалення кредиту в розмірі 250 мільйонів доларів на розвиток прикордонної економічної зони між Ліньцаном (Китай) та Чіншуехо (М'янма) саме в той період, коли цей регіон перетворювався на епіцентр шахрайської індустрії. У звітній документації банку підвищені ризики, пов'язані зі злочинністю, навіть не згадувалися.

Центральним кейсом, що демонструє тотальну неспроможність стандартних KYC-процедур, є історія Донг Леченга, також відомого як Хенг Тонг. Цей бізнесмен, який отримав громадянство Камбоджі королівським указом та змінив ім'я, керував компанією Yunnan Jincheng Group. Його проєкти позиціонувалися як проривні інвестиції в камбоджійську економіку, отримували схвалення на найвищому державному рівні та залучали міжнародних партнерів. Дослідження GI-TOC демонструє, що його кримінальне минуле не було прихованим. Ще у 2008 році китайський суд визнав Донг Леченга винним у сприянні транскордонним нелегальним азартним іграм через його флагманський готель. Його звинувачували у відмиванні понад мільярда доларів. Академічне дослідження 2018 року описувало його бізнес-стратегію в провінції Юньнань як «безпрецедентний випадок інституційного кептиву» — симбіозу бізнесу та політичної еліти. Здавалося б, будь-яка серйозна комплаєнс-перевірка мала би виявити ці факти. Однак вони залишалися поза увагою інвесторів, підрядників та міжнародних банків. Чому? Тому що Донг Леченг вміло скористався «інформаційним розривом». Він змінив юрисдикцію, змінив ім'я, інвестував у створення нового іміджу. Його минуле залишилося в китайських архівах, які не є пріоритетними для міжнародного комплаєнсу, орієнтованого на глобальні бази даних санкцій та інтерполівські ордери. І лише після того, як у 2023 та 2025 роках Велика Британія та США запровадили проти нього санкції, його ім'я стало токсичним. Але на той момент інфраструктуру вже було збудовано, а десятки тисяч людей — поневолено.

Історія Донг Леченга підводить до ще однієї критичної теми, порушеної у звіті: проблеми доступу до інформації. Автори вводять поняття «інформаційного затемнення» як системного бізнес-ризику. Шахрайські комплекси процвітають не лише завдяки корупції, а й завдяки контролю над інформацією. У Камбоджі, Лаосі та М'янмі рівень свободи преси є одним із найнижчих у світі. Це створює унікальний феномен «бульбашки фільтрів». Потенційний інвестор, який проводить базовий пошук в інтернеті, на перших сторінках видачі бачить виключно позитивний контент: грандіозні церемонії відкриття, інтерв'ю з топ-менеджерами, звіти про партнерство з міжнародними брендами. Негативна інформація існує, але вона

похована в глибинах спеціалізованих баз даних, академічних журналів або — що найчастіше — взагалі видалена на вимогу адвокатів позивачів.

Для девелоперів та архітектурних бюро рекомендації стосуються змістовного аналізу технічного завдання. Будь-який запит на проєктування об'єктів, що обмежують особисту свободу, має викликати негайну реакцію. Заґратовані балкони, вікна без можливості відкривання, суцільна огорожа периметру, єдині контрольовані входи-виходи, відсутність природного освітлення в житлових приміщеннях — це не архітектурні особливості, це ознаки в'язниці. Якщо об'єкт проєктується як готель, але містить спальні приміщення казарменого типу на 20–30 осіб, це не помилка проєктування. Це свідомий намір.

Для будівельних підрядників ключовим є впровадження політик протидії торгівлі людьми не лише у власному ланцюгу постачання, але й серед клієнтів. Дослідження фіксує системну асиметрію: компанії готові витрачати ресурси на перевірку того, чи не використовують їхні постачальники сировини рабську працю, але ігнорують питання про те, навіщо їхньому клієнту бетон. Жодна з організацій, опитаних авторами звіту, не отримувала запитів від клієнтів щодо перевірки зв'язків із торгівлею людьми в рамках KYC-процедур. Це свідчить про те, що бізнес досі сприймає ризик торгівлі людьми виключно як ризик репутаційний, а не як ризик отримання доходів від злочинної діяльності та подальшого переслідування за відмивання грошей.

Нарешті, для фінансових інституцій та банків рекомендація є водночас простою і складною: публікуйте обґрунтування своїх рішень. Недостатньо просто оприлюднити список недобросовісних компаній. Необхідно, щоб цей список був пошуковим, щоб інформація про порушення зберігалася в архівах навіть після закінчення терміну санкцій, і щоб інвестори могли зрозуміти, чи мають вони справу з корупціонером, чи з технічним порушником. Прозорість у цьому питанні — це не бюрократична формальність, а інструмент запобігання злочинності.

Висновки:

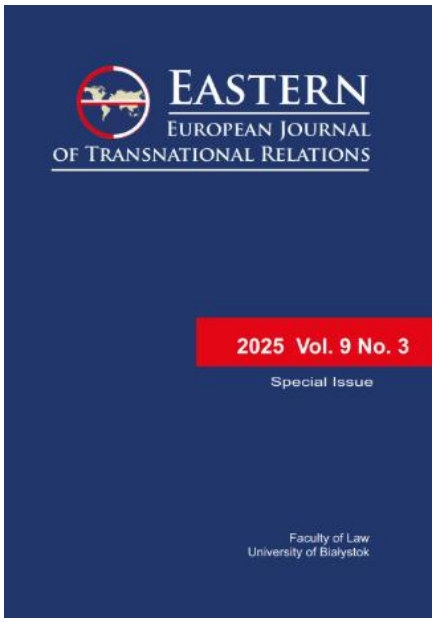
- **Спектр співучасті бізнесу є визначальним.** Між «незнанням» і «прямою участю» існує широка сіра зона пасивної та активної співучасті, де компанії ігнорують червоні прапорці або свідомо адаптують свої послуги під потреби кримінальних операторів.
- **Традиційні KYC-процедури не працюють у гібридному середовищі.** Стандартна перевірка контрагентів не виявляє зв'язків через зміну імен, набуття «золотих паспортів», використання підставних компаній з легальним портфелем або фальшиві афіліації.
- **Інформаційна асиметрія є системним бізнес-ризиком.** Блокування незалежних ЗМІ, переслідування журналістів та агресивні PR-кампанії кримінальних девелоперів створюють «бульбашку фільтрів», де позитивний контент домінує у пошуковій видачі, а критична інформація стає недоступною.
- **Міжнародні фінансові інституції легітимізують кримінальні проєкти.** Азійський банк розвитку та інші багатосторонні банки фактично сприяють відмиванню репутації через непрозорість власних санкційних рішень та фінансування проєктів у зонах з очевидними криміногенними ризиками.

Підсумовуючи, слід наголосити на головному: феномен шахрайських комплексів у Південно-Східній Азії є неможливим без активної чи пасивної підтримки легітимної економіки. Злочинці не будують міста власноруч. Вони не виробляють бетон, не проєктують вентиляцію, не укладають кредитні угоди. Вони купують ці послуги. І вони купують їх у відкриту, часто за ринковими цінами, іноді — з премією за складність умов. Ланцюг постачання скам-індустрії — це не підпільний ринок, це частина глобальної економіки. І поки архітектори проєктуватимуть

в’язниці під виглядом курортів, банки кредитуватимуть сумнівні мегапроєкти без належної перевірки бенефіціарів, а будівельні компанії возитимуть бетон до таборів примусової праці, цей ланцюг залишатиметься замкненим.

Рекомендовані матеріали

Санкційний лабіринт G7/ЄС: Від геополітичної асиметрії до операційного паралічу та феномену Overcompliance [11]



Даний випуск Eastern European Journal of Transnational Relations є фундаментальною збіркою академічних та практичних досліджень, що деконструюють сучасну архітектуру санкційного комплаєнсу через призму правових колізій, геополітичних дилем та операційних провалів. Документ виходить за межі декларативного опису санкційних режимів, фокусуючись на "сірих зонах" імплементації, де політична воля G7 стикається з реаліями національних юрисдикцій та бізнес-процесів. Центральним наративом збірки є теза про трансформацію санкцій з інструменту зовнішньої політики в домінуючий механізм глобального економічного управління, що створює феномен "де-факто екстериторіальності" навіть для тих режимів (як-от ЄС), які де-юре заперечують таку концепцію.

Геополітична асиметрія та "Дилема третіх країн". Аналіз Кінги Редловської (RUSI) вводить концепт "економічної безпеки" як ключового фактора, що визначає поведінку третіх країн (Глобального Півдня) у відповідь на санкції G7. Дослідження розкриває механізм трансляції санкційного тиску через глобальну фінансову інфраструктуру. На прикладі Вірменії та Південної Африки (ПАР) продемонстровано, як "атмосфера регуляторної невизначеності" та загроза втрати кореспондентських відносин з банками США змушують нейтральні держави імплементувати західні обмеження. У випадку Вірменії, попри зростання торгівлі з РФ з $2.6 млрд до $12.4 млрд, банківський сектор змушений застосовувати жорсткі фільтри через страх вторинних санкцій, навіть за відсутності прямих юридичних зобов'язань. Специфічним є кейс дочірнього банку ВТБ у Вірменії, який функціонує в умовах ізоляції від SWIFT, обслуговуючи локальні потоки в рублях, що створює паралельну фінансову реальність. Щодо ПАР, аналіз вказує на розрив між політичною риторикою уряду (нейтралітет, БРІКС) та операційною практикою банків, які через інтеграцію в доларову систему змушені застосовувати overcompliance, де-факто приєднуючись до санкцій G7 всупереч національній політиці.

Тематичні санкції та ілюзія пріоритетності (Magnitsky Acts). Дослідження Орнелли Белфіорі критично оцінює ефективність глобальних режимів санкцій за порушення прав людини та корупцію (Закони Магнитського). Автор аргументує, що попри гучну риторику, боротьба з корупцією ніколи не була реальним пріоритетом санкційної політики, поступаючись геополітичним цілям (зокрема, протидії РФ). Статистика демонструє разючий дисбаланс: менше 500 визначених осіб за корупцію глобально проти тисяч фігурантів у списках по Росії. Аналізуються структурні проблеми імплементації: відсутність механізмів конфіскації перетворює замороження активів на тимчасовий захід, а слабка координація між санкційними органами та кримінальною юстицією дозволяє професійним посередникам успішно

[11] https://eejtr.uwb.edu.pl/issue/view/155

реструктурувати активи через офшорні трасти до моменту накладення санкцій. Це підтверджує тезу про епізодичність та вибірковість застосування тематичних санкцій.

Операційна асиметрія: AML vs Санкції. Даміан Кеммерер пропонує глибокий технічний аналіз інституційної незрілості санкційного комплаєнсу порівняно з режимами ПВК/ФТ. У той час як AML базується на деталізованих директивах, типологіях та стандартах FATF, санкційний комплаєнс в ЄС залишається фрагментованим і реактивним. Ключовий кейс дослідження описує ситуацію в європейському банку середнього розміру, клієнти якого потрапили до списку OFAC. Банк опинився в ситуації "контрактного паралічу": європейське законодавство не визнає екстериторіальні санкції США як легальну підставу для розірвання відносин, тоді як продовження обслуговування загрожувало втратою доступу до доларового клірингу. Банк був змушений піти на свідоме порушення контракту (замороження рахунків без прямої юридичної підстави в ЄС), щоб уникнути екзистенційних ризиків. Цей прецедент ілюструє критичний розрив між юридичними зобов'язаннями за правом ЄС та ризик-менеджментом. Аналіз Директиви (ЄС) 2024/1640 вказує на спробу інтегрувати санкції в структуру AML, проте відсутність єдиних стандартів скринінгу та нагляду залишає банки сам на сам з дилемою.

Нідерландський наглядовий експеримент та судова практика. Катажина Макнотон детально розбирає еволюцію нідерландського підходу, що базується на застарілому Sanctions Act 1977 та переході до нової моделі через закон WIS. Унікальність нідерландської моделі полягає у домінуванні кримінального переслідування (через Economic Offences Act - WED) та застосуванні доктрини *kleurloos opzet* ("безбарвний намір"). Згідно з цією доктриною, для доведення умислу достатньо факту свідомого вчинення дії, навіть без усвідомлення її протиправності. Це радикально знижує поріг доказування для прокуратури.

Ключові судові кейси формують нову правову реальність:

1. **Справа Dieseko:** Компанія сплатила €1.78 млн за участь у будівництві Кримського мосту. Прокуратура довела, що надання технічної підтримки на місці (навіть після продажу обладнання через фінського посередника) є прямим порушенням, відкидаючи аргумент про "непрямий продаж".
2. **Справа ABN AMRO:** Суд визнав, що банк порушив "обов'язок дбайливого ставлення" (duty of care), закривши рахунки клієнта лише на підставі підозр у зв'язках з РФ без належних доказів. Це створює прецедент, де duty of care виступає запобіжником проти бездумного de-risking.
3. **Справа Cicerone:** Суд дозволив примусову передачу акцій підсанкційної особи (Todwick) через механізм консигнації, фактично ігноруючи рекомендації Єврокомісії щодо можливості добровільного переказу. Це рішення базувалося на синергії санкцій ЄС та українського антикорупційного законодавства, що демонструє пріоритет національних інтересів безпеки над корпоративними процедурами.

Феномен Overcompliance як системна функція. Фредерік ван Ессен концептуалізує "надмірний комплаєнс" не як помилку, а як вбудовану характеристику режиму санкцій ЄС. Закони ЄС вимагають від бізнесу гарантованого результату (щоб порушення не сталося), а не просто дотримання певної процедури перевірки. Оскільки ніхто не може дати 100% гарантії, компанії змушені бути параноїдально обережними, щоб уникнути будь-яких ризиків. Відсутність чітких інструкцій (на кшталт "Safe Harbor" в США) змушує компанії самостійно калібрувати ризики, що в умовах невизначеності призводить до відмови від легальних транзакцій. Автор посилається на справу *Jemerak* (CJEU), де нотаріус відмовився посвідчувати угоду через теоретичний ризик надання "юридичних консультацій" підсанкційній особі, що ілюструє параліч через страх відповідальності.

Інші новини

Найгучніші арешти злочинців у 2025 році [12]

Рік 2025 увійде в історію боротьби з транснаціональною організованою злочинністю як час великого очищення. Але чи означають ці арешти кінець епохи безкарності? Чи, навпаки, вони лише підтвердили, що наркобізнес перетворився на системо-утворюючий фактор політики та економіки в регіоні, де держави часто програють війну, яку навіть не завжди готові визнати?

Історія Хосе Адольфо Масіаса Вільямара, відомого як «Фіто», — це не просто кримінальна біографія. Це літопис того, як пенітенціарна система перетворилася на інкубатор злочинних синдикатів. Уявіть собі: людина, яка 2013 року втекла з в'язниці Ла-Рока, потрапила туди знову, і попри це зберегла контроль над одним із найпотужніших угруповань Еквадору. Коли в січні 2024 року охоронці знайшли його камеру порожньою — напередодні планового переведення — стало очевидно, що система згнила не лише зовні, а й зсередини. Втеча Фіто стала каталізатором наймасштабнішої кризи в історії сучасного Еквадору. Президент Даніель Нобоа, опинившись перед обличчям хаосу, коли бойовики брали в заручники телестудії в прямому ефірі, змушений був визнати: держава воює не з бандитами, а з терористичною армією. Оголошення «внутрішнього збройного конфлікту» стало юридичним проривом — уперше армія отримала мандат на ведення контртерористичної кампанії всередині країни без огляду на традиційні обмеження. Фіто переховувався півтора року. Його знайшли не в нетрях джунглів, а в розкішному бункері під елітним маєтком на околиці рідного міста Манта. Цей символізм промовистий: злочинність більше не ховається на маргінесі. Вона інтегрувалася в елітне житло, вона володіє нерухомістю, вона їсть ту саму їжу, що й політики. І коли Фіто менш ніж за місяць екстрадували до США, це стало не просто актом правосуддя, а геополітичним меседжем: Вашингтон повертає собі роль верховного арбітра, вириваючи ключових гравців із юрисдикції слабких держав.

Але Фіто — лише одна сторінка. Його колишній союзник, а згодом заклятий ворог Вільмар Чаварріа Барре, більш відомий як «Піпо», уособлює зовсім інший типаж злочинця. Якщо Фіто спирався на силу в'язничної ієрархії, то Піпо зробив ставку на мобільність, трансформацію та міжнародний шик. Його кар'єра починалася буденно — грабунок банків у Куенці. Але за ґратами його помітив легендарний лідер «Чонерос» Хорхе Луїс Самбрано, відомий як Раскін. В'язниця стала бізнес-школою, де Піпо опанував науку управління злочинними активами. Коли Раскіна вбили в грудні 2020 року, Піпо вивів своє угруповання «Лобос» із коаліції. Те, що сталося далі, — кривавий переділ ринку, який за один лютий 2021 року забрав життя 79 ув'язнених у в'язницях Гуаякіля, Куенки та Латакунги. Піпо скористався хаосом, щоб інсценувати власну смерть. Сім пластичних операцій, підроблене свідоцтво про смерть, втеча через Венесуелу й Колумбію до Іспанії — він створив собі нове обличчя й нове життя. Дубайські хмарочоси, люксові готелі Марбельї, командування групами кіллерів з відстані тисяч кілометрів. Саме в цей період, за даними слідства, «Лобос» могли бути причетними до вбивства кандидата в президенти Фернандо Вільявісенсіо — злочину, що сколихнув усю Латинську Америку. Піпо вважав, що переміг систему. Але система вміє чекати. Його видав звичайний прикордонний контроль при в'їзді з Марокко до Іспанії: підроблені документи, автоматична перевірка,

[12] https://insightcrime.org/news/top-criminal-takedowns-of-2025/

спрацювання бази даних. Листопад 2025 року, Малага. Кінець семилітньої голлівудської кар'єри. Піпо чекає екстрадиції в іспанській камері. Його справа — переконливе свідчення того, що жодна пластика не приховує відбитків злочинної волі.

Якщо Піпо — це історія про міжнародний розмах еквадорської мафії, то Дрітан Гіка, відомий як «Тоні», — проникнення чужоземного капіталу в стратегічні галузі латиноамериканської економіки. Гіка — албанець. Він прибув до Еквадору 2009 року за короткостроковою візою, а за півтора десятиліття побудував транснаціональний конгломерат із відмивання грошей і контрабанди кокаїну до Європи. Його геніальність полягала не в тому, щоб тримати в руках автомати, а в тому, щоб тримати в руках олівці. Гіка купував не території, а людей. Його партнерами стали швагер президента Гільєрмо Лассо, високопоставлені офіцери поліції, впливові бізнесмени. Він майстерно уникав прямого зв'язку з наркоактивами, створюючи горизонтальну мережу підставних компаній. Скандал вибухнув 2023 року, коли журналістські розслідування оприлюднили зв'язки Гіки з оточенням президента. Політичні наслідки виявилися фатальними для Лассо — йому оголосили імпічмент. Сам Гіка втік із країни в день публікації однієї з ключових доповідей. Його переслідували через Туреччину, доки 26 травня 2025 року в Абу-Дабі не спрацював механізм Інтерполу. Справа Гіки — класичний приклад «гібридної злочинності», де бізнес, політика і наркотрафік утворюють нерозривний клубок, розплутати який можна лише спільними зусиллями десятків країн.

Зовсім інший контекст — гватемальсько-мексиканське прикордоння. Алер Самайоа Рекінос, «Чічарра», належав до тої категорії наркобаронів, які десятиліттями балансували між криміналом і легітимністю. Його угруповання «Уїстас» контролювало гірські перевали департаменту Уеуетенанго — стратегічний коридор, через який кокаїн із Південної Америки потрапляв до Мексики, а звідти до США. Шість років Чічарра перебував у списку найбільш розшукуваних злочинців за версією Вашингтона. Його не могли взяти через тотальний захист місцевих громад і корумпованість силових структур. У листопаді 2024 року операція мало не увінчалася успіхом, але Чічарра вислизнув. Його затримали у квітні 2025-го в торговому центрі мексиканського міста Тустла-Гутьєррес. Сцена арешту не мала нічого спільного з бойовиками: поліціянти ввічливо попросили його пройти, не вдягали кайданки, називали «доброю людиною». Сам Чічарра згодом дякував їм за чемність. Ця картина — дзеркало глибокої інтеграції злочинності в соціальний ландшафт. Тут немає героїчних перестрілок. Є буденність: багатий бізнесмен іде з охоронцями, а потім чемно сідає в поліцейську машину. Екстрадиція до США відбулася за лічені тижні.

Колумбійський кейс Хеовані Андреса Рохаса, «Арани», додає до цієї мозаїки ще один тривожний елемент — кризу мирного процесу. «Командос де ла Фронтера» — це угруповання, що сформувалося з уламків FARC після демобілізації 2016 року. Колишні партизани, які не склали зброю, об'єдналися з колишніми парамілітарес, щоб контролювати врожаї коки в Путумайо. 2022 року вони сіли за стіл переговорів із урядом Густаво Петро. Арана був головним переговірником, обличчям «нового» злочинного світу, готового торгувати амністію в обмін на інформацію та здачу позицій. Його арешт 12 лютого 2025 року просто під час пресконференції в готелі Courtyard Marriott у Боготі став холодним душем. Уряд розвів руками: ордер Інтерполу, ініційований США, не підпадає під національні домовленості. Цей епізод продемонстрував трагічну суперечність: для Колумбії Арана — партнер по діалогу, для США — злочинець, який контрабандою відправляє кокаїн до кордонів Техасу.

Однак найбільш промовистим, найбільш символічним і, безперечно, найболючішим ударом 2025 року став арешт Селсо Гамбоа Санчеса. Якщо Фіто — це король в'язниць, Піпо — тінь, що змінює обличчя, Гіка — іноземний інвестор, а Арана — переговірник, то Гамбоа Санчес — це держава. Колишній міністр громадської безпеки, заступник генерального прокурора, магістрат Верховного суду Коста-Рики. Людина, яка десятиліттями формувала правову політику країни, карала злочинців і виносила вироки. Виявилося, що він координував регіональну мережу з

постачання кокаїну для клану дель Гольфо та картелю Сіналоа. Його падіння почалося 2017 року зі скандалу «Ель Сементасо», коли Гамбоа просував інтереси будівельного магната Хуана Карлоса Боланьйоса, який отримав понад 30 мільйонів доларів сумнівних кредитів. Тоді його вперше в історії Коста-Рики звільнили з Верховного суду за вплив на правосуддя. Але справжній масштаб зради розкрився лише через вісім років, коли у червні 2025-го його заарештували в Сан-Хосе за звинуваченням у змові з метою розповсюдження кокаїну. Гамбоа Санчес став живим утіленням феномену, коли правоохоронна система не просто дає збій, а сама перетворюється на інструмент злочинності. Його справа збіглася в часі з ухваленням конституційної поправки, що дозволила екстрадицію громадян Коста-Рики за наркозлочини. Вашингтон негайно зажадав його видачі, але поки що він залишається на батьківщині — під слідством у справах про підробку документів і хабарництво.

Аналізуючи ці шість історій, InSight Crime фіксує зсув тектонічних плит. 2025 став роком, коли латиноамериканська організована злочинність пройшла повний цикл еволюції. Вона починалася як вуличне хуліганство, перетворилася на тюремні братства, потім — на транснаціональні корпорації, а нині інтегрувалася в політичні еліти та судову гілку влади. Фіто — це минуле. Піпо — теперішнє. Гамбоа Санчес — майбутнє, яке вже настало. І це майбутнє лякає, бо розмиває межу між злочинцем і правоохоронцем. Арешти 2025 року стали можливими завдяки безпрецедентній міжнародній координації. США повернули собі ініціативу, використовуючи екстрадицію як головну зброю стримування. Іспанія, ОАЕ, Туреччина, Мексика, Гватемала, Еквадор, Колумбія — усі вони об'єднали зусилля, розуміючи, що поодинці цього ворога не подолати. Але чи достатньо цього?

Як мережа тіньових фірм освоювала державні тендери Узбекистану [13]

Коли на початку лютого 2026 року світ побачило розслідування OCCRP та Finance Uncovered, воно не просто зафіксувало черговий факт корупції, воно оголило механізм, за допомогою якого державні кошти однієї з найбільш закритих економік Центральної Азії безперешкодно перетікають через найпрозоріші юрисдикції світу, залишаючи за собою лише слід зі «сплячих» компаній.

У центрі історії опинився Алмалицький гірничо-металургійний комбінат, державний гігант, що формує дев'ять відсотків усіх податкових надходжень Узбекистану, підприємство, яке президент Шавкат Мірзійоєв називає «перлиною» економіки і готує до публічного розміщення акцій на закордонних біржах.

Британський реєстр компаній Companies House десятиліттями вважався зразком відкритості, але останніми роками дедалі частіше лунають закиди, що ця відкритість існує лише на рівні форми, а не змісту. Історія Lemixon Solutions Ltd та Golders Business Ltd стала чи не найкращою ілюстрацією цього парадоксу. Обидві фірми, зареєстровані за однією адресою в Лондоні, старанно подавали звіти про власну «сплячку» — статус, який передбачає цілковиту відсутність будь-якої економічної діяльності. Жодних транзакцій, жодних працівників, жодних прибутків.

[13] https://www.occrp.org/en/investigation/uzbek-state-crown-jewel-hands-200m-in-tenders-to-secretive-foreign-firms

Саме так вони описували своє існування в офіційних документах, і саме так вони, згідно із законом, не мали права отримувати жодного доходу.

Але поки папери мовчали, портові термінали фіксували інше. Від 2022 року Lemixon виграв не менш як 56 тендерів АГМК на суму понад 22 мільйони доларів. Golders відстав не набагато, додавши до спільного гаманця ще 13 мільйонів. Сталеві труби, алюмінієві листи, промислове обладнання — десятки вантажів перетнули кордони, аби потрапити на склади узбецького монополіста. І все це — від фірм, які юридично вважалися недіючими. Парадокс, який став можливим лише тому, що ніхто не перевіряв, чим насправді займаються ці компанії, допоки журналісти не почали ставити запитання.

Найпоказовішим у цій історії став навіть не сам факт постачання, а реакція системи на зовнішнє втручання. Щойно OCCRP та Finance Uncovered надіслали свої запити, лондонські реєстраційні форми почали змінюватися з небаченою швидкістю. Венді Конрой, літня бухгалтерка, яка ніколи не мала жодного стосунку до Центральної Азії чи гірничої промисловості, зникла з графи «особа зі значним контролем». Натомість з’явився Григорій Хван, 61-річний бізнесмен, відомий насамперед як віцепрезидент Федерації настільного тенісу Узбекистану та власник елітного тенісного клубу під Ташкентом. У документах зазначалося, що він контролює Lemixon ще з 20 листопада 2018 року. Минуло лише кілька тижнів, і Хвана змінив колумбієць Феліпе Герреро, чиє призначення так само датували 2018 роком. Та сама послідовність подій, ті самі дати, ті самі імена — усе це повторювалося і в Golders Business, і в пов’язаній із ними Alrick Solutions Limited. Представник MoreGroup, фірми, яка адмініструвала всі ці компанії, пояснив, що Венді Конрой «ніколи не мала бути внесеною» як контролер, і що «одна особа» стоїть за всіма цими структурами. Імені цієї особи він не назвав, але хронологія подальших подій не залишала сумнівів, ким вона є.

Григорій Хван постає в цьому розслідуванні фігурою, чий вплив простягається далеко за межі тенісного корту. Його клуб відвідували південнокорейські парламентарі, там гостював Отабек Умаров, зять самого президента Мірзійоєва, колишній заступник голови служби безпеки, а нині високопосадовець Олімпійського комітету. Сам Хван у 2023 році отримав з рук президента нагороду «активного підприємця» за внесок в економіку. Він не публічна особа в класичному розумінні, його ім’я маловідоме за межами професійних кіл, але саме воно виринає в кожному епізоді цієї багатоходової схеми. Його син Олексій підписує угоду про купівлю квартири на Манхеттені за 4,4 мільйона доларів від імені багамської компанії Colcot Company Ltd, де Григорій Хван є директором. Сам Григорій Хван на запитання журналістів не відповідає. Його син, почувши ім’я батька, спершу каже, що співрозмовник помилився номером, а потім із паузою запитує: «Григорій — хто це?».

Але повернімося до документів. Серед десятків контрактів, укладених Lemixon та Golders із АГМК, щонайменше тринадцять містять підписи людей, які запевняють, що ніколи їх не ставили. Сім договорів на суму 6,2 мільйона доларів підписані факсиміле Венді Конрой. Найпізніший із них датований 5 грудня 2025 року — тобто через три дні після того, як Конрой офіційно вивели зі складу контролерів Lemixon. Керівництво MoreGroup запевняє, що вона «на сто відсотків» не підписувала цих паперів. Ще шість контрактів Golders на суму 1,4 мільйона доларів містять підпис Руайрі Лафліна-Макканна, колишнього співробітника тієї ж MoreGroup. Сам Лафлін-Макканн заявляє, що не має жодного стосунку до Golders понад п’ять років, і що він «категорично не підписував» жодного з цих документів. Один із контрактів датований 25 листопада 2025 року і все ще ідентифікує його як директора компанії. Лафлін-Макканн уже звернувся до лондонської поліції. Він називає ситуацію «немислимою», адже такий договір, за його словами, мав би пройти щонайменше мінімальну перевірку, під час якої невідповідність підпису та статусу особи була б очевидною. Однак АГМК ці договори прийняв, оплатив і, схоже, не ставив жодних запитань.

Грузинський сегмент схеми вирізняється особливою цинічністю використання так званих «прокладок». Тут головною дійовою особою стала Поліна Останова, 41-річна громадянка Південної Кореї з узбецьким корінням. Уся її професійна кар'єра пов'язана з медичним туризмом: вона допомагала клієнтам організовувати лікування за кордоном, засновувала відповідні компанії, але ніколи не мала жодного стосунку до промисловості, логістики чи великих експортних поставок. Попри це, саме вона в лютому 2025 року придбала п'ять грузинських компаній, серед яких LOSBP LLC та Prof Engineering LLC. Продавцем виступив казахстанець Рахат Науризбеков, який свого часу заснував ці фірми за 350 доларів. Останова заплатила ту саму суму. На момент угоди дві з цих компаній уже мали на руках підтверджених тендерів від АГМК на 65,9 мільйона доларів. Тобто жінка без досвіду, без активів, без жодної репутації в галузі придбала фірми, які вже виграли десятки мільйонів державних коштів. І це не викликало жодних запитань ані в узбецької сторони, ані в грузинських реєстраторів.

Більше того, ці грузинські компанії, отримавши мільйонні підряди та здійснивши численні поставки, так само, як і їхні британські «конкуренти», жодного разу не подали фінансової звітності. Вони декларували відсутність доходів, хоча насправді вели активну торгівлю. Грузинська податкова служба підтвердила, що за наявності прибутку такі дії є порушенням, але відсутність звітів не завадила Остановій продовжувати володіти компаніями, а АГМК — укладати з ними нові угоди. Формально ці грузинські фірми конкурували з британськими за ті самі лоти, створюючи ілюзію ринкової боротьби. Насправді ж усі вони управлялися з одного центру.

Прямих юридичних зв'язків між Остановою та Хваном на папері не було, але соціальні мережі відкрили все. Останова вподобала пости цивільної дружини Хвана. Вона ж виявилася тісно пов'язаною з Феліпе Герреро, тим самим колумбійцем, якого заднім числом призначили контролером британських Lemixon та Golders. Їхнє спільне фото в Самарканді, вподобайки постів автодилера Unicos Cars, де Герреро вказаний контактною особою, спільне представництво корейського косметичного бренду — усе це склало картину, в якій випадкових збігів більше не залишилося.

Сінгапурський напрям виявився найбільш фінансово ємним. Три компанії — Polisteel Solutions Pte Ltd, Ventopro Pte Ltd та Mek Industrial Technology Pte Ltd — сумарно отримали підрядів на понад 102,9 мільйона доларів. Номінальним власником усіх трьох значиться південнокореєць Седонг Чой. Але публічні документи китайської компанії Denair, виробника промислового обладнання, містять згадку, що вони співпрацюють із Mek Industrial Technology через представника, який одночасно пов'язаний із багамською Colcot Company Ltd. А в Colcot директором є Григорій Хван. Після запитів журналістів Denair надіслав уточнення: мовляв, згадка в звітності стосувалася лише того факту, що обидві компанії використовували одного й того самого представника, і про бенефіціарів їм нічого не відомо. Адвокат сінгапурських фірм Марк Лудвіковскі, який працює в Clark Hill Public Strategies і має лобістський контракт із Mek Industrial Technology, запевняє, що Хван не є ані власником, ані контролером цих компаній.

АГМК, який у жовтні 2025 року отримував нагороду на державному антикорупційному форумі за досягнення у сфері прозорості, на запити OCCRP не відповів. На власному сайті комбінат досі наголошує, що «відданий принципам прозорості та підзвітності в управлінні природними ресурсами». Адміністрація президента Мірзійоєва також не відреагувала на звернення журналістів. Мовчать Григорій Хван, Поліна Останова, Седонг Чой, Рахат Науризбеков. Єдиний, хто зробив бодай якусь дію, — це колишній бухгалтер Руайрі Лафлін-Макканн, який самостійно звернувся до британських правоохоронців. Лондонська поліція, посилаючись на захист персональних даних, не підтверджує факт звернення без згоди заявника.

Це розслідування не є історією про «недобросовісних постачальників», яких випадково допустили до державних тендерів. Це історія про системну неспроможність захисту державних

коштів там, де мала б працювати багаторівнева система перевірок. Британський реєстр Companies House, який реформували саме для боротьби з фіктивними фірмами, досі працює за принципом «зареєструй що завгодно, а ми перевіримо, якщо хтось поскаржиться». І навіть коли скарга надходить, виправити дані можна заднім числом, створивши ілюзію, що все завжди було правильно. Грузинський корпоративний сектор, який позиціонує себе як відкритий для інвестицій, дозволяє перепродувати фірми з мільйонними контрактами за 350 доларів людям без жодного досвіду. Узбецький державний гігант, який готується до міжнародного IPO, не помічає, що його контрагенти не звітують про прибутки, не мають сайтів, не ведуть діяльності, а їхні підписи на документах є підробленими.

Понад 200 мільйонів доларів, розпорошених між Лондоном, Тбілісі, Сінгапуром і Нассау, — це не просто збитки бюджету Узбекистану. Це плата за ілюзію прозорості, яку досі купують міжнародні інвестори, дивлячись на гарні звіти та урядові стратегії. Реальність виявляється іншою: за лаштунками державних корпорацій досі діють кланові мережі, які не потребують ані досвіду, ані репутації, ані навіть підписів реальних людей. Їм достатньо вчасно змінити прізвище в реєстрі, поставити факсиміле і дочекатися, поки стихне хвиля журналістських запитів.

Для загального розвитку

Архітектура єдиного нагляду ЄС: Імплементація "Single Rulebook", розширення периметра СПФМ та уніфікація штрафних санкцій [14]

Даний документ є стратегічним технічним роз’ясненням, виданим новоствореним Органом з протидії відмиванню коштів та фінансуванню тероризму (AMLA), що базується у Франкфурті. Він деконструює архітектуру нової загальноєвропейської системи фінансового моніторингу, яка набуде чинності 10 липня 2027 року. Документ має критичне значення для розуміння переходу від директивного регулювання (де кожна країна-член ЄС імплементувала правила з національними варіаціями) до уніфікованого Регламенту (Single Rulebook), що має пряму дію. Основний фокус матеріалу зосереджено на радикальному розширенні периметра СПФМ у нефінансовому секторі та уніфікації наглядових методологій, що має на меті ліквідувати регуляторний арбітраж всередині Європейського Союзу.

Інституційна трансформація та кінець фрагментації. Фундаментальною передумовою реформи, окресленою в документі, є визнання провалу децентралізованої моделі нагляду. Поточна фрагментація правил між державами-членами створила системні вразливості, якими користуються транскордонні злочинні мережі. AMLA позиціонується не просто як координатор, а як архітектор єдиного наглядового простору. Хоча безпосередній нагляд за ВНУП залишатиметься на національному рівні, AMLA отримує мандат на розробку "спільної методології нагляду". Це означає, що національні регулятори втрачають дискрецію у трактуванні ризиків та визначенні тяжкості порушень. Вони будуть зобов'язані оцінювати піднаглядні суб'єкти за єдиними метриками, розробленими у Франкфурті, що фактично запроваджує стандарт екстериторіальної якості нагляду.

Розширення периметра підзвітних суб’єктів. Документ кодифікує значне розширення переліку професій та бізнесів, що підпадають під регулювання. Окрім традиційних категорій (аудитори, бухгалтери, податкові консультанти, нотаріуси, рієлтори, TCSP, торгівці коштовними металами),

[14] https://www.amla.europa.eu/document/download/8c01459a-1769-47d0-9c21-b2c8fdb7d2b7_en?filename=AMLA%20Explainer%20-%20Non-Financial%20Sector%20in%20AML_CFT.pdf

до периметра вперше на рівні ЄС вводяться нові гравці. Особливу увагу приділено сектору професійного футболу (клуби та агенти), для якого встановлено відтермінований дедлайн імплементації – 10 липня 2029 року. Це рішення відображає високий ризик використання трансферного ринку для відмивання коштів через непрозорі структури власності та завищені оцінки вартості гравців. Також до списку включено операторів інвестиційної міграції ("золоті візи"), краудфандингові платформи, кредитних посередників та торгівців культурними цінностями. Важливим нюансом є включення посередників, що оперують у вільних портах (free ports) та митних складах, що закриває давню прогалину у контролі за переміщенням товарів мистецтва та антикваріату.

Технічна дорожня карта та консультації 2026 року. Найбільш аналітично цінною частиною документа є деталізований графік розробки Регуляторних технічних стандартів (RTS) та Імплементаційних технічних стандартів (ITS), які перетворять загальні норми закону на операційні інструкції. Цей графік на 2026 рік розкриває логіку майбутнього комплаєнсу. По-перше, **гармонізація правил (AMLR - Anti-Money Laundering Regulation)**. У першому кварталі 2026 року будуть визначені чіткі стандарти належної перевірки клієнтів (CDD) згідно зі статтею 28(1) AMLR. Це покладе край ситуації, коли вимоги до ідентифікації бенефіціара у Німеччині та на Кіпрі відрізнялися. У третьому кварталі 2026 року будуть встановлені вимоги до загальнокорпоративної оцінки ризиків (Business-wide risk assessment) та моніторингу транзакцій. Це свідчить про зміщення фокусу з формальної ідентифікації на динамічний ризик-менеджмент. По-друге, **групові політики та треті країни**. Стаття 17(3) AMLR, що буде роз'яснена у другому кварталі 2026 року, стосується дій груп компаній у випадках, коли законодавство третьої країни (наприклад, офшорної юрисдикції або РФ) забороняє імплементацію стандартів ЄС. Це критичний момент для міжнародних холдингів, яким, ймовірно, доведеться обирати між виходом з ринку або порушенням вимог ЄС.

Уніфікація нагляду та санкцій. Документ анонсує розробку єдиної методології оцінки "тяжкості порушень" (Gravity of AML/CFT obligation breaches, стаття 53(10) AMLD) та базових сум грошових штрафів (стаття 53(11) AMLD). Це революційна зміна для європейського правового простору. Раніше за одне й те саме порушення (наприклад, неподання звіту про підозрілу транзакцію) у одній країні могли винести попередження, а в іншій – накласти мільйонний штраф. Нова система нівелює цей дисбаланс, запроваджуючи матрицю розрахунку штрафів, обов'язкову для всіх національних регуляторів. Також вводиться поняття "Supervisory Colleges" для нефінансового сектору (стаття 50(13) AMLD), що інституалізує транскордонну співпрацю наглядових органів для контролю за групами, які оперують у кількох юрисдикціях (наприклад, мережі агентств нерухомості або аудиторські фірми "Великої четвірки").

Централізація даних та звітності. Важливим елементом архітектури є створення центральної бази даних AML/CFT (стаття 11(6) AMLAR). Національні регулятори будуть зобов'язані передавати інформацію до цієї бази, що дасть AMLA можливість бачити макро-тренди та виявляти бездіяльність локальних наглядачів. Крім того, стандартизується формат звітування про підозрілі транзакції (стаття 69(3) AMLAR). Це вирішує проблему несумісності даних між різними підрозділами фінансової розвідки, що роками блокувало ефективний обмін інформацією. Для бізнесу це означає необхідність адаптації своїх IT-систем до єдиного європейського стандарту звітності, який буде визначено до кінця 2026 року.

Юридична природа змін: AMLR проти AMLD. Аналіз посилань у документі чітко розмежовує сфери прямої дії та національної імплементації. Більшість вимог до бізнесу (CDD, моніторинг, політики) посилаються на **AMLR** (Regulation), що означає їх пряму дію без необхідності прийняття національних законів. Натомість питання повноважень наглядових органів та штрафів посилаються на **AMLD** (Directive), що залишає певний простір для національних процедур, але в жорстких рамках, визначених AMLA. Цей гібридний підхід дозволяє зберегти

національні правові традиції в адміністративному процесі, водночас уніфікувавши матеріальні вимоги до бізнесу.

Висновки щодо імплементації. Документ недвозначно вказує, що період до липня 2027 року не є часом очікування. Консультації 2026 року де-факто визначать фінальний вигляд вимог. Для суб'єктів нефінансового сектору, особливо нових (футбольні агенти, краудфандинг), це означає необхідність побудови систем комплаєнсу з нуля. Для традиційних суб'єктів (юристи, аудитори) це сигнал про кінець ери "м'якого" нагляду через професійні саморегулівні організації, оскільки методологія нагляду тепер диктуватиметься централізованим органом ЄС, орієнтованим на жорсткі фінансові стандарти.

Алгоритми беззаконня: Як штучний інтелект озброює злочинність і випробовує правоохоронців [15]

Цифрова еволюція злочинності давно вийшла за межі стереотипних уявлень про хакерів. Як свідчить моніторинг, проведений InSight Crime, ми є свідками безпрецедентного синтезу вуличного бандитизму, кримінальних ієрархій та високотехнологічних інструментів, які ще п’ять років тому здавалися недосяжною розкішшю навіть для спецслужб. Штучний інтелект у цьому симбіозі виступає не просто зручним додатком, а потужним каталізатором, що змінює саму природу кримінального промислу.

Найбільш показовим, навіть символічним явищем цього року стало так зване «вайб-кодинг». Цей неологізм, що народився в Кремнієвій долині, описує процес, за якого людина без формальної технічної освіти може створити працездатний програмний продукт, просто спілкуючись із великою мовною моделлю (LLM). Ти описуєш чат-боту, який додаток хочеш отримати, він генерує код, ти копіюєш його, запускаєш, отримуєш помилки, вставляєш їх назад у чат — і так по колу, доки програма не запрацює. Феномен, який виник як демократизація програмування для стартапів і креативних індустрій, стрімко мігрував у кримінальне середовище. І це логічно. Якщо вайб-кодинг дозволяє за вечір створити мобільний застосунок для доставки піци, чому воно не може створити застосунок для крадіжки банківських даних?

Технологічні компанії встановлюють захисні бар'єри — фільтри, які блокують запити на створення шкідливого коду. Але ці бар'єри працюють за принципом пошуку ключових слів. Їх можна обійти евфемізмами, метафорами, непрямими описами. Якщо ти не просиш «написати вірус», а просиш «створити скрипт для тестування корпоративної безпеки, який імітує підозрілу активність», система часто пропускає запит.

Однак справжній прорив відбувся на рівні ШІ-агентів — автономних програмних систем, здатних самостійно ставити цілі, обирати інструменти для їх досягнення та виконувати послідовні дії без втручання людини. Інцидент із системою Claude від компанії Anthropic, яка виявила та зупинила кібер-атаку ШІ-агентів, став історичною віхою. Ми вперше побачили злочин без злочинця. Без оператора, який сидить за клавіатурою. Алгоритм самостійно сканував мережі, виявляв уразливості, тестував вектори атак, адаптувався до захисних механізмів і масштабував інфікування. Якщо раніше хакерські угруповання потребували десятків, а то й

[15] https://insightcrime.org/news/organized-crime-and-ai-5-topics-we-are-monitoring-in-2026/

сотень високооплачуваних фахівців, то тепер невелика група — п’ятеро, десятеро людей — може налаштувати такого агента і спостерігати, як він нищить цифрову інфраструктуру супротивника. І що найстрашніше: ця технологія стрімко дешевшає.

Особливу тривогу в експертному середовищі викликає не стільки складність окремих атак, скільки колосальне розширення поверхні ураження. У світі вже понад 30 мільярдів підключених пристроїв. І майже всі вони вразливі. ШІ робить мішенню все, що має мікропроцесор і вихід у мережу. Холодильники, які замовляють продукти онлайн. Розумні колонки, які слухають розмови вдома. Дитячі іграшки з функцією розпізнавання голосу. Камери відеоспостереження, які виробляються з дефолтними паролями «admin/admin». Медичні імпланти, які передають телеметрію лікарю. Виробники цих пристроїв економлять на кібербезпеці, бо ринок вимагає дешевизни. В результаті мільярди «розумних» девайсів стають ідеальним плацдармом для ботнетів. Злочинці більше не витрачають роки на злам банківських систем у лоб. Вони проникають через «розумний термостат» у приймальні, звідти — через Wi-Fi — у внутрішню мережу офісу, звідти — на сервер з базою даних.

Але було б наївно вважати, що ШІ загрожує нам виключно у віртуальній площині. Паралельно з кібер-виміром відбувається не менш небезпечна, хоча менш помітна для широкої публіки, інтеграція нейромереж у так звані «традиційні» злочинні схеми. Цей процес нагадує гібридну війну. Перші ластівки з'явилися в Перу, де класична схема вимагання, відома як «seco y saco» або фальшиве викрадення, вийшла на технологічний рівень. Раніше шахраї телефонували сім'ям і панічним голосом кричали: «Я тримаю вашу доньку, платіть негайно». Це спрацьовувало, але грубо. Сьогодні більше не потрібно кричати. Достатньо трьох секунд голосу жертви, які легко знайти в Instagram, TikTok або YouTube. Нейромережі сьогодні здатні імітувати не просто набір частот, а інтонацію, тембр, дихання, манеру робити паузи між словами, навіть легку шепелявість. Матері отримують дзвінки від власних «доньок», які схлипують і благають про порятунок. Вони чують рідний голос, і їхній мозок відключає критичне мислення. Вони переказують гроші. А донька тим часом спокійно спить у своєму ліжку або сидить на парах в університеті. Це злочин, який руйнує психіку жертви, підриває базову довіру до реальності, до власних відчуттів. І при цьому він майже не залишає слідів.

Бразилія, яка вже давно перетворилася на глобальний полігон для випробування нових форм злочинності, пішла значно далі. Місцеві угруповання опанували діпфейки в реальному часі — технологію, яка дозволяє підмінювати обличчя під час відео-дзвінка. Тепер, щоб зняти гроші з чужого рахунку, не потрібно красти картку чи підбирати пін-код. Достатньо мати фотографію жертви з соціальних мереж. ШІ будує 3D-модель обличчя, накладає її поверх обличчя зловмисника, і камера банкомату бачить «клієнта», який ніколи не приходив у відділення. Гроші зникають. Система фіксує успішну авторизацію.

І це лише перші кроки. Експерти з тривогою відзначають, що потужні синдикати — мексиканський картель Сіналоа, бразильське Перше столичне командування (PCC) — починають активно рекрутувати до своїх лав кіберзлочинців. Раніше ці два світи існували паралельно: наркоторговці контролювали вулиці та в'язниці, хакери контролювали даркнет. Сьогодні кордони стираються. За ґратами опиняється все більше технічно освічених молодих людей. Вони приносять із собою знання. Так народжуються альянси.

Наступний напрямок, який викликає дедалі більше занепокоєння серед аналітиків правоохоронних органів Європи та Америки, — це стрімка еволюція безпілотних літальних апаратів. Війна росії проти України стала не лише гуманітарною катастрофою та геополітичним землетрусом, але й, на жаль, наймасштабнішим у сучасній історії полігоном для випробування новітніх технологій убивства. Те, що відбувалося над окопами Донбасу та Херсонщини, не залишилося непоміченим кримінальним світом. Цивільні квадрокоптери, придбані в магазинах електроніки, перетворилися на високоточну зброю. Їх оснащують кустарними вибуховими

пристроями, скидають ними гранати. Латинська Америка, як завжди, виявилася напрочуд вправною в імпорті військових інновацій. Comando Vermelho в Ріо-де-Жанейро вже не перший рік використовує дрони для спостереження за пересуваннями поліції. Але 2026 року вони пішли далі: під час смертельної перестрілки з силами безпеки банда застосувала дрони-камікадзе, начинені вибухівкою.

Однак справжня небезпека не в самих дронах, а в тому, що комп'ютерний зір робить їх розумними. Раніше, щоб скинути бомбу, потрібен був оператор, який дивиться в екран і натискає кнопку. Людський фактор обмежував швидкість, масштаб і точність. Сьогодні алгоритми комп'ютерного зору досягли такого рівня, що дрон може самостійно ідентифікувати ціль: обличчя конкретного поліцейського, номерний знак автомобіля, маркування військової техніки. Він може супроводжувати ціль годинами, передаючи координати, або атакувати автономно, без жодного сигналу з центру управління.

На тлі цієї стрімкої експансії кримінального світу держави намагаються дати відсіч. Сканери, оснащені нейромережами, здатні побачити прихований кокаїн у щільності вантажу там, де людське око бачить лише банани. Аналітичні платформи можуть вираховувати приховані фінансові потоки наркомафії, відстежуючи крихітні аномалії в мільярдах транзакцій. Алгоритми прогнозування злочинності обіцяють надіслати патруль на вулицю за годину до того, як там станеться вбивство. Чилі вже використовує такі системи для виявлення злочинних мереж. Еквадор оголосив про впровадження ШІ проти контрабанди, незаконного видобутку корисних копалин та піратського рибальства. Навіть ООН закликає країни досліджувати ШІ як інструмент виявлення корупції.

Висновки:

- **ШІ розвиває високотехнологічну злочинність.** Автоматизація програмування та поява автономних ШІ-агентів дозволяють навіть аматорам створювати складне шкідливе ПЗ, а злочинним угрупованням — масштабувати атаки без людського втручання.
- **Фізична та цифрова злочинність зливаються воєдино.** Традиційні кримінальні практики підсилюються ШІ: від клонування голосів і підробки облич для обходу біометрії до автономних дронів-камікадзе з функціями комп’ютерного зору.
- **Держави програють гонку технологій.** Уряди впроваджують ШІ-системи без належного тестування та громадського контролю, намагаючись наздогнати злочинців. Це призводить до помилкових арештів і створення приватизованих систем стеження.
- **Технологія нейтральна, суспільство — ні.** ШІ не є ані добрим, ані злим; він підсилює наміри тих, хто ним керує.

Але ціна цієї гонки озброєнь лякає експертів з громадянських свобод не менше, ніж сама злочинність. Еквадор обрав для своєї системи безпеки платформу Palantir — ту саму компанію, яка отримала понад мільярд доларів від Пентагону, ту саму компанію, яку називають «державою в державі» Кремнієвої долини. І тут виникає питання: хто контролює алгоритм, який контролює нас? Коли система розробляється закритою корпорацією, працює на закритих серверах, обробляє персональні дані мільйонів громадян без незалежного аудиту та прозорого нагляду, ми отримуємо приватизований цифровий поліцейський апарат. Апарат, який не звітує перед парламентом, який може змінювати свою логіку за рішенням менеджерів.

Технологічний детермінізм, який панував у суспільній думці останні два десятиліття, стверджує: прогрес невпинний, зупинити його неможливо, залишається лише адаптуватися. Але прогрес не є нейтральним. Він не існує у вакуумі. Ми опинилися в ситуації, яку фахівці називають «подвійним випередженням». З одного боку, злочинці випереджають закон, використовуючи ШІ для автоматизації насильства та крадіжок. Вони не обтяжені бюрократією, тендерами,

етичними комісіями. Вони бачать вразливість і б'ють негайно. З іншого боку, держави, намагаючись надолужити втрачене, впроваджуючи технології, чиї побічні ефекти ми ще не встигли усвідомити, не кажучи вже про те, щоб їх регулювати.

Проблема, яку окреслює звіт InSight Crime, не в тому, що штучний інтелект сам по собі є злом. Він не має власної волі, але він має колосальну здатність масштабувати людські наміри. І питання, яке стоятиме перед нами наступне десятиліття, — чи зможемо ми створити алгоритми, які не лише ефективно шукають злочинців, але й надійно захищають невинних. Чи зможемо ми побудувати системи, прозорі для громадського контролю, але непроникні для зловмисників. Чи зможемо ми навчити штучний інтелект не лише рахувати, але й розуміти цінність свободи. Від відповідей на ці питання залежить не просто рівень злочинності, від них залежить, чи залишиться наше суспільство відкритим, вільним і, зрештою, людяним. Бо коли ми передаємо машинам право вирішувати, хто злочинець, а хто жертва, ми маємо бути впевнені, що вони не переплутають. Історія не пробачає помилок. Алгоритми — теж.

Ваша думка важлива!

1. Як, на вашу думку, українські СПФМ можуть побудувати ефективний процес перевірки контрагентів-VASP, щоб це не перетворилося на тотальну відмову від операцій (de-risking), але й не залишило "шлюзи" для брудних криптоактивів?
2. Нова архітектура ЄС передбачає уніфікацію штрафів та пряму дію регламентів, що нівелює національні особливості. Які, на ваш погляд, найбільші операційні виклики чекають на українські фінансові установи та ВНУП при інтеграції у цей жорсткий уніфікований простір?
3. Кейс із Lemixon Solutions доводить, що покладання виключно на офіційні реєстри навіть країн G7 (як-от Велика Британія) є недостатнім. Які альтернативні маркери або джерела даних ви вважаєте найбільш надійними для виявлення фіктивних компаній, коли офіційні документи виглядають бездоганно, але суть бізнесу викликає сумніви?
4. Як поєднати розвиток ринку стейблкоїнів із вимогами ПВК/ФТ/ФР так, щоб технологічна інноваційність не створювала нових каналів для тіньових фінансових потоків та обходу санкцій?
5. Рівень корупційних ризиків у судовій системі залишається високим. Злочинні синдикати здатні не просто «домовлятися» з окремими суддями, а інтегрувати своїх людей на вершину судової ієрархії. Які механізми люстрації та перевірки доброчесності здатні запобігти цьому в Україні?
6. В Україні — одні з найвищих темпів цифровізації державних послуг. Яким чином українські правоохоронні органи можуть адаптуватися до загроз, коли злочинці створюватимуть ШІ-агенти для атак на ці системи?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-07

Бюлетень є аналітичною розробкою методологічної команди Департаменту антилегалізаційної політики Міністерства фінансів України, спрямованою на поширення кращих практик, дослідження новітніх типологій та глобальних регуляторних і правоохоронних тенденцій у сфері ПВК/ФТ/ФР. Видання призначене для підвищення інституційної спроможності всіх учасників AML системи України та сприяння ефективному управлінню ризиками ВК/ФТ/ФР з урахуванням міжнародних стандартів та актів права ЄС.

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