Методологічний бюлетень

Серійний номер: МінФін-AML-2026-21

Травень 2026

# “Не дивись на годинник – роби як він. Рухайся далі!”

Томас Карлайл

**Мета**

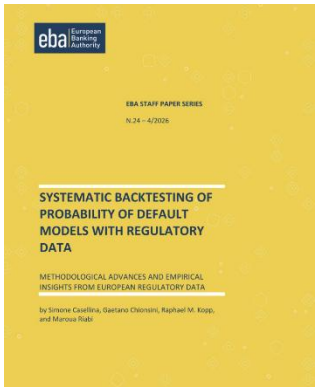
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

### Систематичне ретроспективне тестування моделей імовірності дефолту за допомогою регуляторних даних [1]




Європейське банківське управління (ЕВА) оприлюднило фундаментальний робочий документ, підготовлений групою дослідників (Сімоне Каселліна, Гаетано Кйонсіні, Рафаель М. Копп, Маруа Ріабі). Цей документ відображає концептуальний зсув у європейській парадигмі фінансового нагляду, спрямований на оптимізацію регуляторного середовища та впровадження дата-центричної аналітики у процеси пруденційного контролю. Дослідження безпосередньо відповідає на запити вищого політичного керівництва ЄС щодо необхідності регуляторного спрощення та підвищення операційної ефективності наглядових органів без

[1] https://www.eba.europa.eu/legacy/about-us/staff-papers#:~:text=Systematic%20backtesting%20of%20probability%20of%20default%20models%20with%20regulatory%20data%20%2D%20Simone%20Casellina%2C%20Gaetano%20Chionsini%2C%20Raphael%20M.%20Kopp%2C%20Maroua%20Riabi

компромісів у сфері фінансової стабільності. Відповідно до статті 185 Регламенту (ЄС) № 575/2013 (Capital Requirements Regulation, CRR), кредитні установи зобов'язані здійснювати регулярну валідацію своїх внутрішніх моделей на основі рейтингів (IRB), проте автори констатують, що традиційні підходи, які спираються на ресурсомісткі виїзні перевірки, є недостатньо масштабованими і не забезпечують належного макропруденційного бачення.

Методологічною основою дослідження є використання масивів регуляторних даних, агрегованих EBA у період з 2017 по 2024 роки через шаблон звітності C 08.05 (Common Reporting Framework, COREP). Цей шаблон зобов'язує банки, що використовують IRB-моделі, подавати гранульовані дані: кількість позичальників, показники імовірності дефолту (PD) та фактичні рівні дефолту (DR), дезагреговані за класами активів та рейтинговими категоріями, зведені до єдиної загальної шкали з фіксованими діапазонами PD. Інноваційність запропонованого підходу полягає у зміщенні фокуса ретроспективного тестування (backtesting) з глобального рівня портфеля (де традиційно застосовуються тести на кшталт Хосмера-Лемешова) на мікрорівень окремих рейтингових класів. Такий рівень грануляції є критично важливим, оскільки він унеможливлює ситуацію, за якої надмірна консервативність в одних сегментах портфеля статистично маскує критичну недооцінку ризиків в інших.

Особливої уваги заслуговує статистична корекція, запропонована авторами документа. Канонічний біноміальний тест, який традиційно застосовується для перевірки частоти дефолтів, ґрунтується на припущенні про абсолютну статистичну незалежність подій дефолту серед позичальників. Проте у реальних макроекономічних умовах ця гіпотеза є хибною. Автори впроваджують узагальнену корекцію, яка одночасно враховує кореляцію активів (asset correlation) — вплив спільних макроекономічних факторів на групу позичальників, та серійну кореляцію (serial correlation) — часову залежність показників. Для забезпечення безперервного моніторингу та виявлення стійких у часі помилок калібрування дослідники також інтегрували використання порядкових статистик (order statistics).

Емпірична апробація нової методології на вибірці корпоративних кредитів малому та середньому бізнесу (SME) банків ЄС продемонструвала вражаючі результати. Використання класичного канонічного тесту вказувало на те, що до 16,7% експозицій є неправильно відкаліброваними (верхня консервативна межа). Натомість

**Висновки:**

- **Перехід від традиційних виїзних перевірок до систематичного автоматизованого тестування на основі регуляторних шаблонів (COREP) формує нову вимогу до СПФМ:** архітектура внутрішніх баз даних повинна бути абсолютно прозорою та готовою до алгоритмічної обробки наглядовими органами.
- **Зміщення фокуса валідації на мікрорівень окремих рейтингових класів скасовує можливість компенсації ризиків;** це вимагає від комплаєнс-підрозділів розробки більш точних скорингових моделей для клієнтів, оскільки завищений ризик в одній групі більше не може бути "розчинений" у загальному портфелі.
- **Методологія застосування корекції на кореляцію активів має бути адаптована для потреб ПВК/ФТ:** системи транзакційного моніторингу (TMS) повинні враховувати спільні економічні фактори, які зумовлюють зміну фінансової поведінки групи клієнтів, щоб уникнути генерації масових хибних попереджень (false positives).
- **Залежність між якістю математичних моделей ризику та вимогами до капіталу (виявлена потенційна втрата до 10,3 б.п. капіталу) доводить, що недоліки у сфері управління ризиками безпосередньо впливають на фінансовий стан установи**, перетворюючи питання комплаєнсу на пріоритет рівня правління банку.

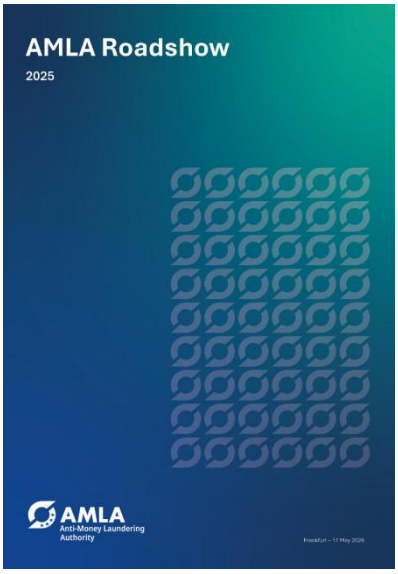
застосування скоригованої методології EBA, яка реалістично враховує кореляційні ефекти, зменшило цю частку до статистично обґрунтованого діапазону 2,9% – 3,5%. Автори також фіксують позитивну динаміку останніх років: частка некаліброваних експозицій має стійку тенденцію до зниження, що свідчить про суттєве підвищення якості внутрішніх банківських даних та успішну інтеграцію додаткових марж консерватизму у відповідь на регуляторний тиск.

Критичним аспектом дослідження є оцінка впливу виявлених недоліків на капітал банків. Автори кількісно виміряли різницю між задекларованими показниками PD та мінімально допустимими рівнями PD, які вимагалися б для забезпечення пруденційної коректності у разі провалу ретроспективного тестування. Було встановлено, що таке гіпотетичне перекалібрування моделей призвело б до зменшення системних коефіцієнтів капіталу першого рівня (Tier 1) у діапазоні від 3,8 до 10,3 базисних пунктів у масштабах усієї банківської системи. Незважаючи на те, що ці цифри не становлять системної загрози, вони чітко демонструють чутливість капіталу до якості математичних моделей та обґрунтовують необхідність постійного нагляду.

Для вирішення проблеми переходу від банківського рівня до макропруденційного аналізу EBA розробило спеціальний механізм агрегації. Відповідно до цього механізму, результати біноміального тесту на рівні окремого рейтингового класу формалізуються через індикаторну змінну (0 — калібрування коректне, 1 — некоректне). Надалі ці бінарні рішення агрегуються в межах банку як середньозважений відсоток за допомогою показника експозиції під ризиком дефолту (Exposure at Default, EAD). Зважування саме за обсягом фінансової експозиції, а не за простою кількістю позичальників, забезпечує адекватне відображення реального економічного ризику. Фундаментальним принципом цієї агрегації є вбудований пруденційний консерватизм: надлишковий капітал висококонсервативних банків не може використовуватися для математичного перекриття ризиків тих установ, чиї моделі недооцінюють небезпеку.

| Аналітичний параметр | Класичний пруденційний підхід (Канонічний) | Інноваційний підхід EBA (Скоригований) | Наслідки для ризик-менеджменту та комплаєнсу |
|---|---|---|---|
| **Математична база тестування** | Гіпотеза абсолютної незалежності дефолтів | Врахування кореляції активів та серійної кореляції | Зниження рівня хибних спрацьовувань під час наглядових перевірок моделей |
| **Рівень аналітичної грануляції** | Агрегований рівень загального портфеля банку | Рівень окремого рейтингового класу позичальника | Неможливість маскувати високоризикові операції (зокрема пов'язані з ВК/ФТ) |
| **Вплив на капітал першого рівня (Tier 1)** | Зниження сукупного показника до 10,3 базисних пунктів | Зниження на рівні 3,8 базисних пунктів | Підвищення стійкості капіталу; прямий зв'язок між якістю даних та ліквідністю |

## AMLA 2026: як Європа об'єднується проти фінансових злочинів [2]




Звіт Управління з боротьби з відмиванням грошей (AMLA), опублікований у 2026 році, є фундаментальним аналітичним документом, який детально підбиває підсумки масштабної дипломатичної та стратегічної місії, здійсненої новою головою відомства Бруною Сего протягом 2025 року. Ця ініціатива охопила всі 27 країн-членів Європейського Союзу, перетворившись на перше глобальне опитування та аудит реального стану європейської системи протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) перед початком активної операційної фази агентства. В основі звіту лежать результати десятків регуляторних раундів та круглих столів, які об’єднали сотні організацій та ключових фігур міжнаціонального комплаєнсу. Програма візитів передбачала проведення обов'язкових засідань із державним сектором — національними наглядовими органами та підрозділами фінансової розвідки (ПФР) — у кожній країні, які у 24 випадках були доповнені розширеними зустрічами з галузевими асоціаціями приватного сектору. У фокус обговорень потрапив максимально широкий спектр підзвітних суб'єктів: від традиційних банків, страховиків та інвестиційних компаній до представників платіжних систем, постачальників криптопослуг (CASPs), а також представників нефінансових професій, таких як юристи, нотаріуси, аудитори, податкові консультанти, агенти з нерухомості, оператори грального бізнесу та торгівці коштовностями. Усі дискусії велися в суворій відповідності до правила Chatham House, що дозволило учасникам відкинути формальний дипломатичний протокол і максимально відверто, без ризику прямої атрибуції думок чи публічного розголосу, вказати на критичні системні прогалини та слабкості європейських фінансових кордонів.

Головним аналітичним пластом звіту є детальна фіксація безпрецедентно стрімкої та агресивної еволюції ландшафту фінансових злочинів, де класичні кримінальні методи відмивання коштів дедалі сильніше переплітаються з високотехнологічними кіберзагрозами. Учасники ринку констатували, що традиційні зони ризику, пов'язані з обігом готівки, непрозорими операціями на ринку комерційної та житлової нерухомості чи використанням складних корпоративних структур з номінальними директорами для приховування реальних бенефіціарів, залишаються потужним інструментом для легалізації доходів від наркотрафіку та корупції. Проте сьогодні ці вразливості накладаються на нові виклики. Зокрема, приватний сектор б'є на сполох через вибухове зростання масштабів фінансового шахрайства та скам-індустрії, де межа між початковим злочином і процесом інтеграції коштів у легальну економіку остаточно стирається. Злочинці активно використовують інструменти штучного інтелекту та технології синтетичних медіа (включаючи діпфейки) для проведення масових маніпуляцій та підробки цифрових ідентичностей, що ставить під загрозу надійність систем віддаленого відкриття рахунків.

Ситуація додатково ускладнюється глобальним упровадженням Регламенту ЄС про миттєві платежі. Хоча ця ініціатива покликана прискорити економічні процеси всередині Союзу, вона одночасно створює критичні операційні ризики для комплаєнс-офіцерів, адже кошти тепер переміщуються транскордонно за лічені секунди у режимі 24/7. Це фактично ліквідує часове вікно, необхідне для класичного попереднього аналізу ризиків, роблячи застарілі системи перевірки (наприклад, пакетну обробку трансакцій наприкінці дня або перегляд звітів наступного ранку) абсолютно неефективними проти сучасних динамічних схем. Паралельно

[2] https://www.amla.europa.eu/document/download/631d6de9-5155-4e32-a791-4b8b65d1f70f_en?filename=AMLA%20Roadshow%20Report.pdf

державний сектор фокусується на викликах, спричинених практичною реалізацією регламенту MiCA та початком системного ліцензування й нагляду за криптосектором. Регулятори відзначають гостру нестачу прозорості у криптотрансферах, транскордонну мобільність активів та часту необхідність покладатися на дороге комерційне програмне забезпечення для блокчейн-аналітики, доступне лише обмеженому колу великих провайдерів. Окремим фактором, що формує карту європейських ризиків, виступає географія та геополітичні зрушення. Після повномасштабного вторгнення росії в Україну та різкої інтенсифікації санкційного тиску з боку ЄС, країни, що мають безпосередню географічну чи економічну близькість до зони конфлікту — зокрема Балтійський регіон, Скандинавія та Східна Європа — змушені були радикально перебудувати свої наглядові пріоритети під виявлення складних схем обходу міжнародних санкцій та протидію пов'язаним із цим кібератакам і програмам-вимагачам.

Аналізуючи причини, чому європейська спільнота досі зазнавала труднощів у боротьбі з цими загрозами, звіт викриває глибокі структурні проблеми та «спадщину» минулих років, що сформувалися за часів панування колишньої регуляторної моделі ЄС. Попередній підхід, заснований на директивах, вимагав від кожної країни самостійного ухвалення законів, що призвело до створення 27 ізольованих, неузгоджених національних систем із кардинально відмінними підходами до оцінки ризиків, практиками нагляду та суворістю правозастосування. Ця фрагментація породила так званий «регуляторний арбітраж», коли міжнародні кримінальні мережі свідомо шукають слабкі ланки в європейській архітектурі й переводять свої операції до країн із лояльнішим або менш технічно оснащеним контролем.

Найбільш тривожний і явний розрив зафіксовано між фінансовими інституціями та нефінансовим сектором. Якщо великі європейські банки та страхові конгломерати під тиском жорстких штрафів інвестували колосальні капітали в автоматизацію комплаєнсу, побудову масштабних інфраструктур моніторингу та найм експертів, то малий бізнес і самостійні фахівці у сферах нерухомості, аудиту, права та нотаріату демонструють критично низький рівень зрілості у сфері ПВК. Більшість таких дрібних суб'єктів мають вкрай обмежене уявлення про свої юридичні обов’язки, не володіють базовими інструментами для належної перевірки клієнтів (CDD) і часто неспроможні ідентифікувати складні індикатори підозрілих операцій. Крім того, звіт ілюструє глибоке світоглядне протиріччя: низьку кількість надісланих повідомлень про підозрілі трансакції нефінансові практиканти часто схильні трактувати позитивно — як доказ чистоти свого бізнесу та відсутності ризиків, тоді як ПФР та наглядові органи однозначно розцінюють цей феномен як маркер тотального недовиявлення та приховування правопорушень. Ситуація погіршується розпорошеністю самого нагляду у нефінансовому секторі, де за одним напрямком можуть відповідати одразу кілька саморегульованих організацій та професійних палат із різним рівнем кваліфікації та повноважень, що розмиває відповідальність і підриває формування єдиної комплаєнс-культури. При цьому загальний кадровий голод, дефіцит бюджетів та застарілі закриті IT-системи є спільним операційним обмеженням як для державних контролерів, так і для приватних фірм по всьому ЄС.

Додатковим істотним викликом є жорстке протиріччя та правова колізія між фінансовим моніторингом та європейським законодавством про захист персональних даних (GDPR). Фінансові установи відкрито заявляють про регуляторну дилему: намагання виконати вимоги щодо транскордонного відстеження незаконних фінансових потоків чи тривалого збереження інформації про клієнтів автоматично створює для них високі ризики отримати суворі санкції за порушення правил конфіденційності GDPR від офісів захисту даних. Аналогічно, відсутність чітких легальних алгоритмів та інструкцій щодо того, які саме дані, в якому обсязі та під якими технічними гарантіями безпеки можна передавати третім сторонам, стає головною перещкодою на шляху розвитку ефективних державно-приватних партнерств та транскордонного обміну фінансовою розвідкою.

Поява AMLA як наддержавного органу та запуск прямо діючого Єдиного зводу правил (Single Rulebook) сприймаються ринком не просто як чергова бюрократична реформа, а як історичний та єдиний шанс кардинально змінити правила гри на європейському континенті й побудувати рівні конкурентні умови. Індустрія покладає колосальні очікування на перші регуляторні результати діяльності нового відомства. Важливим віхами вже стали розроблені та передані до Європейської комісії наприкінці 2025 року перші проєкти Технічних стандартів регулювання (RTS). Ці документи закладають уніфіковану, засновану на аналізі великих даних методологію оцінки невід'ємних та залишкових ризиків фінансових установ, а також чіткі критерії, за якими AMLA визначатиме обмежене коло найбільш системно важливих та ризикованих транскордонних фінансових груп для переведення під свій прямий нагляд із Франкфурта. Наступними пріоритетами визначено стандартизацію правил належної перевірки клієнтів та управління тривалими діловими відносинами. Водночас звіт намагається об’єктивно оцінити надмірно оптимістичні очікування та завищені вимоги ринку, чітко окреслюючи обсяг та межі компетенції новоствореної інституції. AMLA наголошує, що воно є молодою структурою, яке нарощуватиме спроможність поступово, і його діяльність суворо обмежена законодавством першого рівня, ухваленим законодавчими органами ЄС. Відтак, заклики дрібного бізнесу до радикального пом’якшення або повного звільнення від обтяжень у сфері ПВК через технічні стандарти є юридично неможливими, якщо вони суперечать базовому закону. Крім того, пряма щоденна робота з підвищення комплаєнс-грамотності суб'єктів та рутинний нагляд у незрілих нефинансових індустріях залишаються безальтернативною та виключною зоною обов'язків національних урядів на місцях.

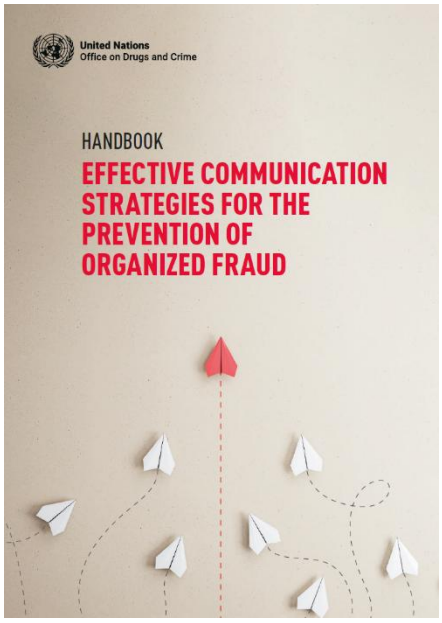
Вектор подальшого розвитку системи, згідно зі звітом, нерозривно пов’язаний із реалізацією масштабної цифрової дорожньої карти та інструментів наглядової конвергенції. AMLA фокусує

**Висновки:**

- **Перехід до цифрового нагляду в реальному часі:** Впровадження регламенту ЄС про миттєві платежі та розвиток AI-шахрайства вимагають від підзвітних суб'єктів та регуляторів негайної відмови від застарілих систем контролю (на кшталт обробки пакетів наприкінці дня). Необхідно впроваджувати автоматизовані системи попереднього моніторингу трансакцій та інструменти передової аналітики даних в реальному часі.
- **Пріоритетне усунення розриву в нефінансовому секторі:** Оскільки рівень практичного впровадження вимог у сфері ПВК/ФТ серед ріелторів, нотаріусів і бухгалтерів залишається низьким, першочерговий акцент має бути зроблений не на новому регулюванні, а на практичній підтримці. Національні органи мають забезпечити доступні спільні інструменти належної перевірки клієнтів (CDD) для малого бізнесу, тоді як AMLA у 2026 році планує запустити дорожню карту навчальних програм для підвищення спроможності національних наглядових органів у цих секторах.
- **Подолання правової невизначеності між вимогами ПВК/ФТ та GDPR.** Для розвитку державно-приватного партнерства та транскордонного обміну інформацією AMLA, EDPS та EDPB мають забезпечити правову визначеність щодо законної й безпечної передачі даних відповідно до статті 75 Регламенту у сфері ПВК.
- **Для ефективної протидії гібридним загрозам державам необхідно створювати міжвідомчі моделі співпраці між сектором безпеки, ПФР, громадянським суспільством, аналітичними центрами та дослідниками дезінформації,** оскільки більшість сучасних гібридних кампаній поєднують інформаційний, соціальний, економічний та політичний вплив одночасно.

зусилля на створенні єдиного наглядового посібника (Common Supervisory Manual) та планує вже у 2026 році запустити перші цільові оцінки конвергенції у фінансовому секторі й перевірки у нефінансових сегментах, щоб не допустити вирівнювання стандартів за «найменшим спільним знаменником» і підтягнути слабкі національні системи до рівня передових. Технологічним ядром реформи має стати розгортання Центральної бази даних ПВК/ФТ, а також глибока модернізація та інтеграція захищеної мережі FIU.net під управлінням AMLA. Це дозволить перетворити розрізнені європейські розвідки на монолітну аналітичну екосистему, здатну автоматизовано виявляти складні міжнаціональні кримінальні ланцюжки та координувати спільні аналітичні розслідування в реальному часі. Наостанок, одним із найважливіших стратегічних напрямків є розв'язання проблеми конфіденційності даних: AMLA вже розпочало офіційний системний діалог із Європейським інспектором з захисту даних (EDPS) та Європейською радою з захисту даних (EDPB). Метою цієї робочої групи є створення узгоджених, безпечних та юридично чистих шаблонів і правил для розгортання повноцінних міжнаціональних партнерств з обміну інформацією, які мають масштабно запрацювати з 2027 року на міцному фундаменті Статті 75 Регламенту AML. Резюмуючи, звіт стверджує, що хоча реформа відбувається в умовах колосального тиску та дефіциту часу, вперше в історії Європи створено всі три необхідні компоненти для перемоги над фінансовою злочинністю: спільну залізобетонну юридичну архітектуру, сильний центральний інституційний мандат AMLA та виражену консолідовану готовність державних і приватних гравців діяти як єдиний транскордонний альянс.

## Комунікативні механізми забезпечення фінансової стійкості: аналіз превентивного фреймворку УНЗ ООН проти організованого шахрайства [3]




Управління ООН з наркотиків і злочинності (УНЗ ООН) у своєму посібнику, підготовленому Глобальною програмою впровадження Конвенції проти транснаціональної організованої злочинності за фінансової підтримки Великої Британії, представляє першу глобальну практичну інструкцію, спрямовану на боротьбу з організованим шахрайством за допомогою стратегічних комунікацій. Головна мета цього фундаментального документу полягає в докорінній зміні підходів до профілактичної та інформаційної роботи — системному переході від розпорошеного, пасивного та одноманітного інформування до високотехнологічних, поведінково обґрунтованих, інклюзивних та етичних комунікаційних моделей, які інтегрують та об'єднують зусилля державного сектору, фінансових інституцій, технологічних гігантів та інститутів громадянського суспільства.

Глибоко аналізуючи поточні виклики та системні недоліки сучасних превентивних заходів, автори посібника детально розкривають складне явище розриву між обізнаністю та дією, котре полягає в тому, що навіть високий рівень абстрактного розуміння ризиків та теоретичних знань не здатний захистити індивіда в момент інтенсивного психологічного тиску, маніпуляцій чи штучно створеного емоційного стресу з боку зловмисників. Зазначена вразливість посилюється

[3] https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_Handbook_on_Effective_Communication_Strategies_for_the_Prevention_of_Organized_Fraud_EN.pdf

через зниження сприйнятливості цільової аудиторії до однотипних інформаційних повідомлень загального характеру, зокрема закликів щодо обережної поведінки в онлайн-середовищі. Додатковим ризиком є використання надмірно деталізованих попереджень, зокрема скріншотів конкретних повідомлень або описів вузьких шахрайських схем, що може обмежувати здатність громадян розпізнавати нові тактики злочинців і формувати хибне відчуття захищеності. Ситуацію ускладнює хронічна ізольованість різних відомств, які діють у власних закритих структурах, що породжує суперечливість меседжів, дезорієнтує суспільство та підриває загальну довіру до офіційних інституцій.

Для подолання цих комунікаційних бар'єрів посібник пропонує інноваційну, орієнтовану першочергово на постраждалу особу чотириетапну модель розгортання шахрайського замислу, яка детально описує фази підходу, безпосереднього обману, здійснення фінансової транзакції та тривалого періоду пост-шахрайства. На кожному з цих критичних етапів транснаціональні злочинні угруповання навчилися філігранно експлуатувати специфічні людські вразливості, такі як соціальна самотність, гостра фінансова скрута, дефіцит часу або штучно сфабрикований авторитет відомих державних чи міжнародних інституцій. Ефективна відповідь на такі комплексні виклики вимагає негайного створення архітектури глибокої синергії між правоохоронними органами, банками, фінтех-компаніями, цифровими платформами та медіа-ресурсами. У цьому контексті документ наполягає на транскордонному впровадженні принципу «єдиного звіту», за якого первинне звернення постраждалої особи до будь-якої організації автоматично та конфіденційно запускає скоординовану відповідь усіх задіяних приватних і державних структур, що суттєво зменшує емоційний і бюрократичний тягар, прискорює блокування активів та повністю нівелює ризики вторинної ретравматизації людини. Саму ж превентивну комунікацію автори вимагають безпосередньо інтегрувати в повсякденні цифрові та фізичні інтерфейси, якими щодня користуються громадяни, — від мобільних банківських додатків та е-платформ пошуку роботи до фізичних касових зон роздрібної торгівлі, де купуються потенційні інструменти шахрайства на кшталт подарункових карток чи здійснюються швидкі перекази.

Захисна комунікація та інструменти стримування, згідно з посібником, мають базуватися на передових поведінкових інсайтах і когнітивній науці, дзеркально протидіючи тим психологічним інструментам маніпуляцій, які використовують зловмисники. Для повної нейтралізації штучно створюваного відчуття ургентності та терміновості рекомендується впроваджувати примусові технологічні «періоди охолодження» та пропонувати користувачам інтерактивні логічні запитання безпосередньо у момент підтвердження підозрілих або нетипових грошових розрахунків, змушуючи мозок перемикатися з емоційного сприйняття на раціональне. Окремим елементом превентивної роботи має стати поширення серед громадян практичних моделей безпечної комунікації, зокрема підготовлених формулювань ввічливої відмови, що дають змогу оперативно припинити контакт зі зловмисником без ескалації ситуації. Важливим елементом довгострокового навчання є застосування методики поведінкової інокуляції через контрольовані симуляції фішингу або соціальної інженерії. Такі навчальні кампанії дозволяють у безпечному середовищі продемонструвати користувачам типові маніпулятивні тактики та одразу надати пояснення щодо ознак ризику, перетворюючи потенційну помилку на практичний освітній досвід.

Особливе місце в посібнику посідає етичний аспект, орієнтація на захист прав людини та повне, безкомпромісне виключення будь-яких практик прихованого чи явного звинувачення жертви. Автори закликають міжнародну спільноту уникати знецінювальної лексики щодо шахрайства, оскільки такі формулювання применшують характер організованої злочинної діяльності та можуть формувати хибне сприйняття відповідальності постраждалих осіб. Натомість необхідно чітко артикулювати сувору кримінальну відповідальність зловмисників, впроваджуючи жорсткі мовні стандарти, де зазначається, що «організовані злочинці застосували високотехнологічні

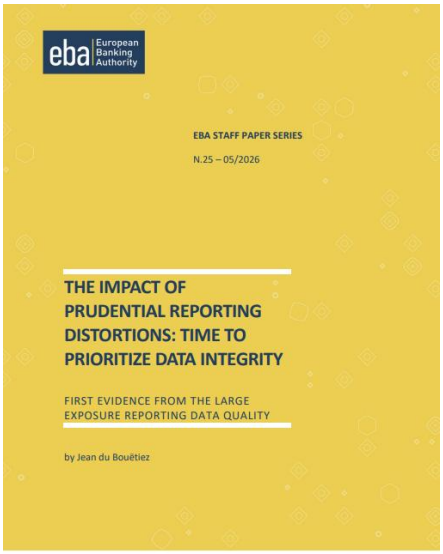
маніпуляції та підступно викрали кошти», а не «громадянин втратив гроші через власну неуважність». Усі звернення та подальша взаємодія з постраждалими мають здійснюватися за принципом безпечного первинного контакту із залученням спеціально підготовлених фахівців першої лінії. Це дозволить забезпечити якісну травма-інформовану підтримку, зменшити ризик повторної травматизації та подолати суспільну стигму, яка часто перешкоджає своєчасному повідомленню про злочини. Для забезпечення інклюзивності документ містить практичні цифрові чек-листи щодо адаптації матеріалів для осіб з обмеженими можливостями (різні форми), низьким рівнем цифрової або фінансової грамотності, а також комунікаційні рекомендації для роботи з дітьми, молоддю та представниками вразливих груп.

Наприкінці посібник детально фокусується на докорінній перебудові національних та міжнародних систем моніторингу й оцінки ефективності превентивних заходів. Замість застарілого оцінювання кампаній виключно за формальними кількісними вихідними даними (такими як загальний наклад роздрукованих брошур, обсяг витраченого бюджету чи кількість поверхневих переглядів соціальної реклами), документ вимагає обов'язкового впровадження глибоких психосоціальних індикаторів. Новітня методологія пропонує оцінювати реальні поведінкові зміни у суспільстві, зокрема через фіксацію та вимірювання динаміки випадків «near misses» — спроб шахрайства, які потенційні постраждалі змогли самостійно, вчасно та усвідомлено розпізнати, успішно перервати та задокументувати завдяки отриманим раніше превентивним знанням, а також через відстеження глибини інтеграції захисної та солідарної поведінки в повсякденні соціальні норми, корпоративну культуру компаній та внутрішні сімейні системи комунікації.

**Висновки:**

- **Організоване шахрайство дедалі активніше використовує психологічний тиск і маніпуляції,** тому фінансові установи та технологічні платформи мають впроваджувати періоди відкладеного підтвердження для нетипових транзакцій із додатковими інтерактивними перевірками, спрямованими на раціональну оцінку дій клієнта.
- **Традиційні формати одноразового інформування знижують ефективність сприйняття ризиків та обмежують здатність громадян розпізнавати нові шахрайські тактики.** У зв'язку з цим профілактичні програми мають впроваджувати методику поведінкової інокуляції через безпечні симуляції фішингу та маніпулятивних сценаріїв, які забезпечують негайне контекстне навчання під час взаємодії користувача з ризиковим елементом.
- **Негативне суспільне сприйняття постраждалих і використання знецінювальної лексики щодо шахрайства ускладнюють повідомлення про злочини та посилюють психологічні наслідки для постраждалих осіб.** У зв'язку з цим державні органи, фінансові установи та ЗМІ мають використовувати нейтральну юридичну термінологію без елементів покладання провини на постраждалого, а також впроваджувати підхід «безпечного первинного контакту» із залученням підготовлених фахівців для надання травма-інформованої підтримки.
- **Оцінка превентивних заходів виключно за кількісними показниками охоплення створює ризик збереження неефективних кампаній.** У зв'язку з цим суб'єкти протидії шахрайству мають орієнтувати системи моніторингу на поведінкові та психосоціальні індикатори, зокрема фіксацію успішно перерваних спроб шахрайства та рівень інтеграції захисної поведінки у повсякденні практики населення.

## Криза якості даних у банківському нагляді ЄС: як помилки у пруденційній звітності викривлюють оцінку ризиків [4]




Документ присвячений критично важливій, але тривалий час недостатньо помітній проблемі європейського банківського нагляду — системним викривленням пруденційної звітності через низьку якість даних та некоректну класифікацію контрагентів у пруденційній звітність щодо великих експозицій. Автор дослідження аналізує масштаби та наслідки помилок у секторній класифікації та присвоєнні кодів економічної діяльності Статистичної класифікації видів економічної діяльності в Європейському Союзі (NACE) у звітності 2 759 кредитних установ Європейської економічної зони станом на 31 грудня 2023 року. Центральна ідея роботи полягає у тому, що проблеми цілісності та якості даних у пруденційній звітності вже виходять далеко за межі суто технічних помилок і безпосередньо впливають на фінансову стабільність, точність оцінки ризиків, наглядові рішення, розрахунок капітальних вимог та формування макропруденційної політики. Документ фактично демонструє, що сучасна система банківського нагляду ЄС надмірно залежить від якості даних, які самі банки подають до регуляторів, а будь-які системні помилки у цих даних здатні масштабно викривлювати результати нагляду та регуляторного аналізу.

На початку дослідження автор наголошує, що якість даних є фундаментальною умовою ефективного фінансового нагляду, оскільки саме на основі пруденційної звітності формуються наглядові рішення, макропруденційні оцінки та регуляторні заходи реагування. Документ проводить паралелі з відомими випадками помилок у статистичних даних та економічних дослідженнях, які мали значний вплив на державну політику. Зокрема, згадується кейс щодо помилкового аналізу співвідношення державного боргу та економічного зростання, а також масштабні ревізії статистики ринку праці США у 2025 році, що виникли через проблеми з якістю вибіркових даних. Автор підкреслює, що навіть відносно «технічні» помилки у даних можуть мати масштабні наслідки для економічної політики, ринкової стабільності та суспільної довіри до регуляторних інституцій. У цьому контексті пруденційна звітність банків розглядається не просто як операційний процес подання інформації, а як критичний елемент архітектури фінансової стабільності Європейського Союзу.

Далі документ переходить до детального аналізу пруденційної звітніості щодо великих експозицій як одного з ключових інструментів пруденційного нагляду відповідно до Регламенту ЄС щодо пруденційних вимог до кредитних установ та інвестиційних фірм. Автор пояснює, що система пруденційної звітніості щодо великих експозицій призначена для моніторингу концентраційного ризику та контролю великих експозицій банків до окремих контрагентів або груп пов'язаних контрагентів. Банки ЄЕЗ зобов'язані регулярно подавати детальну інформацію про великі експозиції, включаючи ідентифікацію контрагентів, типи інструментів, забезпечення, методи кредитного механізму пом'якшення ризику, секторну класифікацію та NACE-коди. Документ особливо підкреслює, що секторна класифікація контрагентів має фундаментальне

[4] https://www.eba.europa.eu/sites/default/files/2026-05/7933effb-048d-45dc-a529-98f430717161/Staff%20paper%20-%20The%20impact%20of%20prudential%20reporting%20distortions%20time%20to%20prioritize%20data%20integrity.pdf

значення для функціонування всієї системи пруденційного регулювання, оскільки вона безпосередньо впливає на розрахунок активів, зважених на ризик, нормативів ліквідності, проведення стрес-тестування, аналіз концентрації ризиків та інші елементи наглядової системи. Автор пояснює структуру секторної класифікації, яка включає центральні банки, органи державного управління, кредитні установи, інвестиційні фірми, інші фінансові корпорації, нефінансові корпорації та домогосподарства, а також детально розкриває нормативну базу, що регулює ці категорії. Особлива увага приділяється тому, що кожен контрагент повинен бути віднесений лише до одного сектору та одного коду NACE, а будь-яке відхилення від цього принципу означає помилкову класифікацію.

Одним із центральних елементів дослідження є демонстрація масштабності та системності проблеми неузгоджених класифікацій. Автор наводить конкретні приклади, які ілюструють, наскільки по-різному банки класифікують одних і тих самих контрагентів. У випадку «Exposure A» один контрагент був одночасно віднесений різними банками до чотирьох різних секторів, включаючи кредитні установи, органи державного управління та інші категорії. При цьому майже 38% загального обсягу експозиції до цього контрагента було класифіковано неправильно. Інший приклад — «Exposure B» — демонструє критичні помилки у присвоєнні кодів статистичної класифікації видів економічної діяльності (NACE), коли фінансова установа масово класифікувалась як суб'єкт енергетичного сектору. Автор наголошує, що ці випадки не є окремими винятками або технічними аномаліями, а відображають системну проблему недостатньої гармонізації у межах європейської системи пруденційної звітності. Документ підкреслює, що навіть незначні на перший погляд помилки класифікації здатні створювати ланцюгові викривлення у розрахунку капіталу, оцінці секторних ризиків та наглядових показників.

Кількісний аналіз демонструє надзвичайно високий рівень поширення таких викривлень. Із 144 744 контрагентів, що фігурували у звітності щодо великих експозицій, 19 003 були задекларовані більш ніж одним банком, що дозволило провести порівняльний аналіз їх класифікації між різними кредитними установами. Серед них 2 991 контрагент був віднесений щонайменше до двох різних секторів, а пов'язані з ними експозиції становили приблизно 65% загального обсягу прямих балансових експозицій цієї групи. Автор підкреслює, що найбільше проблем виникало між категоріями нефінансових корпорацій та інших фінансових корпорацій, а також між органами державного управління та кредитними установами. Аналогічні проблеми були виявлені й у сфері класифікації за кодами NACE, де приблизно 30% контрагентів були віднесені до різних секторів економічної діяльності залежно від банку, який подавав звітність. Документ наголошує, що навіть ці цифри є лише «нижньою межею» реального масштабу проблеми, оскільки аналіз охоплює лише контрагентів, задекларованих більш ніж одним банком, тоді як правильність класифікації багатьох інших контрагентів узагалі не перевірялась.

Важливий блок дослідження присвячений оцінці впливу цих помилок на пруденційні вимоги та дотримання регуляторних вимог. Автор проводить попереднє коригувальне моделювання та аналізує ситуацію після виправлення секторних класифікацій. Результати демонструють суттєві перекручення у звітних показниках: експозиції до органів державного управління були завищені приблизно на 13%, до інвестиційних фірм — на 77%, тоді як експозиції до інших фінансових корпорацій були недооцінені приблизно на 22%. При цьому в окремих країнах Європейської економічної зони різниця між початковими та скоригованими показниками сягала ±45%, що свідчить про серйозну нерівномірність якості пруденційної звітності між юрисдикціями. Документ також детально пояснює, як помилкова секторна класифікація може призводити до порушення вимог Регламенту ЄС щодо пруденційних вимог до кредитних установ та інвестиційних компаній (CRR). Наприклад, неправильна класифікація контрагентів як кредитних установ або інвестиційних фірм дозволяла окремим банкам застосовувати більш м'які ліміти великих експозицій відповідно до статті 395(1) CRR. Автор встановив, що понад 300 банків

потенційно могли неправомірно користуватись такими дерогаціями. Аналогічно, помилкове віднесення контрагентів до органів державного управління або центральних банків дозволяло окремим банкам неправомірно застосовувати винятки відповідно до статті 400(1)(a) CRR, що потенційно приховувало порушення пруденційних лімітів.

Подальша частина документа присвячена аналізу того, як помилки класифікації викривлюють наглядовий аналіз та макропруденційну політику. Автор демонструє, що помилкова секторна класифікація здатна істотно впливати на оцінку активів банків, структуру їхніх експозицій, оцінку суверенних ризиків, аналіз небанківського фінансового посередництва та проведення стрес-тестування. Особливо наголошується, що великі банки є найбільш чутливими до таких помилок: майже всі великі кредитні установи мали відчутний вплив перекласифікації секторів на свої пруденційні показники, а у частини банків масштаб коригувань перевищував 10% загального обсягу прямих балансових експозицій. Автор підкреслює, що це означає потенційне викривлення як мікропруденційного нагляду, так і макропруденційного формування політики на рівні ЄС. Документ фактично показує, що регулятори можуть ухвалювати рішення, спираючись на системно неточні дані щодо секторної структури ризиків у банківській системі.

Висновки:

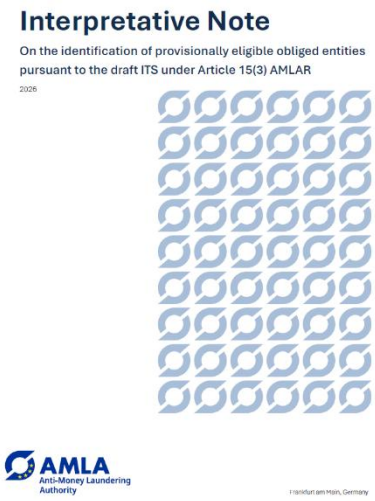
- **Документ демонструє, що проблеми цілісності та якості даних у пруденційній звітності мають системний характер у банківському секторі ЄС та безпосередньо впливають на розрахунок активів, зважених на ризик, капітальних нормативів, показників ліквідності та макропруденційний аналіз.** Необхідне створення централізованих механізмів валідації секторних класифікацій та гармонізованих наглядових механізмів контролю на рівні ЄС.
- **Дослідження показує, що навіть базові секторні класифікації та коди NACE у звітності щодо великих експозицій містять масштабні викривлення, які можуть призводити до неправильного застосування пруденційних винятків, недооцінки ризиків та прихованих порушень регуляторних лімітів.** Це означає, що наглядові органи повинні посилити фокус на управлінні даними та регулярних міжбанківських перевірках узгодженості класифікацій.
- **Автор доводить, що помилкова класифікація контрагентів може суттєво впливати на показники достатності капіталу та призводити до втрати капітальних буферів окремими банками.** Є необхідність у інтеграції оцінки якості даних у наглядовий процес та стрес-тестування.
- **Документ формує підхід, у межах якого якість даних розглядається як елемент фінансової стабільності та системного ризику.** Для регуляторів це означає перехід до постійного нагляду за цілісністю та якістю пруденційних даних.

Окремий надзвичайно важливий блок дослідження стосується впливу помилкової секторної класифікації на достатність капіталу та вимоги до ліквідності. Автор детально пояснює, що секторна класифікація безпосередньо впливає на застосування коефіцієнтів ризику у межах стандартизованого підходу, а після впровадження механізму Basel III output floor — також впливає на моделі внутрішніх рейтингів банків. У межах моделювання скориговані секторні класифікації були використані для перерахунку активів, зважених на ризик, та коефіцієнтів достатності капіталу. Результати показали, що для 340 банків показник загального капіталу зменшився б після виправлення помилок, а для 71 банку абсолютне зниження цього показника перевищувало 0,5%. Частина установ після коригування втрачала значну частину капітальних буферів або навіть порушувала вимоги Pillar 2 Guidance. Автор наголошує, що ці результати демонструють суттєвий вплив проблем якості даних на реальну фінансову стійкість банків. Крім

того, документ пояснює, що помилкова секторна класифікація також здатна викривлювати коефіцієнт покриття ліквідності та коефіцієнт чистого стабільного фондування, оскільки сектор контрагента впливає на класифікацію високоякісних ліквідних активів, розрахунок ставок припливу та відпливу коштів, а також показників доступного і необхідного стабільного фондування. Таким чином, проблема некоректної класифікації впливає не лише на капітал, а фактично на всю систему пруденційного регулювання.

У фінальній частині дослідження автор переходить до ширшого концептуального висновку про необхідність переосмислення ролі управління даними у банківському нагляді ЄС. Документ фактично формує новий підхід, у межах якого якість даних розглядається як окремий елемент фінансової стабільності та системного ризику. Автор наголошує, що нинішня система пруденційної звітності надто сильно залежить від внутрішніх підходів окремих банків до класифікації контрагентів, а відсутність централізованої гармонізованої системи валідації створює ризик накопичення системних викривлень у пруденційних наборах даних. У зв'язку з цим документ закликає до посилення наглядового фокусу на цілісності та якості даних, створення централізованих механізмів перевірки секторних класифікацій, удосконалення стандартів звітності та формування єдиних базових довідкових систем даних на рівні ЄС. Загальний висновок роботи полягає у тому, що якість даних у пруденційній звітності більше не може розглядатися як другорядне технічне питання, а має сприйматись як критичний компонент ефективного банківського нагляду та фінансової стабільності Європейського Союзу.

## Європейський Союз та AMLA: побудова єдиної системи нагляду у сфері ПВК/ФТ [5]




Документ AMLA є одним із перших практичних технічних документів нової європейської системи централізованого нагляду у сфері ПВК/ФТ та фактично формує методологічну основу для майбутнього direct supervision з боку AMLA над найбільш значущими транскордонними фінансовими установами Європейського Союзу. Документ присвячений процедурі ідентифікації попередньо визначених підхвітних суб'єктів — кредитних установ, фінансових установ та фінансових груп, які потенційно підпадатимуть під прямий нагляд AMLA відповідно до статті 12 Регламенту AMLAR. Основний зміст документа полягає у встановленні деталізованої гармонізованої архітектури звітності для збору інформації щодо відповідності критеріям відбору, необхідної AMLA та національним компетентним органам для визначення того, які фінансові установи відповідають критеріям значної транскордонної присутності та можуть бути включені до нового периметра централізованого нагляду у сфері ПВК/ФТ Європейського Союзу. Документ пояснює, що процес відбору розпочинається з ідентифікації підзвітних суб'єктів, які здійснюють діяльність щонайменше у шести державах-членах ЄС, включаючи державу походження, або через установи та структурні підрозділи, або через механізм свободи надання послуг, а також перевищують установлені порогові критерії суттєвості діяльності. При цьому AMLA фактично закладає нову модель наднаціонального наглядового картографування, у межах якої ключове значення мають масштаби транскордонної діяльності, географія операцій, кількість клієнтів та обсяги транзакцій у різних юрисдикціях Європейського Союзу.

[5] https://www.amla.europa.eu/document/download/973ffbce-3020-4110-8d29-935659329ca7_en?filename=Interpretative_Note_Identification_of_Provisionally_Eligible_OEs_AMLA_2026.pdf

Документ надзвичайно детально описує механізм збору інформації щодо відповідності критеріям відбору через гармонізований пакет звітності, який складається з Excel-шаблону та інтерпретаційної записки. AMLA наголошує, що інтерпретаційна записка є супровідним документом до шаблону звітності та повинна використовуватися разом із ним для забезпечення узгодженості набору даних і гармонізованого наглядового тлумачення у всіх державах-членах ЄС. Особливий акцент робиться на тому, що документ не створює нових юридичних зобов'язань, а виконує функцію аналітичних роз'яснень щодо застосування проєкту технічних імплементаційних стандартів відповідно до статті 15(3) AMLAR. Водночас AMLA прямо зазначає, що у випадку конфлікту між інтерпретаційною запискою та обов'язковими правовими актами Європейського Союзу пріоритет мають норми законодавства ЄС. Документ також відображає складність перехідного періоду між AMLD IV/V та новим пакетом законодавства ЄС у сфері ПВК/ФТ, оскільки звітний період для збору інформації — 2025 рік — передує повному набранню чинності AMLR. Саме тому AMLA вказує, що у випадку колізій або прогалин повинні застосовуватися визначення та вимоги AMLD IV/V, імплементовані у національне законодавство держав-членів Європейського Союзу.

Одним із центральних елементів документа є формування нової моделі консолідованої наглядової звітності для фінансових груп. AMLA вводить чітке розмежування між поняттями «підзвітний суб'єкт» та «визначений підзвітний суб'єкт». Підзвітні суб'єкти визначається як компанія, яка безпосередньо заповнює шаблон звітності та подає його національному фінансовому наглядовому органу, тоді як вич+значений підзвітний суб'єкт — це суб'єкт, визначений фінансовою групою для подання консолідованої інформації щодо відповідності критеріям відбору від імені всієї групи. Документ пояснює, що така конструкція є необхідною через відсутність у деяких наглядових органів повної картини корпоративних структур фінансових груп на початковому етапі формування системи прямого нагляду AMLA. Унаслідок цього може виникати ситуація, коли кілька компаній однієї фінансової групи отримують окремі запити на подання інформації. Для уникнення дублювання AMLA дозволяє групі визначити єдиного визначеного підзвітного суб'єкта, який подаватиме консолідовану інформацію щодо всіх кредитних та фінансових установ групи. Таким чином AMLA поступово переходить від фрагментованого національного нагляду до моделі централізованої групової звітності у сфері ПВК/ФТ на рівні Європейського Союзу.

Особливо важливим є блок документа, присвячений перехідним наглядовим механізмам для холдингових структур. AMLA прямо визнає, що холдингові компанії, які відповідно до AMLR стануть пізвітними лише після 10 липня 2027 року, на момент збору інформації ще не мають такого статусу. У зв'язку з цим вони не можуть виступати підзвітними суб'єктами у межах поточного процесу відбору. Документ детально пояснює практичні приклади таких ситуацій та визначає, що у випадках, коли материнська компанія є холдинговою компанією, група повинна визначити інший суб'єкт — наприклад кредитну установу або страхову компанію — як визначений підзвітний суб'єкт. AMLA також наголошує, що самі холдингові компанії повинні бути відображені у структурі звітності через AMD.02.01 або AMD.02.02 залежно від того, чи знаходяться вони в ЄС чи за його межами. Це демонструє, що AMLA вже на етапі становлення архітектури прямого нагляду приділяє значну увагу складним структурам власності, холдинговим моделям та багаторівневим структурам корпоративного управління фінансових груп.

Документ надзвичайно детально регламентує питання управління даними, якості звітності та технічних механізмів контролю звітності. AMLA встановлює, що звітною датою для всієї звітності є 31 грудня 2025 року, а всі грошові суми повинні подаватися виключно у євро із використанням офіційних валютних курсів. Водночас значна увага приділяється цілісності систем наглядової звітності. AMLA наголошує, що захищена структура Excel-шаблону не може змінюватися, а будь-які зміни назв аркушів, формул, механізмів валідації чи інших захищених елементів можуть

призвести до визнання звітності недійсною. Документ запроваджує автоматизовані блокуючі механізми валідації, які генеруватимуть повідомлення про помилки у разі виявлення невідповідностей, відсутньої інформації або неповної звітності. Якщо підзвітний суб'єкт не може забезпечити належну якість даних, він зобов'язаний надати окремі пояснення через форму AMD.00.03 «Коментарі». AMLA також прямо зазначає, що підзвітні суб'єкти повинні підтримувати внутрішні системи контролю, які забезпечують оперативне виправлення та простежуване повторне подання даних. Це свідчить про формування високостандартизованої, орієнтованої на дані наглядової екосистеми, яка базується на автоматизованій наглядовій аналітиці та машинозчитуваній звітності у сфері ПВК/ФТ.

Окремий великий блок документа присвячений структурі шаблонів звітності та деталізації інформаційних полів. AMLA вимагає подання ідентифікаторів LEI, наглядових ідентифікаторів, офіційних юридичних назв, категорій суб'єктів, держав-членів заснування та інформації про наглядові органи у сфері ПВК/ФТ. Документ містить детальні пояснення щодо використання LEI, подання офіційних юридичних назв без скорочень, використання латинських символів для назв, які не записані латиницею, а також класифікації регульованих видів діяльності. Особлива увага приділяється ідентифікації основних та додаткових наглядових органів у сфері ПВК/ФТ, що фактично формує комплексне наглядове картографування всіх фінансових установ та їх наглядових взаємозв'язків у межах Європейського Союзу.

Суттєву увагу AMLA приділяє попереднім фільтрам, які визначають, які саме форми звітності повинні заповнюватися конкретною установою. Документ запроваджує логіку умовної наглядової звітності залежно від наявності материнської компанії в ЄС, головного офісу за межами ЄС, установ або структурних підрозділів в інших державах-членах, а також діяльності в межах механізму свободи надання послуг. Через ці попередні фільтри AMLA формує деталізовану наглядову картину транскордонної структури фінансових груп. Документ демонструє, що AMLA прагне отримати не лише формальну інформацію про юридичних осіб, але й комплексне розуміння операційної присутності фінансових установ у межах Європейського Союзу.

Надзвичайно важливим компонентом документа є підхід AMLA до свободи надання послуг (FPS). Документ фактично створює першу деталізовану наглядову методологію для оцінки транскордонної діяльності фінансових установ у межах режиму FPS. AMLA визначає порогові критерії суттєвості відповідно до проєкту регуляторних технічних стандартів згідно зі статтею 12(7) AMLAR: діяльність вважається суттєвою, якщо у певній державі-члені кількість клієнтів перевищує 20 000 осіб або якщо річний обсяг вхідних та вихідних транзакцій перевищує 50 млн євро. При цьому AMLA наголошує, що для визначення суттєвості необхідно агрегувати всю діяльність фінансової групи у конкретній державі-члені незалежно від того, чи здійснюється вона безпосередньо, через філії, агентів або дистриб'юторів. Водночас підзвітні суб'єкти повинні подавати окремі рядки для кожної комбінації «суб'єкт/держава-член», після чого AMLA самостійно здійснюватиме агрегацію інформації на рівні фінансової групи. Такий підхід свідчить про перехід Європейського Союзу до складного транскордонного картографування ризиків у сфері ПВК/ФТ та централізованого аналізу транскордонних фінансових потоків.

Документ також демонструє суттєве розширення поняття «establishment» у межах нагляду у сфері ПВК/ФТ. AMLA включає до нього не лише дочірні компанії та філії, але й агентські мережі та інші сталі інфраструктури, через які здійснюється фінансова діяльність у межах інших держав-членів. Це має особливе значення для фінтех-сектору, платіжних установ та постачальників послуг, пов'язаних із криптоактивами, які часто використовують розподілені операційні моделі та агентські мережі. AMLA вимагає подання окремого рядка звітності щодо кожного «establishment» або «sister undertaking» та збору розширеної наглядової інформації щодо кожного такого суб'єкта, включаючи LEI, наглядовий орган, категорію діяльності, державу-член, тип «establishment» та масштаби діяльності у межах механізму свободи надання послуг (FPS).

Документ також пояснює, що «sister undertakings» повинні включатися до периметра звітності навіть за відсутності прямого зв'язку власності між підзвітним суб'єктом та відповідним «establishment». Це фактично формує високодеталізовану наглядову карту мережевої структури всього фінансового сектору Європейського Союзу.

У додатку до документа AMLA міститься комплексний розділ із визначеннями, який має критичне значення для гармонізованого наглядового тлумачення у всіх державах-членах ЄС. Документ визначає поняття «клієнт», «фінансова установа», «структурний підрозділ», «інформація щодо відповідності критеріям відбору», «підзвітний суб'єкт» та «визначений підзвітний суб'єкт». Особливо важливим є надзвичайно широке визначення поняття «фінансова інституція», яке охоплює страхові компанії, інвестиційні фірми, структури UCITS/AIF, платіжні установи, постачальників послуг, пов'язаних із криптоактивами (CASPs), центральні депозитарії цінних паперів та інші небанківські фінансові установи. Це демонструє, що AMLA із самого початку формує інтегрований периметр нагляду у сфері ПВК/ФТ, який поширюється практично на весь фінансовий сектор Європейського Союзу, включаючи цифрові фінанси та екосистему криптоактивів. Документ також приділяє значну увагу гармонізованим методологіям підрахунку клієнтів, уникненню подвійного обліку та стандартизованим правилам агрегації клієнтських даних, що свідчить про підготовку AMLA до масштабної наглядової аналітики даних та моделювання ризиків на рівні всього Європейського Союзу.

Висновки:

- **Документ фактично створює першу практичну модель централізованого нагляду AMLA у сфері ПВК/ФТ над транскордонними фінансовими групами ЄС через гармонізовану звітність щодо відповідності критеріям відбору та консолідований збір наглядових даних.** Великим фінансовим групам необхідно уже зараз створювати централізовані системи управління даними у сфері ПВК/ФТ та групові інфраструктури звітності.
- **AMLA формує новий ризик-орієнтований підхід до визначення значної транскордонної присутності через кількість клієнтів, обсяги транзакцій та масштаби діяльності у межах механізму свободи надання послуг.** Це означає, що фінансові установи повинні суттєво посилити внутрішній моніторинг транскордонних операцій та деталізовану аналітику клієнтів і транзакцій у різних державах-членах ЄС.
- **Документ демонструє перехід ЄС до високоавтоматизованої наглядової екосистеми з блокуючими механізмами валідації, стандартизованими шаблонами та машинозчитуваною звітністю.** Є необхідність модернізації IT-систем комплаєнсу, архітектури регуляторної звітності та автоматизованих механізмів контролю якості даних у фінансових установах.
- **AMLA суттєво розширює периметр нагляду, включаючи постачальників послуг, пов'язаних із криптоактивами (CASPs), платіжні установи, страхові компанії, агентські мережі та інші нетрадиційні фінансові структури.** Це означає, що фінтех- та крипто-сектори в ЄС поступово інтегруються у повноцінну централізовану архітектуру нагляду у сфері ПВК/ФТ ЄС.

# Звіти окремих інституцій та експертів

## Оцінка підтримки Росією ядерної програми та військових об'єктів Північної Кореї [6]

Королівський інститут об'єднаних служб (RUSI) проводить системні дослідження глобальних загроз, пов'язаних із діяльністю держав, що підтримують тероризм та розповсюдження зброї масового знищення (ЗМЗ). Аналітичні матеріали інституту, зокрема нещодавні звіти серії "Site Profile", присвячені хімічним об'єктам КНДР (наприклад, "The DPRK's Chemical Facilities: Aoji-ri Area" та "Kanggye Area"), а також розслідування щодо прихованих підводних військових операцій РФ ("Seabed War: Russia's Secretive Defence Units"), формують цілісну картину безпрецедентного рівня координації між авторитарними режимами. Ця співпраця становить критичну загрозу для глобальної системи протидії фінансуванню розповсюдження ЗМЗ (ПФР), оскільки вона спирається на глибоко ешелоновані мережі ухилення від міжнародних санкцій, які інтегрують нелегальну торгівлю зброєю, передачу технологій подвійного призначення та приховані транскордонні фінансові розрахунки.

Консолідований аналіз публікацій RUSI свідчить, що співпраця між Російською Федерацією та Корейською Народно-Демократичною Республікою вийшла за межі ситуативного політичного союзництва, трансформувавшись у стійкий логістичний та фінансовий симбіоз. Забезпечення функціонування таких закритих об'єктів, як хімічні комплекси в Aoji-ri та Kanggye, вимагає постійного припливу високотехнологічного обладнання, прекурсорів та спеціалізованих матеріалів, які КНДР не здатна виробляти самостійно. Для задоволення цих потреб використовуються складні схеми фінансування розповсюдження ЗМЗ, у яких Росія виступає не лише як постачальник, але й як ключовий фінансовий та логістичний транзитер, використовуючи свою фінансову інфраструктуру для приховування реальних бенефіціарів угод та обходу санкцій Радбезу ООН.

**Висновки:**

- **Координація дій між підсанкційними державами вимагає від СПФМ кардинального перегляду алгоритмів виявлення ФР ЗМЗ:** оцінка ризику повинна враховувати не лише прямі зв'язки з КНДР чи РФ, але й складні транзитні схеми постачання товарів подвійного призначення через юрисдикції-посередники.
- **Суб'єктам фінансового моніторингу необхідно посилити контроль за транзакціями у сфері міжнародного торговельного фінансування**, впроваджуючи обов'язкову перевірку сертифікатів кінцевого споживача для високотехнологічного обладнання.
- **Еволюція прихованих військових та диверсійних структур вимагає від підрозділів комплаєнсу глибшого аналізу корпоративної структури клієнтів,** щоб запобігти обслуговуванню компаній-фасадів, які закуповують обладнання в інтересах державних розвідувальних або військових апаратів підсанкційних режимів.
- **Національним регуляторам доцільно інтегрувати розвідувальну інформацію аналітичних центрів (на кшталт звітів RUSI) у національні оцінки ризиків** ПВК/ФТ/ФР для своєчасного інформування фінансового сектору про нові вектори ухилення від санкцій.

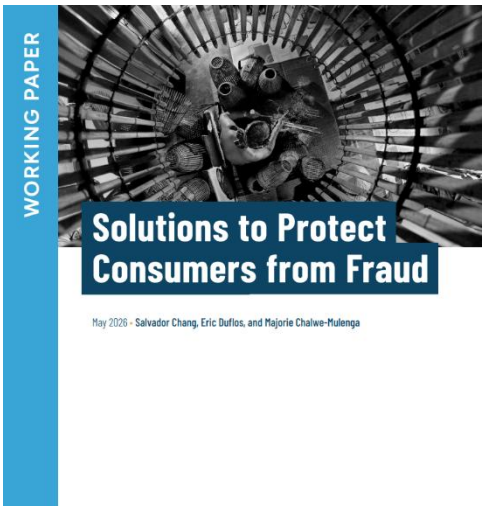
У розрізі ПВК/ФТ/ФР особливу небезпеку становлять механізми взаєморозрахунків, які обслуговують цю гібридну співпрацю. Оскільки обидві юрисдикції перебувають під жорстким

6

санкційним тиском, вони активно розбудовують альтернативні платіжні коридори. Це включає використання багаторівневих компаній-оболонок, зареєстрованих у лояльних або юрисдикціях зі слабким регулюванням, проведення бартерних операцій (зокрема обмін військового обладнання та боєприпасів на сировину чи технології), а також використання криптовалют та нерегульованих платформ децентралізованих фінансів (DeFi) для маскування транзакцій. Дослідження підводних диверсійних спроможностей РФ ("Seabed War") додатково вказує на розвиток фізичної та логістичної інфраструктури для здійснення прихованих операцій, що також вимагає значного тіньового фінансування та створення фіктивних корпоративних структур для закупівлі океанографічного та військово-морського обладнання на Заході.

Інтеграція іранського фактора (як зазначено в матеріалах щодо збройних сил Ірану та проблем американської розвідки) довершує архітектуру цієї "осі обходу санкцій". Співпраця між Москвою, Пхеньяном та Тегераном формує замкнений цикл виробництва, тестування та постачання озброєнь і технологій ЗМЗ, який супроводжується створенням паралельної фінансової екосистеми. Для світової спільноти комплаєнсу це означає, що типології фінансування розповсюдження ЗМЗ більше не обмежуються виявленням прямих транзакцій з КНДР чи Іраном; вони вимагають глибинного аналізу ланцюгів постачання, виявлення прихованого транзиту через треті країни та моніторингу компаній, які беруть участь у торгівлі товарами подвійного призначення. Ефективна протидія цій загрозі потребує від СПФМ впровадження розширених інструментів OSINT (розвідки на основі відкритих джерел), аналізу торговельного фінансування та ідентифікації кінцевих споживачів продукції, що може бути використана на військових і хімічних об'єктах.

## Рішення для захисту споживачів від шахрайства у цифрових фінансах [7]




У травні 2026 року Консультативна група з питань допомоги бідним (CGAP) презентувала розгорнутий робочий документ, присвячений комплексному розв'язанню проблеми фінансового шахрайства у глобалізованому цифровому середовищі. Автори документа констатують, що фінансове шахрайство вийшло за межі локальних інцидентів операційної безпеки, перетворившись на загрозу транснаціонального рівня, яка розвивається з безпрецедентною швидкістю та масштабами. Каталізаторами цієї ескалації стали вибухове зростання ролі соціальних мереж як каналів розповсюдження шкідливого контенту, адаптація генеративного штучного інтелекту (GenAI) кримінальними синдикатами для масового створення фішингових повідомлень та дипфейків, а також масове впровадження систем миттєвих платежів, які позбавляють фінансові установи часу на реверсні дії. Дослідження підкреслює, що шахрайство не лише генерує прямі економічні втрати, а й критично підриває фундаментальну довіру до екосистеми цифрових фінансових послуг (DFS), нівелюючи досягнення у сфері фінансової інклюзії та створюючи масивні потоки брудних коштів, що підлягають подальшому відмиванню, безпосередньо впливаючи на ефективність національних систем ПВК/ФТ.

Фундаментальною класифікаційною новацією є структурування шахрайських дій на дві макрокатегорії: авторизоване шахрайство (скам), за якого жертва під впливом витонченої соціальної інженерії чи психологічного тиску свідомо та самостійно ініціює переказ коштів або

[7] https://www.cgap.org/sites/default/files/publications/Fraud%20Solutions%20WP_web.pdf

розкриває автентифікаційні дані, та неавторизоване шахрайство, яке відбувається без прямої участі жертви шляхом технічного компрометування систем (наприклад, захоплення облікового запису — Account Takeover, ATO). Для протидії цим загрозам CGAP систематизував 56 конкретних ініціатив та рішень, згрупувавши їх у вісім стратегічних напрямів. Цей спектр охоплює: обмін розвідувальними даними, виявлення шахрайської реклами, впровадження телекомунікаційних стандартів безпеки, посилення методів автентифікації користувачів, створення "позитивного тертя" (positive frictions) під час транзакцій, використання поведінкової біометрії, розбудову механізмів повернення коштів та розробку адаптивних поведінкових кампаній для споживачів.

Дослідження глибоко аналізує низку успішних міжнародних прецедентів багатосторонньої співпраці. Знаковим є приклад Індії, де Асоціація фінтеху з розширення прав і можливостей споживачів (FACE) функціонує як визнана саморегулівна організація (SRO). FACE розбудувала архітектуру безпрецедентної взаємодії: вона агрегує масиви скарг на хижацькі кредитні практики, передаючи їх до Резервного банку Індії (RBI) для регуляторного втручання та до Міністерства внутрішніх справ (MHA) для кримінального переслідування. Особливої ефективності системі надає статус FACE як "пріоритетного позначувача" (priority flagger) для корпорації Google: спираючись на верифіковані "білі списки" RBI, ця співпраця дозволила ідентифікувати та видалити понад 4700 шахрайських додатків з платформи Google Play Store станом на серпень 2023 року.

Висновки:

- **Трансформація шахрайських схем з використанням GenAI вимагає від СПФМ впровадження інструментів поведінкової біометрії** (швидкість введення тексту, патерни навігації) для виявлення несанкціонованого доступу або факту маніпулювання клієнтом у режимі реального часу, оскільки традиційної автентифікації вже недостатньо.
- **Застосування концепції «позитивного тертя» (динамічні попередження, затримки ризикових платежів) має бути інтегровано в сценарії транзакційного моніторингу** для запобігання авторизованому шахрайству, знижуючи обсяги незаконних коштів, що потрапляють у систему для відмивання.
- **Ефективна протидія фінансовій кіберзлочинності вимагає створення національних хабів обміну розвідувальними даними**, де СПФМ, правоохоронні органи та технологічні платформи (BigTech, телеком-оператори) можуть оперативно синхронізувати інформацію для блокування шахрайських каналів на ранніх етапах.
- **Регуляторам та СПФМ необхідно розробити збалансовані протоколи ризик-менеджменту, які дозволять використовувати передові AI-моделі для виявлення шахрайства та ПВК/ФТ**, водночас неухильно дотримуючись вимог законодавства про захист персональних даних клієнтів.

Іншим еталонним кейсом є канадська Операція Avalanche — регуляторно-правоохоронна ініціатива під егідою Комісії з цінних паперів Британської Колумбії (BCSC). Проєкт спрямований на деконструкцію специфічного вектора криптографічних злочинів — "approval phishing", коли жертв маніпулятивно змушують підписувати транзакції, що надають зловмисним смарт-контрактам безлімітний доступ до їхніх цифрових активів. Залучивши компанію Chainalysis як технічного партнера, BCSC ідентифікує скомпрометовані гаманці у мережі Ethereum та ретранслює цю розвідувальну інформацію провідним криптобіржам (Coinbase, Kraken, Wealthsimple), які негайно блокують виведення коштів. Лише під час першої фази операції у березні 2025 року було врятовано активи на суму 4,3 млн канадських доларів, що доводить ефективність інтеграції блокчейн-аналітики у наглядову практику.

В Індонезії проблему вирішують через функціонування Satgas PASTI — потужної урядової міжвідомчої цільової групи, до якої входять Управління фінансових послуг (OJK), Банк Індонезії, Національна поліція та Міністерство зв'язку (Kominfo). Група реалізує стратегію "блокади екосистеми": шляхом інтенсивного кіберпатрулювання виявляються неліцензовані платформи кредитування, інвестиційні піраміди та нелегальні криптоопераційї, після чого Kominfo здійснює негайне примусове видалення додатків та блокування доменів на всій території країни. Цей механізм радикально скорочує час життя шахрайських ресурсів.

Документ CGAP також артикулює складні регуляторні дилеми (trade-offs), які супроводжують впровадження антифрод-рішень. Найконфліктнішою є лінія між захистом персональних даних та глибиною моніторингу: найсучасніші системи виявлення шахрайства, зокрема алгоритми на базі ШІ та поведінкової біометрії, вимагають безперервного доступу до надчутливих метаданих користувачів, що створює ризики порушення конфіденційності. Крім того, впровадження жорстких протоколів безпеки (наприклад, штучних затримок платежів або багатофакторної перевірки) може призвести до ненавмисної фінансової ексклюзії маргіналізованих груп споживачів, особливо в країнах з ринком, що формується, та країнах, що розвиваються (EMDE), де відсутній належний інституційний потенціал для балансування цих пріоритетів. Документ наголошує на нагальній потребі формування глобальної регуляторної рамки за участі FATF, FSB та Світового банку для забезпечення транскордонної протидії злочинним мережам, що використовують юрисдикційний арбітраж.

| Назва ініціативи (Юрисдикція) | Координаційний механізм | Застосована технологія / Метод | Практичний результат взаємодії |
|---|---|---|---|
| FACE (Індія) | Саморегулівна організація у партнерстві з державними регуляторами | Алгоритмічний моніторинг екосистеми додатків, статус пріоритетного позначувача | Безпрецедентне видалення 4700+ шахрайських додатків з Google Play |
| Operation Avalanche (Канада) | Комісія з цінних паперів (BCSC) спільно з приватним сектором | Блокчейн-аналітика (спільно з Chainalysis) для моніторингу смарт-контрактів | Превентивне блокування транзакцій біржами; порятунок $4,3 млн CAD |
| Satgas PASTI (Індонезія) | Урядова міжвідомча цільова група | Кіберпатрулювання та адміністративна "блокада екосистеми" | Тотальне блокування доменів неліцензованих платформ та інвестиційних пірамід |

## Гендерний та ідентифікаційний аналіз у межах архітектури протидії гібридним загрозам [8]

[8] https://static.rusi.org/gender-identity-analysis-aide-memoire-hybrid-threats-may-26.pdf

У травні 2026 року Королівський інститут об'єднаних служб (RUSI) представив аналітичний документ "Gender and Identity Analysis Framework for Hybrid Threats", розроблений групою експертів (Клаудія Воллнер, Джессіка Вайт, Рейчел Граймс). Цей звіт є складовою масштабного проєкту з посилення стратегій НАТО щодо протидії гібридним загрозам і пропонує інноваційну оптику для аналізу того, як ворожі державні та недержавні актори інструменталізують соціальні конструкти — гендерні ролі, сексуальність, міграційний статус, етнічність та релігійні переконання — для досягнення підривних політичних цілей. Автори стверджують, що сучасні гібридні кампанії свідомо конструюються навколо цих питань ідентичності для створення ефекту суспільної поляризації, розмивання довіри до демократичних інститутів та послаблення спроможності Альянсу до колективної оборони.

Дослідження фундаментально критикує усталену практику безпекових та військових інституцій, які схильні де-пріоритезувати операції впливу, засновані на маніпуляції ідентичністю, маркуючи їх як "загрози нижчого рівня" (lesser harms) порівняно з конвенційними військовими або кібернетичними викликами. RUSI доводить, що така сегментація є хибною. На рівні людської безпеки цілеспрямовані кампанії цькування, антигендерна риторика та сексуалізований примус спричиняють реальні фізичні та психологічні травми, змушуючи маргіналізовані групи до самоцензури та усунення з публічного простору. На макрорівні державної безпеки це призводить до ерозії демократичної стійкості, штучного звуження кадрового потенціалу для лідерських позицій та формування передумов для масових заворушень, які виснажують національні ресурси і відкривають шлях для глибшого іноземного втручання. Таким чином, питання ідентичності стають повноцінними операційними змінними (operational variables).

**Висновки:**

- **Фінансові розвідки та СПФМ мають розширити традиційні типології фінансування тероризму**, включивши до них індикатори фінансових потоків, що живлять структури (тролеферми, радикальні ГО), які цілеспрямовано розпалюють соціальну поляризацію на ґрунті ідентичності в інтересах ворожих держав.
- **Картографування забезпечувальних екосистем гібридних загроз вимагає від комплаєнс-підрозділів запровадження EDD щодо НПО та медіакомпаній**, які мають ознаки фінансування з високоризикових юрисдикцій.
- **Правоохоронним та наглядовим органам необхідно створити механізми оперативного обміну даними про гібридні інформаційні кампанії** з фінансовим сектором, що дозволить СПФМ своєчасно ідентифікувати та блокувати транзакції суб'єктів, залучених до підривної діяльності.
- **Інструменталізація "юридичної війни" (lawfare) та дезінформації як засобів гібридної агресії формує потребу в розробці нових алгоритмів оцінок ризику**, що враховуватимуть не лише економічні, а й соціально-політичні маркери діяльності клієнтів.

Методологічним ядром документа є запровадження системи структурованих підказок (structured prompts), призначених для військових планувальників, аналітиків розвідки та фахівців зі стратегічних комунікацій. Цей інструментарій дозволяє ідентифікувати приховані патерни в потоках дезінформації, визначаючи не лише об'єкт атаки, але й операційну мету кампанії. Автори наголошують на критичній необхідності переходу від поверхневого аналізу

наративів до комплексного картографування забезпечувальних екосистем (enabling ecosystems). Це означає, що аналітики повинні відстежувати фінансові потоки, механізми "юридичної війни" (lawfare), коаліційні зв'язки між радикальними угрупованнями та організаційні структури, які матеріально підживлюють та реплікують поляризуючі наративи у суспільстві.

Звіт також закликає до визнання гендерно зумовленого примусу та залякування невіддільними елементами ворожого операційного мистецтва (adversary tradecraft), які мають систематично фіксуватися в рамках загальної оцінки загроз. Документ формулює вимогу щодо посилення міжвідомчої та крос-доменної координації, що передбачає безперебійний обмін розвідувальними даними між оборонними, правоохоронними структурами, спецслужбами та цивільними регуляторами. У практичній площині RUSI рекомендує поєднувати оборонні стратегії стійкості (кіберзахист, захист інфраструктури) з проактивними заходами руйнування (disruption), спрямованими на переривання логістичних та фінансових ланцюгів противника.

У площині ПВК/ФТ цей аналіз набуває особливого значення: інструменталізація соціальних поділів вимагає безперервного фінансування через мережі псевдогромадських організацій, фондів та медіаструктур, що відкриває новий фронт для систем фінансового моніторингу у виявленні гібридних форм фінансування тероризму та підривної діяльності.

## «Це просто бізнес»: Як працює сучасна транснаціональна злочинна організація [9]


У сучасному світі, де кордони стають дедалі прозорішими для капіталу, зброї та наркотиків, кримінальні синдикати все частіше нагадують багатонаціональні корпорації. Вони мають вертикаль управління, логістичні департаменти, відділи безпеки, фінансовий моніторинг та навіть власну «цифрову культуру» спілкування. Розслідування, проведене Organized Crime and Corruption Reporting Project, відкриває завісу над буденністю одного з таких угруповань, яке очолює албанець на прізвисько «Тоні» — Дрітан Гжіка. Завдяки витоку тисяч приватних повідомлень із зашифрованого месенджера Sky ECC, який був зламаний європейською поліцією у 2021 році, ми можемо побачити не романтизовану версію кримінального бізнесу з фільмів, а нудну та жорстоку реальність — «просто бізнес», як люблять повторювати самі фігуранти.

Головний герой цього розслідування, Дрітан Гжіка, албанець, який опинився в Еквадорі ще у 2009 році за тимчасовою туристичною візою та зумів стати ключовим гравцем на латиноамериканському наркоринку. Еквадор, який довгий час сприймався як відносно спокійна країна між Колумбією та Перу, за останні роки перетворився на магістраль для кокаїну. Це сталося не випадково: через країну проходить величезний потік легальних товарів — бананів, креветок, квітів — які потребують швидкого транзиту через порти, і саме цю логістичну вразливість використовують наркоторговці. Гжіка зі своєю командою — яскравий приклад того, як іноземці, які приїхали з Балкан, використовують прогалини в місцевій економіці та системній корупції для отримання надприбутків. Використовуючи Sky ECC, «Тоні» особисто керував усім ланцюжком: від переговорів з колумбійськими постачальниками, які контролюють лабораторії

[9] https://www.occrp.org/en/project/the-crime-messenger/its-just-business-texts-reveal-the-daily-work-and-drama-of-an-international-cocaine-syndicate

в джунглях, до найму водіїв вантажівок, управління графіками відправлення контейнерів і вирішення фінансових суперечок з партнерами в Іспанії, Нідерландах та навіть росії.

Структура цієї організації вражає своєю «корпоративністю» та прагматизмом. Експерти зазначають, що албанські трафіканти привнесли в Еквадор бізнес-модель, засновану виключно на ринкових можливостях, уникаючи непотрібних територіальних воєн з місцевими угрупованнями. Вони платять за послуги — за логістику, захист, інформацію — але не втручаються у внутрішні війни еквадорських угруповань. Це прагматизм, що межує з холодним цинізмом. Гжіка шукає «серйозних хлопців», які мають «ноги на землі», укладає контракти на «мінімум дві тонни на місяць» і навіть звертається до постачальників, які контролюють одразу п'ять «кухонь» (так у їхньому сленгу називаються лабораторії з виробництва кокаїну, зазвичай розташовані глибоко в колумбійських джунглях).

У лютому 2021 року в еквадорській провінції Лос-Ріос п'ятьох чоловіків затримали з півтонною кокаїну, знайденою у вантажівці. Наркотик був нарізаний на кілограмові брикети з логотипом «UNICO» — своєрідний бренд, який використовувала мережа Гжіки для маркування своєї продукції. Чати Sky ECC показують миттєву реакцію боса: паніка, підозри та спрага помсти з'являються вже за лічені хвилини після появи новини в місцевих ЗМІ. Цей епізод демонструє дволикість наркотрафіку: поряд з діловими переговорами про логістику, знижки та маржу тут же присутня готовність до фізичного насильства, яке сприймається як звичайний інструмент вирішення операційних проблем.

Що робило цю організацію особливою протягом багатьох років — це глибока та системна інфільтрація державних структур Еквадору, зокрема портової поліції, митниці та навіть антинаркотичного підрозділу. Чати виявляють цілу мережу «друзів» всередині порту Гуаякіля — головного морського вузла країни, через який проходять сотні контейнерів щодня. Ці люди надають «привілейовану інформацію» з комп'ютерних систем терміналів: які контейнери перевірятимуть, де чергують охоронці, коли змінюються графіки. Один із засуджених у цій справі — офіцер поліції, який особисто відповідав за огляд контейнерів на предмет контрабанди. Інший — відставний офіцер на прізвисько «Ґлок» (справжнє ім'я — Ектор Пессантес), який надавав інсайди зсередини антинаркотичної поліції.

Криміналітет буквально звіряв свій календар з графіком роботи правоохоронців. Це не просто хабар — це системний збій держави, коли частина силових структур фактично працює на наркосиндикат. Дослідник Даніель Понтон, декан факультету досліджень безпеки в еквадорському державному університеті, зазначає, що уряд країни так і не зумів належним чином захистити порти, які переважно управляються приватними компаніями, що отримали концесії від держави, і ця приватизація створила безліч сірих зон для корупції.

Логістика перевезень в організації Гжіки була поставлена на потік. Методи, які вони використовували, варіювалися від примітивних до витончених. Найпростіший — так званий «метод сліпого гака», коли наркотики просто залишають в контейнері у сліпій зоні, змішуючи з легальним вантажем без складного маскування. Також практикується вбудовування кокаїну безпосередньо в металеву структуру самого контейнера — підхід, який, за даними Міністерства внутрішніх справ Іспанії, мережа почала використовувати для приховування менших партій після того, як нідерландська влада перехопила вантаж вагою 1,1 тонни у 2020 році.

Окремої уваги заслуговує метод, який вони називають «company to company» — коли трафіканти мінімізують ризики, повністю контролюючи як компанії-експортери в Еквадорі, так і компанії-імпортери в Європі. Це дозволяє їм уникати посередників, які можуть бути ненадійними або завербованими поліцією. Згідно з судовими записами та даними еквадорського бізнес-реєстру, Гжіка, його засуджені спільники та їхні родичі володіли або управляли більш ніж 30 компанями в країні. Особливу роль відігравали компанії з пакування бананів — ідеальне прикриття, адже банани потребують швидкого проходження портів для

збереження свіжості, що дає митниці дуже мало часу на ретельний огляд. Серед компаній, які використовувала мережа, була Agircomtrade, співвласником якої, за даними прокуратури, був сам Гжіка. Іспанія, зі свого боку, стала головним логістичним хабом для європейського розподілу. У листі до еквадорської влади національний суд Іспанії назвав Маріо Санчеса Рінальді, праву руку Гжіки та аргентино-італійського бізнесмена на Коста-дель-Соль, керівником «потужної групи» підприємств з імпорту та експорту продуктів харчування, яка «сприяла логістиці» контрабанди кокаїну для третіх сторін.

Фінансова дисципліна в цьому синдикаті заслуговує на окрему згадку — вона виявилася настільки ж жорсткою, наскільки й винахідливою. Чати рясніють суперечками про борги, прострочення платежів, курси валют, перевірки якості продукту та детальні обговорення маржі. Для переміщення мільйонів доларів через кордони мережа Гжіки використовує підпільну систему переказів готівки, що працює на основі «токенів». Токен — це, як правило, серійний номер доларової або єврової купюри, який слугує паролем: відправник повідомляє цей номер отримувачеві, а той називає його «касиру» у підпільному пункті в Калі, Мадриді, Брюсселі чи Бірмінгемі, щоб отримати гроші. Це дозволяє обходити банківський нагляд та фінансовий моніторинг, але створює нові ризики, пов'язані з людським фактором. В одному з епізодів, що став майже комічним, якби не масштаби, Гжіка та його спільник на прізвисько «Інженер» (засуджений пізніше за відмивання грошей) обговорюють збір готівки в Кіто. Китайський посередник видає на 10 000 доларів менше. Виявляється, кур'єр «злякався». Гроші, ймовірно, просто випали чи були загублені під час панічної втечі. Гжіка, попри свій статус великого боса, особисто вникає в цю різницю, сперечаючись про кожну тисячу, що знову ж таки доводить: для нього це не слава чи влада, а конкретні числа на рахунку.

Іронія долі цієї імперії полягає в тому, що її знищила цифрова безпека — точніше, її відсутність. Вже у вересні 2020 року Гжіка отримав чутки про те, що Sky ECC скомпрометований. «Ми все змінюємо, тому що багато хто каже, що Sky більше не є надійним», — пише він колезі, закликаючи купувати пристрої BC1 — продукт конкурента, який вважався більш захищеним. Це свідчить про те, що інформація про вразливість платформи вже циркулювала у злочинному світі. Однак людський фактор, звичка до зручного інтерфейсу та, можливо, інерція мислення взяли гору. Вони продовжували використовувати Sky майже пів року, аж до березня 2021 року. Ця зневага до базових правил операційної безпеки — або, навпаки, надмірна впевненість у власній невразливості — згодом стала фатальною. Коли європейська поліція зламала шифрування Sky ECC, всі чати, всі суперечки про борги, всі імена друзів та всі токени стали доказовою базою. Це призвело до арештів, конфіскацій та засудження щонайменше 17 членів мережі в Еквадорі, 15 з яких чекають на апеляцію, а ще чотири особи були засуджені за відмивання понад 43 мільйонів доларів, переведених через систему між 2015 та 2023 роками.

Сам Дрітан Гжіка, оголошений одним з найбільш розшукуваних злочинців Еквадору, зумів непоміченим залишити країну ще до хвилі арештів. Його подальша доля стала символом того, наскільки складною є міжнародна координація у переслідуванні наркобаронів. Він був затриманий в Абу-Дабі у травні 2025 року — майже через чотири роки після того, як його чати потрапили до рук слідства. На момент публікації звіту OCCRP він очікує на екстрадицію до Еквадору, де суддя вже видав ордер на його утримання під вартою до повернення. Адвокати Гжіки, які не відповіли на запити журналістів, під час досудового слухання в Еквадорі стверджували, що доказів недостатньо, а законність отримання повідомлень із Sky є сумнівною.

Але навіть якщо його екстрадують та засудять, проблема наркотрафіку в Еквадорі нікуди не зникне. Ренато Рівера наголошує: справа не лише в присутності албанських ділків, а в тому величезному фінансовому потоці, який вони генерують. Ці гроші є паливом для місцевих банд, які постійно борються за шматок цього пирога. Еквадор, колись відносно мирна країна, нині захлинається в крові, а рівень вбивств сягнув історичних максимумів.

«Це просто бізнес», — повторював Гжіка в одному з липневих діалогів 2020 року, скаржачись на затримки платежів. Але цей бізнес залишає після себе зруйновані долі, корумпованих поліцейських та країни, захоплені в заручники війною з наркотиками.

Розшифровки Sky ECC, які лягли в основу цього розслідування, — це не просто сухий доказ у суді. Сотні сторінок чатів, які опрацювали журналісти OCCRP, показують справжнє обличчя глобальної наркотичної торгівлі: це не романтика мафіозних кланів, а виснажлива, нервова та кривава робота, де десять тисяч доларів можуть «загубитися», а людське життя важить менше, ніж вдало провезений контейнер з кокаїном.

І поки Еквадор продовжує захлинатися в крові та кокаїні, ув'язнення однієї людини є лише краплею в морі, але критично важливим кроком у розумінні того, що насправді ховається за фразою «просто бізнес», коли її вимовляє людина, яка будувала свою імперію на стражданнях мільйонів.

**Висновки:**

- **Кримінальний бізнес діє як транснаціональна корпорація.** Організація мала чітку вертикаль управління, довгострокові контракти з постачальниками, сувору фінансову дисципліну та навіть брендування продукції.
- **Корупція в державних структурах є критичною умовою існування таких мереж.** Успіх синдикату залежав не від зброї, а від «друзів». Правоохоронні органи та портова інфраструктура були не бар'єром, а частиною логістичного ланцюжка синдикату.
- **Шифровані месенджери є одночасно головним інструментом і вразливістю організованої злочинності.** Злам чатів поліцією у 2021 році надав прокуратурі безпрецедентний масив доказів — фактично «щоденник» роботи синдикату.
- **Геополітична стратегія використання «логістичних слабких місць».** Еквадор став магістраллю не через власне виробництво кокаїну, а через вразливість портової інфраструктури та величезний обіг легальних товарів, які потребують швидкого митного оформлення.

## Африканський фронтир: як китайські шахрайські синдикати створюють осередки на новому континенті [10]

У квітні цього року китайське посольство на Мадагаскарі зробило безпрецедентний крок, оприлюднивши офіційну заяву для громадськості, в якій попередило про зростаючу небезпеку примусової праці на території цієї острівної держави.

Цей несподіваний дипломатичний крок безпосередньо передував драматичній історії порятунку громадянина Китаю, якому вдалося втекти з одного з шахрайських комплексів в Антананаріву, столиці Мадагаскару. За його словами, він був заманений туди вербувальником, який діяв із Камбоджі — країни, що давно вважається одним із ключових осередків багатомільярдної індустрії кібершахрайства в Південно-Східній Азії.

[10] https://globalinitiative.net/analysis/china-linked-scam-operations-pivot-to-africa-presenting-new-challenges-for-at-risk-countries/

Цей випадок не є ізольованим інцидентом. Натомість він є яскравим симптомом набагато глибшої та системнішої трансформації, яка зараз відбувається в ландшафті транснаціональної організованої злочинності. Якщо раніше подібні епізоди були зосереджені переважно в регіоні Меконгу — від М'янми до Лаосу та Камбоджі, — то тепер тривожні сигнали лунають з різних куточків Африки. Достатньо поглянути на потік оголошень в Telegram та інших соціальних платформах, які заманюють шукачів пригод на «маркетингові позиції» або так звану роботу, пов'язану з «побаченнями» та романтичним спілкуванням, нібито в престижних компаніях Африки. Ці оголошення, часто написані кількома мовами — китайською, англійською, французькою, тайською — є типовими приманками для майбутніх жертв торгівлі людьми, яких потім примушують до роботи в шахрайських кол-центрах.

Усе це змушує дослідників і правоохоронців говорити про тривожний тренд: шахрайські синдикати, що мають тісні зв'язки з Китаєм, дедалі активніше звертають свій погляд на Африку. І це не просто тимчасова корекція маршрутів, а стратегічне переміщення, спричинене глибинними структурними факторами. Оскільки тиск на Південно-Східну Азію — багаторічну «столицю» цих операцій — постійно зростає завдяки скоординованим діям місцевої влади та міжнародних організацій, злочинні мережі активно шукають нові, більш «гнучкі» та лояльні юрисдикції, де правила гри можна диктувати без особливих перешкод.

Довгий час, як наголошується в документі, Африка відігравала в цій системі дещо іншу роль — роль донора робочої сили. Щонайменше з 2022 року синдикати систематично вербували громадян африканських країн для «роботи» у Камбоджі, М'янмі та Лаосі. У полоні цих схем опинялися люди з Кенії, Уганди, Нігерії, Ефіопії, Південно-Африканської Республіки та Зімбабве. Їм пропонували вигадані високооплачувані посади на Близькому Сході або в Південно-Східній Азії, а натомість після прибуття конфісковували паспорти, замикали в обнесених колючим дротом комплексах і змушували щодня по 12-16 годин виманювати гроші в довірливих громадян по всьому світу. Консервативні оцінки, наведені в аналітиці, свідчать, що таким чином було залучено від 10 до 15 тисяч африканців із понад 30 країн. Однак останнім часом географія вербування розширилася, охопивши франкомовні держави — Бурунді, Камерун, Демократичну Республіку Конго і, звісно ж, Мадагаскар, де, власне, й стався скандальний випадок. Ця зміна свідчить про те, що злочинні мережі адаптуються до мовних бар'єрів і використовують колоніальну спадщину для розширення свого впливу.

Але набагато тривожнішим є те, що Африка тепер розглядається не лише як джерело дешевої робочої сили, а як повноцінний хаб для розгортання самих шахрайських операцій. Цьому сприяє низка чинників. По-перше, на континенті вже давно існує своя, хоч і менш технологічна, індустрія шахрайських центрів, особливо в Нігерії та ПАР, що створює певну інфраструктурну та кадрову основу. По-друге, рівень корупції, слабкість правоохоронної системи та, найголовніше, відсутність належного регулювання таких секторів, як гральний бізнес, криптовалютні обмінники та аутсорсингові центри обслуговування клієнтів, роблять багато африканських юрисдикцій надзвичайно привабливими для злочинців.

Аналітики наводять кілька яскравих прикладів ранніх, хоч і не зовсім успішних, спроб злочинців закріпитися на континенті. Зокрема, на початку 2020-х років потужна мережа, пов'язана з Китаєм, намагалася проникнути в Уганду. Кілька ключових забудовників шахрайських комплексів, які раніше діяли в Камбоджі та М'янмі, передислокувалися до цієї

східноафриканської країни. Лідером угруповання був Лю Давей, особа, тісно асоційована з сумнозвісною транснаціональною злочинною організацією, яку очолював легендарний китайський кримінальний авторитет Вань Куок-кой, відоміший під прізвиськом «Зламаний зуб» (Broken Tooth). Ця організація, що мала розгалужені структури по всій Південно-Східній Азії, займалася не лише шахрайством, а й наркоторгівлею та відмиванням грошей. Проте угандійській поліції за сприяння міжнародних партнерів вдалося заарештувати Лю Давея, який до того ж мав проблеми з законом у Китаї та Дубаї за попередні злочини, зокрема за участь у складній транснаціональній схемі з нерухомістю. Його екстрадиція тимчасово зірвала плани синдикату.

Інший показовий випадок стався в Південній Африці в 2023 році. Там спробував закріпитися Бай Чжаохуей, ймовірний голова ще одного величезного злочинного угруповання, яке відіграло ключову роль у створенні багатотисячних шахрайських центрів у М'янмі, перш ніж потрапило під удар тайської влади. Бай Чжаохуей, як з'ясувалося, був пов'язаний з тією ж самою організацією «Хунмень» (Hongmen), яка позиціонує себе як Всесвітня історико-культурна асоціація, але насправді є прикриттям для серйозної транснаціональної злочинної мережі, що перебуває під санкціями США та Великої Британії. І хоча сам Бай, ймовірно, перебрався до Китаю, сама структура «Хунмень» залишається активною в ПАР. Найяскравіший доказ цього — 2025 рік, коли асоціація публічно підтримала компанію, яка цілеспрямовано обслуговує китайськомовний ринок Південної Африки, що побічно свідчить про збереження контролю над фінансовими потоками.

Документ попереджає: це були лише поодинокі успіхи в інформаційній війні та поліцейській роботі, які стали можливими завдяки тому, що окремі ключові фігури вже були добре відомі правоохоронцям. Однак є всі ознаки того, що китайські мережі вже діють у кількох африканських країнах, і їхні операції стають дедалі масштабнішими. Цей розвиток, ймовірно, спровокований зворотною хвилею африканців, які масово повертаються з Південно-Східної Азії після того, як самі зазнали примусу до шахрайства. Ці люди — чи то втікачі, чи то звільнені під час поліцейських рейдів — повертаються додому, маючи за плечима безцінний для злочинців досвід: вони знають внутрішні протоколи роботи центрів, методи вербування, психологічні техніки впливу на жертв і, найважливіше, контакти в організованих групах. Таким чином, Африка отримує не лише нову робочу силу для шахрайства, а й «інструкторів» і «менеджерів», здатних перенести всю технологічну та адміністративну модель на місцевий ґрунт.

Згідно з дослідженнями Глобальної ініціативи проти транснаціональної організованої злочинності, вже ідентифіковано 14 країн, які перебувають у найвищій зоні ризику створення промислових шахрайських центрів. У кожній із цих локацій китайські синдикати підтримують активну присутність в Telegram, де публікують вакансії та координують дії. Крім того, там функціонують підпільні платіжні системи, які використовуються для відмивання шахрайських прибутків. Деякі групи, як-от ті, що базуються на Мадагаскарі, змогли залучити до своїх комунікаційних мереж понад 40 000 учасників — це цифра, яка свідчить про справді промислові масштаби підготовки.

На тлі цих загроз документ звертає увагу на позитивний, хоч і обережний, крок з боку інституцій Африканського Союзу. У березні цього року Операційний центр Континентального командування Африканського Союзу — спеціалізована агенція, яка займається боротьбою з нерегулярною міграцією та торгівлею людьми, — вперше зібрався для розробки конкретного плану дій. Учасники зустрічі, яка, як зазначається, була дуже продуктивною, визнали, що проблема примусової злочинності в шахрайських центрах більше не є виключно азійською. Було створено рамкову угоду для посиленої координації між африканськими країнами, а також висунуто пропозицію про співпрацю між Африкою та Азією, яку підтримав Таїланд — країна, що сама серйозно постраждала від цього явища.

Це, без сумніву, важливі перші кроки, які свідчать про те, що проблема нарешті почала підніматися на найвищий політичний рівень. Проте, як слушно зауважують експерти, цього катастрофічно недостатньо. Щоб запобігти перетворенню Африки на новий глобальний хаб шахрайських центрів і зменшити ризик того, що китайські синдикати нарощують свою присутність на континенті до промислових масштабів, необхідно негайно вжити щонайменше три додаткових групи заходів.

Перша та найважливіша сфера — це координація на рівні кордонів та міграційної політики. Африканський Союз має докласти максимальних зусиль для створення потужних механізмів обміну даними про підозрілих осіб, які перетинають кордони, для гармонізації візових вимог та імміграційних процедур. Операційний центр міг би відіграти тут ключову роль, виступаючи «координатором» між правоохоронними органами різних країн.

Друга сфера — це регулювання та обізнаність. Держави-члени АС мусять бути терміново навчені розпізнавати ранні попереджувальні знаки цього виду шахрайства: від підозрілих оголошень про роботу до незвичної активності навколо готелів або казино. Це має супроводжуватися жорсткішим регуляторним наглядом за тими секторами, які найчастіше використовуються як ширма та для відмивання грошей — за гральним бізнесом, обмінниками криптовалют, платіжними системами. У цьому контексті Асоціація держав Південно-Східної Азії (ASEAN) могла б поділитися цінним досвідом, хоча, звісно, африканське операційне середовище має свої унікальні виклики, пов'язані зі слабкістю інститутів.

І третя, найамбітніша мета — створення глобальної коаліції. Імпульс, створений зустріччю Африканського Союзу, не має згаснути. Натомість його слід використати для розробки спільних ініціатив на кшталт нещодавнього партнерства між ЄС та ASEAN, а також для координації зусиль окремих держав, як-от США, Великої Британії та Південної Кореї, які вже цілеспрямовано працюють над застосуванням санкцій до ключових злочинних акторів. Африканському Союзу, ймовірно, доведеться вступити в прямий діалог із Китаєм, враховуючи, що через територію КНР часто переправляють як африканських жертв торгівлі, так і, можливо, самих злочинців.

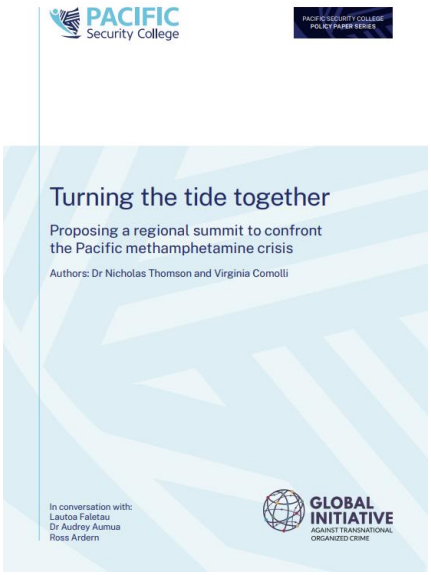
**Висновки:**

- **Географічний зсув загрози:** Шахрайські синдикати, пов’язані з Китаєм, системно переносять свою діяльність із Південно-Східної Азії до Африки через посилення тиску в регіоні Меконгу та пошук більш лояльних юрисдикцій із слабким управлінням.
- **Подвійна роль Африки:** Континент раніше використовувався переважно як джерело робочої сили для шахрайських центрів в Азії, однак тепер там активно створюються власні промислові шахрайські хаби, зокрема в Нігерії, Гані, Зімбабве та на Мадагаскарі.
- **Методи конспірації та масштаби:** Синдикати маскуються під легальний бізнес, використовують Telegram для вербування десятків тисяч учасників, а їхні комплекси часто функціонують як в'язниці для примусової праці.
- **Критична вразливість та потрібна реакція:** Африка залишається надзвичайно вразливою через корупцію та відсутність нагляду за гральним бізнесом і криптовалютами. Вирішальним фактором стане здатність Африканського Союзу запровадити жорсткі прикордонні механізми, посилити регулювання та створити глобальну коаліцію проти шахрайських центрів.

Документ завершується чітким і лаконічним висновком: Африка потребує негайних дій, покращеної координації та тривалої політичної волі, щоб уникнути долі стати новим глобальним осередком шахрайських центрів. Те, як африканські держави відреагують у найближчій перспективі — чи то через проактивну співпрацю, чи через інертність — визначить остаточний вердикт: чи вдасться стримати

експансію китайських синдикатів, чи вони стануть глибоко вкоріненою, майже невід'ємною частиною економічного та злочинного ландшафту континенту, повторюючи сумний сценарій Південно-Східної Азії, але в набагато більших масштабах.

## Як Тихоокеанський регіон намагається зупинити кризу синтетичних наркотиків [11]




Документ присвячений стрімкому поширенню метамфетаміну в державах Тихоокеанського регіону та формуванню комплексної регіональної відповіді на цю кризу. Автори розглядають проблему не лише як питання незаконного наркотрафіку чи діяльності транснаціональних організованих злочинних угруповань, а як багатовимірну кризу, що одночасно охоплює сфери громадського здоров'я, безпеки, соціальної стабільності, державного управління, правопорядку та людської безпеки загалом. Документ демонструє, що Тихоокеанські острови дедалі більше перетворюються з транзитного коридору між великими виробничими центрами метамфетаміну у Південно-Східній Азії та Америці на самостійний ринок споживання наркотиків, а подекуди навіть на потенційний майданчик для локального виробництва синтетичних наркотиків. Автори наголошують, що особливо гостро проблема проявляється у Фіджі, Тонга та Папуа Новій Гвінеї, однак фактично всі держави регіону вже стикаються із зростанням незаконного обігу наркотиків, збільшенням рівня споживання метамфетаміну та супутніми соціальними наслідками.

У документі детально пояснюється, що метамфетамінова криза має глибокі наслідки для локальних громад і державних систем. Вживання наркотиків руйнує соціальну згуртованість, посилює рівень насильства та злочинності на рівні громад, створює значне навантаження на медичні установи, систему правосуддя та пенітенціарну систему. Автори зазначають, що психіатричні відділення, лікарні та місцеві центри охорони здоров'я не справляються з великою кількістю осіб, які потрапляють до системи охорони здоров'я з тяжкими психозами та агресивною поведінкою, пов'язаною із вживанням метамфетаміну. Через відсутність спеціалізованих програм лікування залежності та центрів реабілітації значна кількість наркозалежних осіб потрапляє до системи кримінальної юстиції замість отримання медичної допомоги. Це, у свою чергу, перевантажує суди та місця позбавлення волі, які вже не здатні ефективно реагувати на масштаби проблеми. Документ також підкреслює стрімке зростання випадків ВІЛ, пов'язаних із ін'єкційним вживанням наркотиків та використанням спільних шприців, що створює додатковий масштабний виклик для систем громадського здоров'я регіону.

Автори прямо наголошують, що традиційна модель реагування, орієнтована переважно на правоохоронні заходи, виявилася недостатньою. Попри збільшення ресурсів, міждержавної співпраці та операцій із перехоплення наркотиків, держави регіону не змогли розірвати зв'язок між транснаціональною організованою злочинністю та локальними кримінальними мережами. Водночас збільшення наркотрафіку супроводжується зростанням внутрішнього споживання наркотиків, а самі уряди та громади дедалі частіше визнають, що їхні можливості реагування фактично вичерпуються. У цьому контексті документ просуває концепцію переходу від вузько правоохоронної моделі до комплексного міжвідомчого реагування, яке має об'єднати

[11] https://globalinitiative.net/wp-content/uploads/2026/05/PSC-67702-Policy-Paper-April-2026-04.pdf

правоохоронні органи, систему охорони здоров'я, громадянське суспільство, церковні організації, молодіжні мережі, традиційних лідерів та місцеві громади. Автори фактично формують підхід, заснований на концепції безпеки людини, у межах якої наркотична криза розглядається як загроза не лише державній безпеці, а й безпеці людини, соціальній стійкості та добробуту громад.

Одним із центральних елементів документа є пропозиція провести у 2027 році спеціальний регіональний саміт під егідою Форуму тихоокеанських островів, присвячений кризі метамфетаміну та синтетичних наркотиків. Автори підкреслюють, що цей саміт повинен стати не символічною політичною подією, а кульмінацією тривалого процесу підготовки та регіональної координації. У документі проводиться паралель із регіональною реакцією на пандемію COVID-19, коли Форум тихоокеанських островів активував Декларацію Бікетави для створення Тихоокеанського гуманітарного механізму реагування на COVID-19. На думку авторів, нинішня наркотична криза вже досягла такого рівня, що також потребує використання надзвичайних регіональних механізмів координації. Вони підкреслюють, що криза метамфетаміну охоплює як традиційні, так і нетрадиційні виміри безпеки, у зв'язку з чим її розгляд відповідає комплексному безпековому підходу, закріпленому у Декларації Бое про регіональну безпеку та Стратегії «Блакитний Тихоокеанський континент — 2050».

Документ детально описує етапи підготовки до саміту та наголошує на необхідності створення доказової бази, адаптованої до соціокультурних реалій Тихоокеанського регіону. Для цього автори пропонують проведення швидких національних оцінок у країнах регіону, які мають дослідити масштаби та моделі споживання метамфетаміну, маршрути наркотрафіку, взаємозв'язок між наркотиками та поширенням ВІЛ, вплив кризи на громади, поліцію, судову систему та систему охорони здоров'я, а також оцінити ефективність чинних механізмів профілактики, лікування та програм зі зменшення шкоди. Передбачається, що такі оцінки повинні проводитися у співпраці між урядами, регіональними організаціями, академічними інституціями, громадянським суспільством та місцевими лідерами для забезпечення максимальної відповідності політичних рішень локальним реаліям.

Важливе місце у документі займає підтримка підходів до зменшення шкоди, орієнтованих на громади. Автори наголошують, що громади Тихоокеанського регіону вже самостійно формують локальні моделі профілактики, підтримки та реабілітації, які базуються на участі церков, жіночих організацій, молодіжних мереж та традиційних структур лідерства. Документ підкреслює, що такі ініціативи, очолювані громадами, не повинні розглядатися як другорядний елемент системи реагування, а навпаки — мають стати центральною складовою регіональної політики. Особливий акцент робиться на необхідності розвитку ініціатив зі зменшення шкоди, заснованих на принципі «рівний — рівному», залучення громадських медичних працівників та впровадження культурно адаптованих підходів до реабілітації. Автори застерігають, що надмірна концентрація виключно на кримінальному переслідуванні без одночасного розвитку доступних медичних і соціальних сервісів лише поглиблюватиме проблему, відштовхуватиме людей від системи лікування та посилюватиме епідемію ВІЛ і кризу психічного здоров'я.

Після проведення саміту автори пропонують створення Регіональної стратегії щодо синтетичних наркотиків для всього Тихоокеанського регіону. Розробка цієї стратегії має здійснюватися під координацією Секретаріату Форуму тихоокеанських островів та Секретаріату Тихоокеанського співтовариства із залученням структур безпеки, органів охорони здоров'я, експертних груп, представників громадянського суспільства та релігійних організацій. Документ наголошує, що майбутня стратегія повинна інтегрувати питання громадського здоров'я, правоохоронної

Висновки:

- **Метамфетамінова криза у Тихоокеанському регіоні поступово трансформується з проблеми наркотрафіку у комплексну загрозу безпеці людини, що одночасно охоплює сфери громадського здоров'я, ВІЛ, організованої злочинності, психічного здоров'я та соціальної стабільності.** У зв'язку з цим держави регіону змушені переходити від вузько правоохоронної моделі до багатосекторального реагування із залученням систем охорони здоров'я, громадянського суспільства, церков та місцевих громад.
- **Документ демонструє, що надмірна концентрація виключно на кримінальному переслідуванні без розвитку доступних програм лікування, реабілітації та зменшення шкоди посилює навантаження на судову систему, пенітенціарні установи та медичну інфраструктуру.** У зв'язку з цим пріоритетним напрямом має стати розвиток підходів, орієнтованих на громади, ініціатив зі зменшення шкоди за принципом «рівний — рівному», а також локальних програм профілактики, реабілітації та підтримки населення.
- **Автори пропонують створення нової моделі регіональної координації у сфері протидії синтетичним наркотикам через проведення саміту Форуму тихоокеанських островів та подальше формування регіональної стратегії щодо синтетичних наркотиків.** Такий підхід передбачає інтеграцію безпекових, медичних і соціальних механізмів у єдину систему реагування.
- **Документ підкреслює, що ефективна протидія транснаціональному наркотрафіку потребує постійного збору міжсекторальних даних,** оцінки локальних ризиків та інтеграції позицій місцевих громад у процес формування державної політики й регіональних стратегій безпеки.

діяльності, молодіжної політики, соціальної згуртованості та економічної стабільності в єдину систему реагування. Вона має містити не лише політичні декларації, а й конкретні механізми імплементації, моніторингу, процесів оцінки ефективності та накопичення практичного досвіду, а також механізми регулярного оновлення політики з урахуванням появи нових наркотичних речовин, змін маршрутів наркотрафіку та трансформації моделей споживання наркотиків. Автори фактично пропонують створити довгострокову архітектуру регіональної координації, здатну адаптуватися до еволюції транснаціональних кримінальних загроз.

Окрему цінність документа становлять коментарі регіональних експертів, які доповнюють основний текст практичними міркуваннями щодо реального стану справ у регіоні. У їхніх коментарях наголошується, що нинішня криза вже переросла у масштабну загрозу безпеці людини, яка впливає на молодь, сім'ї, локальні громади та соціальну стабільність загалом. Особливий акцент робиться на необхідності зміцнення довіри між державними структурами та громадами, розвитку міжвідомчої співпраці, обміну інформацією та інтеграції позицій і потреб місцевих громад у процес формування державної та регіональної політики. Експерти також визнають, що країни регіону частково втратили можливість зупинити поширення наркотиків на ранньому етапі, коли лише формувалися канали постачання метамфетаміну. У цьому контексті запропонований саміт розглядається як нове «вікно можливостей» для створення регіональної системи координації та спільної відповіді на кризу. Документ загалом демонструє фундаментальну трансформацію підходів до наркотичної політики у Тихоокеанському регіоні — від традиційної боротьби з наркотрафіком до інтегрованої моделі, у якій питання організованої злочинності, громадського здоров'я, соціальної стійкості та регіональної безпеки розглядаються як взаємопов'язані елементи єдиної системи загроз.

## Інші новини

### Операція Europol Project A.S.S.E.T.: зміна парадигми у виявленні та конфіскації злочинних активів через публічно-приватне партнерство [12]


У травні 2026 року штаб-квартира Європолу в Гаазі стала операційним центром для проведення безпрецедентної за масштабами міжнародної оперативної фази в рамках Проєкту A.S.S.E.T. (Asset Search & Seize Enforcement Taskforce). Ця стратегічна ініціатива, що координується Європейським центром фінансової та економічної злочинності (EFECC), об'єднала ресурси понад 40 правоохоронних відомств, включаючи національні Офіси з повернення активів (AROs), Підрозділи фінансової розвідки та спеціалізовані підрозділи боротьби з організованою злочинністю. Оперативна потужність була суттєво мультиплікована за рахунок безпосередньої участі ключових наглядових та розслідувальних інституцій ЄС і світу: Євроюсту, Європейської прокуратури (EPPO), новоствореного Органу ЄС з протидії відмиванню коштів (AMLA) та Центру фінансової злочинності та боротьби з корупцією Інтерполу (IFCACC). Проте визначальною інновацією цієї операції стала глибока структурна інтеграція з приватним сектором — провідними комерційними банками та представниками індустрії криптовалютних бірж, співпраця з якими відбувалася в рамках платформи EFIPPP (Europol Financial Intelligence Public Private Partnership).

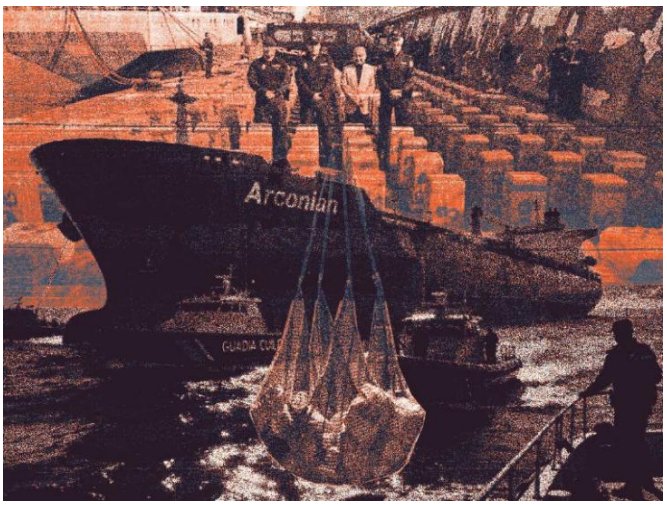
Протягом оперативного тижня з 19 по 22 травня 2026 року спільні зусилля правоохоронців та фінансових аналітиків дозволили ідентифікувати та відстежити вражаючий обсяг активів кримінального походження. Було викрито 884 банківські рахунки, пов'язані з мережами відмивання коштів, ідентифіковано 80 компаній, що використовувалися як корпоративні фасади для легалізації доходів, та встановлено 55 криптовалютних гаманців. У площині матеріальних активів конфіскації підлягали 74 транспортні засоби преміум-класу, одне судно та 44 об'єкти нерухомості, причому лише шість з них мали сукупну підтверджену вартість 5,64 млн євро. Окрім фінансових здобутків, операція мала високий розшуковий результат: було локалізовано двох підозрюваних у тяжких фінансових злочинах, одного з яких успішно заарештовано завдяки оперативній взаємодії з європейською мережею розшуку ENFAST.

Травневі події стали логічним продовженням системної ескалації тиску на кримінальні фінанси, яку забезпечує Проєкт A.S.S.E.T. У січні 2025 року перша глобальна фаза операції зібрала понад 80 фінансових експертів і 43 правоохоронні агенції з 28 країн, що дозволило виявити 53 об'єкти нерухомості (вісім з яких оцінювалися у 38,5 млн євро), понад 220 сумнівних банківських рахунків (на одному з яких зберігалося 5,6 млн доларів США) та заморозити 200 тисяч євро у віртуальних активах. Подальший аналіз розвідувальних даних, отриманих під час січневої операції, призвів до наступного арешту ще 27 млн євро виключно у криптовалютах. Наступним етапом став спеціалізований "крипто-тиждень" у жовтні 2025 року за участю 13 країн, який завершився ідентифікацією 249 криптоадрес загальною вартістю 12,1 млн євро та блокуванням десятків корпоративних рахунків.

[12] https://www.europol.europa.eu/media-press/newsroom/news/europols-project-asset-identifies-millions-in-criminal-assets

Фундаментальне значення Проєкту A.S.S.E.T. полягає в доведенні ефективності нової концепції боротьби з відмиванням коштів: переходу від фрагментованих реактивних розслідувань до проактивного транскордонного обміну фінансовою розвідкою в режимі реального часу між державними регуляторами, правоохоронними органами та СПФМ. Це публічно-приватне партнерство руйнує традиційні юрисдикційні бар'єри, які організована злочинність використовувала десятиліттями, і дозволяє наглядовим органам формувати цілісну картину глобальних тіньових потоків, адаптуючи систему ПВК/ФТ до найскладніших викликів цифрової економіки.

## Безпрецедентний рекорд: що найбільше вилучення кокаїну в Іспанії розповідає про сучасний наркотрафік [13]




У перші дні травня 2026 року іспанські правоохоронні органи провели операцію, яка миттєво стала надбанням світових медіа та предметом пильного вивчення аналітиків із безпеки. В атлантичних водах, на південь від Канарських островів, було перехоплено вантажне судно «Arconian». На його борту виявили понад 30 метричних тонн кокаїну — це найбільше разове вилучення цього наркотику в історії Іспанії та одна з наймасштабніших конфіскацій у світі.

Щоб збагнути колосальність цього вантажу, досить сказати, що його вистачило б для задоволення споживання мільйонів європейців протягом тривалого часу, а вартість на чорному ринку сягає багатьох мільярдів євро. Однак, попри всю важливість кількісного показника, цей рекордний випадок цікавий насамперед якісно: він є своєрідним дзеркалом, у якому відбиваються найглибинніші зміни у світовому кокаїновому трафіку.

Ретельний аналіз події, що базується на даних іспанської влади та матеріалах розслідувань, дозволяє виокремити три фундаментальні зрушення, які перетворюють наркобізнес на дедалі складнішу та небезпечнішу систему. По-перше, це парадоксальний перехід від класичної вертикальної ієрархії до горизонтальної «економіки спільного доступу» до маршрутів і ресурсів, що дозволяє перевозити гігантські партії. По-друге, це геополітичний зсув — остаточне утвердження Західної Африки як головного транзитного хабу та безпечного притулку для європейських наркобаронів. По-третє, це тактична інновація, що робить застарілою традиційну портову логістику: замість заходу в Роттердам чи Антверпен, вантажі тепер передаються на швидкісні катери у відкритому морі, що змінює всю картину боротьби з наркотрафіком.

Заглиблюючись у структуру організації цього рейсу, ми стикаємося з першим великим парадоксом сучасної наркозлочинності. Інтуїтивно здавалося б, що посилення міжнародного співробітництва, технології відстеження суден та жорсткіші перевірки в портах мають підштовхнути кримінальні мережі до дроблення вантажів на дрібніші, менш помітні партії. Але рекордне вилучення Іспанії доводить зворотне: злочинний світ консолідується для досягнення масштабу, який дає нову економію на транзакціях. Виявляється, що 30 тонн кокаїну, захоплених у травні, — це не результат дії однієї суворо централізованої організації, а скоріше спільне підприємство.

[13] https://insightcrime.org/news/what-spains-record-cocaine-bust-says-about-the-drug-trade/

Іспанська влада встановила, що за вантажем стоять сили, об'єднані під терміном «Macro Maffia» — складна мережа злочинних кланів та структур із базуванням у Нідерландах. Ці угруповання останніми роками демонструють надзвичайну динаміку: вони більше не покладаються виключно на латиноамериканських посередників, а активно розширюють власну присутність у Латинській Америці, щоби вести переговори напряму з контролерами плантацій коки та виробничих лабораторій. У випадку з цим конкретним вантажем джерела, яких цитує колумбійська газета El Tiempo, вказують на походження кокаїну з Колумбії — країни, де доступ до сировини та виробництва жорстко контролюється збройними угрупованнями, що десятиліттями ведуть власні війни за території. Таким чином, у Латинській Америці стає дедалі більше європейських «емісарів» та «брокерів» — специфічних посередників, які є сполучною ланкою між місцевими виробниками та європейськими покупцями, забезпечуючи довіру та гарантії в середовищі, де слова «честь» набуває буквального кримінального значення.

Однак на цьому ланцюг не завершується. Для фізичного переміщення понад 30 тонн кокаїну з колумбійських джунглів до Західної Африки, а потім через Атлантику до Європи, знадобилися послуги кількох мереж, що спеціалізуються виключно на логістиці — зберіганні, пакуванні, страхуванні ризиків і безпосередньому транспортуванні різними маршрутами. Варто наголосити, що така фрагментація зовсім не означає розпорошення вантажів. Навпаки, показовим є прецедент 2023 року, коли в порту Альхесірас на півдні Іспанії було вилучено партію кокаїну вагою 9,5 тонни, до організації якої були причетні, за даними слідства, до 30 різних злочинних організацій. Цей факт однозначно засвідчує: сучасний наркотрафік — це не війна один проти одного, а складно організований ринок спільних ресурсів, де конкуренти вміють об'єднувати свої гроші та канали для досягнення спільної вигоди. Тобто мафія стала більш «ринковою» та водночас більш стійкою до ударів: вилучення однієї гігантської партії не знищує жодну окрему організацію повністю, адже ризики поділені між багатьма.

Друга фундаментальна зміна, яку безпрецедентно виразно демонструє цей випадок, — це блискавичне перетворення Західної Африки на глобальний нарковузол. Географія маршруту судна «Arconian» є промовистою: воно вирушило з берегів Сьєрра-Леоне після того, як кокаїн був доправлений туди з Південної Америки. Починаючи з 2019 року, роль країн цього регіону як транзитного майданчика для латиноамериканського кокаїну, що прямує до Європи, зростає драматичними темпами. Історично склалося так, що Західна Африка має слабкі державні інституції, корумповані прикордонні служби та величезне безлюдне узбережжя, яке важко патрулювати. Це робить її ідеальним місцем для перевантаження та тимчасового зберігання наркотиків.

Але справа навіть не в самому транзиті. Справжній шок для міжнародної спільноти стався на початку 2025 року, коли виявилося, що одним із найвпливовіших мешканців Сьєрра-Леоне є людина, яка перебуває в міжнародному розшуку. Мова йде про відомого нідерландського наркоторговця Йоса Лейдеккерса на прізвисько «Болле Йос». У 2024 році нідерландський суд заочно засудив його до 24 років позбавлення волі за організацію масштабних наркопостачань та замах на вбивство. І що ж робить засуджений злочинець? Він переїжджає до Сьєрра-Леоне, де, за даними численних розслідувань, розпочинає стосунки з дочкою президента Джуліуса Маади Біо. Незважаючи на офіційні вимоги Нідерландів про екстрадицію, Болле Йос і досі залишається на волі, почуваючись у цій країні в повній безпеці.

Саме з цим персонажем іспанські джерела, зокрема авторитетна газета El Pais, прямо пов'язують організацію вантажу на «Arconian». Це одне свідчення перевершує будь-які аналітичні звіти. Президентська родина, пов'язана родинними чи іншими зв'язками з наркобароном, стає гарантом безпеки для цілих маршрутів. Тому рекордне вилучення — це не ознака того, що система дала тріщину, а скоріше сигнал, що європейській владі вдалося перехопити лише малу частку того, що проходить через цей «африканський коридор», захищений політичним імунітетом.

І нарешті, третій глибинний висновок, який випливає з аналізу цієї операції, стосується радикальної зміни способів доставки кокаїну на європейський континент. Окрім самої гори наркотиків, іспанські слідчі виявили на борту «Arconian» 42 тисячі літрів бензину — величезні запаси пального, які важко пояснити будь-якими законними потребами судна. Пояснення виявилося водночас простим і шокуючим: величезний корабель не збирався заходити в жоден великий порт. Натомість план полягав у тому, щоб у відкритому морі передати вантаж на швидкісні катери, які потім доправили б кокаїн безпосередньо на берег. Ця зміна тактики є прямою відповіддю на успіхи правоохоронних органів у традиційних європейських портах-гігантах.

Роттердам, Антверпен, Гамбург — ці ворота європейської економіки десятиліттями були головними точками входу для кокаїну, але тепер вони перебувають під безпрецедентним наглядом: сканери, спеціально навчені собаки, агенти під прикриттям і міжнародний обмін даними зробили завантаження контейнера з наркотиками в такому порту надзвичайно ризикованою справою. Тому кримінальні мережі просто обходять цю перешкоду — вони взагалі відмовляються від портів.

На півдні Іспанії, куди, ймовірно, прямував вантаж зі Сьєрра-Леоне, використання швидкісних катерів дозволяє розвантажувати кокаїн у майже будь-якій точці узбережжя, а звідти транспортувати вглиб країни через альтернативні водні шляхи, як-от річка Гвадалквівір. Це створює нові, майже неконтрольовані логістичні ланцюги.

Однак за цю гнучкість доводиться платити людською кров'ю. Використання швидкісних суден невіддільне від зброї. Воно тягне за собою появу зброї, людей, які захищають вантажі, і більше насильства, пов'язаного з використанням цих суден. Трагічним підтвердженням цих слів стала загибель двох іспанських цивільних гвардійців на початку травня 2026 року — вони загинули під час погоні саме за таким швидкісним катером. Цей епізод є жорстокою ілюстрацією того, що еволюція наркотрафіку має прямі та фатальні наслідки для суспільства: чим складнішими стають методи контрабанди, тим вищим є рівень озброєності злочинців і тим більше жертв серед правоохоронців та випадкових свідків.

У підсумку, найбільше вилучення кокаїну в історії Іспанії — це скоріше тривожний дзвінок. Воно показує, що наркомафія адаптується до нових викликів із вражаючою швидкістю, що за горами кокаїну стоять складні альянси між європейськими кланами та африканськими політичними елітами, і що кожна тонна перехопленого порошку супроводжується зростанням хвилі озброєного насильства на вулицях європейських міст.

## Штучний інтелект проти брудних грошей: як поведінковий аналіз змінює фінансовий моніторинг [14]


У той час, коли світова фінансова система генерує квадрильйони транзакцій на рік, а регулятори посилюють вимоги до прозорості зі швидкістю, що не поступається технологічному прогресу, традиційні підходи до боротьби з відмиванням грошей (AML) демонструють свою дедалі більшу неефективність. Саме в цьому розриві між зростаючими обсягами даних, складністю злочинних схем та обмеженими людськими ресурсами комплаєнс-підрозділів і народжуються інновації, здатні змінити саму філософію фінансового нагляду.

[14] https://fincrimecentral.com/flagright-ai-forensics-monitoring/

Однією з найяскравіших таких інновацій став модуль AI Forensics for Monitoring від аналітиків Flagright — система, яка не просто автоматизує окремі завдання, а переосмислює весь ланцюжок AML-розслідувань, починаючи від першого сигналу і закінчуючи аудитованим рішенням.

Щоб зрозуміти масштаб змін, необхідно усвідомити, з якою реальністю щодня стикаються аналітики з протидії фінансовим злочинам. Уявімо типовий робочий процес у традиційному банку або фінтех-компанії: автоматична система моніторингу генерує сповіщення про підозрілу активність — наприклад, транзакцію, що перевищує певний поріг. Далі починається найбільш ресурсомісткий етап — збір контексту. Аналітик відкриває кілька розрізнених баз даних: одну для історії транзакцій клієнта, другу для його ризик-профілю, третю для перевірки контрагентів, четверту для санкційних списків. Він вручну зіставляє дати, суми, географію та поведінкові патерни. Цей процес може тривати від кількох годин до кількох днів — залежно від складності кейсу та кваліфікації фахівця. І щоразу, коли спрацьовує чергове сповіщення (а в великих установах їх можуть бути тисячі на день), цикл повторюється.

Результатом стає ситуація, коли співробітники фізично не встигають опрацьовувати всі сигнали, а найнебезпечніші схеми тонуть у потоці хибних спрацювань. Flagright пропонує кардинальну альтернативу: замість того, щоб змушувати людину йти до даних, система приводить дані до людини. У момент, коли алгоритм виявляє аномалію, модуль AI Forensics миттєво агрегує повний профіль учасника — від багаторічної хронології переказів до останнього оновлення ризик-оцінки, від попередніх прапорців до поведінкових патернів контрагентів. Усе це з'являється на єдиній панелі, яку аналітик може одразу використовувати для прийняття рішення. Таким чином, час від отримання сповіщення до початку змістовного аналізу скорочується на порядки, а ймовірність пропустити критичний доказ через людську помилку знижується до мінімуму.

Однак автоматизоване агрегування даних — це лише перший, хоча й необхідний, рівень трансформації. Справжня сила розкривається на другому рівні: вдосконаленому поведінковому аналізі.

Більшість традиційних AML-систем працюють за принципом жорстких правил або статичних порогів: якщо транзакція перевищує 10 000 доларів або надходить із країни з високим ризиком — генерується сигнал. Такий підхід є примітивним і легко обходиться сучасними злочинцями, які використовують техніки структурування (structuring) — розбивають великі суми на безліч дрібних переказів, аби не перетинати порогові значення. AI Forensics, натомість, будує динамічні поведінкові профілі для кожного клієнта. Система вивчає його звичну активність протягом тривалого періоду: з якою частотою він здійснює перекази, які суми є для нього типовими, з якими географічними регіонами він зазвичай взаємодіє, о котрій годині доби відбуваються його операції, які типи контрагентів домінують у його платіжній поведінці. Коли відбувається нова транзакція, система порівнює її не з абстрактним порогом, а з цим індивідуальним профілем. Якщо клієнт, який зазвичай переказує 500 доларів на місяць, раптом відправляє 50 000 доларів у юрисдикцію, де в нього ніколи не було ділових інтересів, система фіксує аномалію.

Але на цьому аналіз не закінчується — система також порівнює активність клієнта з групами подібних споживачів. Це дозволяє виявити системні ризики, які окремо можуть виглядати нормальними. Наприклад, якщо сотня акаунтів, кожен з яких імітує звичайну комерційну поведінку, починає здійснювати синхронізовані перекази на спільний пул рахунків — на індивідуальному рівні жоден із них не викличе підозри, але на рівні групи аномалія стає очевидною. Саме так виявляються сучасні схеми «розшарування» (layering), де злочинці намагаються загубити слід капіталу, розсіюючи його через безліч легітимних на вигляд каналів.

Окрема, надзвичайно важлива деталь — це прозорість роботи AI модулів. Однією з найбільших проблем у застосуванні складних алгоритмічних систем у регульованих галузях є «проблема чорної скриньки»: алгоритм приймає рішення, але ніхто не може пояснити — чому. Для фінансового комплаєнсу це неприйнятно, оскільки будь-яке рішення про блокування транзакції або закриття рахунку має бути обґрунтованим перед регулятором, а часто — і перед судом.

Система Flagright вирішує цю проблему, супроводжуючи кожен сигнал текстовими поясненнями. Аналітик не отримує абстрактну «оцінку ризику» — він бачить речення на кшталт: «Цей переказ є аномальним, оскільки сума в 20 разів перевищує середню транзакцію клієнта за останні 6 місяців, а отримувач знаходиться в юрисдикції, з якою клієнт раніше ніколи не взаємодіяв». Ця функція є критично важливою не лише для внутрішнього аудиту, але й для демонстрації належності процедур. Регулятори, такі як представники FinCEN, Європейського банківського органу або національних фінансових розвідок, можуть відтворити логіку, яка призвела до того чи іншого рішення. Крім того, зрозумілі пояснення знижують навантаження на досвідчених співробітників — їм не потрібно витрачати час на інтерпретацію складних вихідних даних моделі, вони одразу бачать суть. Це не лише підвищує швидкість, але й зменшує варіативність рішень: різні аналітики, спираючись на одні й ті самі структуровані пояснення, ухвалюють більш послідовні та передбачувані рішення.

Не менш важливим аспектом є питання масштабованості та економічної доцільності. Фінансові установи, особливо швидкозростаючі фінтех-компанії та нео-банки, часто опиняються в пастці: зростання клієнтської бази та обсягу транзакцій вимагає пропорційного збільшення комплаєнс-персоналу. Оскільки кваліфіковані AML-аналітики є дорогими та дефіцитними, а їхня чисельність не може зростати лінійно без зупинки бізнес-розвитку, настає момент, коли система моніторингу починає «захлинатися». Традиційне рішення — наймання ще більшої кількості людей — призводить до зростання операційних витрат, яке може перевищити вигоди від розширення бізнесу.

Flagright пропонує інший підхід: технологію як «мультиплікатор сили». Автоматизація контекстуального збору даних дозволяє одному аналітику обробляти значно більший обсяг сповіщень, ніж раніше. При цьому фокус зміщується від кількості до якості: замість того, щоб гасити пожежі тисячі дрібних сигналів, фахівець може зосередитися на десятках дійсно складних, високоризикових кейсів, які вимагають людського досвіду, інтуїції та глибокого розуміння бізнес-контексту. Для установ, що працюють у кількох юрисдикціях, цей ефект посилюється: система автоматично адаптується до різних порогових значень ризику та вимог звітності — від США до ЄС, від Сінгапуру до ОАЕ. Комплаєнс-менеджери, опитані в рамках підготовки документа, зазначають, що інвестиції в подібні рішення окупаються протягом кількох місяців за рахунок скорочення часу на одне сповіщення та зниження кількості хибно позитивних спрацювань, які раніше також потребували перевірки. У цифрову епоху, коли вартість ручної праці постійно зростає, а регуляторні штрафи за недостатній AML-контроль сягають сотень мільйонів доларів, автоматизація стає безумовною вимогою виживання.

Важливо підкреслити, що система Flagright, попри всю свою алгоритмічну потужність, не намагається усунути людину з процесу прийняття рішень. Навпаки, архітектура системи побудована навколо принципу «людина в циклі» (human-in-the-loop). Кінцеве рішення — блокувати транзакцію, надіслати звіт про підозрілу діяльність (SAR) або закрити рахунок — завжди залишається за досвідченим фахівцем. Машина виконує роль незамінного асистента, який збирає, структурує, аналізує та підсвічує аномалії, але не підміняє собою професійне судження. Цей гібридний підхід є найефективнішим захистом проти еволюції злочинних тактик. Адже фінансові злочинці також використовують технології, штучний інтелект і машинне навчання для маскування своїх схем. У цій безперервній гонці озброєнь тільки тісна співпраця між людським інтелектом, здатним до абстрактного мислення та розуміння контексту, та

машинною ефективністю, здатною обробляти неймовірні обсяги даних у реальному часі, може забезпечити стійку перевагу.

Як слушно зауважують автори, майбутнє — за інтеграцією штучного інтелекту на всіх етапах управління ризиками: від первинної перевірки клієнта (KYC) та скринінгу санкційних списків до виявлення політично значущих осіб (PEP) та автоматизованого управління політиками. Ідеальна картина — це безшовна екосистема, де різні модулі обмінюються даними та сигналами, формуючи 360-градусний огляд інституційного ризику. Кожна транзакція, кожне рішення, кожен звіт стають частиною колективного інтелекту системи, яка постійно навчається та адаптується до нових загроз.

У ширшому контексті, поява таких інструментів, як Flagright AI Forensics, має глибокі наслідки для всієї світової фінансової системи. Вона поступово підвищує бар'єр входу для злочинців. Ще десять років тому для відмивання значних сум було достатньо мати кілька підставних компаній та базове розуміння банківських процедур. Сьогодні, коли алгоритми поведінкового аналізу здатні відстежити аномалію серед мільйонів транзакцій, а автоматизовані системи агрегують контекст за секунди, вартість та ризик злочинної діяльності стрімко зростають. Зловмисникам доводиться витрачати більше ресурсів на маскування, створювати дедалі складніші багаторівневі схеми, що робить їх більш вразливими до викриття.

Для доброчесних учасників ринку це означає чистішу, прозорішу та безпечнішу фінансову екосистему. Для регуляторів — можливість перейти від реактивного (розслідування вже скоєних злочинів) до проактивного нагляду, де потенційні ризики виявляються до того, як вони завдадуть реальної шкоди.

Звісно, жодна технологія не є панацеєю, і злочинці неодмінно адаптуватимуться. Але напрямок руху є однозначним: майбутнє фінансового комплаєнсу — це тісний симбіоз людини та штучного інтелекту, де кожен сигнал розглядається не як ізольоване число, а як частина цілісної поведінкової історії, а рішення приймаються швидко, обґрунтовано та з повним усвідомленням контексту.

## Східний розлом: як контрабанда з Лівії стала головним викликом для Європи [15]


Задовго до того, як західне узбережжя Лівії стало відомим на весь світ як головний плацдарм для відправлень до Італії, на сході країни вже діяли невеликі, але досить організовані контрабандистські мережі. До лівійської революції 2011 року ці угруповання, що базувалися переважно в районі Тобрука та Бенгазі, періодично організовували таємні переправи через море, використовуючи столітні традиції нелегальної торгівлі та відносну автономію східних регіонів.

Після падіння режиму Муаммара Каддафі та занурення країни в хаос громадянської війни міграційні потоки спрямувалися переважно на захід, де концентрувалися найпотужніші

[15] https://globalinitiative.net/analysis/a-smuggling-route-reawakens-movement-surges-between-eastern-libya-and-crete/

злочинні синдикати і звідки відстань до італійських Пелагічних островів – зокрема Лампедузи – здавалася мінімальною.

Цей стан тривав до середини 2022 року, коли почали з'являтися перші ознаки змін. Контрабандисти в Тобруку та навколишніх районах почали організовувати відправлення до Італії, причому часто використовували великі рибальські судна або вантажні баржі, здатні вмістити чотириста і більше мігрантів одночасно. Це була абсолютно нова тактика, розрахована на масовість та ефективність, на противагу попереднім невеликим човнам. Протягом 2022 та першої половини 2023 року цей потік поступово набирав обертів, залишаючись, однак, поза пильною увагою міжнародної спільноти – доти, доки не сталася трагедія, що сколихнула світ. У червні 2023 року одне з таких перевантажених суден, що прямувало з Лівії, затонуло біля узбережжя Греції, забравши життя понад шестисот людей.

До кінця 2023 року контрабандисти, які діяли на сході Лівії, продемонстрували вражаючу здатність до переналаштування. Вони радикально змінили свою операційну тактику: замість великих, помітних суден, вони почали використовувати малі човни, часто надувні або невеличкі рибальські катери, які набагато складніше виявити радарам та патрульним літакам. Крім того, вони перенацілили свої маршрути, обравши замість Італії Крит – острів, розташований дещо далі до східнолівійського узбережжя, ніж італійське узбережжя, але водночас менш захищений у плані патрулювання в той час. Ця зміна тактики виявилася напрочуд ефективною.

Справжнім ключем до розуміння того, чому цей маршрут не лише вижив, а й розквітнув, є аналіз цінової динаміки та внутрішньої конкуренції серед контрабандистських угруповань. За даними інтерв'ю з мігрантами, зібраними у 2024 році, середня вартість подорожі зі східної Лівії до Криту коливалася в діапазоні від 2100 до 3500 євро з людини. Це були значні кошти, які робили маршрут доступним переважно для тих, хто мав доступ до родинних заощаджень або зміг продати все своє майно. Однак у квітні 2026 року грецькі чиновники оприлюднили вражаючі дані: вартість проїзду впала до феноменально низьких рівнів – від 340 до 1450 євро. Це падіння цін на 50–80% за якихось два роки є класичною ознакою того, що ринок став надзвичайно конкурентним.

Джерела, близькі до ситуації в Лівії, підтверджують це припущення. Як зазначається в аналітичних матеріалах, значна частка контрабанди людей у східній Лівії сьогодні контролюється невеликою кількістю родин, які мають багаторічну історію занять контрабандою товарів, автомобілів та, особливо, наркотиків. Для цих кланів, які накопичили значний капітал та розгалужені корупційні зв'язки в місцевих силових структурах, перехід до міграційного бізнесу став логічною диверсифікацією, привабливою насамперед завдяки високій прибутковості та, що критично важливо, відносно низькому ризику кримінального переслідування. Конкуренція між цими кланами призвела до цінової війни, яка робить послуги контрабандистів доступними навіть для мігрантів із порівняно скромними заощадженнями, що, своєю чергою, розширює клієнтську базу та стимулює подальше зростання потоку.

Однак найжахливішою стороною цього бізнесу, яка перетворює його на справжню машину смерті, є умови, в яких відбуваються самі переправи, а також ті ризики, що чатують на мігрантів після того, як їм, можливо, пощастить досягнути грецьких берегів живими. За свідченнями місцевих контактів, зони відправлення на узбережжі східної Лівії контролюються озброєними людьми в масках – це, ймовірно, бойовики, найняті контрабандистськими кланами для забезпечення порядку та залякування. Ці люди не просто спостерігають; вони активно застосовують психологічний та фізичний тиск на мігрантів, змушуючи їх сідати на човни навіть тоді, коли погодні умови є відверто небезпечними – коли море штормить, вітер досягає штормових значень, а хвилі перекидаються через борти крихких суден. Самі човни, навіть якщо вони новозбудовані, часто є відверто непридатними для плавання в умовах відкритого моря: двигуни можуть бути старими, ненадійними, корпуси – недостатньо міцними. Як зазначають

грецькі посадовці, контрабандисти, оптимізуючи свої витрати до краю, забезпечують судно рівно такою кількістю пального, якої, за їхніми розрахунками, має вистачити для досягнення Криту за ідеальних умов. Будь-яке відхилення від курсу через помилку в навігації, погану погоду або поломку двигуна призводить до того, що човен починає дрейфувати без пального, а разом із ним – і без води та їжі, адже запаси також мінімальні. І це ще не все.

Щоб ще більше знизити власні витрати та, що важливо, зменшити ризик бути засудженими за управління судном, контрабандисти розробили цинічну практику: вони вербують або просто примушують самих мігрантів виконувати роль капітана, механіка та штурмана. Декільком обраним мігрантам, які часто навіть не мають жодного досвіду мореплавства, показують, як користуватися GPS-навігатором, як запускати двигун та як проводити дозаправку з запасних каністр. В обмін на цю "послугу" їм пропонують знижку вартості проїзду або навіть безкоштовний перехід. Але ця угода з дияволом має катастрофічні наслідки. Коли такий човен перехоплює берегова охорона Греції або коли його пасажирів рятують після кількох днів дрейфу, саме ці "помічники", які самі є жертвами контрабанди, постають перед грецьким правосуддям як звинувачені в організації нелегального переправлення – злочині, що карається тривалими термінами тюремного ув'язнення.

У цих умовах європейські та міжнародні як урядові, так і неурядові організації, зобов'язані будувати своє планування, виходячи з найбільш реалістичного припущення: високий рівень нелегального переміщення між Східною Лівією та Грецією збережеться, а разом із ним збережуться й ті жахливі ризики, які ми спостерігаємо сьогодні.

## Ваша думка важлива!

1. Яким чином ПФР України та національні регулятори можуть посилити транскордонну взаємодію з новим європейським органом з боротьби з відмиванням грошей — AMLA — з метою мінімізації ризиків використання фінансової системи ЄС для легалізації активів, пов'язаних із країною-агресором? Які практичні аналітичні кейси, напрацьовані Україною в умовах воєнної агресії, можуть бути використані під час формування майбутніх загальноєвропейських технічних стандартів у сфері ПВК/ФТ?
2. Наскільки серйозну загрозу для фінансової стабільності можуть створювати системні помилки у пруденційній звітності, якщо вони впливають на розрахунок капіталу, ліквідності та оцінку ризиків у банківському секторі?
3. Які ризики для захисту персональних даних, комерційної таємниці та кібербезпеки можуть виникнути внаслідок створення масштабних централізованих сховищ даних у сфері ПВК/ФТ на рівні Європейського Союзу?
4. Лівійський кейс демонструє, що війна та вакуум влади стали ідеальним середовищем для формування потужних контрабандистських кланів, які за роки перетворилися на системний бізнес. Наскільки Україна може зіткнутися з феноменом «відкладеної міграції», коли наслідки війни призвели до розквіту контрабанди людей?
5. Як українські банки та фінтех-компанії можуть інтегрувати поведінковий AI-аналіз? Чи будуть готові, на вашу думку, регулятори визнавати такі системи як належний інструмент ризик-орієнтованого нагляду?

## 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-2026-21


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].

AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE