Методологічний бюлетень

Серійний номер: МінФін-AML-2025-29

Липень 2025

“Секрет успіху в тому, щоб діяти!”

Данте Аліг’єрі

Мета

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для суб'єктів первинного фінансового моніторингу (СПФМ), регуляторів та правоохоронних органів.

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

Для регуляторів та правоохоронних органів є інструментом для розробки ефективних стратегій боротьби з ВК, включаючи навчання та координацію дій між різними установами для забезпечення належної співпраці та обміну інформацією.

Звіти міжнародних організацій та окремих юрисдикцій

АУДІОПЕРЕКАЗ

Річний звіт ПФР Нідерландів [1]

Представлений річний звіт ПФР Нідерландів за 2024 рік детально висвітлює зусилля та досягнення підрозділу у запобіганні та боротьбі з ВК, злочинами, що передують ВК, та ФТ як на національному, так і на міжнародному рівнях. Місія ПФР полягає у забезпеченні цілісності фінансової системи шляхом надання високоякісних фінансових розвідувальних даних та раннього виявлення нових тенденцій і феноменів, про які інформуються партнери.

Звіт підкреслює значний вплив нового європейського пакету законодавства з боротьби проти відмивання коштів, прийнятого 30 травня 2024 року, який набуде чинності в липні 2027 року. Цей пакет включає дві постанови (AMLR та AMLAR) і одну директиву (AMLD6), які спрямовані на гармонізацію регулювання та

[1] https://www.fiu-nederland.nl/wp-content/uploads/2025/07/FIU-annual-review-2024.pdf

посилення нагляду на європейському рівні. Очікується, що нове законодавство призведе до більшої уніфікації, посиленої співпраці, суворіших покарань, розширення повноважень для ПФР та збільшення кількості секторів, що підпадають під регулювання.

У 2024 році кількість незвичних транзакцій (UTR) значно зросла майже до 3,5 мільйона, тоді як кількість підозрілих транзакцій (STR) знизилася. Зростання UTR переважно пов'язане зі збільшенням кількості повідомлень від провайдерів платіжних послуг (PSP), криптобірж та компаній, що випускають кредитні картки. Зокрема, кількість UTR від PSP зросла на 40% до 1,4 мільйона, що становить близько 40% від усіх UTR у 2024 році. Кількість UTR від криптобірж зросла більш ніж удвічі до 578 312, що пояснюється зростанням самого крипторинку та наявністю об'єктивних індикаторів, що призводять до збільшення повідомлень при зростанні цін на криптовалюту. Компанії, що випускають кредитні картки, повідомили про 421 189 UTR, порівняно з 10 771 у 2023 році, що головним чином спричинено вказівкою Центрального банку Нідерландів (DNB) про обов'язкове повідомлення про всі форми шахрайства. На противагу, кількість повідомлень від банків значно зменшилася, що пов'язано зі зміною способу повідомлення однією великою банківською установою з індивідуального на зведений, а також із посиленням вимог DNB щодо повідомлення про шахрайство.

ПФР приділяє особливу увагу викриттю складних мереж, використовуючи поєднання співпраці та ризикоорієнтованого підходу. Аналізи показали широке використання юридичних осіб для відмивання коштів та сприяння злочинній діяльності, часто за участю професійних постачальників послуг. Метод "Cash Compensatie Model" (CCM), що полягає в обміні злочинної готівки на легальні безготівкові кошти, залишається значною проблемою. Виявлено випадки зловживання третіми сторонами в платежах для відмивання коштів та обходу санкцій, а також їх зв'язок з підпільними банківськими операціями. Нерухомість продовжує бути високим ризиком для відмивання коштів, використовується для легалізації злочинних доходів та як місце для злочинної діяльності, такої як наркоплантації, незаконні азартні ігри та сексуальна експлуатація.

Шахрайство, як горизонтальне (між приватними особами/юридичними особами), так і вертикальне, залишається однією з найпоширеніших форм злочинності. Особлива увага приділяється шахрайству з пільгами, шахрайству в галузі

Висновки:

- **Значне зростання UTR:** Кількість UTR зросла майже до 3,5 мільйона у 2024 році, що переважно пов'язано зі збільшенням кількості повідомлень від платіжних сервіс-провайдерів, криптобірж та компаній, що випускають кредитні картки. Це вимагає від ПФР та підзвітних організацій подальшого вдосконалення систем моніторингу та аналізу.
- **Вплив європейського законодавства:** Прийняття нового європейського пакету законодавства щодо боротьби з відмиванням коштів у 2024 році (з повною імплементацією до 2027 року) суттєво змінить регуляторне поле, посиливши вимоги до підзвітних установ та можливості ПФР у міжнародній співпраці, вимагаючи активної підготовки.
- **Складність методів відмивання коштів:** Злочинні мережі все частіше використовують складні схеми, такі як зловживання юридичними особами, "Cash Compensatie Model" та треті сторони в платежах, що свідчить про необхідність посилення співпраці між державним і приватним секторами для розробки більш комплексних та системних контрзаходів.
- **Технологічний розвиток як пріоритет:** ПФР активно інвестує в технологічний розвиток, включаючи оновлення основних систем (GoFintel, GoAML) та покращення якості даних через нові форми звітів. Це є критично важливим для ефективного аналізу зростаючого обсягу даних та підтримки конкурентоспроможності у боротьбі з фінансовими злочинами.

охорони здоров'я (часто переплетеному з ССМ), та податковому шахрайству, що призводить до недобросовісної конкуренції. Також виявлено випадки іпотечного шахрайства, коли нелегальні доходи використовуються для отримання надмірних іпотек.

Корупція, включаючи активне та пасивне хабарництво, проявилася в аналізах, охоплюючи як міжнародні компанії, так і державних службовців. Різні форми експлуатації, такі як трудова, сексуальна та дитяча порнографія, також є об'єктом розслідувань ПФР, причому фінансові дані відіграють ключову роль у виявленні цих злочинів.

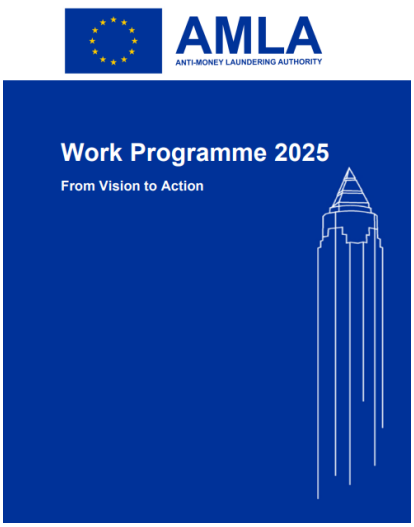
Запобігання обходу санкцій є пріоритетом, при цьому ПФР співпрацює на міжнародному рівні. Виявлено випадки обходу санкцій за допомогою третіх осіб та використання підставних компаній. Регіональна співпраця з місцевими публічними партнерами, зокрема в Роттердамі та Амстердамі, принесла значні результати у боротьбі зі злочинністю.

ПФР активно працює над боротьбою з фінансуванням тероризму, розглядаючи всі аспекти загрози, включаючи джихадизм, правоекстремістські групи та антиінституційних екстремістів. Аналізи включали фінансування придбання вогнепальної зброї, де часто фігурували особи, пов'язані з ультраправими угрупованнями. Звіт підкреслює зв'язок між організованою злочинністю та фінансуванням тероризму, особливо через підпільні банківські операції та "Cash Compensatie Model". Загальна кількість справ з ознаками фінансування тероризму у 2024 році зросла на 35% порівняно з 2023 роком.

У 2024 році ПФР продовжив розвиток технологій, включаючи оновлення систем GoFintel та GoAML для покращення аналізу даних та безпеки. Також розроблено нові індивідуальні форми звітів для підвищення якості даних та запроваджено структурний процес обробки проблем з якістю даних. Організаційний розвиток включав збільшення штату до 109 повного штатного еквіваленту та створення нової функціональної групи "цифрового аналізу" для посилення аналітичних можливостей.

Загалом, звіт демонструє прагнення ПФР адаптуватися до мінливого ландшафту фінансової злочинності шляхом посилення співпраці, впровадження інноваційних технологій та проактивного підходу до виявлення та протидії ВК та ФТ.

Робоча Програма AMLA на 2025 рік [2]



Робоча програма AMLA на 2025 рік є ключовим документом, що окреслює заснування та початкову діяльність Органу по боротьбі з відмиванням коштів та фінансуванням тероризму (AMLA), новоствореного Європейського агентства. 2025 рік визначено як вирішальний момент для колективних зусиль Європейського Союзу у боротьбі з відмиванням коштів та фінансуванням тероризму, де AMLA починає свою фундаментальну фазу з чіткою місією — закласти інституційні, процедурні та стратегічні основи для захисту Союзу від фінансових злочинів. Ця перша Робоча програма відображає статус AMLA як «стартапу» публічної служби і структурована навколо досягнутого прогресу в першій половині 2025 року та пріоритетів на решту року, перетворюючи європейські амбіції на дієві кроки, що відповідають стратегічній прихильності ЄС до фінансової цілісності та безпеки.

[2] https://www.amla.europa.eu/document/download/b78bee2f-16b9-4742-a3a1-23e7aad394ab_en?filename=AMLA_Work_Programme_July%202025_0.pdf

Основний зміст мандату AMLA, викладений у пакеті законодавчих актів про боротьбу з відмиванням коштів, включає три ключові напрямки: завершення Єдиного зводу правил для забезпечення регуляторної конвергенції та послідовності в усіх державах-членах; розробку гармонізованих наглядових практик для ефективного та послідовного нагляду як у фінансовому, так і в нефінансовому секторах; та посилення методів роботи й співпраці ПФР для забезпечення надійного обміну інформацією та посиленої взаємодії з правоохоронними органами. Для сталого та ефективного виконання свого мандату, AMLA визначила довгострокові стратегічні цілі, такі як забезпечення конвергенції та послідовності шляхом створення уніфікованої системи боротьби з відмиванням коштів та фінансуванням тероризму, сприяння співпраці та інклюзивності серед різноманітних зацікавлених сторін, лідерство в технологіях для швидкого реагування на інновації та нові ризики, побудова довіри та підзвітності перед громадянами та інституціями через прозорість та належне управління, а також позиціонування AMLA як провідного гравця у глобальній боротьбі з фінансовими злочинами. Короткострокові операційні пріоритети AMLA на 2025 рік зосереджені на трьох сферах: задоволення операційних потреб через набір персоналу, розробку внутрішнього управління та створення необхідної IT-інфраструктури; підготовка основних функцій, закладаючи основу для координації ПФР та наглядових завдань; та формування ідентичності та видимості AMLA через розробку комунікаційної стратегії.

Висновки:

- **Пріоритет на високоризикових секторах та гармонізації нагляду:** AMLA активно зосереджується на посиленні стандартів ПВК/ФТ для CASP, розробляючи плани для забезпечення конвергенції національних підходів та включення відповідної фінансової розвідки до спільних аналізів, що вимагає постійної уваги та адаптації з боку підзвітних суб'єктів.
- **Завершення «Єдиного зводу правил» та розробка технічних стандартів:** AMLA надає великого значення підготовці 23 заходів Рівня 2/3 (L2/3) до липня 2026 року, що включає розробку регуляторних та імплементаційних технічних стандартів (RTS/ITS) для гармонізації наглядових процесів, розуміння ризиків підзвітними суб'єктами та функціонування ПФР, що зобов'язує суб'єкти постійно моніторити та впроваджувати нові правила.
- **Посилення співпраці та координації ПФР:** AMLA створює надійну рамку підтримки та координації для ПФР, включаючи призначення делегатів ПФР, пілотні спільні аналізи та процеси взаємної оцінки, а також офіційне оформлення співпраці з правоохоронними органами ЄС (Europol, Eurojust, EPPO, OLAF), що є критично важливим для ефективного виявлення та протидії транскордонним фінансовим злочинам.
- **Будівництво фундаментальної інфраструктури та управління ризиками:** AMLA активно інвестує в створення внутрішньої інфраструктури, включаючи набір кваліфікованого персоналу, розвиток IT-систем (EuReCA, FIU.net, Центральна база даних ПВК/ФТ) та забезпечення фінансової автономії, паралельно впроваджуючи заходи з управління ризиками (наприклад, кібербезпека, затримки з набором персоналу), щоб забезпечити стабільну та надійну основу для майбутніх операцій.

Протягом першої половини 2025 року було досягнуто значного прогресу у створенні AMLA. Тимчасова штаб-квартира у Франкфурті почала функціонувати в лютому, а остаточний договір оренди постійних приміщень у вежі Мессе було підписано в квітні, що забезпечило фізичну присутність. Були формально створені структури управління, що включають призначення Голови та початок роботи Виконавчої ради у червні, а також проведення засідань Генеральної ради; прийняті правила процедури та політика щодо конфлікту інтересів. Були підписані Меморандуми про взаєморозуміння (МоВ) з

Європейськими наглядовими органами (ESA) та ЄЦБ для формалізації міжінституційної співпраці, а також розпочато підготовку до офіційної співпраці з Європолом, Євроюстом, EPPO та OLAF. AMLA активно працювала над реалізацією свого мандату, розпочавши роботу над 23 мандатами 2-го та 3-го рівнів (L2/3), які мають бути виконані до липня 2026 року, охоплюючи наглядові процеси, розуміння ризиків та заходи їхнього зменшення для підзвітних суб'єктів, а також функціонування ПФР. Щодо ПФР AMLA почала розробляти рамки підтримки та координації, а також роботу з групами делегатів ПФР. Щодо ресурсів, AMLA активно наймала персонал у ключові функції, прагнучи до кінця 2025 року мати до 120 співробітників, а також розпочала розробку власної IT-інфраструктури, включаючи підготовку до переходу систем EuReCA від EBA та FIU.net, а також проектування Центральної бази даних по боротьбі з відмиванням коштів та фінансуванням тероризму. Фінансово AMLA вже використала значну частину свого бюджету на 2025 рік і готується до повної фінансової автономії з січня 2026 року. Вона також значно покращила свою видимість через активну комунікаційну діяльність, включаючи візити Голови до всіх держав-членів ЄС та активну присутність у соціальних мережах.

Друга половина 2025 року буде зосереджена на поглибленні операційної готовності AMLA, завершенні внутрішніх процедур та підготовці її першого циклу стратегічного планування. AMLA почне здійснювати деякі свої операційні повноваження, зосереджуючись на непрямому нагляді за фінансовими установами та нагляді за нефінансовим сектором, приділяючи особливу увагу постачальникам послуг криптоактивів (CASP) через їх високий ризик. Також розпочнеться розробка методологій та інструментів для майбутніх повноважень прямого нагляду, запланованих на 2028 рік. Політика AMLA передбачає посилену роботу над пріоритетними мандатами L2/3, такими як Регуляторні технічні стандарти (RTS) щодо бази даних AMLA та Імплементаційні технічні стандарти (ITS) щодо наглядової співпраці, з планами проведення публічних консультацій до кінця року. В рамках ПФР, AMLA фіналізуватиме призначення делегатів ПФР, завершить рамки підтримки та координації, ініціюватиме пілотні спільні аналізи та процеси взаємної оцінки. AMLA також розпочне розробку своєї місії та бачення, а також проектів перших єдиних програмних документів (SPDs) на 2026–2028 та 2027–2029 роки, які визначатимуть її стратегічну траєкторію та операційні пріоритети. На цьому етапі AMLA усвідомлює ризики, пов'язані з її початковим розвитком, такі як затримки з набором персоналу, залежність від зовнішніх термінів, юридичні та процедурні невизначеності, а також IT- та кібербезпекові ризики, і активно впроваджує заходи з їх зменшення. Загалом, 2025 рік є роком, коли AMLA закладає основи для своєї майбутньої ролі у зміцненні колективної стійкості Європи проти фінансових злочинів.

Єдиний стандарт розрахунку операційного ризику в ЄС: фінальний звіт EBA щодо Компонента бізнес-індикатора [3]

Фінальний звіт Європейського банківського органу (EBA) від 16 червня 2025 року присвячено впровадженню єдиного підходу до розрахунку капітальних вимог за операційним ризиком у межах ЄС відповідно до змін у Регламенті (ЄС) № 575/2013 (CRR), внесених Регламентом (ЄС) 2024/1623. Звіт конкретизує положення щодо Компонента бізнес-індикатора (BIC), який тепер є єдиною базою для розрахунку капіталу за операційним ризиком, замінюючи попередні модельні та інші підходи. У цьому контексті ключовим елементом є бізнес-індикатор (BI), що є агрегованим показником, заснованим на фінансовій звітності установи, і який

[3] https://www.eba.europa.eu/sites/default/files/2025-06/7918356f-5669-4e11-9ff7-7f4e6b158ff3/Final%20Report%20on%20Business%20Indicator%20mandates%20for%20operational%20risk.pdf

складається з трьох основних компонентів: Компонент відсотків, оренди та дивідентів (ILDC), Компонент послуг (SC) та Фінансовий компонент (FC).

Звіт детально описує методологію визначення складу кожного з цих компонентів, формули їх обчислення, перелік типових елементів, які мають включатися, а також визначає, які саме елементи підлягають виключенню з BI згідно з CRR. В основі формування ILDC лежить уточнення, які саме доходи та витрати з оренди, відсотків та дивідендів слід враховувати, з урахуванням вимог IFRS 16, що стосується оренди. Особлива увага приділяється врахуванню активів, що генерують відсотковий дохід чи витрати, включно з похідними фінансовими інструментами з позитивною справедливою вартістю, що створюють потоки відсоткових платежів. Для SC вказано необхідність детального урахування витрат, пов'язаних із подіями операційного ризику, включно з винятковими втратами, що можуть бути виключені з розрахунку за дозволом компетентного органу. У складі FC окремо прописано особливості врахування торговельної книги та банківської книги, зокрема можливість використання Підходу за пруденційною межею (PBA) замість Облікового підходу (AA) у випадках, коли застосування стандартного облікового підходу призводить до «невиправданого збільшення» показника FC через економічне хеджування. Використання PBA можливе тільки за умови наявності спеціальних внутрішніх політик, процедур, систем контролю та попереднього повідомлення регулятора, а також із дотриманням умов незмінності обраного підходу протягом трьох років.

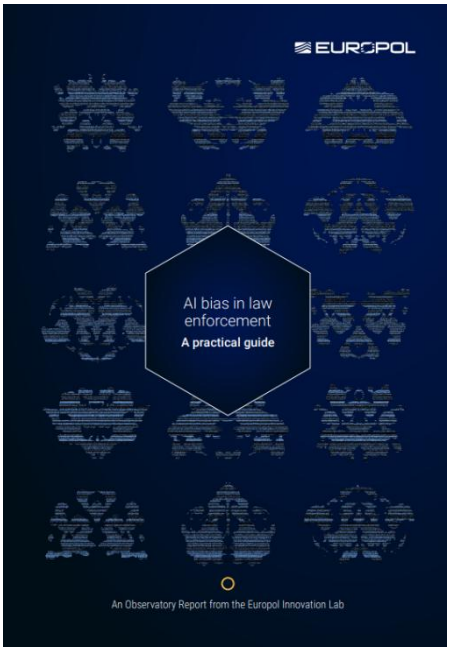
Документ окремо врегульовує порядок коригування BI у випадках злиттів, поглинань або відчужень. Встановлено вимоги до того, як банки повинні включати до BI історичні дані за попередні три роки у разі придбання нових активів або компаній, із застосуванням спрощених методик (включно з коефіцієнтом масштабування в разі злиттів та поглинань або прогнозами), якщо повні історичні дані недоступні або неточні. Для випадків відчуження установам дозволено виключати показники проданих активів або діяльності з BI за умови отримання дозволу від компетентного органу, який повинен оцінити наявність гарантійних зобов'язань або інших факторів, що впливають на операційний ризик. Для дрібних відчужень з річним сукупним впливом менше 5% установлено спрощену процедуру — дозвіл вважається наданим, якщо регулятор не відповів протягом 90 днів, що дозволяє спростити адміністративні процедури для банків.

Висновки:

- Всі установи ЄС повинні застосовувати єдиний Компонент бізнес-індикатора для розрахунку операційного ризику, що передбачає повний перехід від усіх попередніх методів, встановлюючи однакові правила та звітність FINREP як основу для BI.
- Установам дозволено використовувати Підхід за пруденційною межею замість Облікового підходу для Фінансового компонента лише за наявності спеціальних політик, систем, контролів та попереднього повідомлення регулятора, що вимагає суттєвого операційного доопрацювання внутрішніх процесів установ.
- У разі злиття або поглинання банки зобов'язані коригувати BI з урахуванням історичних даних за три роки; якщо дані відсутні — використовуються альтернативні консервативні методики, засновані на факторі коефіцієнту масштабування або прогнозах, що має прямий вплив на планування таких угод та аудит фінансової інформації.
- Для відчуження активів чи діяльності банки можуть отримати дозвіл на коригування BI за умови відповідності чітко визначеним критеріям (включно з відсутністю гарантій за зобов'язаннями проданої діяльності), а для відчужень із сукупним річним впливом менше 5% дозвіл вважається наданим за відсутності заперечень регулятора протягом 90 днів,

Також у звіті детально прописано правила відображення компонентів BI у системі фінансової звітності FINREP, що забезпечує уніфікацію підходів до складання звітності установами ЄС. У цьому контексті EBA наводить карту відповідності між компонентами BI та конкретними фінансовими елементами, що мають бути відображені у FINREP, з урахуванням останніх змін у Міжнародних стандартах фінансової звітності. Звіт формує єдиний підхід, що має забезпечити однакове трактування показників операційного ризику в усіх країнах ЄС, усунути розбіжності в застосуванні різних підходів до розрахунку капіталу за операційним ризиком, а також мінімізувати регуляторний арбітраж і забезпечити відповідність стандартам Basel III. Він передбачає подальше ухвалення розроблених стандартів Європейською Комісією та їхню офіційну публікацію в Офіційному віснику ЄС після розгляду Європарламентом та Радою ЄС.

Упередженість штучного інтелекту в правоохоронній діяльності: практичний путівник для органів ЄС[4]



Документ, підготовлений Europol Innovation Lab у 2025 році, є комплексним аналітичним посібником, мета якого — забезпечити правоохоронні органи держав-учасниць ЄС систематизованими знаннями та практичними рекомендаціями щодо виявлення, запобігання і пом'якшення упередженості штучного інтелекту (AI bias) під час застосування AI-систем у правоохоронній діяльності. Центральним фокусом документа є збалансування інноваційного потенціалу AI з дотриманням принципів справедливості, недискримінації та захисту основоположних прав людини, передбачених, зокрема, Регламентом (ЄС) 2024/1689 (AI Act).

У вступній частині документ пояснює, що застосування AI в поліції та інших правоохоронних структурах здатне суттєво підвищити ефективність — у таких сферах, як аналіз великих масивів даних, ідентифікація підозрюваних, прогнозування злочинності, автоматизоване складання звітів та обробка доказової бази. Однак ці можливості супроводжуються ризиками, пов'язаними з упередженістю як у даних, так і в алгоритмах, що може призводити до помилкових рішень, дискримінації окремих груп населення та зниження довіри до правоохоронної системи загалом.

Окремий блок документа присвячений визначенню та класифікації AI bias. Автори детально описують, що упередженість може виникати на всіх етапах життєвого циклу AI-системи: від формулювання завдання та збору даних до її впровадження і використання в реальних умовах. У період проєктування особливо значущими є упередженість у формулюванні задачі, відображення історичних соціальних нерівностей у даних, нерепрезентативність вибірки, упередженість аннотацій. У фазі розробки наголошується на упередженості вимірювання, упередженості через узагальнення, упередженності навчання та упередженості оцінювання. На етапі розгортання найбільш критичними є упередженість на етапі впровадження, упередженість через неналежне використання та упередженість автоматизації, коли системи

[4] https://www.europol.europa.eu/cms/sites/default/files/documents/AI_bias_in_law_enforcement_-_practical_guide.pdf

використовуються не за призначенням або коли персонал надмірно покладається на їх результати, ігноруючи контекст та здоровий глузд.

У документі наведено класифікацію AI bias не лише за життєвими циклами, але й за джерелами, де виділяються системні, людські та статистичні упередженості. Підкреслюється, що навіть у найретельніше спроєктованих системах упередженість не можна повністю усунути, оскільки AI неминуче відображає соціальні контексти, у яких він працює. Значна увага приділяється викликам, пов'язаним із великими мовними моделями (LLM), які через масштабність навчальних даних легко переймають та транслюють соціальні стереотипи й можуть не враховувати мовно-культурну специфіку різних груп населення.

Окремий розділ присвячено аналізу ризиків та потенційної шкоди, яку може спричиняти упередженість AI у правоохоронній сфері. Особливо гострою проблемою вважається використання аналітики для прогнозування ймовірності скоєння злочинів, визначення зон підвищеної небезпеки чи потенційних підозрюваних. Наводяться реальні кейси, зокрема із Нідерландів (система SyRI), коли AI-рішення визнавалися незаконними через дискримінацію за соціально-економічними або етнічними ознаками.

Ще однією важливою темою документа є визначення метрик справедливості, необхідних для оцінки AI-систем: демографічна рівність, рівність можливостей, паритет прогнозування, а також причинно-наслідкові метрики. Автори наголошують, що вибір конкретної метрики має базуватись на глибокому розумінні соціального контексту та цілей застосування системи. Універсальних рішень немає: те, що працює для однієї задачі, може виявитися неефективним або навіть шкідливим для іншої.

Висновки:

- Впровадження AI в правоохоронній діяльності без системного контролю за похибками може призводити до дискримінації та порушень основоположних прав, особливо у сфері політики прогнозування.
- Для ефективного управління AI bias, правоохоронні мають застосовувати комплексну систему: від етапу розробки до постійного моніторингу, включаючи документацію, багаторівневий контроль за роботою AI-систем з боку людини на всіх етапах її використання правоохоронними органами та участь зовнішніх стейкхолдерів.
- Показники справедливості мають застосовуватись з урахуванням конкретного контексту задачі; універсальні показники справедливості часто не працюють коректно без глибокого аналізу соціально-демографічних факторів.
- Всі AI-системи, що використовуються правоохоронними органами ЄС, повинні відповідати вимогам AI Act, включаючи детальну технічну документацію, оцінку впливу на права людини та систему внутрішнього контролю за дотриманням цих стандартів.

Документ систематизує підходи до зниження AI bias: підготовка та очищення даних, налаштування моделей у процесі навчання, обробка результатів та корекція рішень. Окремо розглядаються компроміси між справедливістю, точністю моделей та конфіденційністю даних, зокрема в умовах високоризикових застосувань, до яких належить правоохоронна діяльність.

У фінальній частині наводяться структуровані рекомендації для правоохоронних органів: створення системи повної документації життєвого циклу AI-систем; впровадження соціально-технічних рамок оцінки з урахуванням історичних, соціальних та демографічних факторів; регулярне навчання персоналу з питань упередженості AI та методів її подолання; обов'язкове тестування моделей до розгортання з перевіркою якості та упередженості даних;

постійний моніторинг AI-систем протягом їхнього життєвого циклу; забезпечення участі людини (human-in-the-loop) у прийнятті рішень; стандартизація процедур оцінки справедливості в межах організації.

Окремо наголошується на відповідальності правоохоронних органів за дотримання вимог AI Act як у ролі постачальників послуг, так і користувачів AI-систем, зокрема у сфері ризик-менеджменту, управління даними, забезпечення прозорості, документації, оцінки впливу на права людини та внутрішнього контролю відповідності. Автори наполягають на мультидисциплінарному підході, із залученням соціологів, юристів, інженерів, правозахисників та громадянського суспільства для забезпечення максимально збалансованого й етичного використання AI в правоохоронній практиці. Документ розглядається як практичний посібник для розбудови в органах поліції ЄС системи управління AI bias, яка одночасно забезпечує ефективність роботи та захист прав і свобод людини.

SARs in Action Issue 32: Оновлення цифрової трансформації, 10 років публічно-приватного партнерства та міжнародна співпраця у боротьбі з економічними злочинами [5]

Тридцять другий випуск журналу, створеного Британським підрозділом фінансової розвідки (UKFIU), який діє під егідою Національного агентства з боротьби зі злочинністю (NCA). Цей випуск є важливим джерелом інформації для широкої аудиторії, до якої входять правоохоронні органи, підзвітні суб'єкти, регулятори, наглядові органи, торговельні асоціації, урядові та міжнародні партнери. Журнал зосереджується на ключових аспектах боротьби з економічними злочинами, зокрема відмиванням грошей, шахрайством, ухиленням від сплати податків, фінансуванням тероризму, а також іншими формами організованої злочинності, такими як сучасне рабство та сексуальна експлуатація. Він поєднує оновлення щодо ініціатив UKFIU, практичні кейси, пояснення процедур та анонси майбутніх подій, надаючи читачам комплексне уявлення про поточну діяльність підрозділу.

Журнал відкривається зверненням заступника директора UKFIU Вінса О'Браєна, який вітає читачів і коротко представляє основні теми випуску. Одним із центральних елементів є оновлення щодо програми цифрової трансформації SARs (Suspicious Activity Reports), яка зосереджена на розвитку Цифрового сервісу SARs (SDS). Цей сервіс дозволяє користувачам, зокрема правоохоронцям, швидко шукати інформацію за такими параметрами, як імена, адреси, номери телефонів та дати народження. Користувачі відзначають зручність інтерфейсу та швидкість отримання результатів. Наразі SDS містить понад один мільйон звітів про підозрілі операції, поданих через нові канали звітності, запроваджені у 2023 році, а саме через Bulk API та SARs Portal. На горизонті заплановано значне розширення бази даних шляхом перенесення застарілих звітів із попередніх каналів звітності. Очікується, що перенесення основних даних завершиться до початку літа 2025 року, після чого сервіс стане доступним для ширшого кола користувачів у межах UKFIU, а згодом і для зовнішніх партнерів.

Ще однією важливою темою є діяльність UKFIU із залучення підзвітних суб'єктів, зокрема через щомісячні семінари, організовані командою Reporter Engagement Team для представників нефінансового регульованого сектору. Ці семінари спрямовані на підвищення обізнаності про

[5] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/752-sars-in-action-issue-32/file

юридичні зобов'язання щодо подання звітів про підозрілі операції у випадках підозри на відмивання грошей або фінансування тероризму. Крім того, UKFIU анонсує випуск нової настанови, яка перебуває в процесі перегляду, і закликає стежити за оновленнями через соціальні мережі. Ці ініціативи підкреслюють зусилля UKFIU щодо поглиблення співпраці з регульованим сектором, що є критично важливим для ефективного виявлення та запобігання фінансовим злочинам.

Значна частина випуску присвячена 10-річчю Публічно-приватного партнерства (PPP) у боротьбі з економічними злочинами, яке було започатковане у 2015 році як Joint Money Laundering Intelligence Taskforce (JMLIT). Ця ініціатива, розроблена спільно NCA, Міністерством внутрішніх справ, Поліцією Лондону, UK Financial та кількома великими фінансовими установами, стала новаторським механізмом для обміну, аналізу та поширення розвідувальної інформації між державним і приватним секторами. За десять років PPP досягло значних результатів, підтримавши 1282 запити за статтею 7 Закону про доходи від злочинної діяльності, сприяло приблизно 1200 операціям та призвело до 419 арештів. Почавши з 12 партнерів, партнерство розширилося до понад 200 організацій, включаючи банки, фінансові установи, інвестиційні компанії, телекомунікаційні фірми, платіжні процесори, постачальників віртуальних активів та інші суб'єкти, які співпрацюють із правоохоронними органами, регуляторами та іншими державними структурами.

PPP нині включає чотири спеціалізовані групи з питань шахрайства, незаконних фінансів, ухилення від податків та фінансування тероризму, а також Форум із криптовалют і Міжнародну робочу групу. Партнерство зосереджується на міжсекторальних загрозах, таких як сексуальна експлуатація дітей, сучасне рабство та торгівля людьми. Через Національний центр економічної злочинності (NECC) було опубліковано понад 100 попереджень для зацікавлених сторін, що сприяло кращому розумінню нових загроз і вдосконаленню методологій захисту в індустрії. Важливим кроком стало впровадження пілотного проєкту Data Fusion, який об'єднав NCA та сім британських банків для пришвидшення обміну інформацією. Спільна аналітична команда, що складалася з правоохоронців, фінансових слідчих і аналітиків даних, створила стратегічні розвідувальні продукти, які допомогли приватному сектору краще захищатися від організованої злочинності, запустити нові розслідування та виявити раніше невідомі злочинні активи. Цей проєкт також сприяв новим звинуваченням у кримінальних справах. У майбутньому PPP планує розширювати співпрацю з технологічними компаніями, соціальними мережами та криптовалютними платформами, щоб адаптуватися до нових загроз і вдосконалювати внутрішні контролі для запобігання злочинності.

У 2025 році Велика Британія взяла на себе президентство в Camden Asset Recovery Inter-Agency Network (CARIN), європейській мережі агентств із відстеження активів, яка є частиною глобальної мережі, що охоплює понад 200 юрисдикцій. Президентство очолюють заступник директора UKFIU Вінс О'Браєн та головний прокурор Адріан Фостер. У березні 2025 року в Валлетті, Мальта, відбулося перше засідання керівної групи CARIN, яке об'єднало оперативних і судових партнерів із 10 країн за підтримки Europol і Eurojust. Під час зустрічі учасники обмінялися інформацією про успішні кейси, прогрес у законодавстві та методиках розслідувань, а також обговорили переваги та недоліки різних підходів до відстеження активів і обміну розвідданими на міжнародному рівні. Мальтійська поліція, Бюро з повернення активів та Фінансова розвідка Мальти представили свої практики боротьби з відмиванням грошей. CARIN планує провести щорічні загальні збори в жовтні 2025 року, щоб визначити стратегічні пріоритети на майбутнє.

Журнал також містить роз'яснення від UKFIU щодо різниці між "вартістю кримінального майна" (Criminal Property Value) та "вартістю майбутньої визначеної діяльності" (Future Specified Activity Value) при поданні звітів про захист від відмивання грошей (DAML). Згідно з Законом про доходи від злочинної діяльності 2002 року (POCA), кримінальне майно є ключовим елементом злочинів,

пов'язаних із відмиванням грошей. Підзвітні суб'єкти повинні чітко описувати кримінальне майно та його загальну вартість у своїх звітах, а у випадку DAML — також оцінювати вартість майбутньої діяльності. У більшості випадків ці значення збігаються, але можуть відрізнятися залежно від обставин. UKFIU рекомендує звертатися за юридичною консультацією у складних випадках, щоб забезпечити відповідність вимогам законодавства.

Документ наводить два приклади успішного використання SARs. У першому випадку підзвітний суб'єкт виявив підозрілі транзакції у кількох пов'язаних бізнес-рахунках, які отримували великі надходження та швидко переказували їх третім сторонам у Великій Британії та за кордон. Розслідування правоохоронних органів встановило, що ці рахунки використовувалися для податкових шахрайств і відмивання грошей, що призвело до замороження рахунків і конфіскації понад £300,000. У другому випадку підзвітний суб'єкт подав DAML після виявлення невідповідностей між фінансовими операціями компанії та даними Companies House. Розслідування виявило, що рахунок був відкритий шахрайським шляхом через крадіжку особистих даних, а жертва не знала про існування рахунку. Правохоронці ідентифікували підозрюваного з попередньою судимістю за шахрайство та заморозили рахунок на суму понад £350,000, розслідування триває.

Висновки:

- **Оптимізація цифрової звітності через SDS:** Цифровий сервіс SARs забезпечує швидкий доступ до даних і планує розширення шляхом інтеграції застарілих звітів поданих до літа 2025 року. Підзвітним суб'єктам і правоохоронцям рекомендується активно використовувати SDS і надавати зворотний зв'язок для вдосконалення системи.
- **Ефективність публічно-приватного партнерства (PPP):** Пілотний проєкт Data Fusion і ширше продемонстрували успіх у виявленні злочинних активів і запуску нових розслідувань. Приватному сектору варто активніше долучатися до спільних аналітичних команд для обміну інформацією та посилення захисту від організованої злочинності.
- **Міжнародна співпраця через CARIN:** Президентство Великої Британії в CARIN у 2025 році відкриває можливості для обміну досвідом і вдосконалення методик відстеження активів. Партнерам рекомендується брати участь у заходах CARIN, зокрема в загальних зборах у жовтні 2025 року, для розвитку глобальної співпраці.
- **Точність у поданні DAML:** Підзвітні суб'єкти повинні чітко розмежовувати "вартість кримінального майна" та "вартість майбутньої діяльності" при поданні DAML, звертаючись за юридичною консультацією у складних випадках, щоб відповідати вимогам Закону про доходи від злочинної діяльності 2002 року.

INTERPOL 2025: Стрімке зростання кіберзлочинності в Африці [6]

Звіт INTERPOL детально аналізує стрімке зростання кіберзлочинності в Африці, підкреслюючи її масштаби, основні загрози, виклики для правоохоронних систем та кроки, спрямовані на зміцнення кіберстійкості. Документ базується на оперативній розвідці, опитуваннях африканських країн-членів INTERPOL, а також даних від приватних партнерів, таких як Trend Micro, Bi Zone та Group-IB. Звіт наголошує на критичній потребі в посиленні міжнародної співпраці, вдосконаленні законодавства, підвищенні кваліфікації правоохоронців та

[6] https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

інвестуванні в технологічну інфраструктуру для протидії кіберзагрозам, які дедалі більше впливають на стабільність, економіку та цифровий суверенітет африканських держав.

Згідно зі звітом, кіберзлочини становлять значну частку всіх зареєстрованих злочинів у Африці, причому дві третини країн-членів INTERPOL повідомили, що кіберзлочини складають середню або високу частку злочинності, досягаючи 30% у Західній та Східній Африці. Найпоширенішими видами кіберзагроз є онлайн-шахрайство, зокрема фішинг, програми-вимагачі (ransomware), компрометація ділової переписки (business email compromise, BEC) та цифровий шантаж, який включає шантаж із використанням сексуально відвертих зображень, створених як добровільно, так і за допомогою штучного інтелекту.

Дані вказують на зростання кількості повідомлень про підозрілі шахрайства на 3000% у деяких країнах за останній рік. Програми-вимагачі становлять серйозну загрозу, особливо в країнах із розвиненою цифровою інфраструктурою, таких як Південна Африка (17 849 випадків у 2024 році), Єгипет (12 281 випадків), Нігерія (3 459 випадків) та Кенія (3 030 випадків). BEC-шахрайство, поширене в Західній Африці, підтримує діяльність організованих злочинних груп, таких як синдикат Black Axe, тоді як цифровий шантаж зріс на 60%, часто із застосуванням зображень, створених штучним інтелектом.

Висновки:

- **Вдосконалення законодавства та інфраструктури:** Африканським країнам слід терміново оновити правові рамки, гармонізуючи їх із міжнародними стандартами, та створити системи повідомлення про кіберінциденти, цифрові сховища доказів і бази даних кіберрозвідки для ефективної боротьби з кіберзлочинами.
- **Посилення співпраці:** Необхідно прискорити міжнародну співпрацю через оперативні мережі та спростити доступ до даних, розміщених за кордоном, а також налагодити чіткі канали взаємодії з приватним сектором для спільного розслідування кіберзлочинів.
- **Інвестиції в підготовку кадрів:** Правоохоронні органи потребують спеціалізованого навчання та доступу до сучасних інструментів, щоб подолати нестачу ресурсів і кваліфікації, про яку повідомили 95% країн.
- **Підвищення обізнаності громадян:** Розширення програм інформування про фішинг, програми-вимагачі та цифрове шахрайство допоможе зменшити кількість жертв і підвищити кіберстійкість суспільства.

Правоохоронні органи Африки стикаються з численними викликами в боротьбі з кіберзлочинністю. Три чверті опитаних країн зазначили, що їхні правові системи потребують значного вдосконалення, тоді як 95% повідомили про нестачу підготовки кадрів, обмежені ресурси та брак спеціалізованих інструментів. Лише 30% країн мають системи повідомлення про кіберінциденти, 29% – сховища цифрових доказів, а 19% – бази даних кіберрозвідки. Міжнародна співпраця також є проблемною: 86% країн вказали на необхідність її покращення через повільні формальні процеси, відсутність оперативних мереж і обмежений доступ до даних, розміщених за кордоном. Співпраця з приватним сектором, яка є ключовою для розслідування кіберзлочинів, також потребує значного вдосконалення, про що повідомили 88% країн, посилаючись на нечіткі канали взаємодії та низьку інституційну готовність.

Незважаючи на ці виклики, звіт відзначає позитивні зрушення. Деякі африканські країни гармонізували свої закони про

кібербезпеку з міжнародними стандартами та інвестували в спеціалізовані підрозділи й інфраструктуру цифрової криміналістики. Успішні міжнародні операції, такі як Operation Serengeti та Operation Red Card, скоординовані INTERPOL, призвели до понад 1000 арештів і ліквідації тисяч шкідливих мереж. Звіт пропонує шість стратегічних рекомендацій для подальшого посилення кіберстійкості, включаючи покращення регіональної та міжнародної співпраці, розширення превентивних заходів і підвищення обізнаності громадськості, а також використання новітніх технологій. Документ є частиною ініціативи INTERPOL African Joint Operation against Cybercrime (AFJOC), яка підтримується Управлінням закордонних справ, співдружності та розвитку Великої Британії та спрямована на зміцнення спроможностей африканських правоохоронних органів у запобіганні, виявленні, розслідуванні та припиненні кіберзлочинів.

Звіт також звертає увагу на нові загрози, такі як шахрайство на основі штучного інтелекту, яке вимагає негайної уваги та скоординованих дій. Кіберзлочинність розглядається не лише як технічна проблема, але як виклик, що загрожує стабільності, миру, довірі громадян і економічному розвитку Африки. Для ефективної протидії необхідна комплексна стратегія, яка поєднує вдосконалення законодавства, інвестиції в інфраструктуру, навчання кадрів і співпрацю з міжнародними та приватними партнерами.

Звіти окремих інституцій та експертів

Азартні ігри та казино [7]

Документ є змістовним дослідженням трансформації грального бізнесу під впливом організованої злочинності, з особливим фокусом на механізми відмивання коштів через онлайн-гемблінг. Автор, фахівець з фінансових злочинів Паоло Апріле, детально висвітлює історичну еволюцію та сучасні виклики у сфері AML/CTF у зв'язку з діяльністю злочинних угруповань у гральному секторі.

Матеріал починається з історичного екскурсу у формування грального бізнесу в США, особливо в Лас-Вегасі, де мафіозні структури, такі як Коза Ностра, використовували казино як потужний інструмент легалізації кримінальних доходів. Через інвестування у будівництво готелів і казино, зокрема Flamingo, Riviera та Tropicana, злочинці зуміли приховати походження коштів, представляючи їх як доходи від легальної діяльності. Попри запровадження закону RICO у 1970-х і посилення федерального контролю у 1980-х, успадкований вплив організованої злочинності досі залишається фундаментальною частиною ДНК грального індустрії США.

Особливу увагу автор приділяє слабкостям Європейського Союзу в регулюванні онлайн-гемблінгу. Через відсутність гармонізованого законодавства країни ЄС застосовують різні режими, що дозволяє злочинцям структурувати діяльність у кількох юрисдикціях для уникнення контролю. Сервери, ліцензії, користувачі та платіжні канали можуть бути розміщені у різних країнах, створюючи безконтрольне середовище. У цьому контексті італійська Ндрангета дедалі активніше інвестує в цифрові платформи ставок, використовуючи фіктивні акаунти,

[7] https://www.canva.com/design/DAGooQ78aAk/6BfJVG8oJU6ReaznVZlJzQ/view?utm_content=DAGooQ78aAk&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=ha8956ce685#2

передплачені картки, викрадені банківські дані та неторговельні віртуальні валюти, щоб уникати відстеження.

Окремим кейсом виступає Мальта - найбільший онлайн-гемблінг-хаб Європи. Завдяки стабільному регуляторному середовищу, низькому податковому навантаженню та спрощеним умовам отримання ліцензій, країна стала привабливою не лише для легальних операторів, а й для кримінальних груп. Розслідування виявляють схеми, в яких мальтійські компанії роками не подають фінзвітності, приховують бенефіціарних власників і використовують номінальних директорів. Спрощена реєстрація, слабкий митний контроль і наявність професійних посередників (юристів, бухгалтерів) лише сприяють цьому.

Злочинні механізми детально описані на прикладі італійської мафії, яка створює компанії в офшорах, легалізує бізнес у Мальті, відкриває точки прийому ставок в Італії, а кошти переказує через установи електронних грошей. Завдяки цим механізмам, що поєднують контрольовані агенції, фіктивні онлайн-платформи і анонімні платіжні системи, організовані злочинні групи змогли прокрутити понад €1 млрд. Аналогічні схеми зафіксовані і в Туреччині, де було припинено діяльність сотень нелегальних платформ і арештовано десятки підозрюваних.

Висновки:

- Онлайн-гемблінг є одним із найвразливіших секторів до відмивання коштів через його транснаціональний характер, цифрові платформи і прогалини в регулюванні, особливо в ЄС.
- Мальта виступає подвійним феноменом - як центр технологічного прогресу в ігровій сфері, так і як осередок легалізації кримінальних доходів через ліцензійні та регуляторні лазівки.
- Сучасні AML-механізми, включно з підозрілими повідомленнями та правилами верифікації, не виконують своєї функції через брак реального контролю, недостатність ресурсів та відсутність міждержавної координації.
- Для ефективної протидії використанню гемблінгу в цілях ВК потрібна радикальна прозорість, обов'язковий обмін даними, уніфіковане законодавство та посилений контроль над фінтех-сектором.

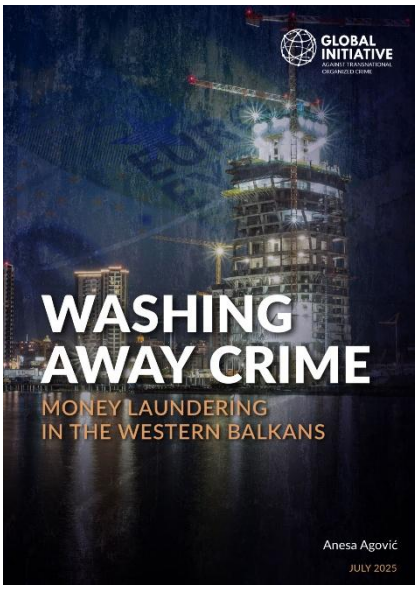
Автор критикує неефективність системи AML: лише 5–10% повідомлень про підозрілі транзакції призводять до реальних розслідувань. Ринок переповнений фіктивним дотриманням - фінансові установи впроваджують технології, але не перевіряють походження коштів, регулятори презентують нормативні документи, але не забезпечують їх реального виконання. Окрема критика стосується відсутності обов'язковості до виконання статті 75 Єдиного зведеного Регламенту ЄС з питань ПВК, яка передбачає обмін інформацією, але залишається рекомендацією. Як наслідок, створюється лише ілюзія контролю, в той час як злочинці безперешкодно використовують прогалини системи.

Відмивання коштів на Західних Балканах: як кримінальні схеми інтегруються в легальну економіку [8]

Документ є ґрунтовним дослідженням, присвяченим аналізу поточних тенденцій, типологій та ключових викликів у сфері відмивання коштів у шести країнах Західних Балкан: Албанії, Боснії і Герцеговині, Косово, Чорногорії, Північній Македонії та Сербії. Він базується на контент-аналізі нормативних документів, судової практики, журналістських розслідувань, а також на

[8] https://globalinitiative.net/wp-content/uploads/2025/07/Anesa-Agovic-Washing-away-crime-Money-laundering-in-the-Western-Balkans-GI-TOC-July-2025.pdf

результатах 99 глибоких інтерв'ю з експертами з правоохоронних органів, фінансових розвідок, регуляторних органів, громадського сектору та приватного бізнесу, проведених наприкінці 2023 — на початку 2024 року.



Основним змістом документа є системний аналіз того, яким чином кримінальні організації, корумповані посадовці та професійні посередники використовують легальні економічні сектори для легалізації доходів, одержаних злочинним шляхом. Автори підкреслюють, що Західні Балкани залишаються вразливою зоною для ВК/ФТ через комбінацію політичної нестабільності, недосконалості судової системи, високого рівня корупції, географічного положення як транзитного коридору для наркотиків, зброї та мігрантів, а також через велику частку тіньової економіки.

Особливий акцент робиться на тому, що головними секторами, через які відмивають кошти, є будівництво та ринок нерухомості, банківський сектор, гральний бізнес (у тому числі онлайн-казино), а також професійні послуги — юридичні, бухгалтерські, нотаріальні. Автори детально описують типології відмивання коштів, які поєднують класичні та сучасні методи. Серед найбільш поширених згадуються: смурфінг (метод відмивання коштів, при якому велика сума грошей поділяється на багато дрібних транзакцій, щоб уникнути уваги фінансових установ та запобігти їхньому виявленню), корпоративне шарування через офшорні компанії та фіктивні юрособи, фіктивні контракти на послуги, фіктивне інвойсування, схеми відмивання коштів через фредитування або позики, маніпуляції з вартістю нерухомості (заниження чи завищення цін), купівля-продаж нерухомості із перепродажем. Окремо згадується активне використання криптовалют, систем Hawala, соціальних медіа та інструментів DeFi для маскування походження коштів.

Автори особливо наголошують на феномені професійних відмивачів коштів — осіб або компаній, які спеціалізуються на наданні послуг із легалізації доходів для злочинних угруповань. У тексті наводяться конкретні приклади із Боснії і Герцеговини, Сербії та Косово, де до схем відмивання залучалися адвокати, нотаріуси, економісти, бухгалтери, а також керівники банківських установ. Наприклад, у Боснії фігурує кейс банкіра, який одночасно займався легалізацією коштів через інвестиції в будівництво.

Дуже детально у звіті описано вплив геополітичних процесів, зокрема війни в Україні та санкцій проти Росії, на збільшення обсягів фінансових потоків із країн високого ризику, зокрема Росії, ОАЕ та Китаю. Ці кошти реінвестуються в будівництво, нерухомість, банківські депозити та інші сектори економіки Західних Балкан, що суттєво ускладнює контроль із боку регуляторів та фінансових розвідок.

Значна частина дослідження присвячена аналізу судових систем та інституційних рамок протидії відмиванню коштів у кожній країні регіону. Виявлено, що хоча формально закони приведені у відповідність до вимог FATF та MONEYVAL, на практиці є серйозні проблеми з їх застосуванням: суди часто ухвалюють умовні вироки, штрафи замість реальних строків, фінансові розслідування проводяться непослідовно, а діяльність фінансових розвідок політично залежна. В окремих випадках зафіксовано пряму участь правоохоронців у схемах відмивання коштів.

Автори аналізують також соціальні аспекти проблеми, включно з роллю жінок у схемах ВК, що часто недооцінюється. Описано випадки, коли жінки виступають не лише як номінальні власники чи «довірені особи», а й як самостійні організатори фінансових схем, зокрема у сферах обслуговування, модного бізнесу, фітнес-індустрії.

Окрема частина присвячена не лише факторам, що генерують «брудні» кошти, а й оцінці тенденцій у таких сферах, як наркоторгівля, торгівля людьми та мігрантами, кіберзлочинність, незаконна діяльність з надання кредитів під надвисокі відсотки, незаконний гральний бізнес, незаконна торгівля зброєю. Детально описані кейси транскордонних схем, де фігурують офшорні компанії, компанії оболонки, брокери Hawala, зокрема між Албанією, Косово, Чорногорією та офшорними юрисдикціями.

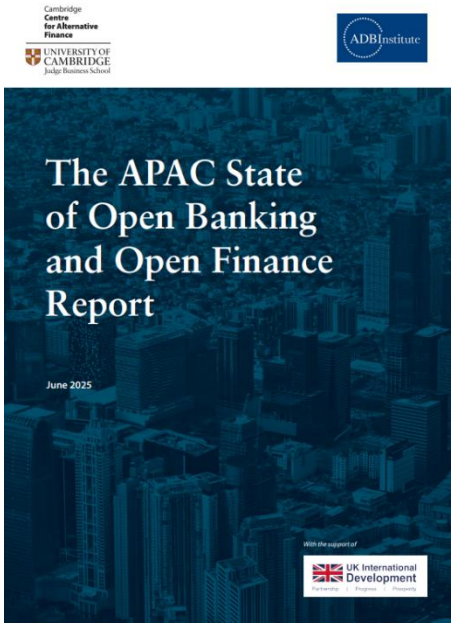
У висновках документ наполягає на необхідності інтенсифікувати переслідування за відмивання коштів як окремий злочин, а не лише як складову організованої злочинності, посилювати інструменти конфіскації активів, реформувати системи судочинства, забезпечити реальну незалежність фінансових розвідок та регуляторів. Пропонується створити регіональну платформу обміну фінансово-розвідувальною інформацією, а також проводити спільні навчання для суб'єктів фінансового моніторингу у форматі FATF/MONEYVAL. Автори також рекомендують країнам регіону гармонізувати підходи до контролю за віртуальними активами, запровадити регулювання криптовалютних бірж та гаманців, створити реєстри бенефіціарних власників з відкритим доступом.

Висновки:

- Основними каналами відмивання коштів у Західних Балканах залишаються будівництво, нерухомість та банківський сектор, що вимагає запровадження жорсткішого регулювання походження капіталу при операціях у цих сферах (наприклад, обов'язкової перевірки джерел фінансування при отриманні дозволів на будівництво).
- Організовані злочинні угруповання широко застосовують як класичні, так і новітні типології відмивання коштів, зокрема криптовалюти, Hawala та структурування через фіктивні компанії. Це вимагає термінового впровадження комплексного контролю за віртуальними активами та створення реєстрів бенефіціарних власників.
- Відсутність незалежності правоохоронних органів та судових систем є критичним бар'єром для ефективної боротьби з ВК/ФТ у регіоні, що потребує впровадження міжнародно контрольованих механізмів моніторингу ефективності розслідувань та переслідувань у сфері ПВК.
- Для зменшення ризиків необхідне створення регіональної платформи обміну фінансово-розвідувальною інформацією з обов'язковим залученням FATF, MONEYVAL та ЄС, а також запровадження спільних тренінгів та стандартів для ПФР країн Західних Балкан.

Загалом документ являє собою повноцінний регіональний аналіз, що дозволяє не лише розуміти локальні особливості кожної країни Західних Балкан, а й бачити системні закономірності, спільні загрози та потенційні точки впливу для міжнародних організацій, урядів та фінансових інституцій. Він може бути використаний як аналітична база для підготовки національних стратегій ПВК, законодавчих змін, підготовки до взаємних оцінок FATF/MONEYVAL, а також як навчальний матеріал для підвищення кваліфікації співробітників фінансових розвідок, банків, правоохоронців та суддівського корпусу.

Як APAC змінює правила гри у відкритому банкінгу: аналітичний огляд глобальних трендів[9]



Звіт є однією з найґрунтовніших аналітичних робіт, присвячених впровадженню концепцій відкритого банкінгу та відкритого фінансування у країнах Азійсько-Тихоокеанського регіону (APAC). Документ побудовано на основі глибокого дослідження у 16 юрисдикціях, із залученням якісних інтерв'ю з ключовими учасниками ринку, регуляторами та галузевими асоціаціями. Основна мета дослідження полягає у фіксації реального стану впровадження відкритого банкінгу та відкритого фінансування, аналізі ключових драйверів, бар'єрів та прогнозів їх подальшого розвитку саме у специфічному для APAC контексті, який характеризується високою різноманітністю економічних моделей, цифрової інфраструктури та регуляторних підходів.

У звіті детально описано концептуальні відмінності між відкритим банкінгом, відкритим фінансуванням та ширшим поняттям відкриті дані. Відкритий банкінг розглядається як механізм, що дозволяє клієнтам банків та платіжних систем ділитися фінансовими даними з третіми сторонами для отримання персоналізованих послуг, тоді як відкрите фінансування розширює ці можливості до страхування, пенсій, інвестицій, кредитування та інших фінансових продуктів. Термін «відкриті дані» виходить за межі фінансового сектору і включає енергетику, транспорт, охорону здоров'я тощо. Окремо підкреслюється, що більшість сучасних систем відкритого банкінгу базуються на API (Application Programming Interfaces), що забезпечують безпечний і стандартизований обмін даними на відміну від застарілих методів екранного зчитуваня даних.

Ключовим аспектом аналізу є типологія моделі регуляторного управління, яка представлена у вигляді континууму від підходу, що базується на регулюванні до підходів, орієнтованих на ринок, з п'ятьма архетипами: Mandated & Standardised Data Sharing, Mandated Data Sharing, Standardised Data Sharing, Guided Implementation та Voluntary. Згідно з результатами дослідження, APAC-регіон унікально відрізняється від глобальної тенденції — 57% юрисдикцій обрали моделі підходу, що орієнтовані на ринок (Guided Implementation або Voluntary), тоді як у світі підходи, що базуються на регулюванні домінують. Це зумовлено як конкурентним ландшафтом банківських послуг у таких країнах, як Гонконг, Сінгапур, Малайзія, так і обмеженими можливостями регуляторів в окремих країнах забезпечити повномасштабне впровадження обов'язкових стандартів.

Особливої уваги заслуговує те, що в APAC фінансова інклюзія визначена як провідна ціль для моделей підходів, що базуються на регулюванні, на відміну від глобального контексту, де пріоритетом є конкуренція. У таких країнах, як Індія та Індонезія, системи відкритого банкінгу та відкритого фінансування використовуються саме для подолання бар'єрів доступу до фінансових послуг для незабезпечених верств населення. Наприклад, в Індії функціонує система Account Aggregator, що надає змогу більш ніж 2 мільярдам фінансових рахунків інтегруватися з екосистемою відкритого банкінгу, забезпечуючи понад 179 мільйонів успішних транзакцій зі згодою клієнтів.

[9] https://www.jbs.cam.ac.uk/wp-content/uploads/2025/06/2025-ccaf-apac-state-of-open-banking-and-open-finance.pdf

Звіт детально аналізує роль Цифрової державної інфраструктури (DPI) як обов'язкової умови успішного впровадження відкритого банкінгу. Серед ключових елементів DPI виділено цифрову ідентифікацію (наприклад, Aadhaar в Індії чи Singpass у Сінгапурі), системи миттєвих платежів (наприклад, PromptPay у Таїланді), стандарти обміну даними та механізми забезпечення згоди споживачів. Автори наголошують, що навіть найкращі технологічні рішення не будуть ефективними без побудови довіри серед усіх учасників екосистеми — від банків до споживачів та третіх сторін.

У рамках аналізу тенденцій впровадження відкритого фінансування зазначено, що розширення за межі банківських продуктів відбувається повільно і вибірково. Лише частина юрисдикцій успішно інтегрувала у відкриті екосистеми страхування, інвестиційні продукти та пенсійне забезпечення. І підхід, що базуються на регулюванні, і підхід, що орієнтується на ринок, стикаються із системними викликами в цьому процесі, включаючи питання захисту даних, забезпечення відповідності стандартам, недовіру клієнтів та недостатню розвиненість технічної інфраструктури.

Серед стратегічних висновків у звіті окремо підкреслено, що навіть ринкові моделі потребують подальшого розвитку у напрямку формалізації стандартів та регуляторного супроводу, особливо з огляду на ризики монополізації ринку великими фінансовими установами. Прогнозується, що у найближчі роки більше APAC-юрисдикцій перейде до моделей підходу, що базуються на регулюванні або змішаних форм управління, що передбачає обов'язкові вимоги щодо обміну даними, стандартизацію процесів та посилення контролю за захистом прав споживачів.

Висновки:

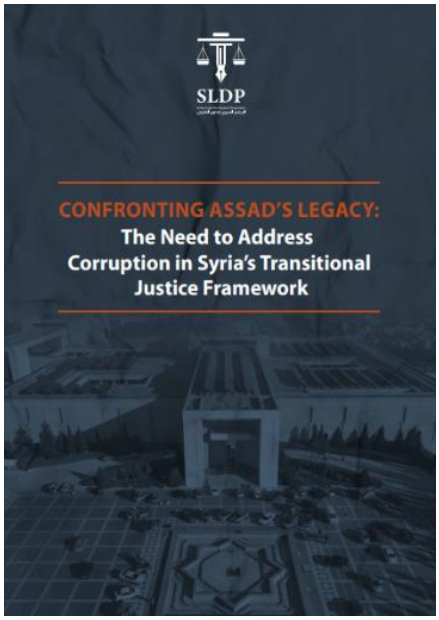
- У 57% APAC-юрисдикцій впровадження відкритого банкінгу здійснюється через ринкові механізми без обов'язкових законодавчих приписів, що вимагає посилення координації та єдиних стандартів для забезпечення цілісності системи.
- Основним політичним орієнтиром, юрисдикцій в APAC, підходу, що базуються на регулюванні є фінансова інклюзія, на відміну від глобального тренду, де домінує конкуренція; це вимагає специфічного налаштування нормативних актів під соціальні виклики регіону.
- Відкрите фінансування впроваджується набагато повільніше за відкритий банкінг, із серйозними бар'єрами у розширенні до секторів страхування та інвестицій, що вказує на необхідність подальших досліджень та пілотних проєктів.
- Юрисдикції APAC демонструють вищий за глобальний середній показник активного обміну фінансовими даними (4 бали серед підходу, що базуються на регулюванні країн проти глобальних 2,9), що підтверджує високий ступінь цифрової готовності регіону до розширення відкритого фінансування.

Завершується звіт закликом до спільної роботи урядів, регуляторів, банків, фінтех-компаній та міжнародних організацій задля створення більш відкритої, інноваційної та інклюзивної фінансової екосистеми в Азійсько-Тихоокеанському регіоні, яка може стати зразком для інших частин світу.

Спадщина Асада: Чому боротьба з корупцією є ключовою для перехідних процесів в Сирії [10]

Документ є глибоким аналізом системної корупції, яка стала невід'ємною частиною режиму Асада в Сирії, її впливу на порушення прав людини та необхідності включення боротьби з

[10] https://sldp.ngo/wp-content/uploads/2025/06/Confronting-Assads-Legacy.pdf



корупцією до рамок перехідного правосуддя. Корупція в Сирії за правління Башара Асада не лише забезпечувала економічне збагачення режиму та його наближених, але й слугувала ключовим інструментом політичного контролю, що зміцнював владу через патронажні мережі, сприяв нерівності, дискримінації та тривалому конфлікту. Документ підкреслює, що без вирішення проблеми корупції перехідне правосуддя в Сирії залишиться неповним, що може призвести до збереження безкарності, відтворення корупційних схем і підриву довіри до нових державних інститутів.

Корупція в Сирії була системною і глибоко вкоріненою, що відображається в низьких позиціях країни в міжнародних рейтингах, таких як Індекс сприйняття корупції Transparency International. У 2024 році Башар Асад отримав сумнозвісне визнання "Людиною року" від Центру дослідження корупції та організованої злочинності (OCCRP) через його роль у створенні корупційної системи, що порівнюється з діяльністю інших авторитарних лідерів, таких як Володимир Путін чи Олександр Лукашенко. Ця система дозволяла режиму не лише накопичувати величезні статки, але й використовувати економічні ресурси для підтримки політичної лояльності. Корупція стала основою економіки війни, де лояльні режиму особи отримували доступ до монополій, контрактів і ресурсів, що сприяло появі так званої "еліти конфлікту" — групи осіб, які збагачувалися на тлі війни через контрабанду, пограбування та контроль над ключовими секторами економіки, такими як паливо, продовольство та реконструкційні проєкти.

Одним із найяскравіших прикладів корупційних практик режиму була торгівля наркотиком каптагон, що перетворила Сирію на "наркодержаву". Виробництво та експорт каптагону контролювалися наближеними до режиму особами, зокрема братом Асада, Махером, та Четвертою дивізією армії. Ця торгівля приносила мільярди доларів щорічно, дозволяючи режиму обходити міжнародні санкції та фінансувати свої операції. Крім того, режим систематично вимагав викупи від сімей затриманих за інформацію чи обіцянки звільнення, що стало відомим як "індустрія зникнень". Ця практика не лише завдавала психологічних і фінансових страждань родинам, але й була значним джерелом доходу для режиму. Іншим проявом корупції було маніпулювання гуманітарною допомогою, коли ресурси спрямовувалися до лояльних регіонів, а опозиційні території залишалися без підтримки, що посилювало страждання населення під час економічної кризи 2011 року та пандемії COVID-19. Так званий "податок на реконструкцію" також використовувався для збагачення режиму, дозволяючи лояльним бізнесменам отримувати вигоду від відновлення зруйнованої інфраструктури.

Корупція в Сирії мала прямий вплив на порушення прав людини, оскільки вона відволікала державні ресурси від базових соціальних послуг, таких як охорона здоров’я, освіта та соціальний захист, що призводило до погіршення умов життя населення. Вона підривала верховенство права, послаблювала державні інститути та сприяла нерівності, зокрема гендерній дискримінації. Жінки в умовах конфлікту ставали особливо вразливими, оскільки часто стикалися з експлуатацією, включно з проституцією, в обмін на доступ до гуманітарної допомоги чи базових ресурсів. Корупція також порушувала принципи недискримінації, визначені Комітетом з прав людини ООН, обмежуючи рівний доступ до прав залежно від політичної лояльності чи соціального статусу.

Документ наголошує, що ігнорування корупції в рамках перехідного правосуддя може мати катастрофічні наслідки для відновлення справедливості та довіри до держави. Якщо економічні злочини, такі як пограбування чи маніпуляція гуманітарною допомогою, не будуть розслідувані,

винуватці порушень прав людини зможуть зберегти свої незаконно отримані статки, що дозволить їм уникати відповідальності. Деякі форми корупції, такі як пограбування чи використання голоду як зброї, класифікуються як міжнародні злочини, що робить їх частиною ширшої системи порушень, які необхідно розглядати в рамках перехідного правосуддя. Крім того, боротьба з корупцією є ключовою для забезпечення справедливого розподілу ресурсів у постконфліктній Сирії, що необхідно для запобігання відтворенню корупційних практик у нових державних структурах.

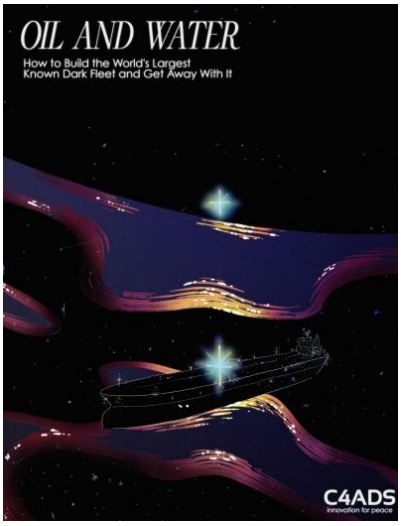
Для ефективного вирішення проблеми корупції документ пропонує інтегрувати її розгляд у перехідне правосуддя через створення спеціалізованих комісій із розслідування економічних злочинів, повернення незаконно отриманих активів і забезпечення прозорості в розподілі гуманітарної допомоги. Підхід, заснований на правах людини, передбачає не лише покарання винних, але й реституцію для жертв, їхню реабілітацію та гарантії неповторення подібних порушень. Жертви корупції, зокрема маргіналізовані групи, повинні мати активну роль у цих процесах, щоб забезпечити справедливість і відновити суспільну довіру до державних інститутів. Документ також підкреслює важливість залучення бізнесів, які отримували вигоду від конфлікту, до процесів встановлення правди в рамках перехідного правосуддя, як це рекомендує Робоча група ООН з питань бізнесу та прав людини.

Висновки:

- **Системна корупція як інструмент режиму:** Корупція в Сирії за режиму Асада була не просто побічним явищем, а ключовим механізмом політичного та економічного контролю, що зміцнював владу через патронажні мережі, економіку війни та наркоторгівлю, зокрема каптагоном, що генерувала мільярди доларів для обходу санкцій.
- **Зв’язок корупції з порушеннями прав людини:** Корупція прямо сприяла порушенням прав людини, відволікаючи ресурси від соціальних послуг, таких як охорона здоров’я та освіта, посилюючи нерівність і дискримінацію, зокрема щодо жінок, які стикалися з експлуатацією в умовах конфлікту.
- **Необхідність інтеграції в перехідне правосуддя:** Без розслідування економічних злочинів, таких як пограбування чи маніпуляція гуманітарною допомогою, та повернення незаконно отриманих активів перехідне правосуддя буде неповним, що дозволить винуватцям уникнути відповідальності та зберегти свої статки.
- **Роль громадянського суспільства та міжнародної спільноти:** Громадянське суспільство має активно просувати зв’язок корупції з репресіями через інформаційні кампанії, а новий уряд і міжнародні партнери повинні розробити прозорі механізми повернення активів і моніторингу гуманітарної допомоги, щоб запобігти відтворенню корупційних мереж у пост-конфліктній Сирії.

Серед рекомендацій документ закликає сирійське громадянське суспільство активно виступати за включення боротьби з корупцією до перехідного правосуддя, проводити інформаційні кампанії для підвищення обізнаності про зв’язок корупції з порушеннями прав людини та вимагати системних реформ через публічну участь і процеси встановлення правди. Новий уряд Сирії має визнати корупцію ключовим елементом перехідного правосуддя, розробити прозорі правові механізми для повернення активів через міжнародну співпрацю та забезпечити справедливий розподіл ресурсів для відновлення довіри до державних інститутів. Міжнародні донори та треті країни повинні посилити моніторинг розподілу гуманітарної допомоги, щоб запобігти її зловживанню, а також надавати технічну підтримку для відстеження та повернення вкрадених активів, що допоможе уникнути відтворення корупційних мереж у постконфліктній Сирії.

Темна флотилія: Як кораблі обходять санкції на торгівлю нафтою [11]



Документ, підготовлений аналітичним центром C4ADS, є глибоким і багатогранним дослідженням діяльності так званої "Темної флотилії" (Dark Fleet), з особливим акцентом на суб-флотилію, яку автори називають "Багатолиций флот" (Protean Fleet). Цей флот, що налічує понад 50 супертанкерів, відіграє ключову роль у транспортуванні нафти з країн, які перебувають під санкціями Заходу, зокрема Росії, Ірану та Венесуели, до країн-покупців, переважно Китаю та Індії. Дослідження розкриває складні механізми обходу санкцій, включаючи використання підставних компаній, маніпуляції з автоматичною ідентифікаційною системою (AIS), фінансові схеми та прогалини в міжнародних морських і фінансових системах. Документ також пропонує практичні рекомендації для підвищення ефективності санкційних режимів і боротьби з незаконною торгівлею нафтою.

Дослідження розпочинається з опису економічної залежності країн під санкціями від доходів від нафти. Наприклад, у 2024 році нафта та газ становили 30% державного бюджету росії (10,5 мільярда доларів США), а в Ірані на 2025 рік прогнозується, що нафта забезпечить 50% бюджету (50 мільярдів доларів). Ця залежність робить нафтові санкції ключовим інструментом тиску Заходу, але, як зазначається, чинні санкційні режими, включаючи цінові обмеження на російську нафту (60 доларів за барель, запроваджені G7 та ЄС у грудні 2022 року), виявилися недостатньо ефективними. Незважаючи на санкції, росія, Іран та Венесуела продовжують експортувати нафту, зокрема до Китаю, який у 2023 році закупив 45% російської, 90% іранської та 68% венесуельської нафти, а також до Індії, яка за період з грудня 2022 року по січень 2024 року імпортувала 37% російської нафти.

Центральним об’єктом дослідження є "Багатолиций флот " — мережа з 56 танкерів, яка, за оцінками C4ADS, транспортувала щонайменше 343,279,857 барелів нафти з країн під санкціями до Китаю з липня 2019 року. З них 45,3% походять з Росії, 45,2% з Ірану та 14,2% з Венесуели. Значна частина флоту (29 суден) належить до класу VLCC (Very Large Crude Carriers), здатних перевозити понад 2 мільйони барелів нафти за рейс. Флот використовує складні методи приховування своєї діяльності, зокрема техніку "AIS handshake", коли одне судно вимикає свій AIS-передавач, а інше тимчасово передає його ідентичність, створюючи ілюзію безперервного сигналу. Наприклад, у грудні 2022 року судно MONOCEROS координувало передачу іранської нафти через серію STS-передач (ship-to-ship transfers) у протоці Малакка, використовуючи судна SCORPIUS і FIONA II для імітації його AIS-сигналу. Іншим методом є AIS-спуфінг, коли судна передають фальшиві дані про своє місцезнаходження, створюючи "неприродні" траєкторії руху, які ускладнюють відстеження. Такі тактики дозволяють приховувати походження нафти та уникати виявлення.

Організаційно флот контролюється єдиною мережею, базованою в Китаї, яка включає 117 підставних компаній і 74 фізичних осіб. Ці компанії зареєстровані в юрисдикціях із низькою прозорістю, таких як Гонконг, Маршаллові Острови та Кайманові Острови, і часто використовують однакові контактні дані, включаючи три електронні адреси та три телефонні номери, один з яких пов’язаний із підсанкційною особою Лі Ї (Li Yi), на яку OFAC накладено санкції у 2019 році за контрабанду іранської нафти. Мережа має зв’язки з раніше підсанкційною "Куньлунською мережею" (Kunlun Network), деякі судна якої були передані флоту після санкцій 2019 року. Фінансування флоту здійснюється через іпотеки на суму понад 750 мільйонів доларів, видані трьома компаніями, зареєстрованими на Британських Віргінських Островах, під

[11] https://c4ads.org/wp-content/uploads/2025/06/OilWater-C4ADS.pdf

керівництвом трьох швейцарських директорів. Ці іпотеки, які часто на 34,8% перевищують ринкову вартість суден, ймовірно, пов'язані з вартістю нафтових угод, а не самих суден. Транзакції в доларах США проходять через американські банки-посередники, що дає США юрисдикцію над цими операціями, але ця можливість не завжди використовується ефективно.

Дослідження підкреслює вразливості західних морських і фінансових систем, які використовує мережа. Панамський морський реєстр, найбільший у світі за кількістю суден, має хороші протоколи перевірки, але складні методи маскування, такі як AIS-маніпуляції та STS-передачі, дозволяють суднам уникати ретельної перевірки. Використання юрисдикцій секретності ускладнює виявлення справжніх власників, а підставні компанії та директори, які часто не мають значної онлайн-присутності, створюють видимість легітимності. Наприклад, адреси директорів мережі розкидані по 10 провінціях Китаю, але значна їх частка вказує Шанхай як місце реєстрації. Мережа також використовує однакових нотаріусів і юристів у Цузі, Гонконзі, Бангкоку та Панамі для оформлення іпотек і суднових документів.

Незважаючи на те, що 43 із 56 суден "Багатолицого флоту" вже перебувають під санкціями OFAC, мережа продовжує діяти, що свідчить про неефективність санкцій, орієнтованих на окремі судна. Документ наголошує, що для ефективної боротьби з незаконною торгівлею нафтою необхідно перейти до системного підходу, спрямованого на кінцевих бенефіціарів і фінансові потоки. C4ADS пропонує низку рекомендацій, включаючи посилення міжурядової координації через обмін інформацією в реальному часі між морськими реєстрами, страховими компаніями, портовими органами та фінансовими розвідками.

Пропонується скасування реєстрації, відмова у доступі до портів і анулювання страховки для суден флоту, а також розслідування фінансових транзакцій у доларах США. Для заохочення портів до співпраці пропонується ділити доходи від аукціонів конфіскованих суден і вантажів. Окремо наголошується на необхідності вдосконалення аналізу маршрутів суден за допомогою супутникових зображень і платформ, таких як Windward Predictive Intelligence, для виявлення підозрілої активності.

Висновки:

- **Санкції, орієнтовані на окремі судна, є недостатньо ефективними,** оскільки 43 із 56 суден флоту вже під санкціями, але мережа продовжує функціонувати. Необхідно зосередитися на виявленні та санкціонуванні кінцевих бенефіціарів і фінансових посередників, включаючи підставні компанії та їхніх директорів, для руйнування мережі.
- **Використання передових технологій, таких як супутникові зображення** та платформи на кшталт Windward Predictive Intelligence, дозволяє виявляти маніпуляції з AIS і STS-передачами, що є критично важливим для відстеження незаконної діяльності "Темної флотилії".
- **Вразливості морських і фінансових систем,** зокрема Панамського реєстру та транзакцій у доларах США, потребують реформування. Посилення процедур перевірки в реєстрах і контроль за фінансовими потоками через американські банки можуть ускладнити обхід санкцій.
- **Міжнародна співпраця** між морськими, фінансовими та правоохоронними органами є ключовою. Обмін інформацією в реальному часі, інспекції суден, конфіскація вантажів і розподіл доходів від аукціонів можуть стимулювати ефективні дії проти мережі.

Інші новини

AMLA очікує високих стандартів боротьби з фінансовими злочинами в криптосекторі [12]

Пресреліз AMLA присвячено офіційному старту повноважень Європейського органу з питань протидії відмиванню коштів та фінансуванню тероризму та визначенню його стратегічних очікувань щодо криптовалютного сектору в умовах нового регуляторного ландшафту ЄС. Основний фокус документа зосереджено на забезпеченні високих стандартів протидії фінансовим злочинам у сфері обігу криптовалют, що розглядається AMLA як пріоритетний напрямок роботи вже з першого року діяльності.

На тлі запуску нової нормативної бази — зокрема Регламенту про ринки криптоактивів (MiCA) — AMLA закликає постачальників послуг, пов'язаних із криптоактивами (CASP), запровадити надійні системи ПВК/ФТ від моменту отримання ліцензії. Підкреслюється, що криптовалютний сектор має високу вразливість до ризиків відмивання коштів та фінансування тероризму, що зумовлено технологічними особливостями, можливостями анонімізації, а також транскордонною природою бізнес-моделей CASP.

AMLA підтверджує, що хоча перший рівень ліцензування та нагляд за криптокомпаніями залишається за національними компетентними органами (NCAs), існує ризик фрагментації підходів до застосування вимог AML/CFT у різних країнах-членах. У зв'язку з цим Орган закликає національні органи нагляду забезпечити наявність ефективних систем внутрішнього контролю у всіх CASPs вже з моменту їх авторизації, щоб мінімізувати регуляторний арбітраж і запобігти нерівним умовам для учасників ринку.

Окремо зазначено, що у щойно оприлюдненій Робочій програмі AMLA на 2025 рік криптовалютний напрям включено до стратегічних цілей як у контексті регуляторного нагляду, так і в межах розбудови розвідувального аналітичного блоку AMLA. Зокрема, планується ініціювання спільного аналізу фінансової розвідки, пов'язаної з криптоактивами, із фокусом на транскордонні типології, нові загрози та вразливості, які виникають у стрімко мінливому цифровому середовищі.

Таким чином, AMLA позиціонує себе як ключовий координатор зусиль на рівні ЄС, що прагне уніфікувати стандарти та забезпечити однакову ефективність ПВК/ФТ-контролю в криптосекторі. Орган демонструє намір тісно співпрацювати з національними та європейськими регуляторами для просування спільних підходів, підвищення прозорості й оперативного реагування на зловживання у сфері цифрових фінансів.

Цей документ є важливим сигналом для ринку, що адаптація до нових вимог AML/CFT для CASP не є майбутнім викликом, а вже теперішнім стандартом.

[12] https://www.amla.europa.eu/document/download/b7546c52-f640-40f0-bebe-322c56399450_en?filename=Press%20release_AMLA_Crypto_15.07.2025.pdf

FCA оштрафувала Barclays на 42 мільйони фунтів стерлінгів [13]

Наглядовий орган Великої британії Financial Conduct Authority (FCA) оштрафував Barclays Bank UK PLC та Barclays Bank PLC на загальну суму 42 мільйони фунтів стерлінгів за окремі випадки порушень у сфері управління ризиками фінансових злочинів. Штраф стосується провалів у протидії фінансовій злочинності між 2015 і 2023 роками, пов'язаних з обслуговуванням двох колишніх клієнтів: фірми з управління капіталом WealthTek та компанії, що займається золотими злитками, Stunt & Co.

У першому випадку, що стосується WealthTek, Barclays Bank UK PLC не зміг перевірити, чи зібрав віе достатньо інформації для розуміння ризику відмивання коштів, перш ніж відкрити кастодіальний рахунок для WealthTek. FCA зазначила, що достатньо було б здійснити "одну просту перевірку" у Реєстрі фінансових послуг, щоб побачити, що WealthTek не мала дозволу FCA на зберігання клієнтських коштів. Незважаючи на це, клієнти внесли 34 мільйони фунтів стерлінгів на рахунок WealthTek у Barclays. Внаслідок цих недоліків, Barclays Bank UK PLC добровільно виплатить 6,3 мільйона фунтів стерлінгів клієнтам WealthTek, які зазнали збитків.

Другий і значно більший штраф у розмірі 39,3 мільйона фунтів стерлінгів стосується Barclays Bank PLC за нездатність належним чином керувати ризиками відмивання коштів, пов'язаними з наданням банківських послуг Stunt & Co. Barclays не зібрала достатньо інформації на початку відносин і не здійснювала належного постійного моніторингу. За трохи більше ніж рік Stunt & Co отримала 46,8 мільйона фунтів стерлінгів від Fowler Oldfield, компанії, яка була в центрі багатомільйонної операції з відмивання коштів. Barclays не вдалося належним чином врахувати ризики відмивання коштів, пов'язані з Stunt & Co, навіть після отримання інформації від правоохоронних органів про підозри у відмиванні коштів через Fowler Oldfield та після того, як дізналася про рейди поліції в обох фірмах. Штраф у розмірі 39,3 мільйона фунтів стерлінгів був зменшений з початкових 56,1 мільйона фунтів стерлінгів завдяки ранньому врегулюванню та повній співпраці Barclays з обома розслідуваннями.

Тереза Чемберс, спільний виконавчий директор FCA з питань правозастосування та нагляду за ринком, підкреслила, що "наслідки поганого контролю над фінансовими злочинами є дуже реальними – вони дозволяють злочинцям відмивати доходи від своїх злочинів, а шахраям – обманювати споживачів". Вона також зазначила, що банки повинні брати на себе відповідальність та діяти оперативно, особливо коли їм стають відомі очевидні ризики. Цей штраф є одинадцятим, який FCA наклала на банк за останні чотири роки за порушення контролю над фінансовими злочинами, і регулятор продовжує наглядати за фірмами, щоб переконатися у дотриманні ними всіх вимог. Barclays заявила, що повністю співпрацювала з обома розслідуваннями та додатково посилила свої можливості у сфері боротьби з фінансовими злочинами та іншого контролю.

[13] https://www.fca.org.uk/news/press-releases/fca-fines-barclays-42-million-poor-handling-financial-crime-risks

"Cocaine Air": Розкриваючи кокаїнові маршрути до Європи [14]

Стаття, підготовлена InSight Crime, аналізує наркотрафік кокаїну з Латинської Америки до Європи, спираючись на справу, висвітлену в документальному серіалі Netflix «Cocaine Air: Smugglers at 30,000 Ft.», який вийшов 11 червня 2025 року.

Серіал розповідає про інцидент 2013 року, коли двох пілотів, Бруно Одоса та Паскуаля Форе, разом із пасажиром Ніколасом Пісапією, заарештували в Домініканській Республіці за спробу перевезення 700 кілограмів кокаїну до Франції на приватному літаку. Цей випадок є відправною точкою для аналізу кокаїнового маршруту до Європи, ролі ключових гравців і еволюції методів транспортування.

Пілоти, які раніше працювали у французьких ВПС, а згодом перейшли до приватного сектору, заперечували свою обізнаність щодо вмісту багажу, стверджуючи, що перевірка вантажу не входила до їхніх обов'язків, але французька влада надала докази їхньої можливої причетності до кількох подібних рейсів із Домініканської Республіки до транзитних пунктів, таких як Еквадор.

Серіал висвітлює судовий процес і людський вимір історії, показуючи точки зору обвинувачених і слідчих. Стаття підкреслює зростання торгівлі кокаїном до Європи, яка, за звітом Державного департаменту США (INCSR), перевищила ринок США. Основними країнами-виробниками є Колумбія, Перу та Болівія, причому Колумбія у 2023 році досягла рекордного виробництва — 2664 метричні тонни кокаїну. Домініканська Республіка слугує ключовим транзитним пунктом, куди наркотики доставляються з Колумбії та Венесуели швидкісними катерами чи рибальськими човнами, а звідти відправляються до Європи через контейнери, нарко-субмарини або приватні авіарейси, які викликають менше підозр.

Ключову роль у ланцюжку відіграють брокери, такі як Франк Колін, який організував рейс, співпрацюючи з Пісапією та наркоторговцем Алі Бушаребом, заарештованим у Іспанії. Брокери координують транспортування наркотиків із країн-виробників до транзитних пунктів і далі до Європи, ймовірно, через зв'язки з великими європейськими кримінальними мережами. Стаття зазначає зростання ролі брокерів, які раніше працювали на одну групу, а тепер надають послуги різним глобальним мережам, що підвищує гнучкість і адаптивність кримінальних структур.

За словами Дугласа Фара, президента IBI Consultants, брокери бувають трьох типів: логістичні, посередники та приховані посередники, які забезпечують зв'язок між локальними і глобальними ринками. Сучасний наркотрафік характеризується диверсифікацією учасників і методів, що ускладнює боротьбу з ним.

Справу «Cocaine Air» представлено як приклад складної системи з трансконтинентальними зв'язками, яка включає використання сучасних технологій, таких як приватні літаки та субмарини, і демонструє, як наркоторговці адаптуються до змін у правоохоронній діяльності. Стаття підкреслює необхідність міжнародної співпраці, модернізації методів моніторингу транспорту та підвищення обізнаності про нові схеми наркотрафіку для ефективної протидії.

[14] https://insightcrime.org/news/cocaine-air-explained-trafficking-europe/

Ваша думка важлива!

1. Які механізми імплементації нового європейського законодавства (AMLR/AMLD6/AMLAR) доцільно застосувати в Україні вже на етапі його підготовки до набрання чинності у 2027 році? Як регулятори та СПФМ можуть синхронізувати свої підходи для забезпечення попередньої адаптації до нових вимог?
2. Як забезпечити ефективне функціонування ризикоорієнтованого підходу до нагляду за постачальниками послуг у сфері віртуальних активів (CASP) в умовах наближення до європейської нормативної бази? Які елементи контролю потребують першочергового посилення на національному рівні?
3. Які цифрові рішення (аналогічні до SARs Digital Service у Великій Британії) доцільно розглядати для автоматизації обробки повідомлень СПФМ в Україні? Які функціональні характеристики таких систем є критичними з погляду ефективності аналізу та зворотного зв'язку?
4. Які типи СПФМ в Україні першочергово потребують оновлення внутрішніх політик для реагування на кіберзагрози, зокрема фішинг, BEC-шахрайство, цифровий шантаж? Як держава може стимулювати їхню проактивну участь у побудові кіберстійкості?
5. Як Україна може адаптувати досвід міжнародного публічно-приватного партнерства (PPP) для створення ефективної моделі співпраці між фінансовими установами, правоохоронними органами та регуляторами для боротьби з відмиванням грошей і економічними злочинами?
6. Як забезпечити баланс між інноваціями фінтех-компаній та захистом персональних даних споживачів в умовах відкритого банкінгу в Україні, враховуючи нові вимоги ЄС, FATF та міжнародний досвід країн APAC?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-29

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

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