Методологічний бюлетень

Серійний номер: МінФін-AML-2025-28

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

Глобальні ризики фінансування тероризму: всебічний огляд та рекомендації FATF 2025 [1]

Документ, підготовлений FATF, є ґрунтовним звітом, який аналізує сучасні ризики фінансування тероризму (TF) і пропонує стратегії їх протидії. Звіт, який є оновленням попереднього видання 2015 року, базується на інформації від країн-членів FATF, міжнародних організацій, таких як ООН, Європол, та інших зацікавлених сторін, включаючи приватний сектор. Він охоплює широкий спектр методів, які терористичні організації, окремі терористи та їхні посередники використовують для збору, переміщення, зберігання та використання фінансових ресурсів, акцентуючи увагу на еволюції цих методів у контексті нових технологій, геополітичних змін і регіональних особливостей. Документ підкреслює глобальний характер загрози TF, наголошуючи на необхідності посилення міжнародної співпраці,

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf

вдосконалення національних регуляторних рамок і адаптації до нових викликів, таких як використання віртуальних активів і цифрових платформ.

Звіт розпочинається з аналізу факторів, що формують ризики фінансування тероризму. Ці фактори включають географічні, економічні та соціальні умови, які створюють сприятливе середовище для TF. Наприклад, регіони з нестабільною політичною ситуацією, слабкими інституціями, пористими кордонами або значною часткою тіньової економіки, такі як Сахель у Африці, є особливо вразливими. Терористичні групи, такі як ISIL, Al-Shabaab чи ADF, використовують контроль над територіями для отримання доходів через експлуатацію природних ресурсів, зокрема нафти, газу, золота, деревини, а також через примусове оподаткування, викрадення з метою викупу (KFR), торгівлю людьми та контрабанду. У документі також згадується державне спонсорство тероризму як рідкісний, але значний ризик, що посилює фінансові потоки для терористичних організацій. Звіт зазначає, що терористичні структури демонструють високу адаптивність, використовуючи як централізовані моделі управління фінансами, так і децентралізовані мережі, що ускладнює їх відстеження.

Далі документ детально описує методи, які терористичні організації застосовують для фінансування своєї діяльності. Традиційні способи включають фізичне переміщення готівки через кордони, використання неформальних систем переказу грошей, таких як хавала, та зловживання традиційними фінансовими інструментами, зокрема банківськими рахунками, кредитними та дебетовими картками. Наприклад, звіт наводить випадки, коли невеликі терористичні осередки використовували кредитні картки для придбання віртуальних активів або здійснення транзакцій за межами юрисдикцій з високим рівнем регулювання. Водночас сучасні технології відкривають нові можливості для TF. Терористичні групи активно використовують віртуальні активи (VAs) і постачальників послуг віртуальних активів (VASPs), соціальні медіа, краудфандингові платформи, електронну комерцію та онлайн-ігрові платформи. Зокрема, ISIL та Al-Shabaab застосовували обмін ігрових балів на реальні гроші, а також продаж мерчендайзу, такого як футболки з символікою організацій, через онлайн-ринки. Зловживання некомерційними організаціями (NPOs) залишається серйозною проблемою: фіктивні благодійні організації створюються для маскування збору коштів на терористичні цілі, як це було в Німеччині з організацією Ansar International e.V., яка фінансувала терористичні групи в Сирії.

Звіт також аналізує еволюцію ризиків TF і прогнозує майбутні тенденції. Однією з ключових тенденцій є децентралізація фінансових операцій терористичних груп, що ускладнює їх виявлення та блокування. Використання нових фінансових інструментів, таких як віртуальні IBAN, та штучного інтелекту (AI) для обходу процедур належної перевірки клієнтів (KYC) створює нові виклики для правоохоронних органів. Наприклад, ISIL-Khorasan активно використовує онлайн-пропаганду та краудфандинг для збору коштів у Європі та Центральній Азії, що свідчить про регіоналізацію та інтернаціоналізацію їхньої діяльності. Африка, зокрема Сахель, визнається глобальним епіцентром тероризму, де місцеві філії ISIL, Al-Qaida та інших груп комбінують традиційні методи (експлуатація природних ресурсів, KFR) з цифровими (віртуальні активи, соціальні медіа). Звіт також звертає увагу на зростаючу роль жінок у фінансових операціях терористичних груп, які використовуються для маскування транзакцій, оскільки вони викликають менше підозр.

Рекомендації, викладені у звіті, зосереджені на посиленні протидії TF через транскордонну співпрацю, вдосконалення оцінок ризиків і адаптацію регуляторних рамок до нових технологій. FATF закликає країни регулярно оновлювати національні оцінки ризиків, враховуючи нові методи, такі як використання VAs, VASPs і краудфандингових платформ.

Особлива увага приділяється державно-приватному партнерству, яке передбачає підвищення обізнаності фінансових установ і технологічних компаній щодо індикаторів TF. Наприклад, звіт

наводить випадок у Таїланді, де аналіз соціальних медіа допоміг виявити краудфандингову кампанію на підтримку терористичної організації. Для захисту легітимної діяльності NPOs пропонується ризик-орієнтований підхід, який дозволяє відрізняти законні гуманітарні ініціативи від фіктивних. Звіт також наголошує на важливості цільових фінансових санкцій і вдосконалення процедур обміну розвідданими між країнами для боротьби з транскордонними фінансовими потоками.

Додаток А містить перелік індикаторів ризиків TF, які включають поведінкові ознаки (наприклад, часте відвідування високоризикових юрисдикцій), економічні (невідповідність транзакцій економічному профілю клієнта), географічні (транзакції з регіонами, близькими до зон конфлікту) та технологічні (використання анонімних віртуальних активів або множинних передплачених карток). Ці індикатори призначені для використання фінансовими установами та правоохоронними органами для раннього виявлення підозрілих операцій.

Звіт завершується закликом до постійного моніторингу нових схем TF і вдосконалення глобальних і національних стратегій протидії. Він підкреслює, що швидкий розвиток технологій і геополітичні зміни вимагають гнучкості та інноваційних підходів, таких як використання аналітики блокчейну для відстеження транзакцій із віртуальними активами. Документ встановлює основу для подальших ініціатив FATF, спрямованих на посилення глобальних зусиль у боротьбі з фінансуванням тероризму, з особливим акцентом на захист вразливих регіонів і секторів.

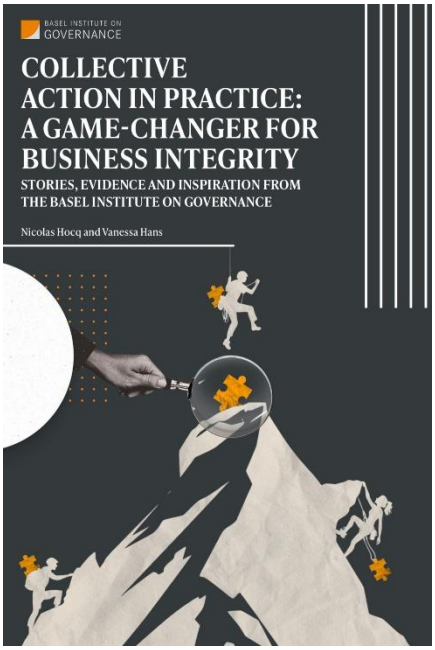
Таким чином, FATF підкреслює необхідність посилення міжнародної співпраці для протидії фінансуванню тероризму, зокрема через обмін розвідданими та гармонізацію санкційних режимів, особливо в регіонах із високим ризиком, таких як Сахель, де терористичні групи активно використовують природні ресурси та неформальні фінансові системи. Для ефективного виявлення підозрілих транзакцій країни повинні впроваджувати ризик-орієнтований підхід до регулювання віртуальних активів і постачальників їхніх послуг, застосовуючи передові технології, такі як аналітика блокчейну, та вдосконалюючи процедури KYC. Держави мають регулярно оновлювати оцінки ризиків TF, зосереджуючись на нових технологіях, таких як штучний інтелект і краудфандингові платформи, та проводити навчання для приватного сектору, щоб підвищити його здатність ідентифікувати підозрілі операції. Для захисту легітимної діяльності некомерційних організацій необхідно розробити чіткі механізми, які дозволяють відрізняти законні гуманітарні ініціативи від фіктивних,

Висновки:

- **Посилення міжнародної співпраці:** Необхідно активізувати обмін розвідданими та гармонізувати санкційні режими між країнами для ефективного блокування транскордонних фінансових потоків терористичних організацій, особливо в регіонах із високим ризиком, таких як Сахель.
- **Регулювання віртуальних активів:** Впровадження ризик-орієнтованого підходу до регулювання віртуальних активів (VAs) і постачальників їхніх послуг (VASPs) шляхом удосконалення процедур KYC та використання аналітики блокчейну для виявлення підозрілих транзакцій.
- **Оновлення оцінок ризиків:** Країни повинні регулярно оновлювати національні оцінки ризиків TF, враховуючи нові методи, такі як використання штучного інтелекту та краудфандингових платформ, і проводити навчання для приватного сектору.
- **Захист NPOs:** Розробити чіткі механізми для захисту легітимних некомерційних організацій від використання в TF, застосовуючи пропорційні регуляторні заходи, щоб уникнути обмеження гуманітарної діяльності.

застосовуючи пропорційні регуляторні заходи, щоб уникнути ненавмисного обмеження гуманітарної діяльності.

Глобальна боротьба з корупцією: роль колективних дій у формуванні чесного бізнес-середовища [2]



Книга, опублікована Базельським інститутом управління у 2025 році, є систематизованим дослідженням феномену колективних дій у сфері протидії корупції та формування доброчесності бізнесу, що базується на емпіричних даних, аналітичних моделях, практичних кейсах і нормативно-правових розробках. Видання має на меті не лише описати історію розвитку цього підходу, а й показати його сучасний стан як глобально визнаної практики, інтегрованої у політики урядів, міжнародних організацій, приватного сектору й громадянського суспільства.

Основний зміст книги побудований навколо трьох стратегічних тем: розвиток знань про колективні дії, його інституціоналізація як глобальної норми та практична підтримка тих, хто впроваджує цей підхід на місцях. У першій частині видання детально представлено еволюцію бази знань через призму B20 Collective Action Hub — найбільшого у світі інтерактивного ресурсу, що об'єднує понад 340 ініціатив колективних дій, понад 270 тематичних публікацій, інструментів, аналітичних оглядів і навчальних матеріалів. Окрему увагу приділено впровадженню нової типології колективних дій, яка розділяє всі ініціативи на ті, що спрямовані на створення діалогу, довіри, обміну знаннями, орієнтовані на спільну розробку галузевих чи національних стандартів доброчесності та такі, що пов'язані з перевіркою виконання стандартів, сертифікацією, аудитом. Ця типологія відображає еволюцію практик колективних дій і пропонує новий аналітичний підхід до класифікації таких ініціатив.

У межах першої частини також розкрито взаємозв'язок між антикорупційною діяльністю, правами людини та цілями сталого розвитку (SDGs). У книзі наводяться результати унікальних консультацій і круглих столів із представниками понад 50 глобальних компаній, що виявили такі системні виклики, як брак координації між функціями комплаєнсу та сталого розвитку у великих компаніях, складність у побудові єдиної системи оцінки ризиків корупції та порушень прав людини, відсутність належного корпоративного розкриття інформації щодо антикорупційних ініціатив та політик у сфері прав людини. Окремо підкреслюється важливість корпоративної культури доброчесності як ключового елементу ефективних програм комплаєнсу, де індикаторами виступає не лише формальна наявність політик, а й активна участь компаній у колективних діях як формі зовнішньої демонстрації зобов'язань.

Друга частина книги присвячена процесу визнання колективних дій як глобального стандарту у сфері протидії корупції та бізнес-доброчесності. У ній детально аналізуються ключові міжнародні документи та політичні рішення, де підхід колективних дій набув офіційного статусу або прямого згадування: зокрема, Рекомендація OECD 2021 року щодо боротьби з підкупом іноземних публічних службовців, Резолюція 10/12 Конференції держав-учасниць Конвенції ООН проти корупції (UNCAC), Політична декларація UNGASS 2021 року, стандарти Світового банку та інших міжнародних фінансових організацій. В окремих розділах розкрито, як колективні дії

[2] https://baselgovernance.org/sites/default/files/2025-06/Collective%20Action%20in%20practice_PDF%20ebook.pdf

стали частиною антикорупційних стратегій G20, зокрема через B20 Integrity and Compliance Task Force. Особливий наголос зроблено на впровадженні вперше в історії Ключовий індикатор ефективності колективних дій (KPI) у межах B20 Brazil 2024, що дозволяє об'єктивно вимірювати рівень залучення урядів G20 до підтримки або участі в щонайменше одній ініціативі колективних дій, причому для аналізу використовуються дані з B20 Collective Action Hub. За даними 2024 року, тільки 45% з 96 країн, включаючи асоційованих членів G20, підтвердили таку участь, що одночасно свідчить як про досягнення, так і про потенціал для подальшого зростання.

Третя частина книги є найбільш практично орієнтованою і присвячена методам підтримки колективних дій на локальному рівні, зокрема для малих і середніх підприємств, організацій громадянського суспільства, державних органів, які шукають партнерські формати боротьби з корупцією. Тут докладно описано такі інструменти, як інтерактивний безкоштовний онлайн-курс «Колективні дії проти корупції», де слухачі проходять симуляцію в ролі підприємця в умовах корупційних ризиків; консультаційно-довідкову службу для оперативного консультування з питань побудови колективних дій; менторські програми для громадських організацій, які впроваджують колективні ініціативи. Наголошується, що саме такі практичні інструменти роблять підхід колективних дій не лише концептуально привабливим, а й реально застосовним для широкого кола учасників у різних країнах та регіонах.

Висновки:

- Колективні дії формалізовані у міжнародних антикорупційних стандартах (OECD 2021, UNGASS 2021, UNCAC CoSP Resolution 10/12) і мають бути інтегровані у національні політики антикорупції та бізнес-доброчесності як обов'язковий або рекомендований елемент.
- Впровадження Ключового індикатор ефективності колективних дій у рамках B20 2024 року створює механізм регулярного моніторингу участі урядів у колективних діях, що дозволяє вимірювати прогрес, ідентифікувати прогалини та формулювати конкретні рекомендації для держав-учасниць.
- Успішність ініціатив колективних дій значною мірою залежить від доступності практичних інструментів: навчальних програм, консультаційної підтримки, шаблонів політик і систем менторства для організацій без достатнього досвіду.
- Компаніям рекомендується системно інтегрувати колективні дії у свою ESG-стратегію, забезпечуючи взаємодію між підрозділами комплаєнсу та сталого розвитку, впроваджуючи індикатори ефективності щодо корпоративної культури доброчесності, зокрема через розкриття даних про участь у колективних діях.

Окремим важливим елементом книги є вшанування пам'яті Гретти Феннер, яка очолювала Базельський інститут управління протягом майже двох десятиліть і фактично була архітектором впровадження та популяризації концепції колективних дій на міжнародному рівні. Її стратегічне бачення полягало у тому, що боротьба з корупцією не може бути ізольованим зусиллям окремих компаній або урядів, а має ґрунтуватися на багаторівневій співпраці, довгостроковій довірі та гнучких механізмах спільного прийняття рішень.

За двадцять років розвитку підхід колективних дій став визнаною глобальною нормою у сфері антикорупційної діяльності, що закріплено в ключових міжнародних документах, таких як Рекомендація OECD 2021 року, Політична декларація UNGASS 2021 року та Резолюція 10/12 UNCAC. Його включення до міжнародних стандартів підтверджує системну роль колективних дій у забезпеченні доброчесності бізнесу на глобальному рівні.

Санкції

Вплив міжнародних санкцій на економічні ресурси росії: фінансовий тиск на воєнні зусилля (2022–2025) [3]

Документ, опублікований Міністерством закордонних справ, співдружності та розвитку (FCDO) Сполученого Королівства, присвячений аналізу впливу міжнародних санкцій на фінансові можливості росії підтримувати воєнні дії після повномасштабного вторгнення в Україну в лютому 2022 року. Охоплюючи період з лютого 2022 року до червня 2025 року, звіт оцінює економічні втрати російської держави, зосереджуючись на двох основних аспектах: втратах податкових надходжень від експорту нафти через розширення дисконту між цінами на російську нафту сорту Urals і глобальним еталоном Brent, а також на іммобілізації російських державних активів у країнах ЄС та G7. Документ детально описує методологію оцінок, ключові терміни, обмеження аналізу та аспекти, які складно кількісно оцінити, підкреслюючи консервативний характер наданих даних.

За оцінкою FCDO, станом на лютий 2025 року глобальні санкції позбавили росію щонайменше 450 мільярдів доларів США. Ця сума складається з 154 мільярдів доларів втрачених податкових надходжень від нафтового експорту, спричинених ширшим дисконтом між ціною на нафту Urals і Brent, та 285 мільярдів доларів іммобілізованих державних активів, що зберігаються в установах ЄС та інших країн G7. Втрати податкових надходжень зумовлені санкціями, які ускладнили росії продаж нафти на міжнародних ринках за вигідними цінами, що призвело до зниження ціни Urals порівняно з Brent. Цей дисконт вплинув на доходи від податку на видобуток корисних копалин (МЕТ) та експортних мит, які росія застосовувала до іноземних продажів нафти, природного газу та нафтопродуктів до їх скасування для нафти та нафтопродуктів у січні 2024 року. За період з лютого 2022 року до червня 2025 року росія отримала 335 мільярдів доларів податкових надходжень від нафтового сектору, але втратила 154 мільярди через ширший дисконт. Ця динаміка ілюструється графіком у документі, який показує втрати в 4-місячних інтервалах, причому частка втрачених доходів відносно загальних надходжень зменшується з часом, що може вказувати на адаптацію росії до санкцій або зміни в структурі експорту.

Щодо іммобілізованих активів, країни ЄС та G7 заморозили російські державні активи на суму приблизно 285 мільярдів доларів, з яких 183 мільярди зберігаються у вигляді депозитів. Ці активи були переведені в долари США за середнім обмінним курсом EUR/USD у березні 2022 року, коли їх було заморожено. Ця сума є значною часткою фінансових ресурсів, які росія могла б використати для підтримки воєнних зусиль. Документ пояснює ключові терміни: Urals crude oil є основним еталоном для оподаткування російського нафтового експорту, Brent crude oil слугує глобальним еталоном цін на нафту, а дисконт між цими цінами відображає вплив санкцій на здатність Росії продавати нафту. Податок на видобуток корисних копалин (МЕТ) є основним джерелом прямих доходів держави від нафтового сектору, тоді як експортні мита, скасовані в січні 2024 року, раніше також наповнювали бюджет. Поточний рахунок охоплює баланс торгівлі товарами, послугами, доходами та трансфертами, а контр-фактичний сценарій описує гіпотетичну ситуацію без санкцій.

Графік у документі показує, що втрати податкових надходжень склали 154 мільярди доларів, тоді як загальні надходження від нафтового сектору досягли 335 мільярдів доларів. Інший графік

[3] https://www.gov.uk/government/publications/estimating-the-impact-of-sanctions-on-russias-war-efforts/estimating-the-impact-of-sanctions-on-russias-war-efforts

розподіляє загальну суму втрат (440 мільярдів доларів) між втраченими податками (154 мільярди) та іммобілізованими активами (285 мільярдів).

Проте аналіз має обмеження. Оцінка є консервативною, оскільки враховує лише прямі втрати державних активів і податкових надходжень, ігноруючи ширший вплив санкцій на економіку росії. Наприклад, не враховуються втрати від заморожених приватних активів, таких як 58 мільярдів доларів, заморожених країнами REPO, або додаткових 26 мільярдів фунтів стерлінгів активів приватних осіб, заморожених у Сполученому Королівстві. Загальні втрати експортних доходів від нафти та газу, ймовірно, значно більші, але їх важко точно оцінити через відсутність надійного контр-фактичного сценарію. Санкції також вплинули на фінанси росії через недоцільні витрати, зокрема через використання активів Національного фонду добробуту (NWF) для підтримки компаній, таких як «Аерофлот» і «РЖД». Аналіз не враховує вплив санкцій на глобальний ринок нафти, зокрема можливе зниження цін через санкційний тиск, і припускає, що обсяги виробництва та експорту нафти залишилися незмінними, хоча ціни та обсяги можуть взаємодіяти. Складність глобального нафтового ринку, на який впливають численні фактори попиту та пропозиції, ускладнює ізоляцію прямого ефекту санкцій.

Звіти окремих інституцій та експертів

Зведення та інформаційна панель щодо фінансових злочинів у Латвії [4]

Документ, підготовлений Financial Crime News, містить ретельний огляд прогресу Латвії у сфері ПВК/ФТ/ФР. Публікація є своєрідним аналітичним референсом напередодні повної оцінки Латвії в межах 6-го раунду взаємних оцінок FATF. Попри позитивний загальний тон, автори наголошують на тому, що ця оцінка має пройти повну перевірку якості у IV кварталі 2025 року.

Перші розділи документу нагадують про історичне тло: протягом десятиліть Латвія позиціонувала себе як регіональний фінансовий центр, орієнтований на приплив коштів з країн колишнього СНД, зокрема росії. Ця модель сприяла масштабним фінансовим злочинам, скандалам з відмивання коштів, залученню сумнівних офшорних фондів та арешту голови Центробанку за хабарництво. Злам настав у 2018 році після оприлюднення звіту MONEYVAL, гучних викриттів (наприклад, ABLV Bank) та попередження про можливе включення Латвії до «сірого списку» FATF.

У відповідь на ці виклики Латвія розпочала глибокі реформи, зокрема:

- деризикінг – істотне зменшення частки іноземних депозитів (з понад 50% у 2015 до 13% у 2022 році);
- заборона обслуговування компаній-оболонок;
- створення механізмів державно-приватного партнерства, зокрема Координаційної групи CCG під керівництвом ПФР;
- розвиток національного реєстру бенефіціарних власників та публічної доступності до даних про PEP;
- перехід до ризик-орієнтованого підходу у нагляді та розслідуванні;
- запуск AML Innovation Hub та Blackbox-інструменту для обміну фінансовою інформацією у псевдоанонімізованому форматі;

[4] https://thefinancialcrimenews.com/latvia-financial-crime-summary-dashboard-by-fcn-2025/

- створення координаційного підрозділу з питань ПВК, що зосереджується на ефективному конфіскуванні активів, включно з некримінальними процедурами.

У 2019–2022 роках Латвія поступово отримала визнання з боку FATF/Moneyval, ставши першою країною-членом MONEYVAL, яка була визнана повністю або здебільшого відповідною всім 40 Рекомендаціям FATF. Вона уникла включення до сірого списку, а у 2022 році успішно завершила процес посиленого моніторингу.

На момент 2023–2024 років, основні ризики для Латвії еволюціонували:

- зменшилася роль зовнішніх загроз, пов'язаних із СНД;
- зросли внутрішні загрози, зокрема з боку тіньової економіки, податкових злочинів, цифрового шахрайства, корупції та нелегального обігу наркотиків і підакцизних товарів;
- новою загрозою стала спроба обходу санкцій проти рф і білорусі, що має не лише ПВК-вимір, а й стратегічне безпекове значення.

Результати Національної оцінки ризиків 2023 року засвідчили прогрес: загальна оцінка здатності протидіяти ПВК зросла до 0,76 (у 2020 – 0,67; у 2017 – 0,50), а за окремими показниками (наприклад, якість стратегії, ефективність ПФР, внутрішня та міжнародна кооперація) – досягнуто максимальних значень (1.00/1.00). Показники сектору кредитних установ покращилися з "середньо-високого" до "середнього" рівня ризику, однак залишаються вразливими певні професійні групи, зокрема інвестиційні фірми, податкові консультанти, рієлтори та оператори азартних ігор.

За результатами 2023–2024 років:

- кількість кримінальних проваджень за ПВК сягнула 124, із яких понад 100 – передано до суду;
- загальна сума конфіскованих активів перевищила €96 млн;
- 183 випадки конфіскації на основі вироків;
- ПФР Латвії отримав нагороду Егмонтської Групі за найкраще розслідування;
- рівень співпраці з міжнародними партнерами – 9.54/10;
- понад 5,500 STR надійшло у 2024 році, з яких 42% — від нефінансового сектору.

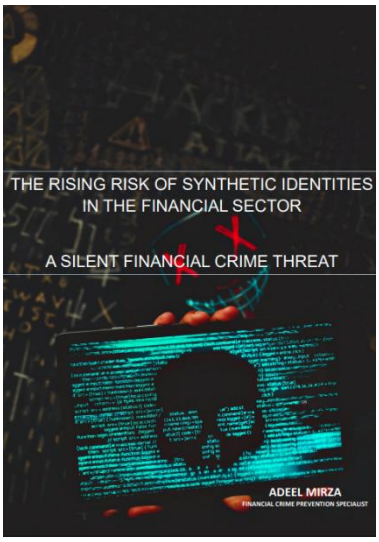
Однак автори звіту наголошують: попри вражаючий прогрес, остаточна ефективність залишається під питанням у сферах БР7 (розслідування ВК) та БР8 (повернення активів). Зокрема, необхідно ретельно проаналізувати реальні результати: рівень засуджень, повноцінне повернення активів (а не лише арешти), ефективність механізмів боротьби з ПВК через третіх осіб (third-party laundering).

Висновки:

- **Латвія успішно здійснила масштабний деризикінг і відмовилась від моделі регіонального фінансового центру**, що дозволило значно знизити рівень зовнішніх ПВК-ризиків — частка іноземних депозитів скоротилася з понад 50% (2015) до 13% (2022), компанії-оболонки були виключені з банківської системи.
- **Впроваджено інноваційні механізми в ПВК-системі**, зокрема AML Innovation Hub, Blackbox для правоохоронців, публічний реєстр КБВ з безкоштовним доступом, що сприяє прозорості та міжнародній співпраці.
- **Загальна результативність у кримінальних провадженнях зросла, проте ефективність розслідувань і конфіскацій залишається неоднозначною**, особливо у частині відмивання коштів та реального повернення активів — FATF має критично оцінити не лише обсяги, а й якість цих заходів.
- **Латвія не є унікальним прикладом, а радше демонструє базовий стандарт того, що необхідно зробити для відновлення довіри**: зміна законодавства, інституційне посилення ПФР, проактивний деризикінг та прозора комунікація з міжнародними партнерами.

Наприкінці зазначається, що хоча Латвія йде попереду в 6-му раунді оцінок FATF, вона не повинна слугувати завищеним бенчмарком, адже її ризик-профіль наразі знижений у порівнянні з багатьма іншими юрисдикціями. Латвія радше демонструє мінімально необхідний стандарт відповідності, що, втім, вже перевищує очікування до багатьох країн.

Зростання ризику синтетичних ідентичностей у фінансовому секторі [5]



Документ підкреслює, що з прискоренням цифрової трансформації у банківському та фінансовому секторах, шахраї паралельно розвиваються, використовуючи технології для експлуатації системних прогалин. Серед найбільш небезпечних і зростаючих типів шахрайства сьогодні є використання синтетичних ідентичностей. На відміну від традиційної крадіжки особистих даних, коли викрадається повна ідентичність реальної особи, шахрайство із синтетичними ідентичностями поєднує реальну та вигадану інформацію для створення нової, фальшивої ідентичності, яка може не належати жодній реальній особі. Ці ідентичності часто є достатньо реалістичними, щоб обдурити передові системи верифікації, створюючи серйозний ризик не лише для фінансової цілісності, а й для зусиль у боротьбі з відмиванням коштів, дотримання санкцій та заходів щодо протидії фінансуванню тероризму.

Синтетична ідентичність — це суміш реальної (часто викраденої) та фальшивої інформації. Наприклад, шахрай може використати реальний національний ідентифікаційний номер або номер соціального страхування (SSN), можливо, викрадений у дитини або померлої особи, у поєднанні з вигаданим ім'ям, датою народження та адресою, щоб створити "нову особу". Після створення, ця синтетична особа може формувати кредитний профіль, відкривати банківські рахунки, отримувати кредити і навіть створювати фіктивні компанії, зрештою зникаючи та залишаючи за собою фінансові та регуляторні ризики.

Ці синтетичні ідентичності є надзвичайно небезпечними, оскільки їх важко виявити, адже жодна реальна особа не може повідомити про їх викрадення. Вони можуть проходити початкові перевірки (onboarding checks), оскільки виглядають як клієнти з низьким ризиком та чистою історією. Синтетичні ідентичності ідеально підходять для легітимізації та інтеграції незаконних коштів під виглядом законних операцій. Вони можуть уникати санкційного скринінгу та списків політично значущих осіб (PEP), використовуючи вигадану особисту інформацію, а також створюють регуляторні сліпі плями, посилюючи вразливості ВК, санкцій та ФТ. Типова схема шахрайства із синтетичними ідентичностями включає створення ідентичності, встановлення довіри через сплату невеликих зобов'язань для формування кредитного сліду, відкриття низькоризикових рахунків або кредитних карток, а потім здійснення шахрайства "bust-out" — максимальне використання кредитів або кредитних ліній та зникнення.

Документ детально описує ризики з точки зору AML, санкцій та фінансування тероризму. Ризик ВК посилюється через анонімний доступ до фінансової системи, що дозволяє відкривати численні низькоризикові рахунки (наприклад, електронні гаманці, передплачені картки), структурувати транзакції трохи нижче порогових значень звітності та накладати незаконні кошти через складні, здавалося б, законні профілі клієнтів. Це експлуатує слабкості в процесах

[5] https://media.licdn.com/dms/document/media/v2/D4D1FAQEmXx0HNrjing/feedshare-document-pdf-analyzed/B4DZfLP5d4HkAY-/0/1751461642284?e=1753315200&v=beta&t=95KsnYDccUWSmYIgsJ3hBdzzrua06DnipsySeT_DP-E

належної перевірки клієнтів (CDD) та "Знай свого клієнта" (KYC), а також дозволяє обходити посилену належну перевірку (EDD), видаючи себе за низькоризикових роздрібних користувачів.

Щодо санкційного ризику, підсанкційні особи або організації можуть приховуватися за синтетичними ідентичностями, використовуючи реальні ID, викрадені у непідсанкційних осіб. Засоби скринінгу можуть не виявити такі профілі, оскільки вони не збігаються з відомими санкційними списками (наприклад, OFAC, ООН, ЄС), що особливо ризиковано у транскордонних транзакціях, де перевірка документів обмежена.

Ризик фінансування тероризму виникає через експлуатацію анонімності рахунків, оскільки терористичні групи можуть створювати синтетичні ідентичності для відкриття рахунків та міжнародного переміщення коштів, збору або переміщення коштів непомітно через краудфандинг або мікротранзакції, управління фіктивними неурядовими організаціями чи підприємствами під фальшивими особами, а також для отримання іноземних пожертвувань на рахунки, що належать синтетичним суб'єктам, таким чином уникаючи моніторингу розвідувальних та правоохоронних органів.

Висновки:

- **Посилення перевірок ідентичності та поведінковий моніторинг: Необхідно терміново оновити KYC/CDD фреймворки** та впровадити багаторівневі системи верифікації, що включають біометрію та валідацію через державні API, а також перейти від статичних перевірок до динамічного аналізу поведінки та транзакційних патернів клієнтів, особливо тих, що були залучені через цифрові канали, для виявлення аномалій та ознак шахрайства типу "bust-out".
- **Інтеграція AI/ML та обмін інформацією**: Фінансові установи мають активно впроваджувати AI/ML рішення для виявлення неочевидних зв'язків та аномалій у множинних заявках, а також тісно співпрацювати з регуляторами, підрозділами фінансової розвідки та кредитними бюро для обміну розвідувальними даними, типологіями та чорними списками, що посилить колективну здатність протидіяти синтетичним ідентичностям.
- **Комплексний підхід до ризиків AML/CTF/санкцій**: Політики AML, CTF та санкційного скринінгу повинні бути оновлені, щоб включати специфічні індикатори синтетичних ідентичностей та поведінкові аномалії, а не лише зосереджуватися на традиційних списках, що дозволить ефективніше виявляти приховані потоки коштів та фінансування тероризму, які використовують ці фальшиві профілі.

Крім того, існують значні регуляторні та репутаційні наслідки, такі як штрафи за порушення норм з ПВК/ФТ та репутаційні збитки за сприяння фінансовим злочинам, а також втрата кореспондентських банківських відносин, якщо ризик сприймається як некерований. Ці ризики посилюються завдяки зростанню цифрового онбордингу, фінтех-продуктів та віддалених фінансових послуг, які зменшують пряму взаємодію та фізичну документацію. Як приклад наведено кейс 2021 року в США, коли федеральні прокурори викрили мережу шахрайства із синтетичними ідентичностями, яка включала понад 7 000 ідентичностей, 25 000+ кредитних карток та 200 мільйонів доларів збитків, обійшовши CDD, санкції та поточний моніторинг.

Для виявлення та запобігання ризику синтетичних ідентичностей фінансовим установам рекомендовано переглядати свої фреймворки KYC/CDD, оновлювати політики AML та санкцій, а також розробляти моделі ПВК/ФТ, які оцінюють не лише статичні дані ідентичності, але й поведінку, мережеві ризики та платіжні патерни. Важливо включати індикатори ухилення від санкцій під час онбордингу та періодичних перевірок, впроваджувати багаторівневі системи верифікації, що поєднують перевірку документів, біометрію. Документ також наголошує на необхідності навчання персоналу першої

лінії та відділів комплаєнсу для виявлення червоних прапорців під час онбордингу та транзакцій, а також на співпраці з регуляторами для покращення керівних принципів онбордингу та стандартів ідентифікації. Координація з регуляторами, підрозділами фінансової розвідки та кредитними бюро для обміну розвідувальними даними та типологіями є не менш важливою.

Серед конкретних рекомендацій щодо контролю, документ пропонує використовувати динамічні моделі оцінки ризиків, засновані на поведінці та цифровому сліді, а також перехресну перевірку за офіційними цивільними реєстрами та біометричними ідентифікаторами. Для багаторівневої верифікації ідентичності пропонується використання біометрії (розпізнавання обличчя + визначення життєздатності) та валідація національних ID через державні API. Рекомендується впровадження скринінгу на основі AI/ML для виявлення аномалій у кількох заявках (наприклад, одна IP-адреса, багато імен) та ідентифікації тонких зв'язків між пристроями, документами та транзакціями. Для специфічних випадків пропонується застосовувати посилений моніторинг транзакцій для клієнтів з обмеженою або новою історією та незвичними потоками коштів, а також переглядати методологію оцінки ризиків, щоб включити такі типології шахрайства, як ризик синтетичних даних. Оновлення фільтрів санкцій та фінансування тероризму має включати поведінкові індикатори, а не лише списки на основі ідентичності, а також скринінг на незвичайні потоки транзакцій. Постійний моніторинг та EDD особливо важливі для нещодавно створених або оцифрованих клієнтів, з постійним відстеженням індикаторів "bust-out": раптового використання кредиту, іноземних переказів або швидких змін балансу. AI та поведінкова аналітика можуть допомогти моніторити цифрову поведінку за кількома точками контакту (ID пристрою, IP-адреса, геолокація) та аналізувати швидкість і послідовність транзакцій для виявлення "bust-out" патернів. Нарешті, постійний скринінг із використанням передових інструментів для регулярної перевірки профілів клієнтів на ознаки маніпуляції ідентичністю та використання галузевих консорціумів і обміну даними для чорних списків або позначених ідентичностей є критично важливим.

Віртуальні активи та постачальники послуг з віртуальними активами [6]

Червневий номер FIH Insights є всеосяжним дороговказом крізь найактуальніші виклики, що постають перед глобальними режимами протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення у зв’язку з бурхливим розширенням ринку віртуальних активів. Видання відкривається звітом із Симпозіуму Financial Integrity Hub-2025, де генеральний директор AUSTRAC Брендан Томас окреслив пріоритети агентства: від переходу до наглядової моделі «data-driven» до розбудови міжнародних альянсів і використання штучного інтелекту в аналізі потоків ВА. Упродовж дня понад 40 спікерів обговорювали суспільні наслідки фінзлочинів, «Tranche 2» - реформи щодо гейткіперів, репутаційні ризики, технологічні шахрайські схеми, специфіку загроз ФР та еволюцію моделей ФТ.

Центральний аналітичний блок присвячено масштабній реформі австралійського законодавства з ПВК/ФТ: прийнятий у грудні 2024 р. Amendment Act замінив терміни «digital currency» та «digital currency exchange» на «virtual asset» і «virtual asset service provider» (VASP), поширив регулювання на NFT, DAO та обміни ВА-ВА, установив вимогу Travel Rule для VASP із

[6] https://www.mq.edu.au/__data/assets/pdf_file/0003/1347159/FIH-Insights-June.pdf

кінцевою датою запровадження 31 березня 2026 р. і закрив прогалини щодо кастодіальних сервісів та супроводу первинних пропозицій токенів. Паралельно Казначейство та Комісія з цінних паперів рухаються до повного фінансового периметра: консультаційний документ CP 381 і оновлена INFO 225 зобов'язують біржі аналізувати правову природу кожного токена, проводити формалізовані «token assessments» і документувати висновки; судові справи Qoin та Block Earner демонструють, як практика судів уточнює межі підліцензованої діяльності та критерії віднесення продукту до фінансової послуги, тоді як AUSTRAC переходить від «education first» до штрафів — зокрема штраф Cointree у березні 2025 р. за несвоєчасне подання SMR .

Глобальна статистика, наведена професором Луї де Кокером, свідчить: із 147 опитаних FATF юрисдикцій 42 узагалі не провели оцінку ризиків ВА, а 27 % ще не визначилися з моделлю регулювання сектору; найболючіші лакуни — децентралізовані DAO та VASP без очевидного місця розташуванняюридичної особи для тесту mind and management, що ускладнює екстериторіальне правозастосування . Особливу загрозу становлять необліковані «self-hosted» гаманці й P2P-транзакції: за даними семи аналітичних компаній, у 2016-2020 рр. вони сягали близько 60% усіх переказів і понад половину їхньої вартості, причому саме в цій площині концентрувалися високоцінові нелегальні схеми, які досі не увійшли до сфери регуляторної уваги більшості країн.

Окремі статті деталізують технологічні вектори ризику. Katherine Shamai виділяє DeFi-платформи, токенізацію реальних активів, міксери та zero-knowledge протоколи як головні драйвери юрисдикційного арбітражу, що ставлять під сумнів дієвість традиційної інституційної моделі. Janya Eighani аналізує аномально високу концентрацію невідповідностей KYC-процедур у VASP стартапах та пропонує мінімальні ліцензійні стандарти, KPI-моніторинг і транскордонні regtech пісочниці для країн із обмеженими ресурсами нагляду . Далі Cuman Podder акцентує дилему приватності та прозорості та пропонує модель сертифікації платформ як компроміс, що збалансовує право інвестора на анонімність і суспільний запит на підзвітність.

Тема NFTs розкрита через призму регуляторної неоднорідності: FATF вважає, що колекційні NFT не є ВА, доки не використовуються як платіжний засіб, однак юрисдикції варіюють підходи; високовартісні NFT-аукціони в традиційних домах Christie's і Sotheby's лишаються поза рамками VASP-режиму та, без обов'язкових KYC, можуть мимоволі стати шлюзами для ВК. Показовим є позов 2023 р. щодо продажу набору Bored Ape Yacht Club за 24 млн USD, який

Висновки:

- Досвід Австралії показує, що гармонізація термінології VA/VASP, поширення регуляторного периметра на NFT, DAO та обміни VA-VA, а також чіткий графік запровадження Travel Rule сприяють закриттю найпомітніших прогалин у нагляді за віртуальними активами.
- Аналітика P2P-ринку свідчить, що «self-hosted» гаманці й прямі транзакції можуть охоплювати до 60 % світового обороту VA, залишаючись переважно поза регуляторним полем; це підтверджує потребу їхнього системного врахування у національних оцінках ризику.
- Приклади J5, Fintel Alliance та ізраїльської криптофорензіки демонструють, що державно-приватні центри блокчейн-аналітики та інтеграція ШІ-інструментів можуть суттєво посилити спроможність регуляторів і ПФР у виявленні складних транскордонних схем.
- Практика з NFT-аукціонами та судові кейси (наприклад, Qoin і Block Earner) окреслюють «сіру зону» ринку цифрового мистецтва: відсутність універсального KYC-режиму й стандартизованої процедури оцінки токенів створює підвищений ризик відмивання коштів через високовартісні колекційні активи.

обвалився в ціні, — справа підкреслює репутаційні й регуляторні ризики для нефінансових посередників .

Практичний вимір правозастосування ілюструє ізраїльська процедура вилучення ВА, описана Амітом Левіним. Після серії справ, у яких обвинувачені вимагали компенсації за втрату курсової різниці, прокуратура розробила чіткий алгоритм, закріплений у відомчому протоколі та підтверджений рішеннями Верховного суду.

Крок перший — фактичне вилучення: правоохоронці отримують приватні ключі та розміщують монети на урядовому гаманці. Протягом 24 годин прокурор зобов'язаний зв'язатися з адвокатом підозрюваного і запропонувати два взаємовиключні варіанти. Перший варіант — «збереження» (preservation): актив лишається у первісній формі, але власник підписує відмову від будь-яких майбутніх претензій щодо можливого падіння курсу. Другий — «конвертація» (conversion): актив негайно продають через ліцензовану біржу або OTC-desk, кошти зараховують на депозит Мінфіну, а власник відмовляється від претензій у разі подальшого зростання курсу.

Якщо жоден варіант не влаштовує підозрюваного, справа передається до суду. Суддя, спираючись на принцип пропорційності, визначає, чи важливіше мінімізувати волатильність (і дозволити державі продати актив), чи зберегти його у натуральній формі, захищаючи майнові права підозрюваного. Ключовий нюанс: держава в Ізраїлі може бути притягнута до цивільної відповідальності за збитки від своїх рішень, а суд — ні. Тому передача остаточного вибору суду одночасно підсилює прозорість і перекладає юридичну відповідальність на орган, який не може бути позивачем у майбутньому процесі.

Заключні сторінки висвітлюють освітні можливості: знижки від CFCE на курси AML/CTF, другий «подкаст-сезон» FIH із серією інтерв'ю (зокрема епізод із Brendan Thomas), а також анонс монографії Australia's Financial Integrity та майбутніх досліджень центру, що підтримують формування глобальної спільноти практиків, орієнтованих на інноваційні методи протидії фінзлочинам.

Аргентина перед викликами відмивання коштів: системні бар'єри та транснаціональні загрози [7]

Стаття, опублікована InSight Crime детально розглядає проблему відмивання грошей в Аргентині через інтерв'ю з Хуаном Феліксом Марто, президентом Фонду досліджень фінансової розвідки (FININT), директором Центру вивчення безпеки, тероризму та фінансових злочинів при Університеті Буенос-Айреса, а також колишнім національним координатором Аргентини з боротьби з фінансовими злочинами. Розмова зосереджується на складних структурних, економічних і системних викликах, з якими стикається країна у протидії відмиванню грошей, розглядаючи їх у ширшому контексті унікального економічного ландшафту Латинської Америки та глобальних стандартів боротьби з фінансовими злочинами. Марто підкреслює, що відмивання грошей є глобальною проблемою, яка щорічно охоплює 2–5% світового ВВП, як оцінює Управління ООН з наркотиків і злочинності, але лише 0,2% цих коштів конфіскується правоохоронними органами. У Латинській Америці ефективність заходів протидії відмиванню грошей обмежується кількома

[7] https://insightcrime.org/news/can-argentina-face-its-growing-money-laundering-challenges/

ключовими факторами: браком матеріальних, технологічних і людських ресурсів, політичною нестабільністю та частими економічними кризами. Однак, на думку Марто, основна проблема криється в самому підході до глобальної стандартизації, який розроблений FATF переважно для економік розвинених країн. Ці стандарти зосереджені на формальній економіці та регульованій фінансовій системі, тоді як у Латинській Америці значна частина економічної діяльності відбувається в неформальному секторі, де злочинні групи активно інтегрують незаконні кошти у формальну економіку, що ускладнює їх виявлення та відстеження.

В Аргентині ситуація ускладнюється високим рівнем неформальної економіки, яка становить 30–40% ВВП, порівняно з 5–8% у таких країнах, як США, Сполучене Королівство чи Німеччина. Цей високий рівень неформальності створює унікальні виклики для виявлення та переслідування відмивання коштів, оскільки традиційні інструменти, такі як перевірка клієнтів і звіти про підозрілі транзакції, не охоплюють неформальні економічні операції. За оцінкою FATF, проведеною наприкінці минулого року, в Аргентині щорічно відмивається близько 30 мільярдів доларів, але правоохоронні органи конфіскують лише 27 мільйонів доларів, що становить менше 0,1% від загальної суми. Марто висловлює скептицизм щодо методології FATF, зазначаючи її непрозорість, але визнає, що ці дані підкреслюють серйозні структурні недоліки в підході Аргентини до боротьби з фінансовими злочинами. Він наголошує, що національні рамки не здатні повною мірою врахувати масштаби та природу неформальних економік, у яких діють злочинні групи, і їх глибоку взаємодію з формальним сектором.

Система кримінальної юстиції Аргентини демонструє значні слабкості у боротьбі з відмиванням грошей. За офіційними даними, за п’ять років було винесено лише 91 вирок за злочини, пов’язані з відмиванням грошей, причому багато з цих справ не стосувалися великих кримінальних мереж. Марто зазначає, що прокурори та судді не мають достатньої підготовки чи спеціалізованих інструментів для проведення складних фінансових розслідувань, необхідних для розкриття та ліквідації великих кримінальних економік. Він критикує глобальний підхід FATF, який вимагає створення складних національних систем для запобігання, пом’якшення та переслідування фінансових злочинів, але оцінює їх ефективність за результатами традиційної системи кримінальної юстиції, яка не готова до таких завдань. Марто закликає політичне керівництво країни взяти на себе відповідальність за реформування системи, щоб забезпечити її здатність протистояти таким загрозам, як наркоторгівля, фінансування тероризму в районі Трьох кордонів (на стику Аргентини, Бразилії та Парагваю) та незаконний рибний промисел уздовж континентального шельфу Аргентини, які генерують значні обсяги незаконних доходів.

Відмивання грошей в Аргентині за своєю природою є транснаціональним, оскільки навіть прості операції, такі як конвертація песо в долари США чи розміщення доходів від злочинів, наприклад, від продажу болівійського кокаїну, у місцевих банках, залучають міжнародні фінансові мережі. Марто підкреслює, що іноземні банки відігравали ключову роль у сприянні системній корупції в Аргентині, визнаючи свою відповідальність лише під тиском юридичних дій, що ускладнює своєчасне припинення таких операцій. Зростання наркоторгівлі, особливо в провінції Санта-Фе та місті Росаріо, значно посилило проблему відмивання грошей. Десять років тому Аргентина вважалася переважно транзитною країною для наркотиків, але тепер Росаріо стало епіцентром насильства, пов’язаного з наркоторгівлею. У 2024 році рівень вбивств у Санта-Фе знизився до 4,83 на 100 000 осіб, що є найнижчим показником за десятиліття, завдяки арештам ключових кримінальних лідерів. Однак Марто ставить питання, чи свідчить це зниження про реальний демонтаж кримінальних економік, чи лише про їх реорганізацію та адаптацію до нових умов. Він наголошує на необхідності зосередитися на фінансовій основі цих груп, щоб зруйнувати економічні структури, які підтримують їх діяльність.

Порівняно з іншими країнами Латинської Америки, Аргентина перебуває на переломному моменті, маючи ще можливість ефективно протидіяти відмиванню грошей до того, як організована злочинність глибше вкоріниться в інституціях і політичних процесах. Хоча корупція та проникнення злочинних груп у сегменти поліції, судової системи та серед окремих законодавців є серйозною проблемою, політична система Аргентини ще не повністю підконтрольна злочинним структурам, на відміну від деяких сусідніх країн, де організована злочинність захопила значні політичні простори. Марто підкреслює, що це відкриває вікно можливостей для впровадження стратегій, які б зупинили кримінальні економіки та запобігли проникненню брудних грошей у політичні кампанії, що є критично важливим для збереження демократичної системи. Він наголошує, що відмивання грошей становить не лише фінансову загрозу, але й політичну та суспільну, оскільки кримінальні економіки підривають безпеку громад і цілісність демократичних інститутів. Марто закликає до переосмислення національних пріоритетів, зосереджуючи увагу на транснаціональних злочинах, таких як наркоторгівля, фінансування тероризму та незаконний рибний промисел, та їхніх фінансових основах. Він виступає за активні політичні та інституційні реформи, які б дозволили Аргентині ефективніше протистояти цим загрозам і захистити суспільство від впливу організованих злочинних груп.

Висновки:

- **Адаптація систем протидії відмиванню до неформальної економіки.** Аргентина повинна адаптувати глобальні стандарти протидії відмиванню грошей до реалій своєї неформальної економіки (30–40% ВВП), розробивши стратегії для моніторингу та регулювання неформальних фінансових транзакцій, де діють злочинні групи.
- **Посилення кримінальної юстиції.** Уряд має інвестувати в спеціалізовану підготовку та інструменти для прокурорів і суддів, щоб підвищити ефективність розслідувань фінансових злочинів і збільшити кількість вироків у резонансних справах.
- **Зупинення транснаціональних фінансових мереж.** Органи влади повинні посилити міжнародну співпрацю для відстеження та припинення транскордонного відмивання грошей, зокрема зосередивши увагу на ролі іноземних банків та операцій з конвертацією валют.
- **Запобігання кримінальному впливу на політику.** Національні та провінційні органи влади повинні запровадити заходи для захисту політичних кампаній від незаконного фінансування, щоб брудні гроші не підривали демократичні процеси.

Сучасне рабство в кавовій галузі: порушення прав працівників у Бразилії [8]

Документ, підготовлений швейцарською неурядовою організацією Public Eye у співпраці з Reporter Brasil, детально описує серйозні порушення трудових прав і умови, близькі до сучасного рабства, на кавовій фермі Mata Verde у штаті Еспіріту-Санту, Бразилія. Ця ферма була частиною ланцюга постачання кооперативу Cooabriel, який співпрацює з Nestlé у рамках програми сталого розвитку Nescafé Plan. Розслідування ґрунтується на свідченнях двох працівників, Журандіра душ Сантуша та Жозе

[8] https://stories.publiceye.ch/modern-slavery-coffee/

Адемілсона де Жезуса Ліми, а також на даних інспекцій бразильського Міністерства праці та аналізі експертів. Документ розкриває системні проблеми в кавовій індустрії Бразилії, включаючи неефективність сертифікаційних систем, брак прозорості в ланцюгах постачання та недостатню відповідальність великих корпорацій, таких як Nestlé.

У центрі розповіді — історія Журандіра душ Сантуша та Жозе Ліми, які у квітні 2023 року були найняті для сезонної роботи на фермі Mata Verde, розташованої за 1200 км від їхнього рідного міста Аракажу в штаті Сержипі. Їм обіцяли гідну зарплату — щонайменше 120 реалів на день (приблизно 22 євро), що значно перевищувало мінімальну зарплату в Бразилії (близько 12 євро на день). Однак після виснажливої двотижневої автобусної подорожі реальність виявилася зовсім іншою. Працівники зіткнулися з нелюдськими умовами проживання: вони спали на тонких матрацах прямо на гнилій дерев'яній підлозі, без дверей, раковин чи душів, із забрудненим питним водосховищем, повним комах, і періодичними відключеннями електроенергії. Санітарні умови були жахливими: туалети часто не працювали, під будинком накопичувалося сміття, що приваблювало щурів і викликало сильний сморід. Їжа була неякісною, переважно складалася з ковбаси, рису та квасолі, що призводило до хвороб, таких як застуди, висипи, грибкові інфекції та шлункові розлади. Один із працівників був серйозно хворий протягом тижня, але медикаментів не надавали, і колегам доводилося скидатися на ліки.

Робота на плантації була фізично виснажливою: працівники вставали о 5:30 ранку, готували їжу після мізерного сніданку (чашка кави та шматок тіста), працювали до 17:00, збираючи кавові ягоди вручну на горбистій і слизькій місцевості. Вони переносили 60-кілограмові мішки з ягодами до дороги, де їх забирали вантажівки. Укуси комах і важкі умови праці викликали головний біль і виснаження. Оплата залежала від обсягу зібраної кави: за кожен 60-кілограмовий мішок платили 16 реалів (2,90 євро), але без належних інструментів працівники могли зібрати в середньому лише три мішки на день, отримуючи менше 50 реалів (9 євро) за 12-годинний робочий день, що становило лише 75% від мінімальної зарплати. Зарплати ще більше зменшувалися через незаконні вирахування за робочий одяг, інструменти, їжу та навіть транспорт до ферми (350 реалів), що призводило до боргової залежності. Працівники не отримували чіткої інформації про розмір боргів чи трудові договори.

Умови праці на фермі відповідали критеріям "сучасного рабства" за бразильським законодавством, включаючи боргову кабалу, погрози, обман і примус. Працівників контролювали озброєні охоронці, а власник ферми погрожував закрити виїзд із села, якщо хтось спробує втекти до сплати "боргів". Жозе Ліма, відчуваючи загрозу, зокрема після того, як помітив пістолет у наглядача, вирішив організувати втечу. Він таємно зв'язався з місцевими трудовими органами та федеральною поліцією, документуючи порушення за допомогою фото та відео. 1 травня 2023 року Жозе, Журандір і ще 12 працівників втекли, дочекавшись автобуса до Аракажу. Наступного дня інспекція Міністерства праці разом із поліцією провела перевірку на фермі, звільнивши ще 10 працівників. Інспектори зафіксували 24 порушення, включаючи відсутність питної води, неналежне житло, боргову кабалу та погрози насильством.

Ферма Mata Verde постачала каву Робуста кооперативу Cooabriel, який є частиною програми Nescafé Plan і сертифікований за стандартом 4C, що позиціонується як соціально та екологічно стійкий. Nestlé заявляє про "нульову толерантність" до порушень прав людини, але розслідування показує, що випадки сучасного рабства в її ланцюгах постачання не є поодинокими. У 2022–2023 роках подібні порушення були зафіксовані на фермах Três Irmãs, Primavera (штат Баїя) та Vista Alegre (штат Мінас-Жерайс), які також постачали каву для Nestlé через Cooabriel або інших посередників. Це вказує на системні проблеми, зокрема через брак прозорості в ланцюгах постачання та неефективність сертифікації 4C. Аудити часто проводяться за кілька місяців до сезону збору врожаю або з попередженням за 1–2 дні, що дозволяє

приховувати порушення. Проблема незадекларованої праці, яка становить до двох третин зайнятості в кавовій індустрії, також ігнорується.

Юридичні наслідки для порушників залишаються мінімальними. Власник ферми Mata Verde погодився виплатити компенсацію (близько 900 євро на особу) лише тим працівникам, які залишалися на фермі під час інспекції. Жозе та Журандір, які втекли, отримали через суд лише 1275 євро кожен, що ледь покрило їхні борги. За даними експертки з трудового права Лівії Міральї, з 2799 роботодавців, звинувачених у сучасному рабстві в 2008–2019 роках, лише 112 були засуджені, і покарання зазвичай обмежуються штрафами або тимчасовим внесенням до "чорного списку", який втрачає чинність через два роки. Судова система часто недооцінює порушення прав працівників, а компенсації за сучасне рабство бувають меншими, ніж за втрату багажу в аеропорту.

Документ підкреслює історичний контекст: кавова індустрія Бразилії історично базувалася на рабстві, і сучасні практики продовжують експлуатувати соціально вразливих працівників, переважно африканського походження. Активіст Жорже Феррейра зазначає, що компанії, такі як Nestlé, перекладають відповідальність за дотримання прав людини на фермерів, не забезпечуючи достатнього фінансування чи контролю.

Nestlé припинила співпрацю з фермами, де виявлено порушення, але не коментує минулі зв'язки з Mata Verde чи конкретні кроки для забезпечення гідних зарплат. Стаття закликає до більшої прозорості, реформування сертифікаційних систем і реальних дій для захисту прав працівників, підкреслюючи особистий вплив таких умов на людей, як Жозе та Журандір, які зазнали травм і фінансових труднощів.

Висновки:

- **Посилення прозорості ланцюгів постачання:** Nestlé та інші корпорації повинні публікувати повні списки ферм-постачальників, а не лише кооперативів, щоб забезпечити можливість відстеження походження кави та виявлення порушень прав людини.
- **Реформування сертифікаційних систем:** Стандарти, такі як 4C, потребують перегляду, щоб включати регулярні, незаплановані інспекції під час сезону збору врожаю та враховувати проблему незадекларованої праці для ефективного запобігання сучасному рабству.
- **Забезпечення гідної оплати праці:** Компанії, такі як Nestlé, повинні гарантувати виплату прожиткового мінімуму (за оцінками Anker Research Institute, майже вдвічі більше за мінімальну зарплату в Бразилії) та заборонити незаконні вирахування з зарплат працівників.
- **Посилення юридичної відповідальності:** Бразильська влада має реформувати судову практику, щоб забезпечити суворіші покарання за сучасне рабство, включаючи реальні тюремні терміни для роботодавців та компенсації для всіх жертв, незалежно від їхньої присутності під час інспекцій.

Як аеропорти та авіакомпанії можуть стати ключовими партнерами у боротьбі з індустрією шахрайства [9]

Документ, опублікований організацією Global Initiative Against Transnational Organized Crime (GI-TOC), авторами якого є Ліндсі Кеннеді та Натан Пол Саузерн, є ґрунтовним аналізом ролі авіаційної галузі в боротьбі з глобальною кризою торгівлі людьми, спричиненою стрімким зростанням кібершахрайських центрів. У тексті детально розглядається, як ці центри, що діють у різних куточках світу, створюють умови для експлуатації сотень тисяч людей, залучених

[9] https://globalinitiative.net/analysis/flying-under-the-radar-how-airports-and-airlines-could-be-vital-partners-in-combating-the-cyber-scam-industry/

обманом до шахрайських операцій під виглядом легальних пропозицій роботи. Автори порівнюють масштаби та організаційну складність цієї проблеми з трансатлантичною работоргівлею, підкреслюючи її нагальність і необхідність залучення аеропортів та авіакомпаній до її вирішення. Документ висвітлює прогалини в чинних практиках протидії торгівлі людьми, виявляє системні недоліки, такі як корупція та відсутність належного навчання персоналу, і пропонує конкретні рекомендації щодо використання потенціалу авіаційної індустрії для запобігання потраплянню жертв до шахрайських комплексів.

Стаття розпочинається з опису масштабів кризи, пов'язаної з кібершахрайством. За останні кілька років сотні тисяч людей, переважно з країн із високим рівнем безробіття або значною кількістю кваліфікованих IT-фахівців, були обманом залучені до так званих "шахрайських комплексів". Ці жертви, часто молоді та освічені, заманюються фальшивими обіцянками легальної роботи, але опиняються в умовах примусової праці, де їх змушують займатися шахрайством під загрозою насильства та в умовах жорсткої експлуатації. Через те, що ці люди не відповідають стереотипному образу жертв торгівлі людьми, вони та особи, з якими вони контактують під час подорожі, часто не помічають важливих ознак небезпеки, таких як нервозність, мінімальний багаж чи незвичайні маршрути. У таких умовах жертви стають особливо вразливими, адже, потрапивши до шахрайських комплексів, вони втрачають доступ до своїх документів і зазнають маніпуляцій та залякувань, що значно ускладнює їх порятунок. Автори наголошують, що запобігання потраплянню жертв до цих комплексів є значно ефективнішим способом боротьби з проблемою, ніж спроби їх визволення після прибуття, оскільки це також порушує ланцюг постачання робочої сили для шахрайських операцій.

Ключовим аспектом, розглянутим у документі, є унікальна позиція аеропортів та авіакомпаній у протидії торгівлі людьми. Згідно з даними Міжнародної організації з міграції за 2021 рік, чотири з п'яти жертв торгівлі людьми перетинають офіційні прикордонні пункти, зокрема аеропорти, що робить авіаційну галузь ідеальним місцем для раннього виявлення потенційних жертв. Аеропорти та авіакомпанії мають доступ до значного обсягу даних про пасажирів, які можуть допомогти правоохоронним органам ідентифікувати підозрілі шаблони. Наприклад, аналіз даних про покупців квитків, маршрути подорожей, частоту рейсів між країнами, відомими як центри кібершахрайства (такими як Філіппіни, Грузія чи Камбоджа), або незвичайні маршрути, які маскують країну походження, може вказувати на діяльність шахрайських синдикатів. Крім того, такі ознаки, як мінімальний багаж, масові переміщення пасажирів із певних країн або різке зростання пасажиропотоку до нових шахрайських хабів, можуть свідчити про переміщення жертв або релокацію шахрайських операцій.

Незважаючи на міжнародні ініціативи, спрямовані на боротьбу з торгівлею людьми в авіаційній галузі, документ вказує на серйозні прогалини в їх реалізації. Наприклад, Закон про сучасне рабство у Сполученому Королівстві (2015) зобов'язує великі організації, включно з авіакомпаніями, звітувати про заходи щодо запобігання торгівлі людьми в їхніх операціях та ланцюгах постачання. Міжнародна асоціація повітряного транспорту (IATA), яка представляє 340 авіакомпаній і 80% світового авіатрафіку, у 2018 році взяла на себе зобов'язання щодо низки ініціатив із протидії торгівлі людьми, а в 2023 році оновила свої рекомендації, наголошуючи на важливості своєчасного повідомлення та навчання персоналу. Міжнародна організація цивільної авіації (ICAO) у 2023 році випустила посібник із боротьби з торгівлею людьми, закликаючи 193 країни-члени впроваджувати політику нульової толерантності до цього явища в аеропортах. Проте реальна практика значно відстає від цих рекомендацій. Автори наводять

приклад лондонського аеропорту, який обслуговує маршрути високого ризику, де працівники служби підтримки клієнтів повідомили, що не отримували відповідного навчання та не знали, як ідентифікувати чи повідомляти про потенційних жертв, хоча авіакомпанія стверджувала, що навчання проводилось для всіх співробітників ще з 2017 року. У аеропорту Пномпеня (Камбоджа) охорона та персонал також не мали знань про процедури виявлення чи повідомлення про можливих жертв торгівлі людьми. Представники оператора аеропорту, французького конгломерату VINCI, заявили, що навчання є обов'язковим, але відповідальність за його впровадження лежить на місцевих адміністраціях аеропортів, що призводить до відсутності централізованого контролю та невідповідностей.

Особливу увагу автори приділяють корупції, яка є серйозною перешкодою для ефективної боротьби з торгівлею людьми. У документі наводяться приклади, що ілюструють цю проблему: у Філіппінах у 2021 році 45 співробітників імміграційної служби були звільнені за хабарі, які дозволяли іноземцям уникати офіційних процедур; у М'янмі прикордонні сили співпрацювали з китайськими злочинними групами для підтримки шахрайських комплексів; у Камбоджі жертви повідомляли, що їхні викрадачі платили місцевій поліції 30 000 доларів США щомісяця за "захист". Такі випадки свідчать про те, що в країнах із високим рівнем корупції, таких як Камбоджа чи країни Латинської Америки, співпраця між аеропортами, авіакомпаніями та місцевими органами влади є ускладненою. Автори також звертають увагу на випадки в аеропорту Пномпеня у 2023–2025 роках, коли невідомі особи, які не були працівниками аеропорту, зустрічали пасажирів у зоні прильоту (airside), забираючи їхні паспорти та проводячи через візові та митні процедури. Ці пасажири, переважно китайці та в'єтнамці, виглядали розгубленими, мали мало багажу та уникали контактів з іншими, що є класичними ознаками торгівлі людьми. Такі дії, на думку експертів, неможливі без співучасті імміграційних служб і адміністрації аеропорту. Представники VINCI заявили, що не знали про ці інциденти, але підтвердили, що подібна присутність сторонніх осіб у зоні airside не має законних підстав і потребує розслідування.

Документ також підкреслює потенціал даних, якими володіють аеропорти та авіакомпанії, для боротьби з кібершахрайством. Інформація про покупців квитків, маршрути подорожей чи шаблони пасажиропотоку може бути ключовою для міжнародних розслідувань. Наприклад, різке зростання пасажиропотоку між країнами, що борються з кібершахрайством, і новими шахрайськими хабами може вказувати на релокацію злочинних операцій. Аналіз даних також може

Висновки:

- **Впровадження обов'язкового навчання персоналу.** Аеропорти та авіакомпанії повинні забезпечити регулярне, централізовано контрольоване навчання для всіх працівників, які контактують із пасажирами, з акцентом на розпізнавання ознак торгівлі людьми, таких як нервозність, відсутність багажу чи присутність супроводжуючих осіб.
- **Покращення обміну даними.** Авіаційна галузь має активно співпрацювати з міжнародними організаціями та правоохоронними органами, надаючи дані про пасажиропотоки, маршрути та покупців квитків, щоб виявляти шахрайські схеми,.
- **Розробка єдиних галузевих стандартів.** IATA та ICAO повинні впровадити обов'язкові стандарти для боротьби з торгівлею людьми, щоб усунути невідповідності в практиках, із чіткими протоколами для повідомлення та співпраці.
- **Посилення контролю в аеропортах високого ризику.** У країнах із високим рівнем корупції, таких як Камбоджа, аеропорти повинні запровадити суворіший контроль доступу до зон прильоту (airside) і перевіряти всіх осіб, які зустрічають пасажирів, щоб запобігти діяльності "супроводжуючих", пов'язаних із шахрайськими синдикатами.

виявити використання складних маршрутів для маскування країн походження або масові перевезення пасажирів із мінімальним багажем. Дослідження авторів показують, що шахрайські центри дедалі частіше залучають жертв із Східної Африки та іноземців із країн Перської затоки, таких як ОАЕ, а також використовують осіб із Центральної Азії для створення фальшивих профілів у романтичних шахрайських схемах. Рекрутери активно використовують Telegram для розміщення фальшивих оголошень про роботу, обіцяючи працевлаштування в одній країні, але транспортуючи жертв до іншої.

На основі цих висновків автори пропонують низку рекомендацій. По-перше, аеропорти та авіакомпанії повинні впроваджувати обов'язкове, стандартизоване навчання для персоналу, яке навчить їх розпізнавати ознаки торгівлі людьми та реагувати на них. По-друге, необхідно покращити обмін даними з міжнародними організаціями та правоохоронними органами, щоб виявляти підозрілі шаблони та координувати дії. По-третє, IATA та ICAO повинні розробити єдині галузеві стандарти для уникнення невідповідностей, спричинених аутсорсингом до приватних консультантів. Нарешті, в аеропортах високого ризику, таких як у Камбоджі, необхідно посилити контроль доступу до зон прильоту та перевіряти всіх осіб, які зустрічають пасажирів, щоб запобігти діяльності шахрайських "супроводжуючих". Документ завершується закликом до співпраці між авіаційною галуззю та міжнародними організаціями для створення ефективної системи протидії торгівлі людьми, що підживлює кібершахрайство.

Фінансова розвідка проти розповсюдження ЗМЗ: роль банків у виявленні та блокуванні ризиків пов'язаних з ФР [10]

Документ є детальним оглядом проблематики протидії фінансуванню розповсюдження зброї масового знищення (ФР) з позиції фінансового сектору, зокрема банків. Матеріал підготовлений Робочою групою з питань ФР UK Finance та охоплює нормативно-правову базу, ризики, методи контролю та ключові виклики, що стоять перед фінансовими установами у сфері боротьби з ФР.

У вступі наголошується, що, попри тривалу увагу до теми ФР у рамках міжнародного права та санкцій, лише відносно нещодавно фінансові установи були прямо зобов'язані оцінювати та контролювати ризики ФР, що особливо посилилося після прийняття стандартів FATF. Зокрема, зростає тиск на банки у зв'язку з очікуваним включенням елементів ФР до системи взаємних оцінок FATF. Документ відзначає слабку взаємодію між публічним і приватним секторами з цього питання, а також необхідність залучення до процесу протидії ФР інших небанківських учасників (перевізників, експортерів, страховиків, продавців товарів подвійного призначення тощо).

Окрему увагу приділено міжнародній нормативній базі — аналізуються підходи ООН, FATF, Сполученого Королівства, США та Європейського Союзу. Висвітлюється ключова проблема — відсутність єдиного міжнародного визначення ФР, що призводить до суттєвих розбіжностей у регуляторних підходах різних юрисдикцій, навіть у межах однієї держави. Це створює виклики для міжнародних фінансових установ, змушених одночасно дотримуватись несумісних правил. У Сполученому Королівстві, наприклад, ФР визначається у вузькому контексті – виключно як

[10] https://www.ukfinance.org.uk/system/files/2025-03/Countering%20Proliferation%20Finance%20-%20A%20Financial%20Sector%20Perspective.pdf

порушення санкцій ООН, тоді як США використовують ширше тлумачення, орієнтоване на визначення FATF.

Розділ з оцінки ризиків докладно аналізує категорії ризиків ФР за клієнтами, географією, продуктами/послугами, транзакціями та каналами доставки. У документі перелічуються галузі з підвищеним ризиком – оборонна промисловість, ядерний, хімічний і біотехнологічний сектори, електроніка, аерокосмічна галузь, морські перевезення, нафтохімія, ринок криптовалют і коштовностей, професійні послуги (особливо постачальники трастових послуг), міжнародна торгівля та логістика, а також працівники й дипломатичні представництва з КНДР. Підкреслюється, що багато таких секторів можуть бути експлуатовані суб'єктами розповсюдження зброї масового знищення без відома самих клієнтів. Наведено приклади, як можна використовувати коди NACE2 для виявлення ризиків ФР, але водночас відзначається обмеженість цього підходу без додаткового аналізу бізнес-моделі клієнта.

У частині, присвяченій системам контролю банку, акцентовано на застосуванні типологій ФР, підходах до KYC і CDD, взаємодії з американськими списками BIS, системах скринінгу транзакцій і найменувань, а також на складності і малоефективності використання списків товарів подвійного призначення в контексті фінансових транзакцій. Підкреслено, що дані про товар у платіжних повідомленнях часто не дозволяють проводити ефективний скринінг, тому запровадження нових стандартів структурованих платіжних полів може стати ключовою умовою підвищення ефективності протидії ФР.

Далі розглядаються серйозні обмеження в здатності банків отримувати чи перевіряти ліцензії на експорт контрольованих товарів, у т.ч. відсутність доступу до даних про відмови в ліцензуванні. Це створює ризики, коли клієнт стверджує про наявність дозволу, але фактично може його не мати. Більше того, поточні системи скринінгу не забезпечують можливості відфільтровувати ризики ФР окремо від загальних санкційних ризиків або ризиків ПВК, через відсутність міток (тегів) ФР у санкційних списках та у внутрішніх розслідуваннях банків. Як наслідок, неможливо побудувати аналітику та звітність для менеджменту саме по інцидентах пов'язаних з ФР, що обмежує здатність банків приймати стратегічні рішення на основі даних.

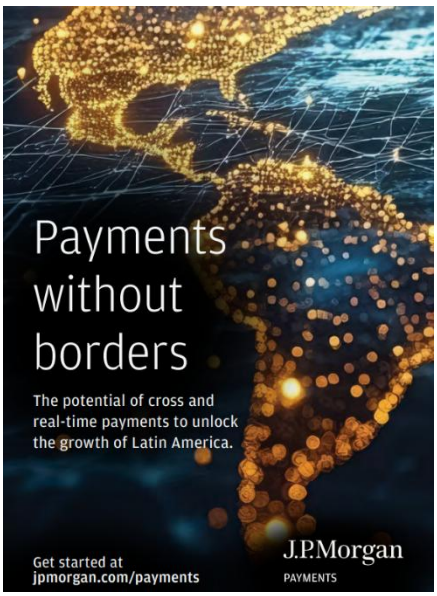
Документ завершується висновками щодо необхідності міжсекторального діалогу, інституційних змін та

Висновки:

- **Необхідність інтеграції ФР у існуючі контрольні рамки ПВК/санкцій.** Фінансовим установам не обов'язково створювати окрему систему для ФР, але потрібно чітко ідентифікувати ризики, пов'язані з ФР в межах існуючих механізмів — із фокусом на клієнтів, транзакції, географію та продукти.
- **Низька ефективність застосування списків товарів подвійного призначення.** Банки неспроможні ефективно використовувати переліки товарів подвійного призначення без зміни формату транзакційних даних. Необхідне оновлення структур SWIFT/ISO-повідомлень для вказання змісту товарів у платежах, що потребує ініціативи на рівні регуляторів.
- **Відсутність стандартизованого позначення ризику ФР шкодить моніторингу.** Поточні системи не розрізняють повідомлення про ризики ФР від загальних санкційних, що унеможливлює створення релевантної звітності. Пропонується технічне оновлення IT-систем з впровадженням маркерів ФР.
- **Ключова роль обміну інформацією та міжсекторальної взаємодії.** Боротьба з ФР виходить за межі банківського сектора — слід активізувати співпрацю з митницями, експортерами, страховиками, транспортними компаніями. Особливо в контексті санкцій на росію та поставок товарів подвійного призначення.

технологічної модернізації, включаючи покращення форматів обміну даними, автоматизованого маркування ризиків ФР, а також розробки ефективної інформації для управлінських рвшень по ФР для банківського керівництва. Наголошується на важливості адаптації існуючих контрольних механізмів ПВК/ФТ до ризиків ФР без створення надлишкових дублюючих структур, але з чітким урахуванням специфіки ФР – зокрема, участі третіх осіб, використання компаній-оболонок, криптовалют та логістичних каналів. Документ демонструє високий рівень розуміння практичних викликів у боротьбі з ФР і слугує ґрунтовним інструментом для самостійного вдосконалення контрольних систем фінансовими установами у відповідності до міжнародних стандартів.

Платежі без кордонів: Новий фінансовий порядок у Латинській Америці [11]



Аналітичний звіт є глибоким дослідженням поточних тенденцій, викликів і перспектив розвитку транскордонних (CBP) та миттєвих (RTP) платежів у Латинській Америці. Документ розкриває трансформаційний потенціал цифрових платіжних інфраструктур у контексті фінансової інклюзії, економічного зростання та регіональної інтеграції, акцентуючи увагу на конкретних прикладах з ключових країн регіону. Звіт базується на емпіричних даних, експертних інтерв'ю, а також аналізі політик, регуляторних режимів і ринкових інновацій, що формують платіжний ландшафт регіону.

На тлі низької динаміки ВВП, високої інфляції та обмеженого фіскального простору, Латинська Америка демонструє прагнення до цифрової трансформації. Цей процес особливо помітний у сфері платежів, де попит на швидкі, доступні й прозорі фінансові послуги стимулює впровадження новітніх технологій. Транскордонні платежі є ключовим елементом міжнародної торгівлі, обслуговуючи потоки товарів, послуг, інвестицій і ремітенсів. Попри домінування традиційної кореспондентської банківської моделі, спостерігається її скорочення (наприклад, у Чилі — на 36%, в Аргентині — на 32% у 2012–2018 роках), що створює запит на більш ефективні альтернативи. У цьому контексті значну роль відіграють Fintech, рішення на базі відкритих API, Big Data, Blockchain і криптоактиви. У звіті наголошується, що CBP у 2023 році становили понад 146 трлн дол. США, з очікуваним зростанням до 250 трлн до 2027 року, а лише 3,5% цього обсягу припадає на роздрібний сектор — однак саме він має найвищий потенціал інновацій і впливу на інклюзію.

Миттєві платежі — інший вектор трансформації, що забезпечує цілодобовий переказ коштів протягом секунд, значно покращуючи управління ліквідністю, фінансову доступність і клієнтський досвід. RTP стають не лише інструментом для кінцевого споживача, а й критичним елементом казначейських рішень для бізнесу. Особливо успішним прикладом є система Pix у Бразилії, яка з 2020 року стала основним інструментом платежів, забезпечивши понад 40 млрд транзакцій на рік. У 2023 році Pix охоплював 75% RTP у Латинській Америці і 14% світового ринку RTP, змінивши структуру платежів і значно скоротивши використання готівки. У Мексиці впровадження Fintech-законодавства, програми Directo a México спільно з Федеральною

[11] https://www.jpmorgan.com/content/dam/jpmorgan/images/payments/latam/jpm-payments-without-borders-english.pdf

резервною системою США, а також зростання обсягу цифрових ремітенсів свідчать про стратегічний підхід до побудови платіжної інфраструктури.

Країни регіону, зокрема Колумбія, Чилі й Аргентина, поступово впроваджують нові рішення, зосереджуючи зусилля на фінансовій інклюзії, розвитку цифрових платформ, інтеграції криптовалют і підготовці до прийняття стандарту ISO 20022. Звіт демонструє, що фінтех-екосистеми у регіоні динамічно розвиваються: з 703 компаній у 2017 році до понад 3 000 у 2023 році. Водночас 77% усіх Fintech зосереджені у п'яти країнах: Бразилії, Мексиці, Колумбії, Аргентині та Чилі. У більшості країн впроваджено механізми пісочниці та нормативні підходи, що сприяють інноваціям.

Значну увагу у звіті приділено впливу криптовалют і цифрових валют центральних банків (CBDC). Країни як Бразилія, Мексика та Колумбія активно працюють над впровадженням CBDC, водночас криптоактиви вже використовуються для P2P і ремітенсів, хоча застосування у B2B-сегменті стримується через волатильність, регуляторну невизначеність і складність інтеграції з бухгалтерськими системами. Латинська Америка демонструє зростаючий рівень відповідності рекомендаціям FATF щодо віртуальних активів, що створює передумови для подальшого розвитку у цьому напрямку. Ремітенси, які в 2023 році сягнули 156 млрд дол. США, мають істотне макроекономічне значення для регіону, а їх дедалі більше цифровізація відкриває нові канали для модернізації СВР.

Висновки:

- **Реалізація RTP (напр., Ріх у Бразилії) є критичним каталізатором фінансової інклюзії та цифрової трансформації.**
  Рекомендація: Національним банкам слід ініціювати або підтримати розробку миттєвих платіжних систем, орієнтованих на P2P та B2B транзакції з відкритими API.
- **Уніфікація стандартів (ISO 20022, API, відкриті фінанси) — умова ефективної регіональної інтеграції та зниження транзакційних витрат.**
  Рекомендація: Розробити дорожню карту технічної інтеграції RTP/СВР у відповідності з глобальними стандартами та спільними регламентами.
- **Фінтех-сектор забезпечує інклюзивний доступ до цифрових фінансів, особливо для малих та середніх підприємств (МСП) та некласичних користувачів.**
  Рекомендація: Сприяти створенню регуляторних пісочниць, фінансуванню інфраструктури для МСП, та партнерству з Fintech для вирішення останньої милі платежів.
- **Цифрові ремітенси, криптовалюти і CBDC вже трансформують СВР, але потребують збалансованого регулювання для мінімізації ВК/ФТ-ризиків.**
  Рекомендація: Посилити нагляд за віртуальними активами відповідно до стандартів FATF (Рекомендація 15, Travel Rule), особливо в країнах з високою долею неформального сектору.

Звіт також охоплює тему економічної інтеграції та торгівлі, зазначаючи важливість регіональних угод (наприклад, Альянсу Тихоокеанських країн) та ініціатив як BIS Nexus Project, який передбачає інтероперабельність RTP через API без потреби у спільній інфраструктурі. Активізація перенесення виробництва ближче до ринку, зростання торгівлі з Китаєм, цифрова трансформація малих і середніх підприємств — усе це формує нову структуру попиту на платежі. У цьому контексті СВР виступають не лише засобом руху капіталу, а й інструментом управління ланцюгами постачання, цифрової комерції та інституційного позиціонування в глобальній фінансовій системі.

Таким чином, звіт детально описує трансформаційний потенціал платіжних систем у Латинській Америці, демонструючи, що інвестиції у СВР та RTP, супроводжувані регуляторною гармонізацією,

технологічною модернізацією та співпрацею між публічним і приватним секторами, здатні перетворити регіон на конкурентоспроможного гравця глобальної цифрової економіки.

Нові виклики, старі платформи: модернізація основних банківських систем як ключ до майбутнього банкінгу [12]

Документ є аналітичним дослідженням, присвяченим стратегічній необхідності модернізації основних банківських систем (CBS) у країнах Південно-Східної Азії. Цей звіт є першою частиною двотомного циклу, в якому розкривається, чому модернізація CBS є критично важливою не лише з технічного, але й з бізнес-погляду, та які фактори змушують банки переглядати свою інфраструктурну архітектуру в умовах цифрової трансформації. Документ акцентує увагу на тому, що нинішня банківська екосистема регіону є надзвичайно динамічною — молоде населення, високі темпи цифровізації, агресивна експансія фінтехів та необанків, зростаючі очікування клієнтів щодо персоналізованого і швидкого обслуговування, а також тиск з боку регуляторів щодо IT-надійності — формують нову реальність, у якій традиційні (часто побудовані на мейнфреймах 20-річної давності) CBS-системи виявляються повністю непридатними до виконання сучасних вимог.

Основною проблемою є те, що більшість банків Південно-Східної Азії утримуються від повної модернізації своїх CBS, натомість зосереджуючись на косметичних, точкових оновленнях, які лише ускладнюють архітектуру систем. Це призводить до надмірної кастомізації, втрати знань усередині організацій і створення надзвичайно складних у підтримці і модернізації систем — феномен, який автори називають «Франкенштейновою архітектурою». Такий підхід має критично високі ризики, про що свідчать провальні кейси банків у Європі та Азії, де проєкти з модернізації завершувалися багаторазовим перевищенням бюджету, мільярдними списаннями інвестицій, відставками керівництва та втратою довіри інвесторів. Попри це, потреба в модернізації CBS стає дедалі гострішою, і документ подає вісім ключових імперативів, які, на думку BCG, не залишають банкам вибору.

Серед них першим називається зростання клієнтських очікувань — у світі, де сервіси за типом доставки їжі чи таксі стали миттєвими, клієнти очікують такої ж персоналізації та швидкості від банків. Для реалізації подібного функціоналу потрібні CBS-платформи з високим ступенем конфігурованості та гнучкості. Другим імперативом є конкуренція з боку фінтехів, які надають безшовні цифрові послуги на всіх етапах клієнтського шляху — від відкриття рахунку до виконання транзакцій. Традиційні CBS, побудовані на пакетній обробці з фіксованою технологічною послідовністю дій, не можуть забезпечити подібну динаміку, інтеграцію та масштабованість. Третій імператив стосується потреби банків шукати нові джерела доходу через інтеграцію в зовнішні платформи: оплата частинами після покупки (BNPL), цифрові гаманці, фбудовані фінансові послуги, співпраця з платформами онлайн-торгівлі. Застарілі CBS системи з їхніми пропрієтарними протоколами не здатні забезпечити масштабну та швидку інтеграцію з третіми сторонами через API. Четвертий аспект — це потреба в операційній діяльності, заснованій на даних: розширене логування, доступ до повної подієвої інформації,

[12] https://media-publications.bcg.com/Core-Banking-System-Modernization-Part-1.pdf?linkId=831419217

вбудована аналітика й можливість прогнозного аналізу — усе це майже відсутнє в поточних системах, які зберігають дані переважно в реляційних базах. Сучасна трансформація потребує побудови «операційних маяків», які дозволяють виявляти прогалини і прогнозувати потреби клієнтів у реальному часі.

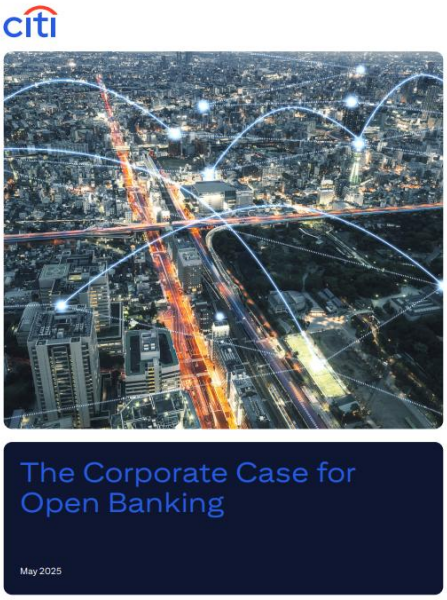
П'ятий імператив — впровадження нових технологій, зокрема створеної для хмарного середовища архітектури, мікросервісного дизайну, масштабування у режимі реального часу, штучного інтелекту/машинного начання. Документ описує кейси, коли CBS повинна витримувати в 6–8 разів більші навантаження під час промокампаній або у «пікові години», і лише сучасні архітектурні підходи дозволяють ефективно масштабуватися без значних додаткових витрат. Шостий фактор — потреба у зниженні витрат: застарілі системи не лише дорогі в обслуговуванні, але й змушують банки переплачувати за неефективну інфраструктуру, не маючи змоги оперативно масштабуватись або змінювати компоненти. Сьомий імператив — зростання регуляторного тиску на надійність IT-систем: регулятори дедалі частіше вимагають обґрунтовану готовність банків до відновлення після інцидентів, і CBS є центральною ланкою такої стратегії, але застарілі платформи не дозволяють гарантувати відмовостійкість і відповідність SLA. Останній, восьмий аспект — це очікування співробітників банку. Технологічні команди прагнуть працювати з сучасними технологіями, а поточні системи не відповідають їхнім очікуванням щодо гнучкості, інтерфейсів, швидкості розгортання змін і методологій DevSecOps/Agile.

Висновки:

- **Більшість банків працює на застарілих системах CBS.** Це значно обмежує швидкість цифрових трансформацій і створює операційні ризики.
  Рекомендація: банки повинні закладати CBS-модернізацію у свої IT-стратегії як базову умову довгострокової життєздатності.
- **Модернізація CBS критично необхідна для аналітики у реальному часі і DataOps.** Застарілі CBS не здатні ефективно підтримувати аналітику, виявлення аномалій або персоналізацію.
  Рекомендація: модернізовані платформи повинні підтримувати повну подієву логіку та API-доступ до структурованих даних.
- **Без відкритих API та архітектури хмарного середовища банки не зможуть інтегруватись у фінтех-екосистему.** Інтеграція з вбудованими фінансовими послугами та відкритим банкінгом неможлива без гнучкої CBS.
  Рекомендація: вибір платформи має базуватись на відкритих стандартах інтеграції
- **Висока вартість утримання застарілих систем обмежує фінансову гнучкість банків.** Відсутність автоматичного масштабування та залежність від постачальників підвищують витрати.
  Рекомендація: необхідно переорієнтувати IT-бюджети з «підтримки поточної діяльності банку» на «інвестування в розвиток і трансформацію».

Загальний висновок авторів полягає в тому, що модернізація CBS є не технічним або факультативним завданням, а стратегічною умовою виживання банків в умовах радикально зміненого ландшафту фінансових послуг. Нинішній стан систем є бар'єром до інновацій, зростання й ефективності, а зволікання лише збільшує майбутні витрати та ризики. У наступній частині цього дослідження буде розглянуто практичну сторону модернізації — шляхи реалізації, стратегії переходу, моделі співіснування старих і нових ядер, а також ключові фактори успішності.

Відкритий банкінг для корпоративного сектору: стратегічний потенціал, практичні рішення та глобальні тенденції [13]



Документ є аналітичною роботою, присвяченою обґрунтуванню цінності відкритого банкінгу для корпоративного сектору з акцентом на практичні кейси та глобальний регуляторний контекст. Основний зміст документа зосереджено навколо того, як відкритий банкінг трансформує функцію корпоративного казначейства, управління ліквідністю та взаємодію компаній з банками та фінтех-екосистемою. В основі цієї трансформації лежить використання інтерфейсів прикладного програмування (API), що забезпечують стандартизований, безпечний і майже миттєвий обмін фінансовими даними між банками, фінтех-компаніями та корпоративними клієнтами.

Документ починається з констатації того, що сучасні компанії діють у глобальному 24/7 бізнес-середовищі, де традиційні методи взаємодії з банківською системою, такі як використання SWIFT або регулярні файли-звіти, вже не відповідають потребам у швидкості та точності фінансових даних. Відкритий банкінг пропонується як рішення, що дозволяє компаніям отримувати реальний час інформацію про залишки на рахунках, проводити платежі та інтегрувати ці функції безпосередньо у свої ERP та TMS-системи (системи планування ресурсів та системи управління казначейством). Водночас підкреслюється, що глобальне впровадження відкритого банкінгу нерівномірне через різні регуляторні моделі: у ЄС, Сполученому Королівстві, Австралії, Сінгапурі та Японії діють обов'язкові правила, а в США поширена ринково-орієнтована модель без жорстких вимог до банків. Це створює виклики для корпорацій, які ведуть діяльність у кількох юрисдикціях, оскільки інтеграція з банками без стандартизованих API перетворюється на складний, дорогий і фрагментований процес.

Окрему увагу документ приділяє технічним моделям відкритого банкінгу, детально пояснюючи відмінності між трьома підходами: багатосторонні API без стандартів, де кожен банк встановлює власні правила; API зі стандартами, де регулятор визначає загальні технічні вимоги; централізовані платформи, де всі банки та треті сторони підключаються до єдиної інфраструктури, як це зроблено у Туреччині чи ОАЕ. Автори підкреслюють, що саме централізована модель є найбільш ефективною для корпоративного сегменту, оскільки мінімізує витрати на інтеграцію, забезпечує єдиний підхід до авторизації, конфіденційності та безпеки даних.

Документ докладно аналізує, як API стають базовим інструментом для оптимізації корпоративної казначейської функції. Описано практичний механізм, за якого API дозволяють підприємству об'єднати інформацію з рахунків у різних банках у єдиний мультибанкінговий інтерфейс у системі TMS або ERP, автоматизувати перевірку залишків, рух коштів та управління ліквідністю без необхідності ручного доступу до банківських порталів. Автори наголошують на таких перевагах API для корпоративного сектору: швидкість (отримання інформації у реальному часі замість очікування на файли від банку), точність (зведення до мінімуму ризиків затримок та помилок через прямий обмін даними), ефективність (автоматизація процесів, зменшення адміністративного навантаження).

[13] https://www.citigroup.com/rcs/citigpa/storage/public/The_Corporate_Case_for_Open_Banking.pdf

Особливої уваги надано темі управління казначейством у режимі реального часу, тобто управлінню корпоративною ліквідністю в режимі реального часу. Описується, що традиційний підхід із використанням SWIFT недостатньо оперативний для великих компаній, що працюють у багатьох країнах, оскільки отримання інформації може займати години чи дні, у той час як у реальному бізнесі кошти вже можуть бути перераховані чи потрібні для нових операцій. За допомогою відкритого банкінгу API компанії можуть в реальному часі бачити залишки, ініціювати платежі, управляти ліквідністю без ризику втрати часу чи інформації. Наведено приклад того, як API дозволяють зменшити кількість «застряглих» коштів, скоротити внутрішньоденний рух коштів між рахунками, оптимізувати кредитні лінії та більш ефективно мобілізувати надлишкову ліквідність.

Окремий розділ присвячено співпраці банків із фінтех-компаніями в рамках концепції Banking as a Service (BaaS). Документ наводить приклади того, як фінтех-провайдери та банки об'єднують свої можливості для створення нових продуктів, таких як прямий платіж з банківського рахунку — рішення для миттєвих платежів без карток, де покупець безпосередньо авторизує платіж зі свого банківського рахунку в інтерфейсі торговця. Такий підхід забезпечує миттєве зарахування коштів, нижчі витрати для продавця, менший ризик шахрайства завдяки відсутності зберігання платіжних даних покупця. Підкреслюється, що розвиток BaaS сприятиме не лише платежам, а й впровадженню страхових, інвестиційних та інших фінансових продуктів безпосередньо в інтерфейси компаній, зокрема через інтеграцію з торгівельні онлайн-платформами.

Документ підкреслює стратегічний вимір відкритого банкінгу у поєднанні з технологіями штучного інтелекту. Описується, що доступ до агрегованих фінансових даних через API створює передумови для використання AI-моделей, які можуть покращити прогнозування, прийняття рішень, виявлення можливостей для інвестицій чи управління ризиками. Однак для цього компанії мають не лише інтегрувати API, а й перебудовувати внутрішні системи, забезпечити відповідну IT-інфраструктуру, перейти від пакетного режиму до повністю автоматизованої обробки даних у реальному часі.

У завершенні автори підкреслюють, що впровадження відкритого банкінгу для корпоративного сектору є довгостроковим процесом, який

Висновки:

- Відкритий банкінг є критично важливим інструментом для корпоративних клієнтів з метою отримання доступу до банківських даних у реальному часі, оптимізації управління ліквідністю та інтеграції казначейських функцій із ERP і TMS-системами. Саме API стають базою цієї трансформації.
- Регуляторні моделі, що передбачають обов'язкове впровадження відкритого банкінгу разом із технічними стандартами (наприклад, у ЄС, Сполученому Королівстві), значно прискорюють поширення рішень відкритого банкінгу, порівняно з юрисдикціями, де домінує ринково-орієнтований підхід (як у США).
- Централізовані платформи відкритого банкінгу з уніфікованими API-стандартами (як у Туреччині чи ОАЕ) створюють більш сприятливе середовище для корпоративних клієнтів, спрощуючи інтеграцію та знижуючи витрати, на відміну від моделей з мультисторонньою інтеграцією без єдиних стандартів.
- Відкритий банкінг сприяє розвитку співпраці банків і фінтех-компаній у рамках Banking as a Service (BaaS), дозволяючи впроваджувати інноваційні фінансові сервіси, зокрема прямі платежі зі банківських рахунків (перекази з рахунку на рохунок), що забезпечують миттєві розрахунки та покращують клієнтський досвід, а також відкривають нові можливості для використання штучного інтелекту в корпоративному фінансовому менеджменті.

потребує як технологічної, так і організаційної трансформації. Компаніям рекомендується починати з малих кроків, не намагаючись впровадити все одразу, поступово інтегруючи нові рішення у діючі бізнес-процеси, адаптуючи персонал до нових умов роботи. Особливо важливою є активна позиція корпоративних клієнтів щодо формулювання очікувань до банків, оскільки саме корпоративний попит визначатиме темпи розвитку екосистеми відкритого банкінгу. Підсумовуючи, документ позиціонує відкритий банкінг не як технічну новинку, а як стратегічно важливий напрямок розвитку корпоративних фінансів у найближчі роки, який уже зараз здатний дати компаніям конкурентну перевагу завдяки більш ефективному управлінню ліквідністю, інтеграції з фінтех-інноваціями та оптимізації операційних процесів.

Інші новини

Як Tether став валютою мрії для відмивачів [14]

Стаття ретельно відстежує походження та результати "Операції Дестабілізація" (Operation Destabilise), яка була ініційована у Сполученому Королівстві в 2021 році після звичайної конфіскації готівки на дорозі. Ця операція викрила транснаціональну схему відмивання грошей, що пов'язувала наркобанди, групи програм-вимагачів, підсанкційних осіб та державних суб'єктів. Усі ці злочинні елементи були об'єднані завдяки використанню стейблкоїна Tether (USDT).

Згідно з наданим звітом, Tether активно використовувався для переведення кримінальних прибутків, отриманих у готівковій формі в Європі, до банківських коштів у Росії та за її межами. Злочинці розробили триетапну модель відмивання грошей: по-перше, збір фізичної готівки; по-друге, її доставка до підсанкційних організацій; і по-третє, компенсація через USDT. Ця модель дозволяла здійснювати транскордонне переміщення вартості повністю поза традиційною банківською системою. Особливо вражаючим є те, що вартість відмивання коштів через Tether, за повідомленнями, становила менше 3%, що значно нижче, ніж у традиційних мережах відмивання готівки. Важливою проблемою, на яку вказує звіт, є мінімальний регуляторний нагляд за діяльністю Tether та його вибіркова співпраця з правоохоронними органами. Станом на січень 2025 року компанія тримала 113 мільярдів доларів у казначейських зобов'язаннях США і повідомила про прибуток понад 13 мільярдів доларів у 2024 році, маючи при цьому менше 200 співробітників.

Стаття також висвітлює певні стратегічні події, які допомагають пояснити поточне позиціонування Tether. Компанія уклала партнерство з Cantor Fitzgerald, великою фінансовою установою США. Ця співпраця додала Tether додатковий рівень легітимності, особливо з огляду на його зростаючу присутність у глобальних фінансових та політичних колах. Водночас на початку 2025 року Tether переніс свою штаб-квартиру з Британських Віргінських Островів до Сальвадору, країни, відомої своєю прокриптовою позицією. За словами генерального директора, цей крок відображає свідому стратегію діяти в рамках регуляторних систем, більш узгоджених з баченням компанії щодо фінансової свободи.

Це розслідування яскраво демонструє, як стейблкоїни змінюють міжнародні фінансові потоки, створюючи нові виклики для контролю за боротьбою з відмиванням грошей та фінансуванням тероризму, а також породжуючи важливі питання щодо юрисдикційного арбітражу, інституційних партнерств та ролі приватних акторів у світовій фінансовій системі.

[14] https://www.economist.com/1843/2025/07/04/how-tether-became-money-launderers-dream-currency

Європа завдає удару по темній мережі: ліквідація Archetyp Market [15]

З 11 по 13 червня 2025 року правоохоронні органи шести європейських країн — Німеччини, Нідерландів, Румунії, Іспанії, Швеції — у тісній співпраці з Європолом та Євроюстом провели масштабну міжнародну операцію, спрямовану на ліквідацію Archetyp Market, найстарішого та одного з найвпливовіших ринків наркотиків у темній мережі. Ця платформа, що діяла понад п'ять років, об'єднувала більш ніж 600 000 користувачів по всьому світу та забезпечувала обсяг транзакцій на суму щонайменше 250 мільйонів євро. Archetyp Market вирізнявся своєю репутацією в кримінальному середовищі, пропонуючи широкий асортимент заборонених речовин, включаючи кокаїн, МДМА, амфетаміни, а також особливо небезпечні синтетичні опіоїди, такі як фентаніл, які становлять серйозну загрозу для громадської безпеки в Європі та за її межами. Платформа налічувала понад 17 000 активних пропозицій, що робило її однією з небагатьох у темній мережі, яка дозволяла торгівлю опіоїдами, сприяючи їх поширенню та посилюючи глобальну проблему наркозалежності.

Операція, що стала кульмінацією багаторічного розслідування, охоплювала скоординовані дії приблизно 300 офіцерів правоохоронних органів, які одночасно діяли в кількох країнах. Основний удар був спрямований на ключові елементи екосистеми Archetyp Market: адміністратора, модераторів, провідних постачальників та технічну інфраструктуру. У Барселоні, Іспанія, було заарештовано 30-річного громадянина Німеччини, який виконував роль головного адміністратора платформи. Цей арешт став центральною подією операції, оскільки адміністратор відігравав ключову роль у підтримці функціонування ринку. Водночас у Німеччині та Швеції правоохоронці провели заходи проти одного модератора та шести ключових постачальників, які забезпечували основний обсяг торгівлі наркотиками через платформу. Технічна інфраструктура Archetyp Market, що базувалася в Нідерландах, була повністю відключена, що унеможливило подальшу діяльність платформи. У ході операції також було конфісковано активи на суму 7,8 мільйона євро, включаючи фінансові ресурси, пов'язані з незаконною діяльністю ринку, що завдало значного економічного удару організаторам та учасникам.

Ця операція стала результатом тривалої та складної слідчої роботи, яка вимагала глибокого аналізу фінансових потоків, цифрових доказів і тісної співпраці між міжнародними партнерами. Правоохоронці використовували передові методи цифрової криміналістики для відстеження транзакцій і встановлення особистих даних ключових учасників. Європол відігравав центральну роль у координації дій, організувавши численні оперативні зустрічі, які дозволили правоохоронним органам різних країн обмінюватися критично важливою інформацією, синхронізувати дії та планувати операцію. Євроюст, зі свого боку, забезпечував юридичну основу для транскордонної співпраці, координуючи виконання запитів про взаємну правову допомогу та європейських слідчих доручень, що було необхідним для проведення арештів і вилучення активів у різних юрисдикціях.

Після завершення активної фази операції на сайті Archetyp Market було розміщено офіційний банер про конфіскацію, який сповіщав користувачів про припинення діяльності платформи. Для посилення ефекту та попередження інших операторів темної мережі Європол і партнери опублікували додаткові матеріали, включаючи спеціальне відеозвернення, спрямоване на підпільну економіку. Цей крок мав на меті не лише інформувати про успішну операцію, а й

[15] https://www.europol.europa.eu/media-press/newsroom/news/europe-wide-takedown-hits-longest-standing-dark-web-drug-market

підкреслити невідворотність покарання для тих, хто займається незаконною діяльністю в темній мережі.

У розслідуванні брали участь численні правоохоронні структури, зокрема Прокуратура Франкфурта-на-Майні та Федеральна кримінальна поліція Німеччини, Національна поліція Нідерландів, Румунська поліція, Національна поліція Іспанії, Шведська поліція, а також американські партнери, включаючи Управління розслідувань національної безпеки (HSI), Кримінальний підрозділ Податкової служби США (IRS-CI) та Міністерство юстиції США. Їхня спільна робота дозволила не лише ліквідувати Archetyp Market, а й зібрати значний обсяг доказів, які можуть бути використані для подальших розслідувань.

За своїм масштабом, тривалістю діяльності та впливом на кримінальне середовище Archetyp Market порівнюють із такими відомими платформами темної мережі, як Dream Market і Silk Road, які також були ліквідовані внаслідок масштабних правоохоронних операцій. Ця операція, очолювана німецькими правоохоронцями, стала одним із найпотужніших ударів по інфраструктурі незаконної торгівлі наркотиками в темній мережі, продемонструвавши, що навіть найстійкіші кримінальні платформи не можуть уникнути відповідальності. Успіх операції підкреслює важливість міжнародної співпраці, використання передових технологій і скоординованих зусиль для протидії кіберзлочинності, а також слугує чітким сигналом для інших операторів темної мережі про те, що їхня діяльність перебуває під пильною увагою правоохоронних органів.

Для загального розвитку

Міжнародні організації, що борються з фінансовими злочинами [16]

Ця публікація детально розкриває ключову роль міжнародних організацій у безперервній боротьбі з фінансовими злочинами, такими як відмивання грошей, фінансування тероризму та фінансування розповсюдження (ПВК/ФТ/ФР), особливо в умовах зростаючої глобалізації.

Основний зміст статті зосереджений на ідентифікації та описі діяльності різних "глобальних воїнів", які роблять значний внесок у розробку та впровадження уніфікованих політик, процедур та практик, спрямованих на захист світової фінансової системи. Серед ключових міжнародних організацій, виділених у статті, є Група розробки фінансових заходів боротьби з відмиванням коштів (FATF), яка відповідає за розробку та моніторинг міжнародних стандартів у сфері ПВК/ФТ/ФР, а також Комітет експертів з оцінки заходів боротьби з відмиванням грошей (MONEYVAL), що оцінює відповідність цих стандартів у країнах-членах Ради Європи. Також згадана Егмонтська Група, яка забезпечує безпечну платформу для обміну

[16] https://amlconsultants.uk/global-warriors-international-organisations-battling-financial-crimes/

експертними знаннями та розвідданими, та Організація економічного співробітництва та розвитку (ОЕСР), що допомагає країнам боротися з міжнародним ухиленням від сплати податків та іншими фінансовими злочинами.

Стаття також висвітлює важливу роль таких організацій, як Transparency International (TI), яка бореться з корупцією, виявляючи та усуваючи лазівки у світовій фінансовій системі, що сприяють відмиванню грошей, та ініціатива "Поділ електронних ресурсів та законів про злочинність" (SHERLOC) від UNODC, що розповсюджує інформацію про Конвенцію ООН проти транснаціональної організованої злочинності. Ініціатива з повернення викрадених активів (StAR), партнерство між Світовим банком та UNODC, допомагає країнам повертати викрадені державні активи. Крім того, підкреслено внесок Міжнародного консорціуму журналістів-розслідувачів (ICIJ) у викриття фінансових злочинів та корупції, що призводить до реформ.

Значна увага приділяється також професійним асоціаціям, які відіграють важливу роль у підвищенні кваліфікації фахівців. Це, зокрема, Міжнародна асоціація комплаєнсу (ICA), Асоціація сертифікованих фахівців з фінансових злочинів (ACFCS), Інститут боротьби з відмиванням грошей та фінансовими злочинами (AMLFC Institute), Асоціація сертифікованих фахівців з боротьби з відмиванням грошей (ACAMS) та Асоціація сертифікованих експертів з шахрайства (ACFE). Ці організації надають професійну кваліфікацію, навчання та підтримку, сприяючи обміну передовим досвідом та розвиваючи знання у сфері запобігання фінансовим злочинам.

Серед викликів, з якими стикаються ці організації, стаття неявно підкреслює глобалізацію, яка полегшує злочинцям переміщення незаконних коштів через кордони, що вимагає колективної та глобальної відповіді. Необхідність "стандартизованих політик, процедур та практик" підкреслює проблему досягнення послідовного впровадження у різних юрисдикціях.

Стратегії, що застосовуються цими організаціями, є багатогранними і включають встановлення стандартів та розробку політики, моніторинг та оцінку, обмін інформацією та розвідданими, нарощування потенціалу та навчання, дослідження та підвищення обізнаності, міжнародну співпрацю та адвокацію. Загалом, стаття наголошує, що надійний, спільний та багатовекторний підхід за участю різних міжнародних організацій є вирішальним для ефективної боротьби з фінансовими злочинами та захисту світової економіки.

Ваша думка важлива!

1. Які заходи може вжити Україна для протидії використанню нових технологій, таких як віртуальні активи та краудфандингові платформи, для фінансування тероризму, особливо з огляду на зростання «сірих» транзакцій у воєнний час, і як забезпечити баланс між регулюванням та підтримкою фінансової інклюзії?
2. Як міжнародне співтовариство та національні регулятори мають реагувати на використання стейблкоїнів, таких як Tether, у схемах відмивання грошей, враховуючи їхню високу ефективність для злочинців та вибіркову співпрацю з правоохоронними органами?
3. Чи можливо, на ваш погляд, інтегрувати принцип "колективних дій" у стратегію ПВК/ФТ в Україні, залучаючи не лише державні органи, а й приватний сектор та громадські організації, з огляду на досвід Базельського інституту управління?
4. Які додаткові механізми чи інструменти, окрім вже існуючих, могли б підвищити ефективність санкційного тиску та мінімізувати можливості для обходу?
5. У контексті зростаючої загрози синтетичних ідентичностей у фінансовому секторі, які практичні інструменти та технології можуть бути найбільш ефективними для українських фінансових установ для їх виявлення та запобігання використанню у схемах ВК/ФТ?
6. Які ключові уроки з досвіду Латвії, що успішно здійснила масштабний деризикінг та впровадила інноваційні механізми в системі ПВК/ФТ, можуть бути застосовані в Україні для подальшого підвищення ефективності боротьби з фінансовими злочинами?

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-2025-28

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].