Методологічний бюлетень

Серійний номер: МінФін-AML-2026-18

Травень 2026

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

Томас Карлайл

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

20-й пакет санкцій ЄС проти росії [1]

Двадцятий пакет санкцій Європейського Союзу, ухвалений 23 квітня 2026 року та імплементований через масштабний масив взаємопов'язаних нормативно-правових актів, становить собою фундаментальний зсув у санкційній стратегії ЄС. Цей пакет сигналізує про остаточний перехід від запровадження базових секторальних ембарго до високоточного таргетування інфраструктури обходу санкцій, придушення тіньових фінансових мереж та ведення асиметричної юридичної війни. Консолідований пакет включає безпрецедентне розширення індивідуальних обмежень: Імплементаційний Регламент (ЄС) 2026/509 додає 117 фізичних та юридичних осіб до списків замороження активів. Стратегічною особливістю цього лістингу є відхід від фокусування на російських політичних фігурах; натомість

[1] https://www.consilium.europa.eu/en/press/press-releases/2026/04/23/russia-s-war-of-aggression-against-ukraine-20th-round-of-stern-eu-sanctions-hits-energy-military-industrial-complex-trade-and-financial-services-including-crypto/

цілями стали технократи, оператори тіньової логістики та широка мережа компаній-прокладок у третіх країнах (зокрема, 6 суб'єктів у Китаї та 8 в ОАЕ), які забезпечують безперебійне постачання західної мікроелектроніки до військово-промислового комплексу РФ.

В енергетичному та логістичному секторах пакет впроваджує критичні обмеження, спрямовані на нейтралізацію так званого "тіньового флоту" та блокування експорту зрідженого природного газу (ЗПГ). Регламент вносить 46 додаткових суден до санкційних списків, збільшуючи загальний обсяг підсанкційного флоту до 632 одиниць, яким заборонено доступ до портів ЄС та отримання морських послуг. Регламент (ЄС) 2026/506 встановлює жорсткі терміни: з 25 квітня 2026 року забороняється надання технічної допомоги, брокерських послуг або фінансування для російських криголамів та ЗПГ-танкерів, а з 1 січня 2027 року ця заборона поширюється на всі інші ЗПГ-танкери, що функціонують в інтересах РФ. Крім того, запроваджується повна заборона на надання послуг ЗПГ-терміналів для російських суб'єктів з 1 січня 2027 року. Для запобігання подальшому розширенню тіньового флоту, європейські оператори відтепер зобов'язані проводити посилену належну перевірку та включати жорсткі контрактні застереження (no-Russia clause) при продажу танкерів.

У сфері торговельного комплаєнсу та експортного контролю 20-й пакет вперше в історії санкційного режиму активує "Інструмент протидії обходу" (Anti-Circumvention Tool) на рівні цілої юрисдикції. Додаток XXXIII прямо забороняє експорт оброблювальних центрів та телекомунікаційного обладнання до Киргизстану через доведені та стійкі ризики реекспорту в Росію. Одночасно суттєво розширено списки товарів військового та подвійного призначення (Додатки VII та XXIII), куди додано промислове обладнання (верстати з ЧПУ, високопотужні трактори), лабораторне скло, мастила, а також хімічні речовини та вибухівку (аматол, нітрогліколь, толуїлендиізоцианат). Імпортні обмеження також посилено: запроваджено річну квоту на імпорт аміаку для запобігання обходу газового ембарго, а також заборонено ввезення солей, хутра, міді, нікелю та алюмінію, що генерують значні доходи для російського бюджету. Додатково встановлено вимоги щодо документального підтвердження походження оброблених діамантів для унеможливлення їх російського походження.

Фінансовий вимір 20-го пакету зосереджений на знищенні архітектури децентралізованих фінансів (DeFi), що використовується РФ для обходу обмежень. З 24 травня 2026 року встановлюється повна заборона на будь-які транзакції з російськими провайдерами послуг віртуальних активів (CASP) та платформами обміну. Безпрецедентним кроком є пряма заборона на операції з цифровим рублем (CBDC Центрального банку РФ) та забезпеченим рублем стейблкоїном RUBx (Стаття 5ba), що є превентивним блокуванням суверенних блокчейн-мереж агресора. Крім того, Стаття 5ad запроваджує транзакційну заборону щодо юридичних осіб (наприклад, Arneis, GPAgent та Platejka), які не є фінансовими установами, але діють як тіньові платіжні інтегратори для приховування міжнародних транзакцій. Водночас виключення із санкційних списків п'яти банків третіх країн (у Китаї та Таджикистані) після надання ними юридичних гарантій щодо припинення обслуговування схем обходу санкцій створює важливий прецедент ефективності вторинного тиску. Пакет також запроваджує заборону на надання послуг з управління безпекою (management security services) російським урядовим та корпоративним клієнтам з 25 травня 2026 року.

Фундаментальною юридичною новацією пакету (Регламент 2026/511 та Рішення 2026/504) є створення потужного механізму захисту європейського бізнесу від асиметричних атак російської правової системи та експропріації активів. У відповідь на масову практику ігнорування арбітражних застережень, європейські компанії отримали право звертатися до судів держав-членів ЄС за судовими наказами (anti-suit injunctions), невиконання яких російськими позивачами призводитиме до накладення штрафів на користь європейського оператора. Більше того, компанії ЄС можуть вимагати компенсації збитків від примусового виконання неправомірних рішень судів РФ у третіх країнах, з можливістю звернення стягнення

на активи російських позивачів, заморожені в межах юрисдикції ЄС. Регламент також запроваджує заборону на транзакції з російськими суб'єктами, які отримують комерційну вигоду від незаконної експропріації європейських активів або крадіжки прав інтелектуальної власності (IP).

Додаткові заходи 20-го пакету спрямовані на боротьбу з російською пропагандою та гібридним впливом. Запроваджено заборону на хостинг та надання послуг для "дзеркальних" веб-сайтів підсанкційних медіа (таких як Russia Today та Sputnik), що забезпечує швидке блокування клонів пропагандистських ресурсів. Також встановлено категоричну заборону для європейських дослідницьких та інноваційних установ приймати будь-яке грантове чи донорське фінансування від російського уряду. Водночас Рішення 2026/504 запроваджує точкові дерогації для розморожування коштів на користь державних посередників, які реалізують європейську культурну політику в РФ (наприклад, міжнародні школи чи інституції підтримки меншин), що вимагає від комплаєнсу банків застосування надскладних протоколів цільового моніторингу транзакцій.

Паралельно з російськими заходами, Імплементаційне Рішення (CFSP) 2026/503 та Регламент (ЄС) 2026/505 усувають регуляторні розбіжності між санкційними режимами РФ та Білорусі, ліквідовуючи "мінську лазівку". У межах цього розширення до санкційних списків додано трьох нових юридичних осіб, інтегрованих у транскордонні логістичні схеми забезпечення армії РФ. Ключовим заходом для протидії системному TBML стала заборона на надання послуг, безпосередньо пов'язаних з туристичною діяльністю в Білорусі, оскільки фіктивні туристичні контракти масово використовувалися для прихованого переміщення капіталу в межах Союзної держави.

Висновки:

- **Модернізація інструментарію блокчейн-аналітики та моніторингу:** Необхідність екстреної інтеграції цифрового рубля (CBDC) та стейблкоїна RUBx у системи моніторингу транзакцій, а також впровадження алгоритмів ретроспективного пошуку взаємодій з усіма російськими CASP та компаніями тіньового процесингу (Arneis, GPAgent, Platejka).
- **Глибокий аналіз логістичних і торговельних мереж:** Запровадження обов'язкового скринінгу IMO-номерів для виявлення 632 суден "тіньового флоту", перевірка контрактів купівлі-продажу танкерів на наявність "no-Russia clause", та встановлення презумпції заборони на торговельне фінансування операцій з постачання високотехнологічного обладнання до Киргизстану.
- **Рекалібрування комплаєнсу у сфері судочинства та експропріацій:** Адаптація внутрішніх політик фінансових установ для опрацювання судових наказів, сприяння зверненню стягнення на заморожені активи РФ як компенсації за порушення контрактів, та блокування транзакцій компаній, причетних до крадіжки інтелектуальної власності ЄС.
- **Синхронізація ризиків для Білорусі та РФ:** Уніфікація сценаріїв моніторингу для обох юрисдикцій з метою блокування транзиту через фіктивні контракти (особливо у сфері нещодавно заборонених туристичних послуг) та виявлення прихованих контрагентів нових логістичних компаній, внесених до санкційного списку.

Цифровізація та інновації — можливості та ризики для фінансового здоров'я [2]

Документ являє собою аналітичний огляд Інституту фінансової стабільності Банку міжнародних розрахунків (BIS), підготовлений за підсумками міжнародного семінару «Досягнення стабільності, стійкості та інклюзивного зростання через фінансове здоров'я». Авторський колектив — Джон Фрост, Джермі Преніо, Ватсала Шріті та Девід Симінгтон — розглядає цифровізацію фінансових послуг крізь призму концепції фінансового здоров'я населення (financial health), яку документ принципово відокремлює від більш вузького поняття фінансової інклюзії. Фінансове здоров'я визначається як чотирьохвимірний конструкт, що охоплює здатність індивіда управляти поточними фінансами, формувати стійкість до фінансових шоків, досягати коротко- та довгострокових цілей, а також відчувати суб'єктивну впевненість у власному фінансовому майбутньому. Саме ця концептуальна рамка задає аналітичну основу всього дослідження і водночас вказує на принципові виміри, за якими цифрові інновації слід оцінювати: не лише за показниками доступності послуг, але й за реальними змінами в добробуті домогосподарств.

Одним із найбільш аналітично значущих висновків документа є констатація погіршення показників фінансового здоров'я у низці країн, попри безпрецедентне поширення цифрових фінансових послуг, — парадокс, який автори кваліфікують як емпіричну головоломку сучасної фінансової регуляторики. У США частка «фінансово вразливих» домогосподарств знизилася під час пандемії COVID-19, проте повернулася до допандемічних рівнів у 2024 році. У Бразилії показник «поганого» фінансового здоров'я погіршився впродовж 2020–2023 років. Найбільш показовим є кейс Кенії, де частка «фінансово нездорових» домогосподарств зросла з ~60% до ~80% між 2016 та 2021 роками і стабілізувалась на цьому рівні у 2024-му — і це попри масове поширення мобільних грошей M-Pesa та платформ цифрового кредитування. Авторський аналіз встановлює, що головними драйверами кенійського погіршення були макроекономічні чинники — інфляція продовольчих цін, падіння реальних доходів та міграція зайнятості від офіційного до неформального сектора. Таким чином, документ формулює принципово важливе аналітичне застереження: цифровізація не може компенсувати несприятливі макроекономічні умови і, за відсутності системного регуляторного контролю, здатна як посилювати, так і послаблювати фінансовий добробут.

Документ систематизує емпіричні свідчення щодо п'яти ключових секторів, де цифрові технології об'єктивно покращують фінансове здоров'я. У сфері платежів особлива роль відводиться системам миттєвих платежів (Fast Payment Systems, FPS), які функціонують у понад 135 юрисдикціях станом на 2025 рік. Квазіекспериментальне дослідження впровадження Unified Payments Interface (UPI) в Індії демонструє, що в округах, які першими прийняли це нововведення, доходи домогосподарств і підприємців зросли суттєво швидше порівняно з тими, хто ввів це пізніше, підтверджуючи причинно-наслідковий зв'язок між прийняттям безготівкових платежів та підвищенням добробуту. У Бразилії система Pix знизила потребу малого бізнесу у зовнішньому фінансуванні оборотного капіталу завдяки прискоренню обігу коштів. Щодо кредиту — альтернативні дані (транзакційна активність на платформах електронної комерції, дані QR-платежів) та методи машинного навчання розширюють доступ до кредиту для суб'єктів, яких традиційні скорингові моделі відносять до «виключених». Так, аргентинська платформа Mercado Libre встановила, що 30% фактично кредитоспроможних МСП було б відхилено за класичними критеріями кредитних бюро.

[2] https://www.bis.org/fsi/fsibriefs31.pdf

Аналіз ризиків для фінансового здоров'я, якому присвячена значна частина документа, спирається на нову глобальну статистику та свідчить про системний масштаб загроз. За даними глобального опитування GASA/Feedzai (2024), майже половина респондентів стикалася зі спробами шахрайства щонайменше раз на тиждень; загальний обсяг втрат від шахрайства у світі оцінюється у 1 трильйон доларів США на рік, при цьому в окремих країнах (Пакистан, Кенія, Індія, Таїланд, Південна Африка) збитки перевищують 3% ВВП. Генеративний штучний інтелект (GenAI) суттєво підвищив якість та переконливість фішингових атак і діпфейків, впровадивши «шахрайство як послугу» (fraud-as-a-service) навіть для технічно непідготовлених зловмисників. Паралельно документ фіксує структурну проблему надмірної заборгованості у сфері цифрового кредитування: у всіх п'яти юрисдикціях, охоплених опитуванням GSMA, позичальники з цифровими кредитами з більшою ймовірністю мали прострочену заборгованість, ніж ті, що використовували традиційні кредитні продукти. Особливу тривогу викликає Buy Now, Pay Later (BNPL): продукт непропорційно використовується молодими дорослими з низькими кредитними рейтингами та значним борговим навантаженням, що призводить до вищих рівнів простроченої заборгованості порівняно з класичним споживчим кредитом.

Документ окремо та детально аналізує ризики для роздрібних інвесторів, що виникають унаслідок поширення застосунків для інвестування та використання інструментів генеративного AI (зокрема ChatGPT) для отримання фінансових порад. За даними дослідження 2023 року, 47% американців покладаються на ChatGPT для вибору акцій; у Великій Британії станом на 2025 рік 33% роздрібних інвесторів використовують подібні інструменти. При цьому такі сервіси функціонують поза системою нагляду, прозорості та підзвітності, генеруючи авторитетно звучащі, але потенційно некоректні рекомендації. Інвестиційні застосунки активно застосовують елементи гейміфікації, соціальних мереж та програм лояльності для стимулювання торгівлі ризикованішими активами — підхід, який документ кваліфікує як маніпулятивний, спрямований проти інтересів клієнта. Зростання ринку криптоактивів, включаючи волатильні мем-коїни, в поєднанні з доступністю кредитних продуктів (маржинальна торгівля, похідні інструменти) особливо небезпечне у країнах з формованими ринками, де рівень фінансової грамотності нижчий.

Висновки:

- **Зростання цифрового кредитування без пропорційного нагляду за рівнем заборгованості вимагає від СПФМ інтеграції індикаторів фінансового здоров'я у системи транзакційного моніторингу та профілювання клієнтів.** Регулятори вже фіксують вищий рівень дефолтів серед цифрових позичальників у всіх п'яти юрисдикціях дослідження — що є прямим індикатором нефінансових ризиків для СПФМ у категорії кредитних продуктів.
- **Глобальний збиток від шахрайства у $1 трлн та поширення фішингу за допомогою GenAI (deepfake, vishing, BEC) вимагають від СПФМ невідкладного перегляду ризик-індикаторів:** традиційні порогові та поведінкові правила не вловлюють персоналізовані AI-сценарії, тому підрозділи ПВК/ФТ мають впровадити поведінкові моделі виявлення та перейти від реактивного блокування до превентивного втручання у режимі реального часу.
- **Запровадження режимів відповідальності за шахрайство у низці юрисдикцій (APP reimbursement у Великій Британії, Singapore SRF) означає, що СПФМ зобов'язані переглянути внутрішні процедури реагування на шахрайство та механізми відшкодування:** невідповідність новим вимогам несе пряму операційну та регуляторну відповідальність, включаючи ризик санкцій за системне недотримання вимог захисту споживачів.

Регуляторні відповіді, розглянуті у п'ятому розділі документа, відображають щонайменше три паралельні стратегії. По-перше, запровадження режимів відповідальності за шахрайство: система Shared Responsibility Framework Сінгапуру (MAS/IMDA) та вимога відшкодування за несанкціоновані платежі (APP scams) британського PSR встановлюють конкретні зобов'язання для банків і платіжних систем щодо компенсації жертвам. По-друге, регулювання цифрового кредитування: Резервний банк Індії, Центральний банк Кенії та нігерійська FCCPC ввели ліцензування цифрових кредиторів, вимоги до розкриття інформації та заборону автоматичного кредитування для обмеження надмірної заборгованості. По-третє, IOSCO розробляє дорожню карту безпеки роздрібних інвесторів онлайн, що охоплює стандарти для фінінфлюенсерів, копі-трейдингу та цифрових практик залучення. Паралельно акцент ставиться на цифрових публічних інфраструктурах (DPI) — системах цифрової ідентифікації, FPS та механізмах обміну даними — як необхідному підґрунті для інклюзивних та ефективних фінансових екосистем.

Підсумковий висновок документа носить принципово методологічний характер: оскільки вплив цифрових інновацій на фінансове здоров'я залишається емпіричним питанням, що варіює залежно від контексту, єдина надійна стратегія регуляторів полягає в удосконаленні системи вимірювання — запровадженні дезагрегованих індикаторів фінансового здоров'я, що поєднують об'єктивні та суб'єктивні метрики. BIS прямо застерігає: без паралельних інвестицій у цифрову грамотність, доступний дизайн продуктів і надійні канали підтримки цифрова трансформація ризикує поглиблювати наявні нерівності, а не долати їх.

Ефективний доступ до інформації про бенефіціарну власність: рекомендації Open Ownership щодо дизайну режимів доступу [3]

Документ організації Open Ownership, підготовлений Джулі Ріале та Тімоном Кіпе у квітні 2026 року, становить вичерпне методологічне керівництво для урядів, що впроваджують або вдосконалюють системи прозорості бенефіціарної власності (Beneficial Ownership Transparency, BOT). Документ позиціонує ефективний доступ до даних про КБВ як принципово двоякий концепт: орієнтований на користувача (user-centred) — здатний задовольнити реальні потреби різноманітних суб'єктів у використанні інформації — та відповідальний (responsible) — такий, що дотримується прав на приватність і захист персональних даних і здатний витримати судові виклики. Документ виходить з основоположної тези, що режим доступу визначає результативність усієї реформи BOT: без продуманого, диференційованого доступу реєстри залишаються формальними структурами, не здатними досягти своїх декларованих регуляторних цілей.

Центральним нормативним контекстом документа є рішення Суду ЄС у справі Sovim від листопада 2022 року, яке кваліфікується як переломний момент у глобальних дискусіях щодо доступу до даних про КБВ. Суд визнав, що невибіркове надання широкому загалу доступу до відомостей про бенефіціарних власників є незаконним втручанням у право на приватність і захист персональних даних, незалежно від подальшого використання таких відомостей і навіть без настання реальної шкоди для суб'єктів даних. Принципово важливо, що Суд відхилив аргументацію директиви AMLD5 щодо того, що публічний доступ «може сприяти» або «допомагав би» боротьбі з ВК/ФТ, як недостатньо переконливе обґрунтування суворої

[3] https://oo.hacdn.io/media/documents/oo-briefing-effective-access-2026.04.pdf

необхідності обмеження приватності. Водночас у рішенні прямо підтверджено, що широке коло суб'єктів поза державним сектором — журналісти-розслідувачі, організації громадянського суспільства, суб'єкти, які вступають в угоди з компанією, — мають законний інтерес в отриманні доступу до інформації про КБВ. Це рішення категорично спростувало поширену позицію, згідно з якою боротьба з ВК є виключно прерогативою державних органів.

Методологічний каркас документа побудований навколо трирівневої підготовчої роботи, що передує проектуванню режиму доступу. По-перше, чітке визначення цілей реформи — від вузьких (виключно ПВК) до широких (демократична підзвітність, публічні закупівлі, управління природними ресурсами). Документ наводить позитивні приклади Канади (ціль — «запобігання незаконній діяльності, підвищення довіри до корпоративних інституцій та забезпечення функціонування ринку») та Острову Святої Єлени, що закріпив чотири широкі цілі у законодавстві. По-друге, аналіз правових рамок: у більшості юрисдикцій дані КБВ становлять персональні дані та підпадають під дію відповідного законодавства. При цьому документ фіксує принципові відмінності у визначенні персональних даних: тоді як Регламент ЄС GDPR використовує широке визначення, провінція Онтаріо прямо виключає з його дії інформацію про особу, що діє у комерційній або офіційній якості. По-третє, ідентифікація та дослідження користувачів — підхід, що дозволяє імплементаторам обґрунтовувати права доступу на основі конкретних потреб, а не широких припущень.

Документ систематизує типологію користувачів, виокремлюючи чотири категорії. Урядові користувачі охоплюють реєстраторів, правоохоронні органи з мандатом щодо цілей ВОТ, регуляторів, закупівельні організації та суб'єктів, що відповідають за видачу ліцензій або контроль у стратегічних секторах. Приватний сектор потребує доступу для виконання статутних зобов'язань у межах ПВК/ФТ, проведення належної перевірки та управління ланцюжком постачань, а також контролю відповідності санкційним вимогам. Особлива роль відводиться комерційним постачальникам рішень для роботи з даними, які усувають технічні та операційні бар'єри доступу — зокрема транскордонні. Організації громадянського суспільства (НПО, медіа, академічна спільнота) забезпечують наглядові та підзвітні функції в демократичних суспільствах: документ демонструє, що багато правоохоронних органів активно використовують їхні розслідування як джерело оперативної розвідки. Нарешті, окрема категорія «інших» охоплює, наприклад, орендарів (що мають підстави знати власника компанії-орендодавця) та потенційних інвесторів.

Проектування рівнів (шарів) доступу є аналітичним ядром документа. Кожен рівень визначається трьома параметрами: хто має доступ і для яких цілей (разом із механізмами автентифікації), які функції зручності використання забезпечуються, та які захисні заходи застосовуються. Документ наполягає на тому, що система з двох і більше рівнів дозволяє знайти більш тонкий баланс між доступом і приватністю. Публічний доступ (як у Вірменії, Еквадорі, Нігерії та Великій Британії) найефективніший для усунення тертя і найбільш інклюзивний, оскільки охоплює користувачів, які не вписуються в жодну визначену категорію. Проте Транспаренсі Інтернешнл задокументувала, як дивергентні реалізації AMLD4/5 у державах-членах ЄС призвели до хаотичної транскордонної системи з різними визначеннями, процедурами та строками обробки. Для юрисдикцій, що впроваджують доступ на підставі законного інтересу (Legitimate Interest Access, LIA), документ формулює конкретні вимоги до операціоналізації: попереднє визначення груп користувачів за видом діяльності (а не за регуляторним статусом — наприклад, «журналістська діяльність», а не «зареєстрований журналіст»), ненадмірно обтяжливі процедури подання заявок, взаємне визнання у межах юрисдикцій (як це передбачає AMLD6), чіткі строки обробки (AMLD6 встановлює 12 робочих днів) та процедури оскарження.

У частині функцій зручності використання (usability features) документ спирається на розроблену Open Ownership рамкову методологію та диференціює чотири виміри: обсяг (scope)

— охоплення всіх юридичних форм, включаючи трасти та інші правові утворення, що традиційно виключалися; зміст (content) — надійні ідентифікатори осіб та компаній; доставка (delivery) — структуровані формати даних (JSON, CSV, XML), API-доступ, масові завантаження; пошук (search) — можливість пошуку за назвою компанії, ім'ям бенефіціарного власника та іншими параметрами. Кейс Норвегії ілюструє, як суто технічна прогалина — можливість пошуку лише за номером компанії, але не за ім'ям бенефіціарного власника, та обмеження до одного запиту за часовий проміжок через API — суттєво обмежує здатність проводити системний крупномасштабний аналіз. Кейс Transparency International France демонструє, як відсутність API для масових завантажень змусила дослідників вручну обробляти п'ять мільйонів веб-сторінок при дослідженні нерухомості.

Захисні заходи документ розглядає в єдиному контексті з дизайном рівнів: журнали доступу та аудиторські сліди — обов'язкові для обмежених рівнів, особливо щодо великих масивів чутливих даних; умови використання — для закріплення обмеження цілей та запобігання зловживанням; режими захисту — для осіб, відкритих до непропорційних ризиків. Документ приділяє значну увагу забороні розкриття інформації про особу, яка здійснила запит, бенефіціарному власнику (anti-tip-off provision): AMLD6 та законодавство Люксембургу прямо забороняють розкриття особи запитувача, дозволяючи розкривати лише його функцію або професію. Британські Віргінські Острови автоматично повідомляють компанію лише про юридичну особу, що подала запит — але не конкретну фізичну особу. Окремо підкреслюється, що режим захисту персональних даних, за якого особи, що перебувають під непропорційним ризиком (наприклад, жертви переслідувань або члени релігійних меншин), можуть подати заявку про захист певних полів до публікації, є не

Висновки:

- **Рішення CJEU у справі Sovim (2022) та впровадження AMLD6 фактично змінюють операційну модель KYC/CDD для СПФМ, що працюють в юрисдикціях ЄС:** підрозділи комплаєнсу зобов'язані формалізувати процедури отримання доступу до даних КБВ через механізм LIA або укласти угоди з комерційними постачальниками даних, оскільки публічний доступ до реєстрів суттєво обмежено, а надійні альтернативні джерела верифікації бенефіціарної власності є прямою вимогою Рекомендації FATF 24.
- **12-денний строк обробки запитів за AMLD6 (порівняно з 8 тижнями за режимом UK Trust Registration Service) свідчить про критичну нерівність у часі доступу між юрисдикціями:** СПФМ, що проводять транскордонні розслідування або обслуговують компанії з КБВ нерезидентом, мають завчасно налагодити інфраструктуру API-з'єднань або агрегаторів даних для мінімізації затримок у процесах EDD та розслідування підозрілої діяльності.
- **Кейс Чилі (зниження виявлених конфліктів інтересів у публічних закупівлях на 69% після інтеграції BOT-даних у систему скринінгу) є прямим аргументом для СПФМ на користь розширення профілювання контрагентів за межі базових KYC-перевірок** — зокрема автоматизованого скринінгу ланцюжків власності на предмет зв'язків з PEP, підсанкційними суб'єктами та юрисдикціями підвищеного ризику.
- **Системні прогалини транскордонного доступу до даних BOT (відсутність уніфікованих ідентифікаторів для entity resolution між реєстрами різних юрисдикцій) вимагають від СПФМ формування внутрішніх баз накопиченої інформації** про складні транснаціональні структури власності та визначення чітких процедур ескалації до ПФР у справах, де встановлення КБВ неможливе через інформаційну асиметрію.

просто передовою практикою, але й правовою вимогою відповідно до позиції Генерального адвоката ЄС.

Транскордонний вимір доступу виявляється системним бар'єром для ефективності реформ BOT, що окремо систематизується у документі. Ретроспективний аналіз фіксує: більшість механізмів обміну інформацією між юрисдикціями (Egmont Group, ARIN, Interpol) є за запитом і повільними; виняток становить Автоматичний обмін інформацією (AEOI) для цілей оподаткування, що охоплює більшість юрисдикцій, але обмежений лише податковими органами. Найбільш перспективним інструментом залишається система BORIS (Beneficial Ownership Registers Interconnection System), що передбачена пакетом AMLD6 і забезпечуватиме єдиний інтерфейс для доступу до реєстрів усіх 27 держав-членів ЄС для кваліфікованих користувачів. Надійні ідентифікатори для розв'язання проблеми ототожнення осіб та компаній між юрисдикціями (entity resolution) залишаються критичним невирішеним технічним завданням, яке наразі частково вирішується комерційними постачальниками та неурядовими організаціями з обробки даних.

Додаткові міркування документа охоплюють три аспекти. По-перше, плата за доступ: усі категорії користувачів підтвердили, що вартість доступу створює бар'єри для ефективного використання; допустимою є диференційована модель (безкоштовний публічний доступ плюс платні преміальні продукти для комерційних суб'єктів, як у Великій Британії), але плата не повинна використовуватися як засіб мінімізації втручання у приватність. По-друге, моніторинг та оцінка впливу: систематичне документування використання реєстрів є необхідним як для ітеративного вдосконалення, так і для захисту режиму доступу від правових викликів — що підтверджується дослідженнями у Чилі, де впровадження BOT у закупівлях призвело до зниження кількості виявлених конфліктів інтересів на 69% за два роки. По-третє, закріплення балансу в правових рамках: система має бути заснована на законодавстві, а не нав'язана ним — принцип, що вимагає гнучкого, технологічно нейтрального законодавства, яке визначає параметри, а не специфікації системи.

Еволюція кіберзагроз — шифрування, проксі та AI на службі кіберзлочинності [4]

Звіт Europol являє собою комплексний документ, що охоплює структуру та динаміку кіберзлочинності в ЄС. Назва видання 2026 року — «Як шифрування, проксі та штучний інтелект розширюють кіберзлочинність» — точно відображає центральну тезу документа: формування ширшого «розриву у швидкості» (velocity gap) між можливостями кіберзлочинців і правоохоронних органів (ПО). Цей розрив обумовлений тим, що комерційно доступні інструменти AI дозволяють злочинцям знизити бар'єри входу, масштабувати операції та здійснювати злочини без прямої участі в них — тоді як правоохоронці стикаються з системними перешкодами: наскрізним шифруванням (E2EE) у комунікаційних платформах, юрисдикційними бар'єрами та обмежувальними або неузгодженими режимами збереження даних у провайдерів.

Перший структурний блок звіту присвячений інфраструктурним «сприяючим факторам» кіберзлочинності. Dark web демонструє трансформацію: загальні маркетплейси фрагментуються і поступаються місцем спеціалізованим платформам із вужчими пропозиціями (інструменти для шахрайства, брокерський доступ, послуги зловмисного програмного забезпечення), а середня тривалість їх існування скорочується. Показовим

[4] https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf

прикладом є ліквідація у червні 2025 року маркетплейсу Archetyp Market (понад 600 тисяч користувачів, обсяг транзакцій понад 250 млн євро, 17 тисяч оголошень) у ході скоординованої операції Europol та Eurojust за участі п'яти країн. Уже у липні 2025 року новий маркетплейс BlackOps запустився, оголосивши 41 942 товарні позиції, і до листопада 2025 року розширився до 63 979 — підтверджуючи гіпотезу про мобільність та адаптивність кримінального ринку. У сфері хостингу злочинні мережі переходять від стандартного BPH (bullet-proof hosting) до власної пропрієтарної інфраструктури, усуваючи необхідність реагувати на судові ордери. Паралельно резидентні проксі-сервіси маскують зловмисний трафік під звичайний інтернет-трафік домашніх пристроїв у різних країнах, значно ускладнюючи атрибуцію.

Криптовалюти відіграють у кіберзлочинності роль, що далеко вийшла за межі платіжного засобу: вони стали самостійним інструментом обфускації у ширшому ландшафті організованої злочинності. Документ фіксує три ключові тренди 2025 року. По-перше, зростання використання «монет конфіденційності» (privacy coins) у схемах відмивання коштів від атак-вимагачів: ці активи резистентні до інструментів блокчейн-відстеження. По-друге, chain-hopping через блокчейн-мости дозволяє злочинцям миттєво переміщувати активи між різними блокчейн-мережами, ускладнюючи відстеження; технологія є легітимною та необхідною для інтероперабельності блокчейнів, що ускладнює регуляторну реакцію. По-третє, «mixing-as-a-service»: смарт-контрактні міксери та децентралізовані біржі (DEX) з автоматизованими маркет-мейкерами (AMM) витіснили повільні coinjoin-сервіси для суб'єктів, що потребують швидкого ввиведення незаконних коштів в офіційну фінансову систему. Знаковим прикладом є ліквідація у листопаді 2025 року сервісу Cryptomixer: з моменту запуску у 2016 році через нього пройшло понад 1,3 млрд євро в біткоїнах; під час операції вилучено понад 12 терабайт даних та активи на суму понад 25 млн євро.

Четвертий вимір кіберзлочинної інфраструктури — автоматизація та AI — документ характеризує як такий, що суттєво трансформує оперативні можливості кримінальних мереж. Dark web залишається хабом для розробки зловмисних великих мовних моделей (LLM), з яких усунені етичні обмеження та фільтри легітимних комерційних рішень. Для підвищення точності та якості кримінального результату моделі налаштовуються на зразках зловмисного програмного забезпечення, керівництвах з реалізації шахрайських схем та методиках ухилення від виявлення. Перспективу, на яку документ звертає особливу увагу, становить поява агентного AI (agentic AI) — систем, здатних до автономного оперативного планування і виконання без прямої участі людини, — що у разі широкого кримінального впровадження здатна підняти загрозу онлайн-шахрайства до безпрецедентних масштабів.

Онлайн-шахрайські схеми (Online Fraud Schemes, OFS) характеризуються у документі як найбільш швидкозростаючий сегмент організованої злочинності у 2025–2026 роках, з тенденцією до переходу від моделі масштаб/різноманіття до моделі швидкість/операційна безпека. Серед значущих розробок виділяється промислова еволюція SIM-боксів: у справі, що розслідувалася у 2025 році, латвійська мережа з семи осіб експлуатувала інфраструктуру з 1 200 SIM-бокс-пристроїв, що обслуговували 40 000 SIM-карт із телефонними номерами, зареєстрованими на осіб з понад 80 країн, і на її основі було створено понад 49 мільйонів онлайн-акаунтів. Поряд зі стандартним фішингом зафіксовано зростання застосування IMSI-перехоплювачів (IMSI catchers) та SMS-бластерів, що примусово переключають пристрої на протокол 2G, фактично виводячи кримінальну активність «поза радаром» комерційних телекомунікаційних операторів і руйнуючи традиційні ланцюжки доказів. Атаки-relay на платіжні термінали (terminal-to-terminal та card-to-terminal) протягом 2025 року зростали у ЄС. Кража цифрових активів через зловмисне ПЗ (дрейнери) оформилася у повноцінну систему crime-as-a-service (CaaS), а зловмисна реклама (malvertising) на великих онлайн-платформах (VLOP) дозволяє злочинним афілійованим маркетологам індустріально таргетувати жертв.

Сегмент програм-вимагачів (ransomware) залишається домінуючою кіберзагрозою у ЄС. У 2025 році Europol ідентифікував понад 120 активних ransomware-брендів, кількість атак стабільно зростає. Документ фіксує паралельно дві трансформації ринку: фрагментацію брендів (операції є короткотривалими, часто ребрендуються) і консолідацію через коаліції (у вересні 2025 року оголошено альянс DragonForce, LockBit і Qilin). Фокус вимагання зміщується від шифрування до загрози публікації вкрадених даних — оскільки сучасні підприємства краще підготовлені до втрати даних, ніж до репутаційних та правових наслідків публічного витоку. Серед значущих операторів 2025 року: Qilin (розширені DDoS-можливості, автоматизація атак на SSL VPN Fortinet, 80–85% прибутку для афіліатів), Akira (розширення на віртуалізовану інфраструктуру), DragonForce (новаторська послуга аналізу ексфільтрованих даних та підготовки індивідуалізованих вимагальницьких матеріалів — більше 20% від суми викупу), LockBit 5.0 (оновлені антифорензичні механізми, цінова доступність — близько 400 євро). Критичний структурний ризик, що окремо аналізується, полягає у розмитті меж між комерційними кіберзлочинцями та державними гібридними акторами: останні використовують кримінальні мережі як опосередковані інструменти для дестабілізуючих операцій, включаючи DDoS-атаки (операція Eastwood проти NoName057(16) у липні 2025 року), — перетворюючись лише на ще одних клієнтів у системі CaaS-економіки.

Окремий аналітичний розділ документа присвячено сексуальній експлуатації дітей онлайн (CSAM), де технологічна трансформація набула найбільш тривожних форм. Кількість звітів CyberTips NCMEC щодо фінансового вимагання, пов'язаного з дітьми, зросла на 70% у першому півріччі 2025 року порівняно з тим самим періодом 2024-го. Ліквідована у 2025 році стримінгова

Висновки:

- **Масштабне поширення privacy coins, chain-hopping через блокчейн-мости та DEX для відмивання доходів від програм-вимагачів вимагає від СПФМ негайного присвоєння транзакціям через DEX та блокчейн-мости статусу підвищеного ризику у системах транзакційного моніторингу:** традиційні порогові правила є неефективними щодо автоматизованих мікроплатежів через міксери, натомість аналіз мережевих зв'язків гаманців і моніторинг on-chain адрес, ідентифікованих Europol, є обов'язковими компонентами оновленої процедури скринінгу VASP-контрагентів.
- **Встановлена гібридизація між комерційними кіберзлочинними мережами та державними акторами (проросійські групи NoName057(16), DragonForce, Qilin) означає, що платежі у криптовалюті, пов'язані з адресами гаманців цих груп, є потенційними порушеннями санкційного режиму:** підрозділи фінансової розвідки зобов'язані оновити санкційні сценарії для охоплення криптоадрес, визначених у відкритих даних Europol та OFAC, а також запровадити моніторинг транзакцій через необанки з прискореним онбордингом, що може використовуватися як вектор потенційного обходу KYC.
- **Промислова зрілість CaaS-ринку — SIM-ферми, дрейнери як повноцінна послуга, голосові AI-боти для попереднього відбору жертв — означає, що СПФМ мають адаптувати сценарії моніторингу до виявлення мікрошахрайських патернів:** повторювані невеликі перекази на адреси DeFi-протоколів або необанків, розосереджені за часом нижче порогів звітності, є ключовими індикаторами структурованих шахрайських схем, що вимагають окремих правил виявлення.
- **Зростання монетизації CSAM через криптовалютні підписки та токен-моделі є прямою вимогою до СПФМ щодо впровадження спеціалізованих сценаріїв моніторингу:** транзакції до відомих криптоадрес, пов’язаних із CSAM (що публікуються ПО у відкритих базах takedown-операцій) мають автоматично тригерити ескалацію SAR відповідно до зобов'язань СПФМ за національним законодавством та стандартами FATF щодо злочинів проти дітей.

платформа Kidflix налічувала 1,8 мільйона зареєстрованих користувачів і близько 80 тисяч завантажених відео; розслідування охопило понад 35 країн і призвело до ідентифікації близько 1 400 підозрюваних та порятунку 39 дітей. Фундаментальним новим ризиком, що детально аналізується, є AI-генерований CSAM (синтетичний CSAM): масова доступність генеративних AI-інструментів призводить до промислового масштабування виробництва матеріалів із сексуальним насильством над дітьми, одночасно ускладнюючи ідентифікацію реальних жертв та порушуючи регуляторні механізми, розроблені для органічного контенту. E2EE-платформи стали основним середовищем для груп з обміну CSAM: велика доступність для необізнаних у технологіях злочинців у поєднанні з фактичною непрозорістю для правоохоронців формує якісно новий рівень загрози. Мережа The Com, що складається переважно з дітей віком від 8 до 17 років, поєднує в собі CSE, кібератаки, вимагання, насильство та violent extremism, становлячи один із найскладніших оперативних та аналітичних викликів для правоохоронців у кількох країнах-членах ЄС.

Перспективна оцінка документа формулює чотири стратегічні пріоритети. По-перше, інвестування ПО в AI-можливості для превентивного виявлення та розуміння еволюції загроз при дотриманні основоположних прав і захисту даних. По-друге, адвокатування регуляторних рамок для врегулювання зловживань E2EE-платформами у поєднанні з розширенням ініціатив з публічно-приватного партнерства з постачальниками онлайн-послуг. По-третє, гармонізація політик збереження даних — не лише щодо строків, але й щодо того, які саме дані зберігаються — у цифрових постачальників послуг для забезпечення своєчасного доступу слідчих. По-четверте, забезпечення доступу до масивів даних, що зберігаються у постачальників онлайн-послуг, в якості передумови ефективного виявлення та переслідування злочинців. Документ завершується принциповою тезою: здолати «розрив у швидкості» технологічними засобами необхідно, але недостатньо — без поглибленої публічно-приватної взаємодії правоохоронці не матимуть доступу до даних, без яких ідентифікація кіберзлочинців залишається неможливою.

Звіти окремих інституцій та експертів

Анатомія транснаціональної злочинності долини Меконгу [5]

Звіт, підготовлений Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC) у партнерстві з урядом Австралії, пропонує зріз поточних кримінальних тенденцій у п'яти країнах регіону — Камбоджі, Лаосі, М'янмі, Таїланді та В'єтнамі.

Цей документ є глибокою діагностикою взаємопов'язаних системних проблем, які перетворюють долину Меконгу на унікальний простір, де легальна та нелегальна економіки не просто співіснують, а живлять одна одну. Організована злочинність тут ніколи не виникає з якоїсь однієї причини — натомість вона є наслідком складної мережі чинників: слабкості державних інституцій, корупції, стрімкого розвитку інфраструктури, значних обсягів іноземного капіталу, особливо китайського, та поступового, але неухильного звуження простору для незалежного громадянського суспільства й медіа.

[5] https://globalinitiative.net/wp-content/uploads/2026/04/Mekong-Risk-Monitor-Issue-2-April-2026.pdf

Кожен із чотирьох основних сюжетів звіту — аналіз лаоської провінції Кхаммуан як «гарячої точки» злочинності, дослідження ринку наркотиків у Камбоджі через інтерв'ю зі споживачами, феномен так званих банківських «мулів» у Таїланді та нова хвиля обмежень для незалежної преси у В'єтнамі — ілюструє цю багатовимірну реальність. Розгляньмо кожен із цих випадків докладно, щоб зрозуміти, як локальні вразливості перетворюються на транснаціональні загрози.

Почнімо з Лаосу, а точніше — з провінції Кхаммуан, яка у звіті постає як своєрідний «вузол» кримінальної активності. Географічно Кхаммуан розташована в одному з найвужчих місць лаоської території, утворюючи своєрідний сухопутний міст між Таїландом на заході та В'єтнамом на сході. Через провінцію проходить національна траса №12, яка з'єднує місто Тхакхек на березі Меконгу (навпроти тайської провінції Накхонпханом) із в'єтнамським прикордонним переходом Чало в провінції Куангбінь.

У червні 2025 року тайська влада оголосила про початок робіт над новою трасою. І хоча офіційно це подається як крок до економічної інтеграції, звіт чітко вказує на зворотний бік медалі: будь-яке покращення інфраструктури в цьому регіоні неминуче полегшує логістику не лише для легальних вантажів, а й для наркотрафіку, контрабанди диких тварин та інших видів нелегальної діяльності. Статистика це підтверджує. Протягом 2025 року в'єтнамські прикордонники затримали на цьому маршруті чотирьох громадян Лаосу та трьох в'єтнамців, які намагалися перевезти понад 500 кілограмів кристалічного метамфетаміну, 120 тисяч таблеток метамфетаміну, 3 кілограми героїну та 600 кілограмів кетаміну. Тайські правоохоронці також регулярно перехоплюють великі партії наркотиків із Кхаммуану. Показовим є випадок 14 січня 2026 року, коли на річці Меконг було вилучено мільйон таблеток метамфетаміну, а двох громадян Лаосу заарештовано.

Водночас самі лаоські правоохоронці не сидять склавши руки: за даними Управління з боротьби з наркотиками провінції Кхаммуан, з червня по грудень 2025 року вони вилучили понад 1,2 мільйона таблеток метамфетаміну та заарештували 185 осіб, причетних до наркоторгівлі та перевезень. Однак, як слушно зазначають автори звіту, ці успіхи слід розглядати в контексті глибокої корупції, яка пронизує лаоські правоохоронні органи. У 2025 році Лаос посів 109-те місце зі 182 країн Індексу сприйняття корупції Transparency International. Одним із ключових драйверів корупції є мізерна заробітна плата поліцейських, яка на початковому рівні становить приблизно 3 мільйони кіпів, або близько 140 доларів США на місяць. В умовах високої інфляції цієї суми просто не вистачає на життя, що робить співробітників надзвичайно вразливими до пропозицій хабарів з боку злочинних синдикатів.

Але наркотики — це лише частина кримінальної екосистеми Кхаммуан. Провінція також є важливим транзитним хабом для незаконної торгівлі дикими тваринами. Лаос, який межує з ключовими країнами-споживачами та експортерами диких тварин — Камбоджею, Таїландом, М'янмою, В'єтнамом і Китаєм, — десятиліттями використовується як перевалочний пункт. Попри те, що Лаос є стороною Конвенції про міжнародну торгівлю видами дикої фауни та флори, що перебувають під загрозою зникнення (CITES), з 2004 року, обмежені спроможності правозастосовних органів дозволяють цьому бізнесу процвітати.

У 2018 році тайська влада заарештувала в Накхонпханомі (навпроти Кхаммуан) одного з найвідоміших у світі контрабандистів диких тварин Бунчая Бача, якого в 2023 році засудили за організацію мережі з переміщення рогів носорогів та слонової кістки між Лаосом, Таїландом і В'єтнамом. Того ж року лаоська влада вилучила в Кхаммуані три тигрові туші, які прямували до В'єтнаму тією самою трасою №12, а тайські прикордонники в Буенгкані перехопили чотирьох тигренят вартістю 42 тисячі доларів, які, ймовірно, походили з нелегальних ферм із розведення у провінціях Кхаммуан і Болікхамсай. Крім того, в Накхонпханомі було конфісковано 930 виробів зі слонової кістки, також контрабандою переправлених із Кхаммуан. На території самої провінції

розташовані два національні парки — Гін Нам Но (об'єкт Всесвітньої спадщини ЮНЕСКО) та Накхай-Нам Тхун. Попри охоронний статус, незаконні вирубки лісу та браконьєрство там залишаються серйозною проблемою. І знову ж таки, інфраструктурні проєкти відіграють роль каталізатора.

Третя, і, мабуть, найбільш тривожна тенденція, пов'язана з Кхаммуан, — це поширення кібершахрайських центрів (cyber scam operations). Раніше епіцентром цієї індустрії в Лаосі вважалася Спеціальна економічна зона «Золотий трикутник» із казино Kings Romans, заснована санкціонованим США китайським бізнесменом Чжао Веєм. Однак, як свідчать дані звіту, тепер такі операції вкорінюються і в Кхаммуані. У 2025 році там було заарештовано кількох громадян Лаосу та іноземців, причетних до онлайн-шахрайства (хоча деталі слідства не розголошуються). У грудні 2025 року поліція Тхакхека підтвердила, що група китайських громадян намагалася використати два місцеві готелі для створення скам-центрів.

Хоча ці випадки поки що менші за масштабами, ніж індустріальні скам-центри в Камбоджі чи М'янмі, сама тенденція до дифузії викликає серйозне занепокоєння. Особливу увагу привертає іноземна, насамперед китайська, інвестиційна активність у регіоні. Під час візиту в грудні 2025 року дослідники GI-TOC спостерігали будівництво багатоквартирних комплексів та іншої житлової забудови, пов'язаної з прибуттям іноземних інвесторів. Примітно, що це будівництво відбувається на землі, де раніше розташовувалися державні установи, що порушує питання про те, які вигоди отримує місцева влада і чому саме цю територію було виділено інвесторам.

Друга велика тема звіту переносить нас до Камбоджі, де дослідники GI-TOC провели унікальне польове дослідження, опитуючи споживачів наркотиків у трьох різних локаціях: столичному Пномпені, прибережному місті Сіануквіль та сільській провінції Пурсат. Метою цього дослідження було заповнити колосальні прогалини в офіційній статистиці, яка здебільшого базується на даних про вилучення наркотиків та арешти, а отже, відображає не стільки реальну ринкову активність, скільки ефективність (або неефективність) правоохоронних органів. У країні, де правоохоронна система є недофінансованою, а іноді й свідомо обмеженою, такі дані можуть бути не просто неповними, а й відверто оманливими.

Головною метою було зрозуміти, як географія впливає на доступність, ціни та практики споживання. Найпомітнішим результатом стало абсолютне домінування кристалічного метамфетаміну, відомого як «лід». Він є найпоширенішим, найлегше доступним і найдешевшим наркотиком для всіх категорій населення — незалежно від віку, статі чи професії. Жоден з опитаних не зміг назвати вагу дози в грамах або міліграмах. Замість цього кількість наркотику визначалася виключно через ціну та попередній досвід. Мінімальною сумою покупки є приблизно 4 долари США, але це дуже маленька кількість. Споживачі часто змушені об'єднуватися: вони складаються по 10, 15 або 20 доларів, купують наркотик на групу, а потім ділять його між трьома-чотирма особами.

Менш поширеними, але також присутніми на ринку є таблетки метамфетаміну (відомі як WY або ya ba) та кетамін. WY сприймають як додатковий наркотик, який іноді додають до кристалічного метамфетаміну для посилення ефекту, але його відносно висока ціна — близько 5 доларів за таблетку — часто робить його занадто дорогим для повсякденного вживання. Кетамін, своєю чергою, використовується переважно в нічних клубах Пномпеня та Сіануквіля. Низька вартість кристалічного метамфетаміну, яка збігається із загальнорегіональною тенденцією зниження цін на синтетичні наркотики в Східній та Південно-Східній Азії до найнижчого рівня за десятиліття, робить його доступним навіть для найменш оплачуваних працівників Камбоджі. Цікаво, що, хоча готівка залишається основним засобом платежу, деякі споживачі повідомили про використання онлайн-банкінгу, найчастіше через додаток місцевого банку ABA, що дозволяє здійснювати швидші та більш непомітні транзакції.

Географічна диференціація виявилася надзвичайно промовистою. Сіануквіль, колись тихе рибальське містечко, а тепер місто хмарочосів, казино і великої кількості іноземців, описаний споживачами як середовище з високою доступністю та низькими цінами. Кристалічний метамфетамін там можна придбати приблизно за 5 доларів за умовну одиницю. Попит стимулюється казино, розважальними закладами, будівельними майданчиками та високою плинністю робочої сили. Транзакції є частими, але обережними, вони відбуваються через соціальні мережі. Продавці, як правило, не бажають мати справу з незнайомцями, побоюючись арешту чи обману. З часом постійні клієнти можуть отримувати трохи більшу кількість або гнучкіші ціни. Деякі споживачі самі стають дрібними дилерами, формуючи невеликі мережі для закупівлі та розповсюдження наркотиків на суму близько 300 доларів одночасно, які розпродаються протягом 10–14 днів залежно від попиту.

У Пномпені наркотики, особливо кетамін, широко продаються в клубах, барах та караоке-закладах. Як і в Сіануквілі, новим покупцям потрібне представництво, оскільки продавці рідко мають справу з незнайомцями. Деякі споживачі в столиці стверджували, що дистриб'ютори діють під захистом поліції та високопосадовців, які нібито отримують хабарі за попередження про рейди або забезпечення безпеки. Вони також стверджували, що самі поліцейські та військові купують і вживають наркотики.

На противагу цьому, провінція Пурсат є набагато більш обмеженим середовищем. Там наркотики важче дістати, вони дорожчі, а сам процес купівлі є більш прихованим. Продавці виявляють значно більше обережності.

Різниця в діяльності правоохоронних органів відіграє вирішальну роль. У Пурсаті дилери платять місцевій поліції від 300 до 1000 доларів на місяць за можливість безперебійно вести бізнес. Поліцейські облави там є частішими та помітнішими, що підвищує ризики для споживачів і, відповідно, ціни. У Сіануквілі, навпаки, споживачі вважають, що поліція обізнана про вживання наркотиків, але не втручається через відсутність стимулів або вигоди від арештів.

Що стосується ланцюга постачання, то споживачі мають про нього дуже обмежені знання, знаючи лише безпосереднього продавця, але не місце походження наркотику. Більшість продавців і споживачів є громадянами Камбоджі, що суперечить поширеному сприйняттю, ніби місцевий ринок наркотиків керується переважно іноземцями. Офіційні дані це підтверджують: із 26 421 особи, затриманої за наркозлочини в 2025 році, лише 1118 були іноземцями.

Третя велика тема звіту заглиблюється у світ фінансових операцій, а точніше — у феномен так званих «мул-акаунтів» (mule accounts) у Таїланді. Це банківські рахунки або електронні гаманці, які використовуються для переказу або зберігання незаконно отриманих грошей. Злочинні угруповання використовують корпоративні рахунки, купують існуючі рахунки або платять людям за відкриття нових. У деяких випадках жертв обманюють або примушують надати доступ до своїх рахунків.

Масштаби цього явища в Таїланді вражають. Між червнем 2024 та лютим 2025 року під наглядом центрального банку країни було заморожено понад 2 мільйони підозрілих рахунків, що належали більш ніж 150 тисячам осіб. За даними Міністерства цифрової економіки та суспільства, з жовтня 2023 року по березень 2025 року у зв'язку з мул-акаунтами було заарештовано 5399 осіб.

Хоча саме явище не є новим, інновації у фінансовій сфері, зокрема повсюдне поширення онлайн-банкінгу та банківських додатків, відкрили двері для його індустріалізації. Купівля та продаж мул-акаунтів стали надзвичайно простими та професійними. Рахунки відкрито продаються та рекламуються в інтернеті, зокрема в соціальних мережах. Повідомляється, що люди продають свої особисті банківські рахунки за ціною від 1500 до 2000 тайських батів (приблизно 47–63 долари США). Інші здають свої рахунки в оренду, іноді на подобовій основі.

Також продаються банківські картки та SIM-картки, зареєстровані та прив'язані до мобільних банківських додатків.

Хоча більшість рахунків використовується для дрібних «мулів», колишній власник сайту онлайн-азартних ігор пояснив, що деякі рахунки використовуються для великих транзакцій, а власники рахунків можуть заробляти значні суми. У таких випадках ціна купівлі рахунку може стартувати від 30 тисяч батів (приблизно 946 доларів), приносячи власнику щомісячний прибуток у розмірі 5–10 тисяч батів (157–315 доларів). Однак часто рахунки отримують через обман або маніпуляції.

Особливу тривогу викликає еволюція цього явища у відповідь на регуляторні заходи. У березні 2023 року Банк Таїланду та Асоціація тайських банків запровадили біометричну верифікацію (сканування обличчя) для всіх мобільних банківських транзакцій, що перевищують 50 000 батів (близько 1577 доларів), щоб боротися з мул-акаунтами та запобігати кіберкрадіжкам. Однак злочинці швидко знайшли обхідні шляхи. По-перше, все ще можна здійснювати кілька транзакцій на суму до 200 000 батів на день (близько 6300 доларів), минаючи вимогу сканування обличчя. Але набагато більш тривожним наслідком стало виникнення феномену так званих «стаєнь для мулів» (mule stables) — місць, де власників мул-акаунтів утримують під примусом, щоб ті проходили сканування обличчя для банківських додатків, дозволяючи здійснювати перекази. Жертв заманюють або вивозять до цих локацій через фальшиві оголошення про роботу в соціальних мережах. У деяких випадках людям наказують відкрити п'ять чи шість рахунків і змушують реєструвати SIM-картки, які потім прив'язують до банківських додатків.

Окрім особистих рахунків, злочинці активно використовують корпоративні мул-акаунти — рахунки, відкриті на ім'я компаній-оболонок або фіктивних підприємств. Основна перевага корпоративного рахунку полягає в тому, що він дозволяє переказувати більші суми за одну транзакцію, і для нього не потрібне сканування обличчя. Крім того, відкрити корпоративний рахунок напрочуд просто. Наприклад, Kasikorn Bank дозволяє бізнесу відкрити до п'яти рахунків, просто використовуючи верифікацію через мобільний банкінг. А Krungsri Bank пропонує послугу виїзного відкриття корпоративного рахунку, після чого клієнти можуть проводити онлайн-транзакції через мобільний банкінг після схвалення.

З огляду на високий обсяг транзакцій, що проходять через корпоративні рахунки, процеси розслідування, судового переслідування та замороження рахунків є набагато складнішими та тривалішими. Хоча тайський уряд запровадив низку заходів, включно з Центральним реєстром шахрайства (Central Fraud Registry) для обміну інформацією між банками та масовим блокуванням акаунтів, що призвело до замороження понад 3,3 мільйона рахунків до листопада 2025 року, така політика мала й серйозні негативні наслідки. Тисячі людей і малих підприємств були помилково позначені як потенційно шахрайські, що призвело до блокування їхніх рахунків. Тому, як наголошують автори, необхідно розробляти більш зважені, пропорційні та цілеспрямовані заходи, які б не карали вразливі групи населення, а зосереджувалися на всьому ланцюгу шахрайства, виявляючи як джерело операції, так і кінцеві бенефіціарні рахунки.

Нарешті, четвертий сюжет звіту звертається до В'єтнаму, де аналізується зв'язок між економічним зростанням і звуженням простору для незалежних медіа та громадянського суспільства. На перший погляд, це може здаватися внутрішньополітичним питанням, але автори переконливо доводять, що воно має пряме відношення до боротьби з організованою злочинністю та корупцією.

У грудні 2025 року Національна асамблея В'єтнаму ухвалила 51 закон та 39 резолюцій, включно з поправками до Закону про кібербезпеку та Закону про пресу, через пришвидшену процедуру, без громадських петицій чи протестів. Ці зміни надають владі широкі повноваження керувати IP-адресами, зобов'язують інтернет-провайдерів надавати IP-адреси на вимогу органів

кібербезпеки, а також дозволяють Міністерству громадської безпеки примушувати медіа та журналістів розкривати свої джерела, включно з викривачами, «для цілей розслідування, судового переслідування та винесення вироків». Переміщення цих повноважень від судів до правоохоронних органів сигналізує про більш жорстке медіа-середовище в майбутньому.

Звіт нагадує, що у В'єтнамі не завжди було так. Після дозволу на підключення до інтернету в 1997 році та економічних реформ, які включали приватизацію в медіа-секторі, на початку 2000-х років виник відносно відкритий простір для обговорення таких тем, як злочинність і корупція. Поправки до Закону про пресу 1999 та 2016 років дозволили медіа займатися прибутковою діяльністю та укладати партнерства з приватними компаніями, що надало їм певної фінансової незалежності. У період між 2013 і 2019 роками в'єтнамські онлайн-ЗМІ опублікували понад 3000 статей про понад 40 окремих корупційних інцидентів.

Однак із ухваленням Закону про кібербезпеку 2018 року та «Плану розвитку преси до 2025 року» в 2019 році цей період скінчився. План обмежив ліцензії лише установами, афілійованими з Комуністичною партією, заборонив журналам створювати новинний контент (включно з репортажами про корупцію) та призвів до закриття або ребрендингу багатьох незалежних медіа. Між 2019 і 2023 роками регулятори наклали на медіа-організації 146 штрафів, а загальна сума штрафів зросла з 450 мільйонів донгів (близько 17 тисяч доларів) у 2020 році до 2,1 мільярда донгів (близько 81 тисячі доларів) у 2023 році. У 2020 році за ґратами опинилося шестеро журналістів, у 2021-му — восьмеро.

На думку авторів звіту, звуження простору для громадянського суспільства та незалежних медіа має прямі економічні та безпекові наслідки. Без незалежної журналістики та громадського нагляду корупція залишається непоміченою. Коли громадські групи та медіа юридично позбавлені можливості висвітлювати такі випадки, злочинні мережі стають дедалі більш укоріненими, а місцева стійкість до їхнього впливу руйнується. Це, своєю чергою, підриває довіру інвесторів, для яких доступ до точної та своєчасної інформації є критичним. Як підсумовують автори, зростання економіки, безпека та відкритість не є взаємовиключними. Навпаки, просування транспарентності та підзвітності бізнесу й державних органів через збір і публікацію достовірної інформації є запорукою довгострокової стабільності та захисту національної безпеки. Лідери думок, які виробляють верифікований контент про злочинність та корупцію, не повинні стикатися з обмеженнями, а

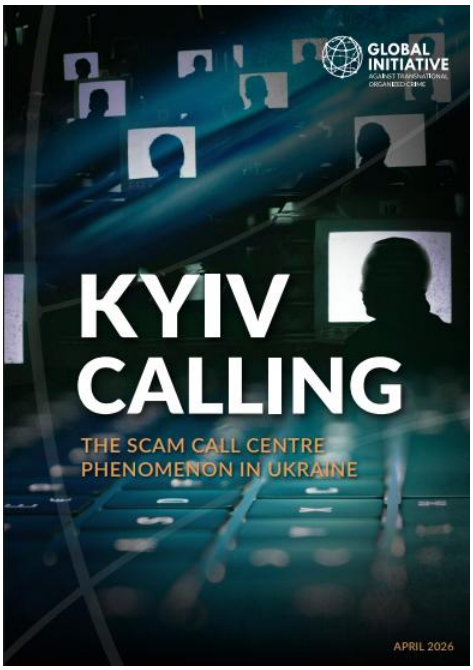
Висновки:

- **Синергія інфраструктури та злочинності:** У регіоні Меконгу розбудова транспортних коридорів та спеціальних економічних зон парадоксальним чином знижує ризики для кримінальних синдикатів, полегшуючи логістику наркотрафіку та контрабанди диких тварин.
- **Домінування метамфетаміну та його цінова доступність:** Кристалічний метамфетамін став наркотиком для найбідніших верств населення Камбоджі через рекордно низькі ціни. Споживачі орієнтуються не на вагу дози, а на вартість у кілька доларів, що свідчить про глибоку фрагментацію ринку та високу адаптивність системи розповсюдження.
- **Фінансові обмеження (біометричний контроль в банках) не зупинили злочинців**, а лише трансформували їхні методи, породивши явище «центрів для мулів» — місць примусового утримання людей для щоденного сканування обличчя в банківських додатках, що є формою сучасного рабства.
- **Звуження громадянського простору як загроза економіці:** Обмеження незалежних медіа та посилення контролю за інтернетом у В'єтнамі, хоча й подаються як заходи безпеки, насправді підривають боротьбу з корупцією та зменшують довіру інвесторів.

міжнародні технологічні компанії повинні відігравати роль у захисті таких голосів від державного тиску.

Таким чином, другий випуск звіт пропонує цілісне бачення регіону, де організована злочинність процвітає завдяки поєднанню географічних, інфраструктурних, економічних та інституційних чинників. Кримінальні мережі адаптуються швидше, ніж державні інституції, вони використовують прогалини в управлінні, корупцію та технологічні інновації на свою користь. Відповідь, як наголошується у звіті, має бути комплексною та міжурядовою, спрямованою не лише на арешти та вилучення, а й на усунення першопричин.

Як індустрія шахрайських кол-центрів стала викликом для України та світу [6]



Протягом останнього десятиліття у тіні великої війни та стрімкої цифровізації в Україні визріло явище, яке дослідники та правоохоронці дедалі частіше називають однією з наймасштабніших кримінальних індустрій сучасної Європи.

Йдеться про шахрайські кол-центри — так звані «офіси», які за оцінками аналітиків GI-TOC, станом на кінець 2025 року могли об'єднувати до 60 тисяч працівників по всій країні та генерувати до одного мільярда доларів США щомісячного доходу. Цей феномен не є унікально українським — подібні центри діють у Південно-Східній Азії, Східній Європі, Латинській Америці, — але в Україні він набув особливих рис: глибокого зв'язку з традиційною організованою злочинністю, системного захисту з боку корумпованих правоохоронців, своєрідної «патріотичної» легітимізації та, що найважливіше, здатності до блискавичної технологічної еволюції навіть на тлі повномасштабної війни.

Щоб зрозуміти масштаб, достатньо порівняти одну цифру: середні збитки від простого онлайн-шахрайства (фішингових листів або фейкових магазинів) в Україні у вересні 2024 року становили близько 15 євро, тоді як у випадку з адресним дзвінком, де з жертвою будується довірливий діалог — аж 212 євро. Саме ця різниця, яка постійно зростає, пояснює, чому бандити 1990-х, які колись займалися рекетом, тепер масово перекваліфіковуються на майстрів з соціальної інженерії.

Історичне коріння українських скам-центрів тягнеться до Ізраїлю, де в середині 2000-х років розквіт так званих «бінарних опціонів» створив цілу індустрію телефонного шахрайства. Коли ізраїльська влада в 2017 році заборонила цю практику, знання, скрипти, технології та схеми відмивання грошей мігрували до Грузії, а звідти — до України. Проте справжнім каталізатором стала російсько-українська війна. Після анексії Криму та початку збройного конфлікту на Донбасі в 2014 році Дніпро та Київ стрімко перетворилися на столиці телефонного шахрайства, а на початку 2020-х років, коли журналісти OCCRP викрили глобальну мережу Milton Group, стало зрозуміло, що йдеться не про поодинокі осередки, а про системний бізнес з міжнародними зв'язками — від Албанії та Північної Македонії до Грузії та колишніх радянських республік.

Повномасштабне вторгнення 2022 року спочатку призвело до падіння активності: шахраї, як і решта бізнесу, розгублено завмерли на кілька тижнів. Але потім стався дивовижний злам. По-

[6] https://globalinitiative.net/wp-content/uploads/2026/04/Kyiv-calling-The-scam-call-centre-phenomenon-in-Ukraine-GI-TOC-April-2026.pdf

перше, воєнний стан та посилення патрулювання зробили неможливими старі злочинні промисли (такі як вуличне шахрайство), бо вони потребують фізичної присутності на місці. По-друге, з'явилася нова, емоційно заряджена ніша: «патріотичний скам». Тисячі українських шахраїв отримали моральний дозвіл (як вони його називали — «відбілювання репутації») працювати «по росії», прикриваючись війною. Як сказав один з експертів, найрозумніші злочинці завжди використовують геополітику: не брудни там, де живеш і працюєш. Війна надала ідеальне алібі.

І все ж, попри пафосні заяви про боротьбу з ворогом, реальність виявилася куди прозаїчнішою. За даними Кіберполіції України, дзвінки до росії, навіть в 2022–2023 роках ніколи не перевищували 10-15 відсотків від загального обсягу трафіку. Решта жертв мешкали в самій Україні або країнах Європейського Союзу. Народний депутат, який працював у тимчасовій слідчій комісії Верховної Ради, прямо зазначив під час інтерв'ю дослідникам: «Колл-центру байдуже, на кому заробляти. Вони кажуть, що працюють проти росії, але насправді більшість "клієнтів" — в Україні чи ЄС». Особливо цинічним виявилося цілеспрямоване полювання на внутрішньо переміщених осіб — людей, які втратили дім, роботу, соціальні зв'язки та найбільш вразливі до маніпуляцій. Окрім того, шахраї створювали фальшиві благодійні збори на армію, пропонували «порятунок» нібито полонених родичів, обкрадали матерів загиблих військових. Цей спектр діяльності наочно демонструє, що мораль у цьому бізнесі — товар, який купується та продається залежно від кон'юнктури.

Однією з найпарадоксальніших характеристик українських скам-центрів є їхня радикальна відкритість. Всупереч уявленню про те, що злочинний бізнес ховається в підвалах чи закритих анклавах, ці «офіси» займають найкращі приміщення в ділових центрах Києва, Дніпра, Одеси, Львова, Ужгорода. Вони встановлюють скляні двері з електронними замками, камери спостереження, наймають охоронців, проводять поліграф для нових співробітників — аби відсіяти журналістів та випадкових людей. Але водночас вони активно публікують вакансії, ловлять молодь у TikTok, розклеюють флаєри на вулицях. Автори дослідження продемонстрували це на конкретному прикладі: переглянувши кілька відео одного з HR-менеджерів скам-центру в TikTok, вони змогли визначити, що дівчина працює в Оболонському районі Києва, знайшли кафе, яке вона відвідує, а потім за орієнтирами — смугастим балконам та вивісці супермаркету «Сільпо» — вирахували точну адресу офісу. За допомогою сайту з оголошеннями про оренду вони з'ясували, що на третьому поверсі бізнес-центру пропонують приміщення на 58-65 робочих місць за 12 тисяч доларів на місяць. Такі центри — не схованки, а цілком легітимні на перший погляд роботодавці.

Але за фасадом «сучасного офісу» криється жорстока і невільницька система. Вона має чітку вертикальну ієрархію. На нижньому щаблі — «холодники», які обдзвонюють потенційних жертв, діючи за готовими скриптами. Вони отримують мізерну ставку, їх легко замінити, і саме вони найчастіше залишають роботу без особливих наслідків. Над ними — «клозери» (closers), які доводять угоду до кінця, переконують жертву переказати гроші, встановити шкідливе ПЗ, продиктувати паролі. Клозери — це золотий фонд скам-центрів. Вони отримують відсоток від викрадених сум, але ціною стає особиста свобода. Колишня HR-менеджерка одного з центрів у Дніпрі розповіла дослідникам, що досвідчених клозерів, які намагаються піти, залякують, б'ють електричним струмом, «вивозять у ліс», погрожують пошкодити пальці і кінцівки.

У Дніпрі існує угруповання «Дев'ятки», яке користується особливо жорстокою репутацією: якщо ти пішов від «Дев'яток» до іншої «організації», то більше ніколи не зможеш працювати в жодному офісі — це договір, скріплений страхом. Поряд із «Дев'ятками» аналітики називають угруповання «Хімпром», яке спочатку спеціалізувалося на продажі синтетичних наркотиків, а потім перепрофілювало свої кол-центри на шахрайство. Їхні «сітки» контролюють більшість великих центрів не лише в Україні, але й, за деякими даними, у росії та країнах Азії.

Технологічний арсенал сучасного скам-центру вражає. Дослідники з GI-TOC описують цілий спектр інструментів, які раніше вважалися прерогативою спецслужб або великих корпорацій. Для підробки документів використовуються автоматизовані системи, які за секунди генерують банківські листи з філігранними печатками, підписами та реквізитами конкретної жертви. Для зламу комп'ютерів — AnyDesk, TeamViewer або навіть спеціальні застосунки для людей із вадами зору, які через зловживання перетворюються на інструменти віддаленого контролю.

До березня 2025 року, поки російська влада не заблокувала його, головним інформаційним донором для шахраїв був телеграм-бот «Око Бога» (God's Eye), який збирав великі дані з соціальних мереж, пошуковиків, відкритих баз і дозволяв одним кліком побачити паролі, картки, графік пересувань, родинні зв'язки жертви. Окрім того, за невеликі гроші на даркнеті купуються бази даних людей, схильних до азартних ігор, біржової торгівлі або надмірного кредитування — це готові мішені з підвищеним «коефіцієнтом довіри». Шахраї використовують спуфінг (spoofing) — підміну номера телефону, який висвічується на екрані жертви, так що той бачить справжній номер банку або поліції. І навіть державний застосунок «Дія», яким пишається вся країна, має переконливого фейкового двійника, що використовується для викрадення персональних даних.

Проте найбільші зміни, які описує звіт, ще попереду. Дослідники фіксують зародження нового феномену — «crime as a service», тобто злочинності як послуги. Вже сьогодні на підпільних форумах можна придбати готовий пакет для запуску власного скам-центру: скрипти дзвінків для різних країн, CRM-системи, бази контактів, інструкції з найму персоналу, а іноді — продають навіть працівників. Вартість такого «бізнесу» може становити всього кілька сотень або тисяч євро.

Але справжня революція — це штучний інтелект. Уже зараз AI-перекладачі дозволяють українському оператору, який не знає ні слова по-чеськи або японськи, вести переконливу розмову з носієм мови, використовуючи збереження інтонації та тембру. Deepfake-технології дозволяють підмінити обличчя або голос довіреної особи — наприклад, «подзвонити» від імені сина чи начальника. А голосові боти вже навчилися вести первинний діалог без участі людини, відсіваючи недовірливих і передаючи «готового» клієнта живому оператору.

На думку експертів, у майбутньому поняття колл-центр втратить сенс: не треба буде ні центру, ні навіть дзвінків у класичному розумінні. Чат-боти, фейкові оголошення та таргетовані рекламні кампанії виконуватимуть всю роботу, а людина-шахрай залишатиметься лише на фінальній стадії — підтвердження транзакції. Це означає, що географія, мова, фізичне приміщення та навіть «дах» в правоохоронних органах перестають бути обов'язковими ресурсами. Будь-яка харизматична або цинічна людина з доступом до даркнету зможе відкрити власний «скам-бізнес зі спальні», що зробить боротьбу з ним експоненційно складнішою.

Тепер варто поговорити про найболючіший аспект проблеми — так званий «дах», тобто системний захист з боку правоохоронних органів. Це не конспірологія, а реальність, яку підтверджують і колишні співробітники колл-центрів, і народні депутати, і навіть деякі документи, що потрапили до журналістів. Дослідники цитують одного з колишніх працівників: «Дах — це поліція, все тримається на особистих зв'язках. Коли починається рейд, поліція закриває центр, виганяє всіх геть. Співробітники отримують вихідний — а наступного дня все працює далі». Щомісячна плата за такий захист, за різними оцінками, становить від 10 до 15 тисяч доларів. Передаються гроші через спеціальну особу — «переговорника», який знаходить контакт у певному відділку поліції або прокуратурі, укладає негласну угоду: ви нас не чіпаєте, ми працюємо.

Член тимчасової слідчої комісії Верховної Ради розповів, що щоразу, коли комісія виїжджала в певний регіон, дзвінки від місцевих колл-центрів завмирали на два-три дні — ще до того, як комісія публікувала свій графік. «Зрозуміло, де витік», — підсумував він. Інший член комісії

зазначив, що проблема вже не просто в кримінальному бізнесі, а у формуванні «злочинної еліти», вбудованої в структуру взаємодії з правоохоронними органами та місцевою владою.

Спроби натиснути на цю систему дають результати, але вони часто носять точковий характер. Після призначення в червні 2025 року генеральним прокурором Руслана Кравченка розпочалася хвиля гучних ліквідацій. У липні тільки в Дніпрі закрили 25 офісів. До кінця року рахунок пішов на десятки. У грудні 2025 року Україна разом з європейськими партнерами демонтувала транснаціональну мережу з центрами в Києві, Дніпрі та Івано-Франківську, яка ошукала 47 європейців майже на мільйон євро.

Однак дослідники застерігають: поки не зламано саму систему рейдерського захисту, ці рейди ризикують залишитися виключно показовими — старий «дах» може бути не знищений, а переформатований. На підтвердження цього вони нагадують, що тимчасова слідча комісія пропрацювала лише рік, її мандат не продовжили, а парламент не затвердив її звіт. Це наочно демонструє, наскільки політично вразливою є боротьба з індустрією, що має потужних покровителів.

Глобальний розмах українських скам-центрів викликає окрему тривогу. Якщо на початку 2010-х років жертвами ставали переважно росіяни та українці, то сьогодні географія сягає щонайменше 29 країн. Особливо активізувалися центри, спрямовані на Чехію, Польщу, Латвію, Румунію, Німеччину, Канаду та США. Для цього наймають викладачів мов, створюють окремі підрозділи для різних ринків. Але найтривожніша тенденція, яку відмічають автори звіту — поява оголошень про роботу в кол-центрах російською та українською мовами на сайтах Словаччини, Польщі, Греції та Болгарії. Це означає, що скам-бізнес фізично мігрує за межі України — можливо, разом з хвилею біженців. Частина цих оголошень пропонує безкоштовне житло, а деякі навіть кажуть про можливість працювати з будь-якої точки Європи через віддалений доступ.

Життя всередині скам-центру нагадує скоріше психологічну в’язницю. Колишні співробітники розповідають, що середній вік нового рекрута — 15-28 років, причому згадувалися навіть 14-річні діти. Їх заманюють красивими дівчатами, які грають роль «HR-приманки», або «історіями успіху» — коли їхні «ровесники» демонструють куплені автівки та айфони. Одна з колишніх співробітниць розповіла, що їй обіцяли 800-1000 доларів, але натомість вона отримувала 250, оскільки решта мала надходити з комісійних, яких не було. Інший хлопець, який прийшов на співбесіду з розклеювання листівок, дізнався, що роботи розклейника немає, натомість є вакансія «дзвонити людям в інших країнах.

Система використовує штрафи за помилки, спізнення, зайву каву. Робочий день може тривати 12 годин, шість-сім днів на тиждень, особливо якщо ти не виконуєш план. Деякі офіси працюють у дві зміни — день і ніч — щоб обдзвонювати різні часові пояси, а співробітників селять у гуртожитки. Втекти складно. Один з опитаних сказав дослідникам: «Якщо хороший клозер іде без дозволу, його знайдуть і покарають. Б’ють до крові, а потім показують фото». Інший додав: «Чув, що можуть лишити без пальців на руках або ногах. Якщо намагаєшся втекти, можуть вивезти в ліс». Навіть якщо людина фізично покидає центр, психологічні зміни залишаються назавжди: «черствість, жадібність, порожнеча в очах», «ти думаєш, що ти володар, що використовуєш моральне насильство, але насправді ти просто злодій», — резюмує одна з колишніх працівниць.

Попри певний оптимізм, пов’язаний зі зменшенням кількості скарг від українських громадян, які вже навчилися не вестися на примітивні схеми з блокуванням карток, загальна картина залишається загрозливою. Кількість скам-центрів дійсно скоротилася після закриття доступу до інтернету в СІЗО та після російського закону про блокування IP-телефонії (який набув чинності у вересні 2025 року). Але цей спад, на думку аналітиків, є скоріше паузою для переформатування. Грошові потоки просто змінюють русло. Замість десятків тисяч дзвінків від живих операторів

з'являться сотні тисяч діалогів від AI-ботів. Замість оренди дорогих бізнес-центрів — дисперсна робота з дому через Starlink та VPN. А замість кількох великих «сіток» — тисячі дрібних індивідуальних скамерів. У такому світі старе поняття колл-центр стане архаїзмом — не буде кол-центру, зате буде більше шахрайства, ніж будь-коли.

Автори звіту пропонують п'ять ключових контрзаходів, які корелюють з п'ятьма характеристиками системи. Перший — закрити «вітрину»: активно моніторити сайти з вакансіями та соціальні мережі, ділитися розвідданими з правоохоронцями, створити законодавчі стимули для орендодавців, щоб вони перестали здавати приміщення скам-центрам, і проводити кампанії, які розвінчують міф про «легкі гроші» в таких офісах.

Другий — бити не по окремих центрах, а по мережах: будувати справи проти власників «сіток», створити спеціальні статті Кримінального кодексу за електронне комунікаційне шахрайство.

Третій — зламати щит захисту: відновити політичну волю, зробити боротьбу з корупцією в правоохоронних органах пріоритетом, а західним партнерам — чинити тиск на українську владу, чітко даючи зрозуміти, що «кришування» центрів, які шкодять громадянам, є неприйнятним.

Четвертий — спростити міжнародні розслідування: розробити стандартизовані протоколи, які зменшать вартість транскордонних справ, і продовжувати інвестиції в такі платформи, як Global Signal Exchange.

І п'ятий — використовувати оборонний AI та державну стратегію: Україні потрібна комплексна анти-скам-стратегія, яка координує технологічні рішення, робить провайдерів послуг відповідальними (включаючи штрафи) та водночас виховує кібергігієну як персональну відповідальність. Кампанія НБУ «Шахрай, гудбай» — хороший початок, але вона має перерости в постійну освітню програму.

Наприкінці аналітики GI-TOC роблять висновок: на момент написання звіту Україна все ще має шанс запобігти перетворенню на глобальний центр скам-індустрії, подібний до «Золотого трикутника» Південно-Східної Азії. Але час обмежений. Якщо не подолати корупційний захист, не оновити законодавство та не адаптуватися до викликів AI, то навіть після перемоги у гарячій війні Україна ризикує залишитися з холодною, але не менш руйнівною епідемією — епідемією довіри.

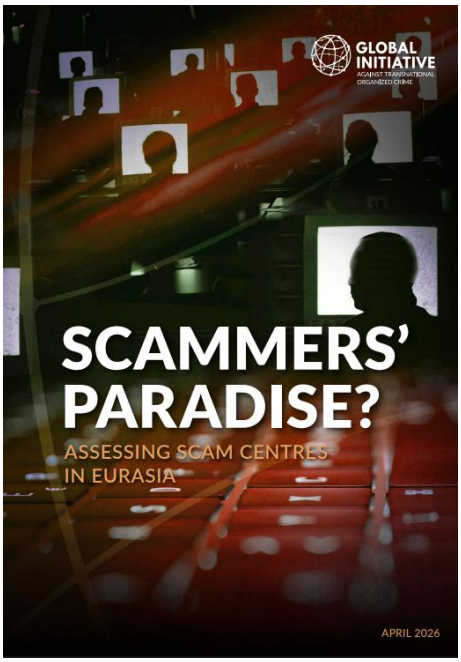
Чи зможе Україна зробити рішучий крок від «столиці скаму» до країни, де шахрайство є нетерпимим, — залежить від політичної волі влади та

Висновки:

- **Колосальні масштаби та консолідація:** В Україні діє близько 60 000 працівників скам-центрів, які генерують до $1 млрд щомісяця. Ринок жорстко контролюється всього трьома великими злочинними «сітками», що свідчить про високий рівень організованості та монополізації.
- **Системний «дах» у правоохоронних органах:** Ключовою умовою існування індустрії є корупційний захист. Окремі підрозділи поліції та прокуратури отримують щомісячну плату, попереджаючи про рейди або роблячи їх показовими, що унеможливлює ліквідацію мереж без політичної волі.
- **Глобальна експансія замість «патріотичного скаму»:** Попри риторику про боротьбу з Росією, основна маса жертв (понад 80–90%) — це мешканці України та країн ЄС, США, Канади.
- **Технологічний злам моделі:** Штучний інтелект та сервіс «злочинність як послуга» змінюють природу загрози. Великі офіси в бізнес-центрах поступово замінюються на децентралізовану роботу, де один скамер з AI-перекладачем здатен завдати шкоди, як цілий центр, що робить стару модель правового реагування неефективною.

тиску партнерів. Але якщо судити за темпами, з якими еволюціонує цей бізнес, вікно можливостей швидко зачиняється.

Трильйон доларів у тіні: Глобальна імперія скам-центрів та її обличчя [7]



Звіти GI-TOC, об'єднані спільною темою аналізу глобального феномену скам-центрів, пропонують читачеві складну, багатошарову картину злочинної екосистеми, яка за своєю адаптивністю, технологічною оснащеністю та фінансовою міццю перевершує багато традиційних форм організованої злочинності. Разом вони створюють аналітичну панораму, яка демонструє, як локальні осередки шахрайства, підсилені глобальними факторами, перетворилися на одну з найприбутковіших і найбільш руйнівних загроз XXI століття, кидаючи виклик національним суверенітетам та міжнародній правоохоронній співпраці.

Масштаб явища важко осягнути. За оцінками Global Scam Alliance, лише у 2024 році шахраї по всьому світу викрали понад один трильйон доларів США, що становить майже один відсоток світового валового внутрішнього продукту. Ця астрономічна цифра є лише вершиною айсберга, адже вона не враховує психологічних травм жертв, руйнування сімейних бюджетів, банкрутства малих підприємств та ті мільярди доларів, які не потрапляють до офіційної статистики через сором або необізнаність постраждалих. Автори звітів наголошують: ми маємо справу не з окремими злочинцями і навіть не з організованими групами, а з цілісною екосистемою — складною, взаємопов'язаною та неймовірно живучою.

Її фундаментом є шість «прискорювачів сили», які поєднують локальне вкорінення з глобальним охопленням. Перший — це здатність до мережевої взаємодії: скам-центри рідко діють ізольовано, вони є частинами ширших транснаціональних злочинних мереж, які обмінюються знаннями, програмним забезпеченням, базами даних та навіть персоналом.

Другий фактор — технології та концепція «злочинності як послуги» (crime-as-a-service). Сьогодні будь-хто, хто має мінімальний капітал, може придбати в даркнеті все необхідне для запуску скам-центру: від CRM-систем та готових скриптів діалогів до баз даних витоків персональної інформації та послуг з відмивання грошей.

Третій фактор — інфраструктура відмивання коштів, яка включає в себе все: від випадкових «грошових мулів» (money mules), які за невелику винагороду позичають свої банківські рахунки, до складних ланцюжків транзакцій через криптовалютні біржі та міксери, що роблять неможливим відстеження активів.

Четвертий, і, мабуть, найбільш токсичний фактор — це політичний захист («дах»). Скам-центри процвітають там, де корумповані чиновники, правоохоронці або навіть представники вищого політичного керівництва отримують частку прибутку в обмін на невтручання або активне сприяння. Рівні цього захисту варіюються від дрібних хабарів тюремним наглядачам у Колумбії,

[7] https://globalinitiative.net/wp-content/uploads/2026/04/Scammers-paradise-Assessing-scam-centres-in-Eurasia-GI-TOC-April-2026.pdf
https://globalinitiative.net/wp-content/uploads/2026/04/Scam-centres-Combating-a-global-phenomenon-GI-TOC-April-2026.pdf

які фактично організовують роботу шахрайських центрів прямо у в'язницях, до системної інтеграції скам-бізнесу в державні структури, як це показано на прикладі Грузії.

П'ятий фактор — люди. Scam-центри потребують робочої сили різного рівня кваліфікації: від програмістів та IT-фахівців до звичайних операторів, які цілодобово ведуть романтичне листування або обдзвонюють потенційних жертв. Цей сектор приваблює людей як обіцянками надприбутків (відомі випадки, коли керівники відділів у грузинських кол-центрах заробляли до 30 000 доларів на місяць), так і шляхом примусу та торгівлі людьми, що особливо поширено в Південно-Східній Азії, але починає фіксуватися і в Євразії.

Шостий, і останній фактор — геополітика. Злочинці виявилися напрочуд чутливими до глобальних політичних зрушень. Пандемія COVID-19, яка перевела комунікації в онлайн, стала для них золотою жилою. Війна в Україні відкрила нові горизонти: з'явилися схеми з фальшивими зборами на потреби армії, «евакуацією» родичів із зони бойових дій, а також цілі кампанії «патріотичного шахрайства», коли українські центри цілеспрямовано атакують росіян, знаючи про повну відсутність правової співпраці між двома країнами. Ця розколота реальність — найкращий друг шахрая.

Окремої уваги заслуговує аналіз соціальної інженерії, який пропонують автори. На відміну від примітивного спаму, розрахованого на натовп, соціальна інженерія — це мистецтво побудови довіри. Шахрай може тижнями або навіть місяцями вести романтичне листування, видаючи себе за привабливого лікаря або військового, перш ніж заговорити про гроші. Він може зателефонувати жертві, представляючись співробітником банку, і вже знати її адресу, дату народження та останні чотири цифри картки, отримані з даркнету. Це створює ілюзію безпеки та легітимності, роблячи критичне мислення жертви практично беззахисним.

Але майбутнє, яке описують автори, виглядає ще більш загрозливим. Штучний інтелект (AI) стирає межу між масовим спамом та цільовою атакою. Генеративні нейромережі дозволяють створювати deepfake-відео за участю знаменитостей або політиків, які рекламують фальшиві інвестиційні платформи. Інструменти клонування голосу за лічені хвилини можуть відтворити тембр та інтонації голосу вашої дитини або начальника, щоб виманити гроші. Великі мовні моделі здатні вести тисячі реалістичних діалогів одночасно, фактично виконуючи роботу цілого колл-центру. Автори звітів влучно зауважують, що ми рухаємось до зміни парадигми: від ситуації, де AI допомагає людині-шахраю, до ситуації, де людина-оператор лише налагоджує та контролює AI-керовані шахрайські кампанії. Беззаперечним доказом того, що ця загроза вже не гіпотетична є те, що дослідникам вдалося створити AI-агента, здатного здійснювати успішні шахрайські дзвінки за собівартістю близько одного долара.

Якщо глобальна частина дослідження окреслює загальну теорію, то регіональний аналіз Євразії наповнює її конкретним змістом. Цей регіон є унікальним полігоном, де переплітаються пост-радянська спадщина, бурхливе зростання інтернет-проникнення (у Грузії частка населення, що користується інтернетом, зросла з 27% у 2010 році до 72% у 2020-му), глибока корупція та запеклі геополітичні конфлікти. Дослідники GI-TOC виокремлюють Україну, росію та Грузію як головні «гарячі точки» активності скам-центрів, тоді як Білорусь, Вірменія та країни Центральної Азії виступають переважно як країни-мішені, хоча ситуація там швидко змінюється.

Росія постає у звіті як складна й суперечлива картина. З одного боку, в країні спостерігається епідемія телефонного шахрайства: за оцінками, втрати громадян у 2024 році сягнули 3,2 мільярда доларів, а щоденна кількість шахрайських дзвінків, попри всі зусилля, становила 5-6 мільйонів. З іншого боку, російська державна риторика наполегливо створює міф про зовнішнього ворога — стверджується, що майже всі шахрайські дзвінки надходять з України. Навіть коли в москві чи санкт-петербурзі викривають величезний колл-центр, в офіційних релізах незмінно з'являється згадка про «кураторів зі Служби безпеки України». Це створює «туман війни», який унеможливлює об'єктивний аналіз масштабів внутрішньої загрози та

заважає розробці ефективних стратегій захисту, оскільки будь-яке обговорення проблеми блокується звинуваченнями в «ворожій пропаганді».

Водночас, звіт показує, що в росії існує потужний власний скам-ринок, який виріс із пенітенціарної системи. У середині 2010-х років сотні «чорних» колл-центрів функціонували прямо у в'язницях з мовчазної згоди або за активної участі корумпованого персоналу. Згодом цей бізнес вийшов на волю, орендуючи офіси в ділових центрах москви вербувальники відкрито публікують вакансії в Telegram. Росія також демонструє приклад того, як антишахрайські заходи можуть стати інструментом посилення державного контролю. Для протидії «спуфінгу» (підміні номерів) уряд не лише блокує дзвінки через WhatsApp та Telegram, але й запускає власний месенджер «Max», який збирає персональні дані, викликаючи аналогії з китайським WeChat. Баланс між необхідним захистом та ризиком створення цифрового концтабору — це питання, яке в російському контексті вирішується далеко не на користь першого.

Найбільш яскравим та водночас найбільш тривожним регіональним кейсом є Грузія. Це невелика країна з населенням близько 3,7 мільйона осіб, яка стала справжньою «меккою» для високотехнологічних, надприбуткових скам-центрів, що працюють в основному на німецькомовну та англомовну аудиторію.

Дослідження GI-TOC простежує історичне коріння цього явища. Усе почалося з міграції ізраїльських шахрайських операцій, які після ухвалення Ізраїлем у 2017 році закону, що забороняв продаж бінарних опціонів за кордон, шукали нові безпечні гавані. І вони знайшли їх в Україні та Грузії. Такі компанії, як Milton Group, GetFinancial та Envirotech, просто «скопіювали та вставили» свою бізнес-модель у нові юрисдикції, наймаючи місцевих юристів, бухгалтерів та менеджерів. Але те, що відбувається у Грузії сьогодні, йде набагато далі від звичайного корпоративного шахрайства. За свідченнями численних анонімних джерел — адвокатів, журналістів, колишніх співробітників — скам-центри в Грузії мають потужний політичний «дах», який сягає найвищих рівнів влади. Якщо в Україні зв'язок з правоохоронцями є переважно транзакційним («сплатив — і тебе не чіпають»), то в Грузії, за словами одного з джерел, це «державна операція». Злочинці виступають у ролі посередників, а самі колл-центри розглядаються як джерело «чорних грошей» для правлячої партії.

Атмосфера страху та самоцензури, яку відчули дослідники під час роботи в Тбілісі, красномовно свідчить про глибину проблеми. Інтерв'ю доводилося проводити в громадських місцях, а прохання про анонімність були тотальними. Один із респондентів зауважив: «У Грузії можна обговорювати будь-який злочин, окрім колл-центрів та антиурядових протестів».

Цей клімат тиску безпосередньо впливає на правоохоронну практику. Справа компанії Morgan Limited стала хрестоматійною. Після гучного журналістського розслідування OCCRP та обшуків, проведених ще у 2019 році, прокуратура звинуватила компанію в привласненні як мінімум 5 мільйонів євро у громадян Німеччини, Словаччини та Словенії. Однак 27 червня 2025 року прокуратура уклала з обвинуваченими угоду про визнання вини, за якою всі вони були звільнені з-під варти, сплативши лише штраф. І що найважливіше — компанія фактично одразу відновила свою роботу. Слідчі дії були не більш ніж показовим фарсом. Така ж доля спіткала інші великі центри, як-от Black Rock та AK Group, попри те, що за фінансовими документами останньої було встановлено крадіжку понад 35 мільйонів доларів за три роки.

Автори звіту роблять гіркий висновок: у Грузії бізнес скам-центрів почувається як «абсолютно легітимний». І це при тому, що самі співробітники таких центрів у Грузії заробляють неймовірні гроші: керівники відділів — до 30 000 доларів на місяць, а високоефективні оператори можуть отримувати бонуси у вигляді автомобілів. Ця індустрія стала невід'ємною частиною грузинської економіки та політичної системи.

Проблема людського ресурсу насправді є найболючішим нервом усієї проблематики. Вона розкриває спектр від свідомих, добре оплачуваних фахівців до безправних жертв торгівлі людьми. У Грузії чи росії працівник скам-центру часто є висококваліфікованим фахівцем зі знанням мов, який свідомо обирає злочинну кар'єру через величезні заробітки, недосяжні в легальній економіці. І він може вільно звільнитися, якщо захоче — ринок там конкурентний, існує навіть «полювання за фахівцями» між різними угрупованнями.

На іншому полюсі — Південно-Східна Азія, де дослідження GI-TOC описує справжнє рабство. Людей з різних країн, зокрема з росії, Узбекистану та Киргизстану, заманюють обіцянками високооплачуваної роботи в IT-сфері. Прибувши на місце — у спеціальні ізольовані центри в М'янмі, Лаосі чи Камбоджі, — вони потрапляють у боргову кабалу, зазнають тортур, і єдиний їхній шлях до порятунку — це працювати на злочинців.

Автори зазначають, що такі практики більше не обмежуються Азією: повідомлення про утримання працівників силою надходять з Гани, Нігерії, Пакистану та навіть Об'єднаних Арабських Еміратів. І ця проблема створює зловісний цикл. Коли жертвам торгівлі вдається повернутися додому, вони часто стикаються з кримінальним переслідуванням. Китай, наприклад, вже висунув звинувачення десяткам тисяч своїх громадян, репатрійованих з Південно-Східної Азії. Маючи судимість і не маючи змоги знайти легальну роботу, ці люди з великою ймовірністю знову повернуться до шахрайства, але вже як свідомі організатори або наставники для новачків. Тому автори наполягають на необхідності комплексних програм реінтеграції та делікатного підходу до питання кримінальної відповідальності за дії, вчинені під примусом.

Нарешті, геополітичний чинник виявляється тим глобальним тлом, яке робить усі ці проблеми практично нерозв’язними в короткостроковій перспективі. Війна створила нову реальність. Західні країни, які десятиліттями розбудовували механізми співпраці з росією через Інтерпол чи Євроюст, сьогодні відмовилися від цього.

Шахраї, як зауважує один із співрозмовників дипломатів, надзвичайно швидко навчилися грати на цих протиріччях. Вони знають, що поки політики сваряться, вони можуть безкарно використовувати територію однієї країни для атак на громадян іншої. Водночас, усередині пострадянського простору спостерігається зворотна тенденція: країни, які зберігають лояльні відносини з москвою — Білорусь, Казахстан, Киргизстан, Узбекистан — посилюють регіональну співпрацю. Вони проводять спільні операції, обмінюються даними та гармонізують законодавство. Однак ця співпраця часто має політичне забарвлення і використовується для просування наративів, які вигідні кремлю, зокрема про те, що всі біди йдуть з України.

У підсумку світ опинився у фрагментованій правоохоронній реальності, де різні блоки країн мають різні правила гри, а шахраї

Висновки:

- **Феномен scam-центрів досяг масштабу глобальної індустрії.** У 2024 році шахраї викрали понад $1 трильйон, що становить майже 1% світового ВВП.
- **Політичний захист є фундаментальною умовою процвітання скам-центрів.** Найбільші та найстійкіші центри існують не в правовому вакуумі, а завдяки корумпованим зв’язкам.
- **Геополітичні конфлікти стали найкращим союзником шахраїв**. Війна в Україні не лише породила нові шахрайські схеми, але й зруйнувала міжнародну правоохоронну співпрацю.
- **Штучний інтелект змінює саму природу загрози.** Технології deepfake, клонування голосу та великі мовні моделі автоматизують соціальну інженерію, стираючи межу між масовим спамом та цільовою атакою.

вправно маневрують між ними так само, як їхні жертви не вміють відрізняти справжній дзвінок з банку від підробленого.

Підсумовуючи аналіз цих двох знакових документів, варто сказати, що вони пропонують свіжий, системний погляд на проблему, яку часто недооцінюють. Це не просто про дрібних шахраїв, які обдзвонюють бабусь. Це про те, як організована злочинність адаптується до цифрової ери, інтегрується з корумпованими державами та використовує найбільші геополітичні трагедії для власного збагачення.

Автори закликають до цілісної відповіді, яка не обмежуватиметься арештами окремих операторів, а буде спрямована на демонтаж усіх шести факторів-прискорювачів. Це означає необхідність гармонізувати законодавство, щоб зробити соціальні мережі та криптобіржі більш підзвітними. Це потребує створення нових, наступальних AI-інструментів, які можуть захистити людей, а водночас — широких просвітницьких кампаній. І, нарешті, це вимагає визнання того, що багато з тих, хто працює в скам-центрах, є такими ж жертвами, які потребують реінтеграції, а не просто покарання.

Без такої комплексної, багатосторонньої та стратегічної відповіді світ спостерігатиме лише подальше зростання, міграцію та дифузію цього явища. Скам-центри стануть ще більш розосередженими, ще більш технологічними та ще більш інтегрованими в тканину світової економіки та політики, продовжуючи викачувати трильйони доларів і руйнувати мільйони життів.

Інші новини

Як Африка стає стратегічним тилом іранської кримінальної інфраструктури [8]

Поки світова спільнота, затамувавши подих, стежить за драматичною ескалацією в Ормузькій протоці, а аналітичні центри від Вашингтона до Тель-Авіва генерують тисячі сторінок аналітики про військові альянси, нафтові ринки та вразливість глобальних морських шляхів, поза зоною прямого конфлікту залишається простір, який отримує катастрофічно мало уваги. Цей простір — Африка.

Її роль як традиційного транзитного хабу для нелегальної торгівлі, відмивання коштів та фінансових потоків, пов'язаних із близькосхідними конфліктами та санкційними режимами, системно недооцінюється міжнародною спільнотою. І ця аналітична прогалина є не просто академічним упущенням, а критичною вразливістю глобальної безпеки, адже сьогодні йдеться не просто про контрабанду чи локальну корупцію, а про можливе тотальне переформатування цілої паралельної економіки, яка десятиліттями живила близькосхідні проксі-війни. Африка, яку багато хто звик сприймати як пасивного реципієнта зовнішніх впливів, сьогодні ризикує стати активним тилом, головним операційним майданчиком та інституційним захистком для мереж, які забезпечують виживання іранського режиму в умовах безпрецедентного тиску.

[8] https://globalinitiative.net/analysis/how-the-middle-east-conflict-is-creating-the-conditions-for-the-convergence-of-criminal-finance-in-africa/

Коли така держава, саме існування якої десятиліттями тримається на кримінальній інфраструктурі — як Іран, що перебуває під жорсткими санкціями Заходу, — стикається з безпрецедентним військовим тиском, її тіньові мережі не зникають і не капітулюють. Вони діють за законами біологічного виживання складних систем: фрагментуються, адаптуються, мутують і шукають нових партнерів, мігруючи туди, де контроль найслабший, інституційна пам'ять найкоротша, а розрив між формальними регуляціями та реальним наглядом є найбільшим.

Сьогодні Африка, з її строкатою мозаїкою суверенних юрисдикцій, слабкими прикордонними службами, високим рівнем корупції та стрімко зростаючими, але погано регульованими фінансовими потоками, опиняється в епіцентрі цієї експансії. Те, що останні два десятиліття функціонувало як другорядний транзитний маршрут, сьогодні перетворюється на головну зону релокації, де іранські мережі можуть не просто ховати активи, а й будувати нову, більш стійку архітектуру ухилення від санкцій. І парадокс полягає в тому, що саме тиск на Іран — військовий, економічний, дипломатичний — стає тим каталізатором, який пришвидшує цю кримінальну міграцію на континент, де вже існують готові канали, посередники та попит.

Щоб зрозуміти всю глибину та системність цієї загрози, слід спершу відновити в пам'яті та проаналізувати природу самого санкційного режиму Ірану. Це не просто економіка, що страждає від зовнішніх обмежень, і не набір розрізнених злочинних схем. Це цілісна, централізовано керована система інституційного обману, яка відточувалася роками виживання в умовах тотальної фінансової блокади. Ісламська Республіка навчилася переміщувати нафту через складні ланцюжки перевалок у міжнародних водах, повністю стираючи її походження та справжнього власника. Наркомережі, що тягнуться від афганського опіуму до європейських споживачів, використовують іранських посередників як найнадійніших логістів, які ніколи не свідчать проти своїх роботодавців. Зброя — від балістичних ракет до безпілотників — через павутину підставних компаній досягає проксі-сил на різних континентах, від Лівану до Ємену та Сахелю. Фіктивні компанії, обмінні пункти, трейдери сировини оперують мільярдами доларів, приховуючи кінцевих бенефіціарів у лабіринтах корпоративних структур, зареєстрованих у юрисдикціях з нульовою прозорістю. Це не побічний продукт корупції, не «тіньова економіка» як її часто розуміють, а відточена, професійна кримінальна методологія, де обман зводиться в ранг державної політики, а інструменти організованої злочинності слугують цілям національної безпеки. І військовий тиск на саму державу, хоч би яким інтенсивним він був, не знищує цю структуру. Він лише запускає процес її примусової еволюції: мережі розбиваються на дрібніші, автономніші ланки, змінюють географію маршрутів, освоюють нові технології і культивують партнерства саме там, де регуляція є слабкою, але фінансовий доступ до світової економіки залишається відкритим.

Десятиліттями Африка виконувала для цих мереж суто допоміжну, транзитну функцію. Вона була територією, через яку наркотики, зброя та нелегальна нафта рухалися на північ, у бік Європи та багатих ринків Перської затоки. Однак сьогодні, під дією нового геополітичного тиску, континент ризикує здійснити якісний стрибок: із транзитної території він перетворюється на зону постійної релокації, де іранські мережі можуть не лише проводити операції, а й відтворювати свою інфраструктуру — від логістичних хабів до підставних банків. Цей перехід від транзиту до релокації є ключовим концептом для розуміння того, що відбувається прямо зараз.

І найкраще цю динаміку ілюструє, як не парадоксально, звичайне на перший погляд золото. Адже золото є унікальним інструментом у світовій фінансовій системі, і його унікальність має подвійну природу. Легально це резервний актив, який центральні банки купують мільярдними партіями. Але з точки зору кримінального використання, золото має магічну властивість: воно абсорбує нелегальну вартість з офіційної фінансової системи, повністю «відмиває» її у фізичному просторі та вивільняє в іншому місці, практично не залишаючи жодних цифрових слідів. Достатньо одного разу переплавити брудні злитки, або змішати їх з легітимною рудою, і їхнє походження зникає назавжди без жодного сліду, без можливості відстеження. Для

держави під санкціями, яка прагне будь-якими засобами конвертувати свої доходи в ліквідні активи, обходячи західний фінансовий моніторинг, золото є не просто вигідним товаром, а майже ідеальним, стратегічним інструментом збереження та передачі вартості.

І саме Африка є головним і найбільш вразливим джерелом цього золота. Велетенські обсяги кустарного золота, що видобувається в охоплених конфліктами та слабких державних інституціях Демократичній Республіці Конго, Південному Судані, Центральноафриканській Республіці, а також у Судані, Чаді та низці інших країн, десятиліттями транспортуються через складну регіональну мережу. Головні транзитні вузли — Уганда, Руанда, Камерун, Кенія, Чад, Бурунді.

Кінцевий пункт призначення переважної більшості цих потоків — Дубай. Різні міжнародні розслідування та оцінки свідчать, що до 95%, а за деякими оцінками навіть більше, всього контрабандного золота зі Східної та Центральної Африки осідає саме в цьому місті. Механізм давно відпрацьований, прозорий для обізнаних і водночас абсолютно непроникний для зовнішнього контролю. Золото прибуває в Дубай без жодної достовірної документації про його походження, без сертифікатів. На місці воно потрапляє до місцевих афінажних заводів, отримує офіційний сертифікат «дубайського» або «еміратського» золота і виходить на світові ринки як абсолютно легітимний продукт, який може купувати будь-який центральний банк, ювелірний дім або інвестиційний фонд. Різниця між ціною кустарного золота в Конго та ціною сертифікованого золота в Дубаї становить сотні доларів за унцію, і саме ця різниця фінансує посередників, логістів та корумпованих чиновників.

Але чому це стає критично важливим саме в контексті Ірану? Тому що Об’єднані Арабські Емірати, і передусім Дубай, вже давно визнані всіма профільними міжнародними структурами — від FATF до Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) — як ключовий, можливо, найважливіший центр незаконної іранської фінансової діяльності за межами самого Ірану.

Це явище отримало назву «тіньова банківська система» (shadow banking). Обмінні пункти, хавали та невеликі фінансові доми в ОАЕ, які часто навіть не мають формального банківського ліцензування, щорічно обробляють мільярди доларів від імені компаній та фізичних осіб, безпосередньо пов’язаних із підсанкційними іранськими структурами, зокрема Корпусом вартових ісламської революції (КВІР) та його комерційним крилом «Хатам аль-Анбія». Більше того, дубайські фірми неодноразово фігурували в розслідуваннях як ключові посередники в нещодавньому різкому сплеску незаконних транзакцій із використанням криптовалют, які також пов’язують з Іраном, який навчився обходити санкції через майнінг біткоїна та операції зі стейблкойнами.

Отже, ми маємо справу з тим, що Дубай об'єктивно виступає ідеальною, географічно та інституційно зумовленою точкою конвергенції для двох величезних, різнорідних на перший погляд нелегальних потоків: з одного боку — африканське конфліктне золото, яке потребує легалізації, з іншого — іранські підсанкційні капітали, які потребують інвестиційних інструментів. Вони починають використовувати одні й ті самі логістичні канали, одну й ту саму фінансову інфраструктуру, одних і тих самих посередників. Те, що раніше існувало паралельно, майже не перетинаючись, сьогодні під тиском зовнішніх обставин починає зливатися воєдино, утворюючи небезпечний симбіоз, де африканська сировина фінансує близькосхідні проксі-війни, а іранські технології обману допомагають африканським контрабандистам виходити на нові рівні.

Розгляньмо Кенію як типовий, майже хрестоматійний приклад однієї з ключових ланок цієї системи, що працює вже сьогодні. Кенія, попри свою мізерну, практично символічну частку у світовому видобутку золота (офіційно країна виробляє близько пів тонни на рік), функціонує як

один із найпотужніших транзитних хабів для всього кустарного золота регіону. Тони металу, видобутого в ДР Конго та Південному Судані, регулярно транспортуються через Найробі.

Як це відбувається з точки зору документообігу? Партія золота в'їжджає в Кенію з сусідньої країни, часто без будь-якого митного оформлення, або з оформленням за сфальсифікованими документами. Потім, залишаючись на території Кенії кілька днів чи тижнів, вона отримує новий пакет документів, який презентує її вже як кенійське золото — з фіктивними актами про видобуток, фіктивними дозволами на експорт та фіктивними контрактами з місцевими посередниками. Реальний власник вантажу, країна походження та історія фінансування видобутку повністю зникають за цією паперовою ширмою. Цей розрив між формальним дотриманням правил (наявність сертифікатів, ліцензій, контрактів) та реальним ефективним наглядом (перевіркою відповідності цих документів фізичній реальності) створює фінансове та логістичне середовище, яке є ідеальним для систематичної експлуатації з боку мереж, що перебувають під санкційним тиском.

Цей дисбаланс існував у золотому бізнесі Східної Африки десятиліттями. Але зараз змінюється сама мотивація до його використання. Якщо раніше ця «сіра зона» використовувалася переважно локальними гравцями для уникнення податків або контрабанди невеликих обсягів, то сьогодні в неї заходять високоорганізовані, добре фінансовані та захищені державними інтересами Ірану актори. Вони мають досвід, масштаб і технологічну спроможність перетворити цю сіру зону на чорну діру глобальної фінансової системи.

Проблема, однак, полягає не лише в об'єктивному існуванні цих потоків та їх посиленні. Навіть більшою проблемою є те, як африканська система розвідки, безпеки та фінансового моніторингу на цю загрозу реагує — або, точніше, як вона не реагує. Регіональні органи безпеки Африки, зокрема структури Африканського Союзу та окремі національні розвідки, добре усвідомлюють, що пов’язані з Іраном мережі ухилення від санкцій діють на континенті. Про це неодноразово свідчили звіти, наприклад, комітету з моніторингу санкцій ООН щодо Сомалі та Еритреї. Але головна аналітична та операційна пастка полягає в тому, що ця діяльність зовсім не схожа на традиційну, звичну для африканських поліцій організовану злочинність. Вона не виявляє себе через вуличні арешти, перестрілки між кланами чи помітні конвої з наркотиками. Вона не залишає трупів чи відкритих збройних сутичок. Натомість вона рухається через майже непомітні для пересічного спостерігача механізми: транзакції в середніх розмірах, сотні криптогаманців, що активуються на кілька годин, та рутинну паперову роботу — реєстрацію нових компаній, отримання експортних сертифікатів, митне декларування вантажів із символічною вагою. Саме ця «сірість» іранського відмивання коштів робить його невидимим для традиційних інструментів правоохоронних систем Африки.

У сфері африканської фінансової розвідки слабкості мають не стільки технічний характер, скільки глибокий інституційний. Підрозділи фінансової розвідки (ПФР) різних країн, регулятори сировинних ринків, митні служби та класичні правоохоронні органи (поліція, жандармерія) діють, як правило, у повній ізоляції один від одного. У них немає спільних платформ для обміну даними, їхні бази даних не інтегровані, а їхні повноваження часто свідомо обмежені, щоб уникнути політичної чутливості. Ситуація ускладнюється ще й тим, що багато африканських країн мають тісні економічні та дипломатичні зв'язки з Іраном, а в деяких випадках — і з його регіональними союзниками, що робить політично чутливим будь-яке системне розслідування іранських слідів.

Саме для протидії такого типу транснаціональним, багатовимірним загрозам, які потребують координації, і був створений Африканський механізм поліцейської співпраці (AFRIPOL). Його мандат передбачає саме об'єднання зусиль різних національних поліцій для боротьби з організованою злочинністю, що не має кордонів. Однак реальність така, що відстеження ухилення від санкцій через товарні ринки, особливо через ринок золота, вимагає від AFRIPOL та

його партнерів безпрецедентного, надзвичайно високого рівня міжвідомчої координації. Йдеться про одночасну інтеграцію щонайменше трьох типів даних: по-перше, фінансові дані від ПФР, по-друге, торговельна статистика та логістичні дані від митних служб, і по-третє, оперативна розвідувальна інформація від поліції та спецслужб. Цей рівень координації, який передбачає не просто обмін листами, а спільні бази даних, спільні слідчі групи та спільні аналітичні центри, досі не є практикою в жодному з африканських регіонів.

Можна виокремити три невідкладні, конкретні та взаємопов'язані кроки, які мають бути зроблені африканськими інституціями безпеки, бажано ще до того, як нові конфігурації іранських кримінальних мереж остаточно консолідуються в довгострокові. Перший крок стосується аналітичної спроможності. AFRIPOL у співпраці з регіональними економічними спільнотами має доручити національним підрозділам фінансової розвідки країн Східної та Центральної Африки провести терміновий, поглиблений брифінг для своїх аналітиків — не загальний, а цільовий. Цей брифінг має бути присвячений виключно індикаторам ухилення від санкцій у регіональній торгівлі золотом. Досвід роботи міжнародних фінансових розслідувань показує, що патерни стають очевидними, коли знаєш, куди саме дивитися. Без цього навіть найкращі аналітики будуть сліпі.

Другий крок має бути політико-правовим. Регіональні рамки співпраці, зокрема структури Африканського Союзу з питань миру та безпеки, повинні кваліфікувати ухилення від міжнародних санкцій як один із пріоритетних видів транснаціональної організованої злочинності. Наразі, на жаль, це питання часто сприймається як суто зовнішньополітичне, «чужа війна», яка не стосується внутрішньої безпеки африканських держав, або як проблема, яка делегована окремим державам для двостороннього врегулювання. Така інституційна фрагментація грає на руку лише кримінальним мережам, які ці розриви успішно експлуатують.

І третій крок — найбільш довгостроковий, але й найважливіший. Потрібен стійкий, роками незмінний аналітичний фокус на комерційних, фінансових та сировинних шляхах, що сполучають африканські ринки, особливо ринки Східної Африки та Сахелю, з Об'єднаними Арабськими Еміратами. Цю роботу не можна залишати на ентузіастів або разові міжнародні проєкти. Вона має координуватися через постійно діючі регіональні механізми, зокрема через методологію так званого «аналізу вузлів» (junction analysis), яка вивчає не окремі злочини, а точки фізичного або фінансового перетину різних злочинних потоків. Відстеження цього руху дасть безцінне розуміння того, як геополітичний тиск на Близькому Сході безпосередньо та прямим чином трансформується в ризики організованої злочинності на самому континенті. Африка отримає інструмент для передбачення, а не просто реагування.

На тлі поточної драматичної ескалації на Близькому Сході, наслідки для глобального ландшафту організованої злочинності залишаються майже поза увагою. А потенційний вплив усього цього на Африку — на її слабкі інституції, молоді ринки та вразливі кордони — залишається практично невидимим, недослідженим. І це саме та вразливість, яку континент, що прагне стати глобальним центром економічного зростання, не може собі дозволити ігнорувати.

Умови для конвергенції нелегальних ринків африканського золота та іранського ухилення від санкцій вже сформовані. Інфраструктура готова. Посередники на місцях. Канали для руху капіталів відкриті. Ключове запитання сьогодні полягає не в тому, чи відбудеться ця конвергенція — вона вже починається. Питання в тому, чи лідери регіональних та континентальних правоохоронних структур Африки зможуть діяти на випередження, стратегічно, за допомогою запропонованих вище інструментів, перш ніж динаміка, що лише зароджується, перетвориться на незворотні, усталені довгострокові коридори. І ціна зволікання тут вимірюватиметься не лише мільярдами втрачених доларів, які могли б піти на розвиток, а й стабільністю цілих регіонів, життями людей і самою здатністю африканських держав контролювати власну територію та ресурси. Небезпека є реальною, масштабною та нагальною.

Арешт Кінахана: Перемога у війні з транснаціональною злочинністю, чи ні? [9]

Арешт Деніела Кінахана в Дубаї, що відбувся 21 квітня 2026 року, без перебільшення можна назвати однією з найрезонансніших подій у європейському правовому полі за останнє десятиліття. Однак, як це часто буває в царині транснаціональної організованої злочинності, справжнє значення цієї події лежить не стільки в самому факті затримання, скільки в тих правових, інституційних і кримінальних наслідках, які лише починають розгортатися.

Заарештований за ірландським ордером, Кінахан — якого вважають не просто формальним лідером, а скоріше «архітектором» сучасної фази розвитку однойменного картелю — тепер перебуває на етапі екстрадиції. Слово «етап» тут ключове. Як наголошує колишній детектив ірландської поліції Ноель Браун, член експертної мережі GI-TOC, цей арешт варто сприймати як «половинну перемогу». Це не тріумфальний фінал багаторічної саги, а скоріше момент істини для нових механізмів міжнародної співпраці, тест на міцність для нещодавно підписаних угод про екстрадицію між Ірландією та Об'єднаними Арабськими Еміратами, а також потужний сигнал для всього злочинного світу, що десятиліття «безпечних гаваней» у Перській затоці поступово відходить у минуле.

Щоби зрозуміти всю вагу цього арешту, необхідно заглибитися в генезис угруповання, яке Кінахани будували кілька десятиліть. Картель розпочинав свій шлях як відносно локальне кримінальне угруповання в Дубліні в 1990-х роках. Однак завдяки стратегічному мисленню Крісті Кінахана — батька Деніела — та сприятливій кон'юнктурі ірландського економічного буму, організація швидко вийшла за межі острівної держави. Ключовим елементом їхнього злету стала здатність поєднувати грубу силу традиційного наркотрафіку з фінансовою витонченістю та налагодженням стратегічних альянсів із провідними міжнародними синдикатами, зокрема південноамериканськими постачальниками кокаїну.

Перша хвиля інтернаціоналізації власного бізнесу привела Кінаханів до Іспанії, де вони створили опорні пункти на узбережжі Коста-дель-Соль. Але справжнім проривом у сенсі захисту від правоохоронних органів стала подальша релокація до Дубая. ОАЕ, з їхньою м'якою візовою політикою, складною банківською системою та неохочістю до співпраці з західними спецслужбами минулих років, перетворилися на ідеальну «тиху гавань» для злочинних еліт.

Деніел Кінахан, який виріс у тіні свого батька, зумів не лише зберегти, а й радикально примножити цю спадщину. Якщо Крісті завжди демонстрував обережність, залишаючись тінню, то Деніел обрав іншу траєкторію: він наважився на публічну легітимацію. Його проникнення у світ професійного боксу стало класичним прикладом того, як лідери організованої злочинності намагаються купити собі респектабельність, соціальний капітал і, найголовніше, політичний вплив. Організація гучних боїв, дружба з відомими промоутерами та спортсменами — це не

[9] https://globalinitiative.net/analysis/half-a-victory-the-implications-of-daniel-kinahans-arrest-for-transnational-organized-crime/

просто вибір хобі; це системна спроба вибудувати «парасольку» захисту, створити образ бізнесмена та філантропа.

Однак саме ця публічність зіграла з Деніелом злий жарт. Вона зробила його ціллю номер один для правоохоронних органів, які раніше часто не знали, на кого саме спрямовувати зусилля. У відповідь на його видимість влада Ірландії, за підтримки США (що запровадили санкції проти родини Кінаханів) та інших європейських партнерів, сформувала безпрецедентну коаліцію для його переслідування.

Розширення впливу картелю супроводжувалося неймовірним зростанням рівня насильства, кульмінацією якого стала війна між кланами Хатч і Кінахан. Цей конфлікт, що розпочався 2016 року, перетворив вулиці Дубліна та іспанського узбережжя на поле бою, позначене серією публічних ліквідацій, підривів автомобілів і жорстоких відплат. Саме ця кривава різанина остаточно зруйнувала залишки негласного соціального контракту злочинного світу з державою та призвела до політичного тиску, що змусив ірландський уряд діяти за межами своєї юрисдикції.

Детектив Браун, який був безпосередньо залучений до цієї справи, зазначає, що розслідування такого рівня вимагає двох-трьох років тільки на збір доказової бази. Після цього робота з Державною прокуратурою (Director of Public Prosecutions, DPP) може зайняти ще кілька років, як і сталося у справі проти Кінахана. Рішення про висунення звинувачень було ухвалено на початку 2026 року, а невдовзі після цього Високий суд Ірландії затвердив ордер на арешт. Це був підсумок колосальної роботи — оперативної, слідчої та бюрократичної. Але найскладніша частина ще попереду.

Процедура екстрадиції, яка чекає на Кінахана, є тим місцем, де його адвокати матимуть змогу змагатися з державою. Як слушно зазначає Браун, «половинна перемога» означає, що хоча ордер визнаний суддею в ОАЕ і арешт відбувся, сама екстрадиція — це не акт миттєвої видачі, а багаторівневий судовий процес. Кінахан має право оскаржувати видачу через як мінімум дві апеляційні інстанції в судах ОАЕ. Це стандартна правова процедура, і в демократичних суспільствах (а також у юрисдикціях, які прагнуть виглядати такими) вона має бути вичерпана. Тільки після цього, якщо апеляції будуть відхилені, стане можливою фізична передача підозрюваного Ірландії. Тому будь-які прогнози про швидкий суд у Дубліні є надто оптимістичними. Юридична машина, заведена в цій справі, працюватиме місяцями, а можливо, й роками. І навіть після повернення до Ірландії, як нагадує Браун, існує прецедент, коли особи, екстрадовані з величезними труднощами, зрештою були виправдані через недостатність доказів або процесуальні порушення. Жоден результат не є гарантованим.

Чудовим індикатором того, як може розвиватися справа Кінахана, є нещодавня екстрадиція та засудження Шона Макговерна. Його затримали в ОАЕ наприкінці 2024 року та екстрадували навесні 2025 року в рамках тієї самої нової угоди між Ірландією та Еміратами. Після прибуття до Ірландії Макговерн, якого назвали одним із ключових виконавчих керівників угруповання, визнав провину за звинуваченнями в керівництві злочинною організацією, включно з організацією тяжких насильницьких злочинів. Йому загрожує до 30 років ув’язнення.

Цей прецедент є юридичним маяком: він демонструє, що ірландські суди — і ймовірно, Спеціальний кримінальний суд (Special Criminal Court), який традиційно розглядає справи про тероризм та організовану злочинність без участі присяжних через ризики залякування, — кваліфікують такі діяння як одні з найтяжчих. Для Деніела Кінахана, якому офіційно інкримінують «керівництво діяльністю злочинної організації з метою скоєння вбивств та інших серйозних злочинів» (відповідно до Criminal Justice Act 2006), потенційний вирок може бути в тій самій категорії. Але важливо розуміти специфіку: це звинувачення у злочинній змові та лідерстві, а не у скоєнні конкретних убивств. Довести таку статтю складніше, ніж прямий злочин, але у випадку визнання вини покарання є дуже суворим.

Однак історія з Макговерном має й інший, не менш важливий вимір: вона є доказом ефективності нової екстрадиційної архітектури. Браун нагадує, що дипломатичні зусилля Ірландії в ОАЕ не були спонтанною реакцією на справу Кінахана. Міністерство юстиції та Міністерство закордонних справ Ірландії вели системну роботу щонайменше з 2019 року, вибудовуючи довіру та технічну взаємодію із своїми колегами в Абу-Дабі та Дубаї. При цьому дуже важливим є контекст: Ірландія не була піонером. Нідерланди та Велика Британія також успішно домагалися екстрадицій з ОАЕ, що свідчить про формування ширшого, системного тренду. Емірати, які довго зазнавали критики за те, що стали «кримінальним офшором», де можна відкупитися від правосуддя, дедалі більше інтегруються в глобальну правову систему. Це раціональний вибір: ОАЕ прагнуть залучати «чисті» інвестиції, розвивати туризм і фінансовий сектор, а наявність на їхній території кримінальних фігур створює репутаційні ризики. Тому арешт Кінахана слід розглядати не як окремий випадок, а як частину великої геополітичної угоди, де безпека обмінюється на статус.

Що ж відбуватиметься у злочинному підпіллі після цього арешту? Відповідь на це питання є найменш однозначною. Браун із реалістичним скепсисом зазначає, що сучасні організовані злочинні угруповання часто є набагато менш ієрархічними, ніж їх зображають у фільмах. «Картель» — це зручний ярлик, але в реальності — це мережа відносно автономних груп, пов'язаних родинними, фінансовими або просто партнерськими зв'язками. Фрагментація, за словами детектива, вже давно відбулася. Тому вилучення однієї ключової фігури — навіть такої харизматичної, як Деніел Кінахан — не призведе до колапсу всієї системи.

Швидше, ця подія стане каталізатором для двох можливих сценаріїв. Перший — період гострої конкурентної боротьби за контроль над потоками доходів і зв'язками всередині розрізнених фрагментів колишньої «імперії». Такі перехідні періоди майже завжди супроводжуються сплеском насильства, оскільки амбітні молодші партнери намагаються усунути суперників, а старі наставники бояться стати мішенню. Підвищення рівня вбивств і замахів у Європі (особливо в Ірландії, Іспанії та Нідерландах) є цілком прогнозованим побічним ефектом.

Другий сценарій — швидке заповнення вакууму ззовні, коли інші транснаціональні угруповання (наприклад, балканські чи італійські клани) спробують взяти під контроль ланцюги постачання, які раніше контролювали Кінахани. Що стосується кокаїнового ринку Європи в цілому, то на ньому ця подія, найімовірніше, позначиться мінімально. Чому? Тому що він уже є високодиверсифікованим і зрілим: Альбанські, Турецькі, Італійські, Голландські угруповання давно створили власні канали, а колумбійські та еквадорські виробники безпосередньо співпрацюють з десятками посередників. Кінахан, хоч і був могутнім гравцем, ніколи не був монополістом.

З іншого боку, з точки зору верховенства права, арешт Кінахана має колосальне символічне значення, яке важко переоцінити. Протягом довгого часу організована злочинність діяла за логікою «довгих рук»: якщо ти маєш достатньо грошей, ти можеш переселитися в юрисдикцію, де тебе не дістануть, і продовжувати управляти бізнесом через захищене спілкування. Дубай, росія, деякі країни Латинської Америки вважалися такими «тихими гаванями». Арешт Кінахана в ОАЕ разом із попереднім арештом Макговерна надсилає потужний сигнал: для вищих ешелонів криміналітету більше немає абсолютно безпечних місць.

Емірати продемонстрували готовність бути надійним партнером Заходу в обмін на інвестиції, технології та політичну підтримку. Браун акцентує увагу на вирішальному факті: незважаючи на арешт Макговерна, інші фігуранти справи не покинули Дубай поспіхом, що свідчить про їхнє усвідомлення — варіантів для втечі більше не існує. Це є ознакою того, що можливості злочинців вибирати безпечну юрисдикцію катастрофічно звузилися.

Окремим, надзвичайно важливим виміром цієї історії є перспектива конфіскації активів. Бюро з повернення кримінальних активів Ірландії (Criminal Assets Bureau, CAB) має потужні інструменти

цивільної конфіскації, які не потребують обов'язкового кримінального вироку. Механізм «непоясненого багатства» (unexplained wealth order) дозволяє вилучати майно, якщо його власник не може надати законних джерел доходів, пропорційних вартості цього майна. Однак, як зазначає Браун, саме кримінальний вирок — доведення провини у керівництві злочинною організацією — є тим юридичним молотом, який робить цивільну конфіскацію значно легшою та неоспорюваною. Вирок Кінахана (якщо він відбудеться) стане для CAB потужним аргументом у судах різних країн.

Однак труднощі колосальні. Статки Кінаханів розкидані по всьому світу — вони вкладені в нерухомість, бізнеси, трасти, криптовалюти, предмети розкоші. І хоча арешт лідера дає надію на розморожування деяких банківських рахунків, процес репатріації цих грошей до ірландської скарбниці триватиме роками. Більше того, багато активів, ймовірно, вже переписані на підставних осіб, родичів, або надійно заховані за фасадами офшорних компаній. Тому конфіскація — це окрема битва, яка може виявитися не менш важкою, ніж сама екстрадиція.

Підсумовуючи, арешт Деніела Кінахана слід розглядати як важливий маркер у глобальному протистоянні транснаціональній злочинності. Він демонструє, що дипломатія може бути продовженням поліцейської роботи, що судові ордери з невеликої європейської країни здатні перетнути кордони багатих еміратів, а старі концепції «недоторканності» грошей та зв'язків починають руйнуватися.

Однак риторика перемоги була б передчасною: юридичний шлях Кінахана через апеляції в ОАЕ, потім — через лабіринт ірландського судочинства, є вкрай непередбачуваним. Підпільний світ вчиться адаптуватися: фрагментація структур робить їх менш уразливими, а ринок наркотиків продовжує функціонувати за законами попиту та пропозиції, які не залежать від долі однієї людини.

І все ж, це — послання злочинцям: час тихих гаваней спливає. І хоча остаточна крапка в цій історії буде поставлена не сьогодні і не завтра, саме зараз закладається прецедент, який визначатиме правила гри на найближчі десятиліття. Подальший розвиток подій залежатиме від того, чи зможе Ірландія ефективно скористатися наданим шансом, перетворивши арешт на обвинувальний вирок, а вирок — на реальну конфіскацію активів.

Для загального розвитку

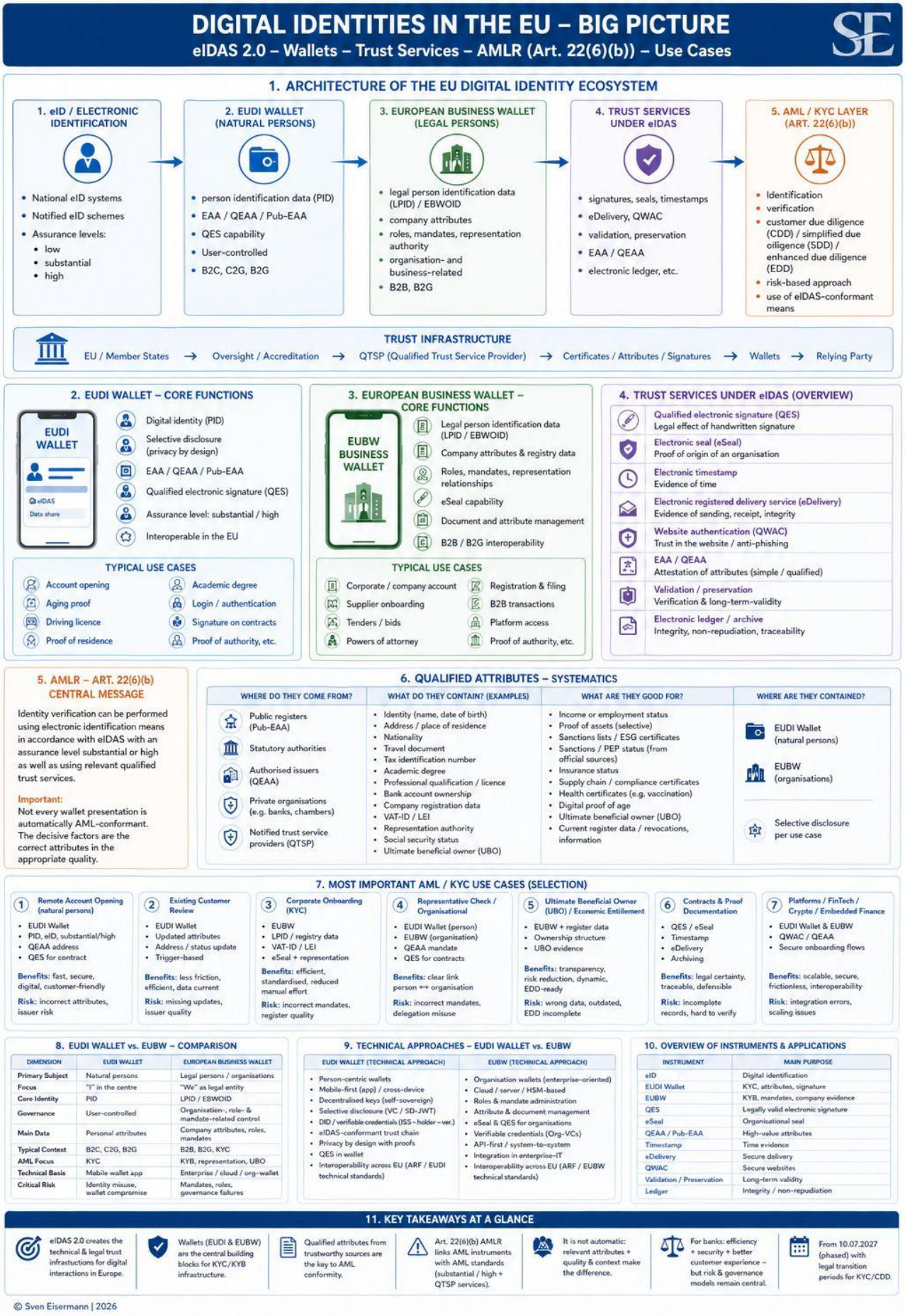
Цифрова ідентичність у ЄС: від "гаманця" до нової інфраструктури AML/KYC [10]

Дискусія навколо нового AML Regulation дедалі частіше виходить за межі класичних питань комплаєнсу: хто є клієнтом, як встановити бенефіціарного власника, які документи прийняти, як

підтвердити джерело коштів або повноваження представника. У центрі цієї дискусії поступово з'являється інше питання: **якою має бути довірена цифрова інфраструктура, на яку зможе спиратися фінансовий моніторинг у цифровій економіці?**

Саме тут eIDAS 2.0 та EUDI Wallet стають набагато більшими, ніж просто черговим "цифровим гаманцем". Вони формують основу нової європейської моделі цифрової ідентичності, де ідентифікація особи, підтвердження атрибутів, електронні підписи, печатки, часові мітки, електронні довірчі послуги та перевірені джерела даних поступово інтегруються у єдину систему довіри. Європейська Комісія прямо описує eIDAS як рамку для цифрової ідентичності та

[10] https://www.linkedin.com/posts/sven-eisermann_in-recent-discussions-around-the-new-eu-aml-activity-7454118671959977984--RPu?utm_source=share&utm_medium=member_desktop&rcm=ACoAABgm5rMBtRqIjMMJhrodqUyKnSXiynEaC40



автентифікації, покликану забезпечити довіру до транскордонних електронних взаємодій і цифрових послуг у ЄС.

Ключова ідея, яку добре демонструє прикріплена схема, полягає в тому, що **EUDI Wallet не існує у вакуумі**. Він є лише одним із елементів ширшої архітектури. Поруч із ним — національні eID-схеми, європейські бізнес-гаманці або організаційні wallet-рішення для юридичних осіб, кваліфіковані постачальники довірчих послуг, сертифікати, електронні атестації атрибутів, механізми перевірки повноважень, реєстрові дані, засоби селективного розкриття інформації та інструменти для використання цих даних у KYC/KYB-процесах. Нове регулювання ЄС щодо цифрової ідентичності встановлює правову рамку для безпечної та інтероперабельної екосистеми цифрової ідентичності, у центрі якої перебувають європейські цифрові гаманці для фізичних і юридичних осіб.

Для AML/CFT це має принципове значення. Традиційна модель KYC часто побудована навколо збирання копій документів, сканів паспортів, виписок, довідок, корпоративних документів та ручної перевірки їхньої актуальності. У такій моделі комплаєнс-процес є дорогим, повільним, фрагментованим і вразливим до помилок. eIDAS 2.0 пропонує іншу логіку: не просто передавати документ, а передавати **перевірений атрибут** — наприклад, ім'я, дату народження, адресу, податковий номер, статус представника компанії, підтвердження повноважень, дані з реєстру, підтвердження професійної ліцензії або інші відомості, видані чи підтверджені довіреним джерелом.

Це змінює саму природу KYC. У центрі вже не стільки "документ", скільки **достовірність походження даних, рівень гарантії, актуальність атрибутів і можливість їх перевірити технічно та юридично**. Для фізичної особи це може означати швидше відкриття рахунку, підтвердження віку, місця проживання, академічного статусу або права на підписання договору. Для юридичної особи — підтвердження реєстраційних даних, організаційної структури, повноважень директора чи представника, мандату на укладання правочину, зв'язку між фізичною особою та компанією, а в перспективі — елементів структури власності чи економічного інтересу.

Особливо важливо, що новий AMLR прямо створює міст між AML-комплаєнсом і цифровою ідентичністю. Регламент (ЄС) 2024/1624 встановлює єдині AML/CFT-правила, які будуть прямо застосовуватися в державах-членах, а його основні положення почнуть застосовуватися з 10 липня 2027 року, за окремими винятками для певних категорій суб'єктів. У контексті CDD AMLR передбачає використання електронних засобів ідентифікації та релевантних довірчих послуг, пов'язаних з eIDAS, зокрема для перевірки ідентичності клієнтів та бенефіціарних власників. Подальші технічні стандарти мають визначити, які саме атрибути повинні містити такі електронні засоби ідентифікації та кваліфіковані довірчі послуги для цілей стандартної, спрощеної та посиленої належної перевірки.

Тому ст. 22(6)(b) AMLR може стати однією з найважливіших норм для майбутнього цифрового онбордингу в ЄС. Її значення не лише в тому, що вона дозволяє використовувати електронну ідентифікацію. Її реальне значення в тому, що вона поступово переводить KYC з площини "прийняти документ від клієнта" у площину "отримати перевірені атрибути з довіреної цифрової інфраструктури". Це може суттєво вплинути на банки, платіжні установи, CASP, страхові компанії, фінтех-платформи, професійних посередників, а також на нефінансові сектори, де ідентифікація клієнта, перевірка повноважень і встановлення реального контролю мають критичне значення.

Водночас важливо не спрощувати картину. **Wallet сам по собі не дорівнює KYC.** Це один із головних меседжів схеми. Не кожне пред'явлення даних із гаманця автоматично забезпечує виконання вимог AMLR. Вирішальними будуть конкретні атрибути, їхнє джерело, рівень гарантії, актуальність, можливість відкликання або оновлення, якість верифікації, а також відповідність конкретному ризиковому профілю клієнта. Саме тому проєкт RTS щодо CDD передбачає, що якщо електронний засіб ідентифікації або кваліфікована довірча послуга не містить усіх

необхідних атрибутів для ідентифікації та перевірки клієнта чи бенефіціарного власника, підзвітний суб'єкт має отримати та перевірити відсутні атрибути іншими засобами.

Це дуже близько до підходу FATF щодо цифрової ідентичності. FATF ще у 2020 році наголошувала, що регульовані суб'єкти повинні застосовувати поінформований ризик-орієнтований підхід до використання digital ID для CDD: розуміти рівень гарантії системи цифрової ідентичності та оцінювати, чи є він належним з огляду на ризики клієнта, продукту, юрисдикції та каналу взаємодії. Тобто цифрова ідентичність не скасовує ризик-орієнтований підхід, а навпаки — робить його більш технічно вимогливим.

Для банків та інших підзвітних суб'єктів це означає появу нового шару комплаєнс-архітектури. Потрібно буде оцінювати не лише клієнта, а й саму цифрову інфраструктуру: хто видав атрибут, чи є постачальник довіреним, який рівень гарантій застосовується, чи є атрибут кваліфікованим, чи можна перевірити його відкликання, чи відповідає набір атрибутів вимогам AMLR, чи покриває він конкретний сценарій CDD, SDD або EDD. У перспективі AML-політики фінансових установ будуть містити не лише процедури роботи з паспортами, реєстрами та корпоративними документами, а й матриці прийнятності цифрових атрибутів, довірчих послуг і кваліфікованих джерел.

Для KYB-сценаріїв потенціал ще більший, але й складність вища. Якщо для фізичної особи базовий набір атрибутів може бути відносно зрозумілим, то для юридичної особи потрібна багаторівнева перевірка: реєстраційні дані, чинність компанії, адреса, органи управління, представники, повноваження, бенефіціарна власність, контроль, групова структура, санкційні ризики, зв'язки з високоризиковими юрисдикціями. Європейський бізнес-гаманець або аналогічні організаційні wallet-рішення можуть стати практичним інструментом для підтвердження частини цих даних, але вони не усунуть потребу в аналітичній оцінці структури власності, ризикового профілю, ділової мети та економічного змісту відносин.

Саме тому майбутнє AML/KYC у ЄС, ймовірно, буде гібридним. Для простих і низькоризикових сценаріїв EUDI Wallet може суттєво спростити та пришвидшити процес ідентифікації клієнта, зменшивши кількість документів, ручних перевірок і зайвих дій під час онбордингу. Для складніших або високоризикових сценаріїв wallet стане лише одним із джерел інформації, яке потрібно поєднувати з реєстрами, санкційним скринінгом, UBO-аналізом, транзакційним моніторингом, аналізом поведінки клієнта та іншими елементами EDD.

Окремої уваги заслуговує принцип селективного розкриття. З AML-погляду він може виглядати як виклик: комплаєнс хоче отримати достатньо даних, а клієнт — розкрити мінімум. Але саме тут виникає баланс між AML/CFT, GDPR і цифровою довірою. У багатьох випадках суб'єкту не потрібно знати весь документ або всі персональні дані. Йому потрібно знати конкретний факт: особа досягла певного віку; адреса підтверджена; особа має право діяти від імені компанії; документ або атрибут чинний; сертифікат не відкликаний. Якщо система дозволяє перевірити саме цей факт без надмірного збору даних, це може посилити як комплаєнс, так і захист приватності.

Однак ризики залишаються суттєвими. Перший ризик — **помилкова довіра до технології**. Якщо установа сприйматиме будь-який атрибут гаманця як достатній для KYC, вона може пропустити відсутні або неякісні дані. Другий ризик — **невідповідність атрибутів AML-вимогам**: наприклад, гаманець підтверджує особу, але не дає достатньої інформації для встановлення бенефіціарного власника або повноважень представника. Третій ризик — **інтеграційні помилки** між інфраструктурою гаманця, банківськими системами, санкційним скринінгом і транзакційним моніторингом. Четвертий — **ризик емітента**: якість даних залежить від того, хто їх видав, як вони оновлюються і як швидко відкликаються. П'ятий — **операційна нерівність** між великими установами, які зможуть швидко інтегрувати нові інструменти, і меншими суб'єктами, для яких це стане дорогим технологічним викликом.

З регуляторної точки зору найважливіше завдання полягає в тому, щоб не перетворити цифрову ідентичність на формальну “галочку” у процедурі KYC. Навпаки, регулятори мають допомогти ринку зрозуміти, які типи електронної ідентифікації прийнятні для яких сценаріїв, які атрибути є мінімально необхідними, коли потрібні додаткові джерела, як документувати покладання на цифрові атрибути, як перевіряти якість постачальників довірчих послуг і як поєднувати онбординг на основі гаманця з поточним моніторингом. Європейська Комісія вже прийняла низку імплементаційних актів щодо wallet-екосистеми, довірчих послуг та електронних атестацій атрибутів, що має забезпечити інтероперабельність, відкликання атрибутів і прийнятність гаманців зареєстрованими у ЄС.

У стратегічному сенсі eIDAS 2.0 може змінити роль AML-комплаєнсу в цифровій економіці. AML більше не буде лише процедурою, яка “наздоганяє” клієнта після того, як він прийшов у банк або на платформу. Він дедалі більше вбудовуватиметься у цифрову інфраструктуру взаємодії між особою, бізнесом, державою, реєстрами та фінансовими установами. Якщо ця модель спрацює, KYC/KYB стане швидшим, стандартизованішим і менш фрагментованим. Якщо ні — ринок отримає ще один складний технологічний шар, який не зменшить, а збільшить комплаєнс-навантаження.

Феномен юрисдикційного дрейфу: чому централізований комплаєнс стає сліпим до локальних загроз [11]

Сучасний світ фінансових регуляцій нагадує не стільки чітко накреслену мапу з усталеними маршрутами, скільки бурхливе море, де кожна держава встановлює власні правила судноплавства, часто змінюючи їх без попередження.

Для міжнародних фінансових інституцій, які оперують одночасно в десятках юрисдикцій, підтримка єдиної системи протидії відмиванню грошей (AML) перетворюється на завдання, що межує з неможливим.

Кожна країна оновлює своє законодавство з власною швидкістю, реагуючи на локальні загрози — від вибухового зростання децентралізованих фінансів до витончених схем торгівельного відмивання коштів, що використовують ланцюги постачання сировини чи контейнерні перевезення. Саме в цьому динамічному, майже хаотичному середовищі виникає явище, що отримало назву «юрисдикційний дрейф» (jurisdictional drift). Цей термін описує стан, коли централізована комплаєнс-модель, побудована на універсальних принципах, поступово втрачає здатність адекватно враховувати специфічні законодавчі нюанси, різні пороги спрацьовування для обов’язкової звітності та неоднаковий ризик-апетит різних суверенних територій. І якщо не впровадити проактивну стратегію синхронізації автоматизованих систем із цими динамічними правовими ландшафтами, організації ризикують зазнати системних збоїв, які не лише підривають цілісність глобальної фінансової системи, але й привертають найпильніший регуляторний нагляд із наслідками у вигляді багатомільйонних штрафів, репутаційних втрат і навіть кримінальних переслідувань.

Ключ до розуміння проблеми полягає в тому, що закони у сфері AML не є статичними документами, викарбуваними на камені. Навпаки, це живі інструменти, які змінюються й

[11] https://fincrimecentral.com/navigating-jurisdictional-drift-aml-compliance/

адаптуються під динаміку локальних соціально-економічних та безпекових пріоритетів. Те, що вважається взірцевою практикою в одному регіоні, може бути абсолютно недоречним в іншому.

Розгляньмо конкретний приклад: Європейський Союз протягом останніх років зробив грандіозний фокус на прозорості кінцевої бенефіціарної власності та тотальному регулюванні постачальників послуг віртуальних активів, включаючи криптовалютні біржі та гаманці. Водночас інші юрисдикції, скажімо, деякі країни Південно-Східної Азії, можуть першочергово зосередитися на моніторингу транзакцій із нерухомістю високої вартості, де традиційно осідають мільярди брудних грошей, або на неформальних системах переказу коштів на кшталт хавали, які століттями існують поза формальним банківським сектором. Коли фінансова установа працює на перетині цих юрисдикцій, її система моніторингу повинна бути достатньо гнучкою, щоб її ключова логіка виявлення підозр — ключові слова, алгоритми поведінкового аналізу, патерни транзакцій — була чутливою до цих локальних пріоритетів. Якщо ж система помилково класифікує діяльність, яка в одній країні вважається низькоризиковою, а в іншій щойно була перекваліфікована як високоризикова, інституція впадає в стан функціональної невідповідності. Це означає, що вона стає сліпою до тих самих активностей, які вона за законом зобов'язана виявляти, розслідувати та повідомляти про них у відповідні органи.

Ця складна картина стає ще більш заплутаною через різну швидкість, з якою різні законодавчі органи рухаються. Уявімо собі країну, яка раптово стає жертвою скоординованої хвилі тероризму або масштабної схеми виведення капіталу. У відповідь уряд може запровадити надзвичайні заходи, змінивши юридичне визначення «підозрілої транзакції» буквально за одну ніч. Новий закон може знизити поріг спрацьовування для звітності з 15 000 до 5 000 доларів або додати цілі нові категорії транзакцій, що підлягають обов'язковому скринінгу. Якщо централізований комплаєнс, який часто представляє собою монолітну IT-систему, не оновлюється з тією самою гнучкістю, він продовжує працювати за застарілими параметрами, використовуючи вчорашні визначення для оцінки сьогоднішніх ризиків.

Це створює глибокий і вкрай небезпечний розрив між внутрішньою оцінкою ризиків банку, яку формує його автоматизована система, та його фактичними правовими зобов'язаннями перед державою, де він отримав ліцензію на діяльність. І тут важливо зрозуміти, що ризик юрисдикційного дрейфу не є виключно технологічним. Це не просто питання застарілого програмного забезпечення чи браку обчислювальних потужностей. Це глибоко структурний ризик, адже він зачіпає саму основу бізнесу — фундаментальну інтерпретацію того, що взагалі вважається протиправною дією, яка підлягає звітуванню. Коли ця інтерпретація розходиться між системою і законом, інституція не просто порушує правила — вона втрачає здатність їх розуміти.

Переходячи до технічної площини, ми стикаємося з головною перешкодою на шляху ефективного управління юрисдикційними вимогами — вродженою негнучкістю багатьох застарілих платформ моніторингу. Більшість із цих систем народжувалася в епоху, коли головним принципом була уніфікація: один набір правил для всіх потоків даних, однакова логіка для всіх ринків. Цей «один розмір підходить усім» (one-size-fits-all) був зручним, поки регуляторні вимоги не почали змінюватись з такою швидкістю. Коли ж сьогодні постає потреба впроваджувати різноманітні, специфічні порогові значення, різні правила зберігання даних, різні часові вікна для звітності, такі монолітні системи починають буксувати. Вони стикаються з конфліктуючою логікою — правило для однієї юрисдикції може суперечити правилу для сусідньої — та з надмірним обчислювальним навантаженням, адже кожну транзакцію доводиться перевіряти за десятками різних наборів правил. У підсумку, намагаючись задовольнити всі вимоги одразу, адміністратори систем часто змушені йти на компроміс, створюючи усереднені налаштування, які не працюють ефективно ніде.

Це явище заслуговує окремої назви — «розмивання якості виявлення» (detection quality dilution). І воно є головним чинником зростання кількості хибнонегативних спрацьовувань —

тих найнебезпечніших випадків, коли система просто не помічає локальних патернів відмивання коштів (наприклад, специфічних схем легалізації через імпорт певних товарів або характерних мереж підставних осіб), тому що ці патерни не досягають глобальних, усереднених критеріїв. В результаті мільйони доларів брудних грошей можуть вільно проходити через рахунки інституції, поки комплаєнс-менеджери спантеличено знизують плечима, не розуміючи, чому їхня «надійна» система мовчить.

Додатковим і часто недооціненим шаром складності є архітектура даних. Адекватна протидія відмиванню грошей вимагає агрегації та глибокого аналізу величезних масивів інформації — про клієнтів, контрагентів, транзакції, географічні зв'язки. Однак кожна територія, особливо після запровадження таких регуляцій, як GDPR у Європі, має власні закони про захист даних і конфіденційність. Ці закони часто прямо забороняють передачу певних типів даних за межі юрисдикції або вимагають їхньої анонімізації. Таким чином, централізований комплаєнс-хаб не може просто так зібрати всі дані до купи в одному дата-центрі в умовному Делавері чи Лондоні. Ця фрагментація даних означає, що моделі машинного навчання, які намагаються виявляти складні схеми, часто доводиться навчати на менших, ізольованих, локальних наборах даних. А будь-який статистик підтвердить: чим менша вибірка, тим більша ймовірність того, що модель втрачає статистичну значущість, стає упередженою (biased) і легко піддається «перенавчанню» (overfitting) під випадкові шуми, а не під реальні загрози. У підсумку ми отримуємо не єдиний механізм, а фрагментовану систему з розрізнених комплаєнс-моделей, кожна з яких має власні слабкі місця. Управляти такою системою надзвичайно складно, проводити її аудит — ще складніше, але найгірше те, що вона стає надзвичайно вразливою до прогалин, які досвідчені злочинні мережі навчаються виявляти й експлуатувати з вражаючою ефективністю.

Отже, що ж робити? Як інституція може не просто виявити, а й виправити юрисдикційний дрейф, перш ніж він призведе до катастрофи? Відповідь криється у впровадженні безперервного, майже рефлекторного зворотного зв'язку між юридичною аналітикою та технічним виконанням. Комплаєнс-менеджери мають перетворитися на детективів, які постійно шукають перші сигнали проблеми.

І найпершим таким сигналом, за даними багатьох розслідувань, є раптова зміна співвідношення між кількістю транзакцій, що спрацювали як «червоні прапорці», та кількістю фактично поданих підозр (Suspicious Activity Reports, SAR) у конкретному регіоні. Якщо протягом кількох місяців цей показник різко падає — наприклад, система сигналізує про тисячу підозр на день, але комплаєнс-підрозділ подає лише одну SAR на тиждень, або навпаки, система мовчить, але місцеве законодавство вимагає звітувати про кожну транзакцію понад певну суму, — це вірна ознака того, що параметри системи безнадійно застаріли. Локальні вимоги просто випередили можливості моніторингу.

І тут потрібна модульна архітектура комплаєнсу. Замість монолітного глобального ядра, зміна якого вимагає місяців тестування та затвердження, інституція повинна мати можливість незалежно оновлювати локальні набори правил. Це дозволяє оновлювати логіку виявлення з тією самою швидкістю, з якою змінюється законодавство.

Але цифри й алгоритми — це лише половина битви. Найціннішим джерелом інформації про юрисдикційний дрейф залишаються люди, які працюють на місцях. Локальні комплаєнс-команди володіють тим знанням, яке рідко можна знайти в базах даних: вони знають, як регіональні злочинні угруповання адаптуються до нових законів, які нові схеми з'являються на вуличному рівні, які легальні бізнеси раптово починають працювати як ширми. Ці інсайти мають бути не просто почуті, а системно інтегровані в роботу центральних команд. Регулярні «сесії налаштування» (tuning sessions) мають стати рутиною: з одного боку місцеві експерти, які розповідають про нові патерни шахрайства, з іншого — аналітики даних, які перетворюють цю інформацію на чіткі параметри детекції, ключові слова, поведінкові тригери. Важливо, що кожне

таке коригування має бути задокументоване з абсолютною прозорістю та «пояснюваністю» (explainability). Аудитор або регулятор має побачити чіткий слід: яка конкретна зміна в законодавстві, яке локальне спостереження чи який аналіз даних призвели до певних змін. Такий підхід перетворює комплаєнс із реактивного, вимушеного та дорогого задоволення на стратегічну перевагу.

Фінальна мета всіх цих зусиль — створення не просто «сумісної», а справді стійкої (resilient) комплаєнс-екосистеми. Термін «стійкість» тут означає не здатність блокувати атаки, а здатність продовжувати ефективно функціонувати в умовах постійних регуляторних змін. Це вимагає радикального зсуву в мисленні: від статичного контрольного списку, де ризик оцінюється раз на рік, до динамічної моделі, керованої аналітикою розвідки (intelligence-driven model). Сучасна стійка організація використовує передову аналітику не просто для моніторингу сьогодення, а для прогнозування майбутнього. Аналізуючи геополітичні тренди, публічні заяви регуляторів, економічні індикатори та навіть риторику міжнародних органів, можна з високою точністю передбачити, в якому напрямку змінюватиметься AML-політика тієї чи іншої країни. Якщо система політичної напруги в регіоні зростає, можна очікувати посилення контролю за фінансуванням тероризму. Якщо країна оголошує про запуск національної цифрової валюти, можна очікувати нових правил щодо криптопереказів. Інституція, яка навчилася читати ці сигнали, починає технічну підготовку — оновлення словників, модифікацію алгоритмів, навчання персоналу — задовго до того, як новий закон буде офіційно опубліковано. Це «випереджальне налаштування» різко скорочує те небезпечне вікно вразливості, яке традиційно відкривається між набуттям чинності новим законом і першою адекватною реакцією на нього з боку банку.

І нарешті, стійкість неможлива без архітектурної гнучкості. Ті самі монолітні системи минулого мають поступитися місцем платформам з відкритою архітектурою, які дозволяють швидко інтегрувати сторонні програмні рішення, спеціалізовані API та зовнішні бази даних. Уявіть собі AML-фреймворк, який працює не як закрита фортеця, а як операційна система, до якої можна «підключати» нові модулі за потребою. Припустимо, одна з країн де присутній банк раптово запроваджує жорсткі закони щодо відстеження походження дорогоцінних металів та каміння. Замість того, щоб переписувати тисячі рядків коду своєї основної системи, стійка інституція просто купує або розробляє спеціалізований інструмент моніторингу ланцюгів постачання та інтегрує його через стандартизований інтерфейс. Через місяць, коли загроза зміниться, цей модуль можна так само легко замінити на інший.

Які ж технологічні рішення можуть допомогти в цьому? Найперспективнішим напрямком виглядає підхід до машинного навчання, коли модель тренується на децентралізованих даних, що залишаються на локальних серверах у кожній юрисдикції, не перетинаючи кордонів. Замість того, щоб збирати чутливі дані про клієнтів в одному місці, алгоритм відвідує кожну локальну модель, «вивчає» її патерни, а потім повертає до глобальної моделі лише узагальнені, анонімізовані оновлення.

У цьому контексті успіх програм AML більше не вимірюватиметься примітивними метриками на кшталт «скільки повідомлень подано». Він вимірюватиметься більш витонченим показником — здатністю організації орієнтуватися в складній павутині глобальних законів із хірургічною точністю та бездоганною доброчесністю. Процвітатимуть ті інституції, які зрозуміють просту, але глибоку істину: юрисдикційний комплаєнс — це не серія окремих, не пов’язаних між собою регуляторних перешкод, які треба подолати. Це цілісний, багатовимірний виклик, який вимагає безпрецедентної інтеграції трьох критичних компетенцій: глибокої юридичної експертизи, передової науки про дані та далекоглядного стратегічного мислення.

Лише ті, хто зможе поєднати ці три елементи та підтримувати пильний, постійний фокус на специфіках кожного локального ринку, не розмиваючи при цьому високої глобальної картини,

зможуть не просто захистити себе від руйнівних ризиків юрисдикційного дрейфу. Вони зможуть перетворити комплаєнс на справжню стратегічну зброю та відігравати провідну роль у глобальній битві проти міжнародної фінансової злочинності.

Ваша думка важлива!

1. Технологія блокчейн мостів є легітимною та необхідною для функціонування DeFi, але водночас є ключовим інструментом відмивання злочинних доходів — чи можливо регулювати її використання, не знищивши при цьому саму інфраструктуру децентралізованих фінансів?
2. Якщо Африка стає зоною релокації кримінальної інфраструктури, наскільки доцільно Україні ініціювати створення спеціальних міжвідомчих робочих групи з країнами регіону (зокрема Кенією, Угандою) для обміну розвідувальними даними про транзит російської зброї, іранських дронів та підсанкційних фінансових потоків?
3. Наскільки може масове безробіття серед молоді та ветеранів після війни, разом із легкою доступністю «злочинності як послуги», спричинити нову хвилю ще більш децентралізованого та технологічного шахрайства, яке неможливо буде контролювати традиційними правоохоронними заходами?
4. Як Україні знайти баланс між використанням «патріотичного шахрайства» проти громадян рф як інструмент інформаційної та економічної війни та ризиком легітимізувати всередині країни кримінальні практики, які обертаються проти власних громадян та міжнародних партнерів?
5. Як Україні під час повоєнної відбудови врахувати ризики кримінального використання інфраструктури ще на етапі її проєктування, щоб нові транспортні коридори не перетворилися на маршрути для контрабанди зброї, наркотиків чи торгівлі людьми?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-18

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

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