Методологічний бюлетень

Серійний номер: МінФін-AML-2025-34

Серпень 2025

“Маленька дія часто спричиняє великий поштовх”

Ноа Скалін

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.

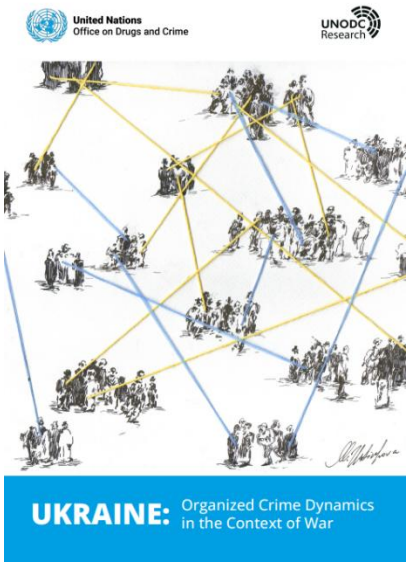
Містить актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

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

Динаміка організованої злочинності в контексті війни [1]

АУДІОПЕРЕКАЗ



У звіті Управління Організації Об'єднаних Націй з наркотиків та злочинності (UNODC) досліджується вплив повномасштабного вторгнення російської федерації в лютому 2022 року на кримінальне середовище України. Звіт охоплює період з січня 2021 року до червня 2024 року, з додатковими даними за 2019-2020 роки для контексту. Основний акцент зроблено на динаміці організованої злочинності та незаконних ринках, включаючи наркотрафік, онлайн-шахрайство, контрабанду зброї, торгівлю людьми та сприяння незаконному перетину кордону. Методологія дослідження ґрунтується на аналізі публічно доступних офіційних статистичних даних, вторинній літературі, судових рішеннях та інтерв'ю з ключовими інформаторами, включаючи представників державних органів та злочинного світу.

[1] https://www.unodc.org/documents/data-and-analysis/Ukraine/Ukraine_OC_Study.pdf

Після початку повномасштабного вторгнення злочинна діяльність, зокрема незаконна торгівля, спочатку скоротилася, але згодом зросла у 2023 році, хоча й не досягла довоєнних масштабів. Українська злочинна «екосистема» є складною і нею не домінує жодна організація. Традиційні злочинні структури, як-от «злодії в законі», були суттєво послаблені завдяки національним правовим та санкційним заходам. У той же час, спостерігається зростання кількості організованих злочинних груп, що займаються виробництвом і продажем синтетичних наркотиків, а також управлінням кол-центрами для здійснення онлайн-шахрайства. Влада України залишається активною в боротьбі з організованою злочинністю, використовуючи законодавчі, кримінально-правові та санкційні заходи. Залежність від донорської допомоги та кредитів спонукала уряд зосередитися на боротьбі з тими видами злочинів, які шкодять іміджу країни, наприклад, з незаконними кол-центрами, що обманюють громадян ЄС.

У сфері наркотрафіку відбулися значні зміни. Після вторгнення у 2022 році кількість вилучень наркотиків різко знизилася, але у 2023 році знову зросла. Головним трендом є зміна трафіку з опіатів на синтетичні наркотики, зокрема катинони, що відповідає загальнорегіональним тенденціям у Східній Європі. Наркотрафік, який раніше здійснювався через морські порти, перемістився на західні сухопутні кордони. Зокрема, обсяг вилучень героїну та кокаїну в 2022-2023 роках значно впав, тоді як вилучення амфетамінів та іншої «синтетики» зросло. Великі злочинні угруповання, такі як «Хімпром», домінують на ринку синтетичних наркотиків, розширюючи свою діяльність на інші кримінальні ринки, зокрема кібершахрайство. Крім того, спостерігається зростання виробництва синтетичного метадону всередині країни. Збільшення споживання наркотиків також пов'язане зі стресом та травмами, спричиненими війною.

Онлайн-шахрайство через кол-центри набуло колосальних масштабів. Кількість таких злочинів у 2023 році більш ніж потроїлася порівняно з попередніми роками. За оцінками, в Україні діє близько 1500 незаконних кол-центрів, які щорічно отримують доходи в розмірі мільярдів доларів. Жертвами шахраїв часто стають внутрішньо переміщені особи та біженці, яких обманюють, обіцяючи державні виплати. Організаційна структура кол-центрів є ієрархічною, з чітким розподілом ролей, і вони часто використовують особисті дані жертв, придбані в даркнеті. Злочинні організації, такі як «Хімпром» та «Дніпровські», активно залучені в цей вид злочинної діяльності.

Контрабанда зброї та її незаконне обіг залишаються переважно низькорівневою та немасштабною діяльністю, яку здійснюють окремі особи, а не організовані злочинні групи. Незважаючи на величезну кількість зброї, що з'явилася в обігу після вторгнення, доказів широкомасштабного транскордонного трафіку зброї з України наразі немає. Правоохоронні органи відзначають зростання кількості вилучень гвинтівок, гранат і гранатометів, що свідчить про зростання внутрішнього обігу зброї. Проте, цей сплеск не відповідає масштабам інтенсивності війни, що може свідчити про ефективні зусилля правоохоронців, логістичні обмеження. Серед нових ризиків — потенційна експлуатація організованими злочинними групами технологій, пов’язаних з модифікацією цивільних дронів для військових цілей.

У сфері контрабанди товарів та митного шахрайства, за оцінками, Україна втрачає мільярди доларів щороку. До війни контрабанда здійснювалася шляхом приховування вантажів або використання підроблених документів. З початком вторгнення виявлена контрабанда, зокрема сигарет, різко скоротилася, особливо морськими шляхами. Проте, спостерігається зростання контрабанди на західних кордонах з Угорщиною. Правоохоронці зауважують, що контрабандисти переорієнтувалися на інші види злочинної діяльності, зокрема на сприяння незаконному перетину кордону для чоловіків призовного віку.

Торгівля людьми зросла через масове переміщення населення. Правоохоронні органи зафіксували спад кількості злочинів, пов'язаних з торгівлею людьми у 2022 році, з невеликим відскоком у 2023 році, однак цифри залишаються нижчими за довоєнний рівень. Вразливість до

торгівлі людьми зросла серед внутрішньо переміщених осіб (ВПО), яких обманним шляхом залучають до примусової праці під виглядом гуманітарної допомоги. Внутрішня торгівля людьми, як правило, носить опортуністичний характер і в більшості випадків здійснюється окремими особами.

Сприяння незаконному перетину кордону чоловіками призовного віку стало новою сферою діяльності для злочинних груп. Після введення заборони на виїзд для чоловіків віком 18-60 років, злочинці почали організовувати незаконні перетини кордону через лісові шляхи та річки, а також за допомогою корупційних схем з отриманням підроблених документів, які надають право на виїзд. Ці схеми включають фіктивні шлюби та отримання фальшивих довідок про непридатність до військової служби. Національна поліція відзначає, що ціна за такі послуги значно зросла після посилення мобілізаційного законодавства у травні 2024 року.

Висновки:

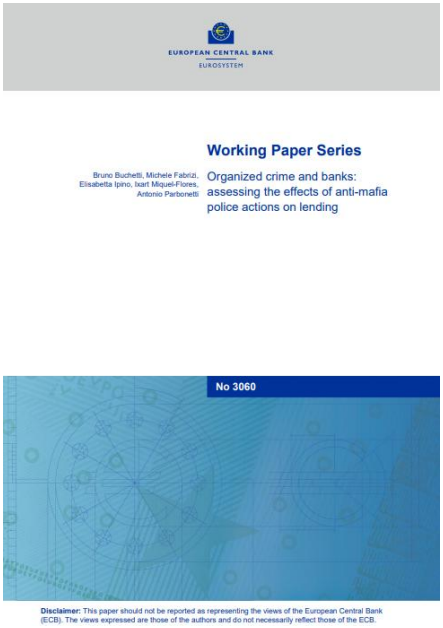
- **Правоохоронні органи повинні адаптувати свої стратегії боротьби зі злочинністю, фокусуючись на кіберпросторі та західних кордонах України**. Існуючі злочинні мережі, зокрема "Хімпром", швидко переорієнтувалися на ринки синтетичних наркотиків та онлайн-шахрайства, використовуючи даркнет та кол-центри. Замість фокусу виключно на традиційних злочинах, необхідно інвестувати в кіберрозвідку, зміцнення міжнародної співпраці у сфері кіберзлочинності та посилити контроль на західних кордонах для протидії зміненим маршрутам трафіку.
- **Необхідно негайно впровадити комплексну програму для управління обігом зброї після війни.** Хоча наразі не виявлено значних масштабів транскордонного трафіку зброї, величезна кількість зброї та боєприпасів в країні створює серйозні довгострокові ризики. Необхідно розробити та реалізувати план добровільної здачі зброї, створити єдиний централізований реєстр зброї та проводити навчання для правоохоронців, щоб ефективно протидіяти її потенційному незаконному обігу після завершення бойових дій.
- **Для захисту найбільш уразливих верств населення необхідно розробити та реалізувати цільові превентивні кампанії.** Значне зростання кількості шахрайств проти ВПО, біженців та родичів військовослужбовців вимагає негайної інформаційної роботи. Держава має співпрацювати з неурядовими організаціями та приватним сектором для інформування населення про нові шахрайські схеми та забезпечення ефективних механізмів подання скарг.
- **Сприяння незаконному перетину кордону чоловіками призовного віку створює додаткові виклики для безпеки та боротьби з корупцією**. Правоохоронні органи повинні зміцнити співпрацю з прикордонними службами сусідніх країн для обміну інформацією про методи та маршрути незаконного перетину. Також критично важливо продовжувати розслідування та притягнення до відповідальності корумпованих чиновників та посередників, які сприяють цим схемам, щоб не допустити використання цих каналів для інших форм злочинної діяльності в майбутньому.

Організована злочинність та банки: оцінка впливу антимафіозних дій поліції на кредитування [2]

Дослідження ЄЦБ аналізує, що відбувається з банківським кредитуванням законних компаній після поліцейських операцій проти мафії в окремих муніципалітетах Італії. Автори поєднали судові матеріали про компанії з ознаками зв'язку з організованою злочинністю з помісячними

[2] https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp3060~2ea4ebd7aa.en.pdf?09dd4374f5132f72d2d8f542e284fc26

мікроданими про кредити з бази AnaCredit та наглядовою інформацією про банки. Це дозволило простежити, як зникнення кримінально інфільтрованих фірм впливає на доступ до фінансування законних підприємств у тих самих або прилеглих муніципалітетах і секторах.


EUROPEAN CENTRAL BANK
EUROSYSTEM

Working Paper Series

Bruno Buchetti, Michele Fabrizi, Elisabetta Ipino, Isart Miquel-Flores, Antonio Parbonetti

Organized crime and banks: assessing the effects of anti-mafia police actions on lending

No 3060

Disclaimer: This paper should not be reported as representing the views of the European Central Bank (ECB). The views expressed are those of the authors and do not necessarily reflect those of the ECB.

Теоретично робота виділяє два механізми. посилення фінансового посередництва: коли кримінальні гравці зникають, конкуренція та прозорість на ринку зростають, законні фірми активніше інвестують і частіше звертаються по кредит. Другий — інформаційний: поліцейські дії «підсвічують» приховані ризики та зв'язки, через що банки певний час обережніші у ціноутворенні та ризик-менеджменті. На перетині цих механізмів і формуються спостережувані зміни у кредитуванні та ставках.

Ключовий емпіричний результат: після зачисток зростає обсяг банківських позик для законних компаній у постраждалих муніципалітетах. У середньому приріст становить близько 0,8%, а в місцевостях із вищою щільністю мафіозної інфільтрації або там, де вилучені фірми активно займалися кришуванням, ефект сильніший — до приблизно 1,6–2,1%. Водночас на короткому відрізку підвищуються середні процентні ставки та оцінена банками ймовірність дефолту позичальників (PD). Автори трактують це як тимчасову «премію за невизначеність»: система перебудовується на нову, більш конкурентну й прозору, і банки закладають додатковий ризик, доки інформаційні асиметрії не зменшаться.

Важлива відмінність проявляється між типами кредиторів. Банки з глибокою локальною присутністю та доступом до «м'якої інформації» про клієнтів (наприклад, кооперативні та загалом вітчизняні установи) підвищують ставки помірніше, адже краще розуміють реальну платоспроможність місцевого бізнесу. Натомість іноземні та не-локальні банки, які більше покладаються на «жорсткі» метрики, реагують різкішим подорожчанням кредиту. Подібну картину видно і за досвідом роботи з ризиковими позичальниками: установи, які раніше не стикалися з клієнтами з кримінальними зв'язками, «перестраховуються» сильніше, тоді як банки з відповідним досвідом майже не змінюють ціноутворення, бо ці ризики вже враховані в їхніх моделях.

Окремий внесок роботи — тверді «реальні» ефекти на продуктивність. Уражені муніципалітети демонструють підвищення агрегованої продуктивності (дохід на працівника з урахуванням активів) після зачистки, причому найбільше — там, де мафія практикувала кришування. Це узгоджується з перерозподілом часток ринку від неефективних (кримінально інфільтрованих) до ефективніших фірм за посередництва кредиту.

Висновки:

- Після антимафіозних операцій кредитування законних фірм у постраждалих муніципалітетах зростає на ≈0,8% (до 1,6–2,1% у найбільш уражених/рентних зонах): це вікно можливостей для стимулювання інвестицій.
- Ціна кредиту й оцінка PD короткостроково підвищуються: регуляторам і муніципалітетам варто закладати перехідний ризик-премію у програми доступного фінансування (гарантії/контргарантії), аби не загальмувати відновлення.
- Продуктивність на рівні галузь-муніципалітет зростає після зачистки, особливо там, де було мафіозне кришування: варто пріоритезувати реформи ділового середовища (спрощення процедур, конкуренція в держзакупівлях) саме в цих зонах, аби закріпити ефект.

Дескриптивні порівняння до інтервенцій підкреслюють, що «кримінальні» фірми мають вищий PD, коротші строки, більше застав і трохи вищі ставки, що створює негативні зовнішні ефекти для фінансового сектору ще до дій правоохоронців. Політично-регуляторний меседж авторів прагматичний: системне зменшення мафіозної присутності не лише розчищає канали фінансового посередництва, а й запускає довготривалий перерозподіл капіталу; важливо підтримувати прозорість і спроможності банків до збору «soft information», аби згладжувати інформаційні асиметрії у перехідний період.

Річний звіт ірландського підрозділу з питань дотримання вимог з ПВК [3]

Цей звіт, виданий AMLCU — підрозділом Міністерства юстиції Ірландії, — описує діяльність відомства як компетентного органу з нагляду за визначеними нефінансовими установами та професіями, які мають запобігати використанню своїх бізнесів для відмивання коштів та фінансування тероризму. Звіт відображає роботу AMLCU за 2024 рік, що є частиною імплементації ірландського законодавства, яке, своєю чергою, базується на стандартах FATF та ЄС. AMLCU виступає як компетентний орган за замовчуванням у тих випадках, коли для певної категорії підзвітних суб’єктів не існує іншого наглядового органу.

У 2024 році AMLCU провело 749 перевірок, що на 14% більше, ніж у 2023 році. Більшість перевірок були виїзними. Перевірки охопили різні сектори, при цьому найбільша кількість перевірок була у дилерів дорогих товарів (HVGD) — 419, за ними йшли надавачі трастових та корпоративних послуг (TCSPs) — 163, та надавачі гральних послуг — 66.

Інспектори AMLCU оцінюють дотримання компаніями їхніх ключових зобов'язань відповідно до Закону від 2010 року, включаючи документування оцінки ризиків, проведення належної перевірки клієнтів (CDD), а також наявність внутрішніх політик, процедур та програм навчання. У звіті надано детальну розбивку рівнів відповідності за секторами. З 163 перевірених TCSPs, 110 повністю відповідали законодавчим нормам, 29 — частково відповідали, і лише 1 — не відповідав. Для HVGDs, 102 повінстю відповідали нормам, 64 — частково , і 9 — не відповідали. У 2024 році AMLCU видало 49 розпоряджень (directions), що є юридичними інструкціями для забезпечення відповідності.

У звіті зазначається, що вторгнення росії в Україну та пов'язані з ним фінансові санкції є важливими факторами, які можуть вплинути на бізнеси, що перебувають під наглядом AMLCU, особливо на тих, хто займається торгівлею дорогоцінними металами, такими як золото, та деяких TCSPs. Хоча AMLCU не є компетентним органом щодо санкцій, воно надає своїм підзвітним суб'єктам інформацію та вказівки щодо різних пакетів санкцій. Ця діяльність є частиною ширших національних зусиль, які координує Міжвідомчий комітет з міжнародних санкцій (CDISC), членом якого є Міністерство юстиції.

Згідно з даними, наданими ПФР Ірландії, загальна кількість STR, отриманих від усіх типів бізнесів у 2024 році, становила 35 544, що є зниженням у порівнянні з 52 222 у 2023 році. Проте загальна кількість повідомлень, поданих усіма суб'єктами, включаючи спеціальні повідомлення для країн ЄС (STReu), склала 60 753, що на 12% менше, ніж у 2023 році. AMLCU, зі свого боку, подало 59 повідомлень компетентного органу (CAR) до ПФР Ірландія та Податкової служби, повідомляючи про інформацію або підозру у відмиванні коштів чи фінансуванні тероризму.

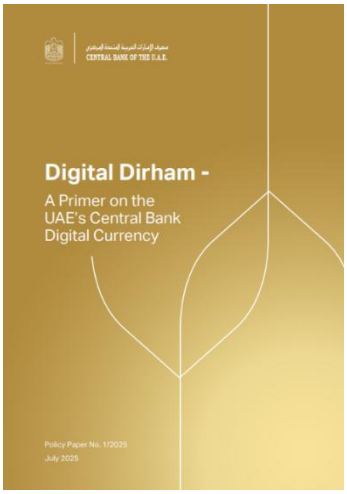
[3] https://www.amlcompliance.ie/wp-content/uploads/2025/07/AMLCU-2024-Annual-Report-.pdf

У звіті обговорюється розширення регуляторних повноважень AMLCU. Робоча група рекомендувала надати AMLCU право накладати адміністративні штрафи. Цю рекомендацію буде реалізовано шляхом впровадження режиму адміністративних санкцій у зв'язку з транспозицією нової 6-ї Директиви ЄС про протидію відмиванню коштів (EU 2024/1640), яку було узгоджено державами-членами у 2024 році. AMLCU також активно проводить просвітницьку роботу, зокрема підтримує спеціальний веб-сайт, www.amlcompliance.ie, який є ключовим інструментом для надання інформації та ресурсів. У 2024 році AMLCU провело спеціальні заходи (streetscape events) у великих містах, поєднуючи інспекції з інформаційними семінарами для місцевих підприємств.

Висновки:

- **Розширення повноважень для підвищення ефективності:** Заплановане надання AMLCU права накладати адміністративні штрафи є критично важливим для підвищення ефективності нагляду. Це дозволить швидше та гнучкіше реагувати на порушення, ніж через поточну систему, яка може вимагати тривалішого судового переслідування.
- **Цільова просвітницька робота та співпраця є запорукою успіху:** Активні заходи AMLCU та публікація детальних посібників є ефективними методами для підвищення обізнаності та рівня відповідності у секторах з високим ризиком. Ці зусилля мають бути масштабовані, щоб охопити всі підприємства та допомогти їм зрозуміти свої зобов'язання і запровадити ефективні заходи ПВК/ФТ.
- **Посилення нагляду за санкційними ризиками:** AMLCU має підтримувати посилену пильність у секторах, що можуть бути схильні до впливу санкцій, пов'язаних із вторгненням в Україну. Активна взаємодія та поширення інформації є ключовим для запобігання обходу санкцій та дотримання міжнародних зобов'язань.
- **Аналіз та поглиблення співпраці щодо STR:** Зменшення загальної кількості STR може вказувати на певні тенденції, але AMLCU, подавши 59 CARs, демонструє проактивну позицію. Постійний діалог та співпраця з ПФР Ірландії та іншими компетентними органами є життєво важливими для забезпечення того, щоб будь-яке зниження кількості STR відображало не зменшення пильності, а скоріше більш цілеспрямовану та ефективну систему звітності.

CBDC як інструмент фінансової трансформації: політика та досвід ОАЕ з Digital Dirham [4]



Документ є комплексною політичною запискою Центрального банку Об'єднаних Арабських Еміратів, яка окреслює стратегічні засади, дизайн, політичні рішення, ризики та стан реалізації національної цифрової валюти центрального банку – Digital Dirham (цифровий дирхам). У вступній частині наголошується, що поява Digital Dirham є відповіддю на трансформацію глобальної фінансової архітектури та потребу адаптувати монетарну систему до вимог цифрової економіки. Центральний банк розглядає Digital Dirham як безпечний, програмований та доступний «цифровий аналог готівки», який зберігає статус законного платіжного засобу, забезпечує довіру, притаманну грошам центрального банку, і водночас відкриває нові можливості для інновацій у сфері платежів. Його поява стала логічним етапом багаторічної програми Financial Infrastructure

[4] https://www.centralbank.ae/media/lczb23l4/cbdc-short-report_july.pdf

Transformation (FIT), метою якої є модернізація платіжної системи, стимулювання фінансових інновацій та посилення ефективності монетарної політики.

Важливе місце у документі займає пояснення політичних і стратегічних рішень, що визначили концепцію Digital Dirham. Центральний банк прагне підвищити стійкість фінансової системи, поліпшити механізми передавання сигналів монетарної політики та гарантувати безперервний доступ суспільства до грошей центрального банку у цифровому форматі. Серед ключових переваг відзначається здешевлення та прискорення платежів, зниження операційних витрат, посилення конкуренції у фінансовому секторі та розширення фінансової інклюзії. Digital Dirham має забезпечити доступність фінансових послуг для небанківських і слабко охоплених груп, включно з численною міграційною робочою силою в ОАЕ. Окремо підкреслюється значення транскордонних розрахунків і участі країни у проєктах на кшталт mBridge, що створює передумови для посилення міжнародної ролі дирхама у регіональній та глобальній торгівлі.

Водночас документ приділяє багато уваги потенційним ризикам і шляхам їх мінімізації. Йдеться про можливу дестабілізацію банківських депозитів у разі високої популярності CBDC як «безпечного активу» у кризові періоди, однак цей ризик знижено завдяки відсутності відсотків на цифрові кошти та запровадженню лімітів на обсяг утримання. Монетарна політика зберігатиме стабільність за умови, що цифровий дирхам використовуватиметься передусім як платіжний інструмент, а не засіб заощадження. Для уникнення виключення окремих категорій населення Центральний банк планує впроваджувати програми цифрової фінансової грамотності та забезпечувати простий і доступний формат користування. Ще один виклик стосується конфіденційності: надмірна анонімність може сприяти відмиванню коштів, тоді як надмірний контроль – обмежувати економічну свободу. Тому обрана збалансована модель, у якій персональні дані зберігатимуться у ліцензованих фінансових посередників, транзакції матимуть рівень псевдонімності, а водночас залишатиметься можливість ідентифікації та відстеження у разі підозри на фінансовий злочин відповідно до вимог KYC/AML/CFT. Не менш важливими є питання кібербезпеки: у документі зазначається, що система побудована на приватній технології розподіленого реєстру (DLT), протестована з урахуванням стресових сценаріїв і забезпечує високу стійкість до кібератак.

Дизайн Digital Dirham вирізняється низкою особливостей. Розповсюдження здійснюватиметься за дворівневою моделлю: Центральний банк випускатиме валюту і зберігатиме контроль за монетарною стабільністю, тоді як ліцензовані фінансові установи, обмінні компанії, постачальники платіжних послуг та фінтехи з відповідними ліцензіями забезпечуватимуть розподіл і надання цифрових гаманців. Гаманці матимуть багаторівневі ліміти залежно від категорії користувачів – резиденти, бізнес, туристи, при цьому передбачено інноваційні функції, як-от дочірні гаманці (sub-wallet) для батьків і дітей, програмовані соціальні виплати чи смарт-гаманці для туристів. Усі операції здійснюватимуться на базі приватного блокчейну із контрольованим доступом з поєднанням токенізованого і акаунтного підходів, що гарантує безпеку, інтеграцію з іншими платіжними системами та потенціал для розвитку цифрових активів. Digital Dirham буде повністю конвертованим у всі форми грошових коштів, номінованих у дирхамах, а також інтегрованим із монетарними інструментами CBUAE, включаючи резервні вимоги та депозитні й кредитні операції.

Окремий акцент зроблено на юридичному фундаменті. У жовтні 2023 року було ухвалено Федеральний закон №54, яким внесено зміни до базового закону про Центральний банк і фінансові інститути. Завдяки цьому цифрову валюту прямо визнано законним платіжним засобом нарівні з готівкою, а Раді директорів CBUAE надано повноваження врегульовувати технічні аспекти емісії. Це створює міцне правове підґрунтя для впровадження нової форми грошей і закладає гарантії для користувачів та фінансових інституцій.

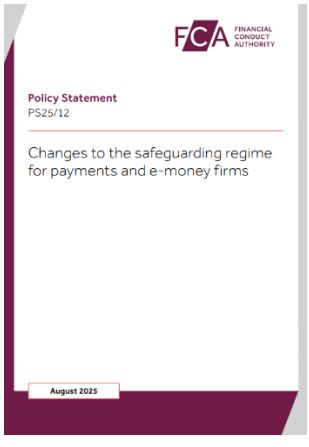
Документ також детально описує стан реалізації проєкту. Перша фаза (березень 2023 – червень 2024) включала розробку платформи емісії, тестування MVP (мінімально життєздатний продукт) у рамках mBridge, проведення пілотного роздрібного запуску з кількома банками та впровадження чотирьох практичних сценаріїв використання: токенізовані активи, соціальні виплати у програмованій формі, смарт-гаманці для туристів та дочірні гаманці для сімейного використання. Ці експерименти продемонстрували гнучкість та інноваційність Digital Dirham, зокрема можливості програмування цільового використання коштів чи створення нових бізнес-моделей. У другій фазі передбачено поступове впровадження повномасштабного використання у роздрібному, оптовому та транскордонному сегментах, із подальшою інтеграцією у багатосторонні системи та розширенням кола практичних застосувань.

Висновки:

- **Регуляторний фундамент створено** – законодавчо Digital Dirham вже визнаний законним платіжним засобом; CBUAE готовий до масштабного запуску.
- **Фінансова стабільність захищена** – встановлено ліміти зберігання, Digital Dirham не приносить відсотків, що знижує ризики відтоку депозитів з банків.
- **Програмованість відкриває нові сервіси** – CBDC застосовується у соціальних виплатах, туризмі, токенізації активів, що стимулює розвиток цифрової економіки.
- **Баланс між ПВК/ФТ і приватністю** – впроваджена модель з KYC, псевдонімністю та відсутністю зберігання персональних даних на реєстрі, що одночасно зберігає права користувачів і підтримує боротьбу з фінансовими злочинами.

У завершенні наголошується, що успіх Digital Dirham залежатиме від обережної, поетапної і водночас інноваційної імплементації, тісної співпраці з приватним сектором та державними інституціями, постійного моніторингу ризиків і технологічних змін. Центральний банк прагне досягти балансу між стабільністю і розвитком, забезпечити захист від фінансових злочинів, гарантувати кіберстійкість та розвивати фінансову інклюзію, при цьому не перетворюючи цифрову валюту на інструмент заощадження, а використовуючи її насамперед як універсальний і програмований платіжний засіб. Таким чином, документ подає Digital Dirham не лише як технологічну інновацію, а як стратегічний інструмент державної політики, спрямований на зміцнення позицій ОАЕ у глобальній фінансовій екосистемі.

PS25/12 як дорожня карта для ринку активів у Сполученому Королівстві: бачення FCA [5]



Документ є підсумковою публікацією британського регулятора фінансових ринків, що фіксує офіційну позицію з питань оновлення регуляторного режиму для компаній, які здійснюють діяльність у сфері управління фондами та функціонування інвестиційних ринків. Це підсумок тривалого процесу консультацій, у межах якого розглядалися як практичні виклики галузі, так і стратегічні завдання державної політики у сфері фінансів. FCA у документі демонструє, що його підхід не є суто технічним: він прагне не тільки встановити чіткі правила, але й забезпечити, щоб вони були пропорційними, досяжними та відповідали як потребам ринку, так і завданню захисту інвесторів. У цьому сенсі документ є не лише збіркою нормативних вимог, а й

[5] https://www.fca.org.uk/publication/policy/ps25-12.pdf

аналітичною рамкою, яка пояснює, чому ці вимоги виникають, які ризики вони покликані знизити та які очікувані ефекти мають принести.

У вступі FCA підкреслює, що ринок управління активами перебуває під впливом глобальних трансформацій: інтеграція міжнародних стандартів, перехід до нових моделей регуляторного нагляду після Brexit, зростання ролі ESG-факторів, а також зрушення в поведінці інвесторів, які вимагають більшої прозорості та відповідальності від фінансових установ. На цьому тлі Сполученому Королівству потрібно зберігати баланс між регуляторною жорсткістю та привабливістю ринку для міжнародних інвестицій. Регулятор прямо наголошує: оновлення правил спрямоване не на створення додаткових бар'єрів для бізнесу, а на забезпечення довгострокової стабільності, що вигідно всім учасникам фінансової системи.

Важливим елементом документа є детальний виклад результатів консультацій із галуззю. FCA демонструє відкритість і пояснює, які саме питання викликали найбільшу кількість коментарів. Наприклад, серед основних занепокоєнь бізнесу були витрати на впровадження нових стандартів розкриття інформації та управління ризиками, а також питання пропорційності для невеликих компаній. Деякі учасники ринку побоювалися, що надмірна зарегульованість може знизити їхню конкурентоспроможність. Водночас інші респонденти наполягали на необхідності високих стандартів прозорості та контролю, оскільки саме вони є запорукою довіри інвесторів. У підсумку FCA у документі показує, як кожен коментар був врахований: деякі пропозиції були прийняті, інші — відхилені, а частина модифікована. Це підкреслює принцип пропорційності та зваженості, що є характерним для британського регуляторного підходу.

Важливим тематичним блоком документа є корпоративне управління та відповідальність керівних органів. FCA наголошує, що проблеми минулого, пов'язані з кризами фондів і банкрутствами компаній, часто виникали через розмиту відповідальність, недостатній рівень підзвітності та неефективну роботу рад директорів. У нових правилах чітко фіксується, що кожна ключова управлінська функція має бути закріплена за конкретною особою, яка нестиме персональну відповідальність. Рада директорів повинна мати не лише формальну, а й реальну можливість контролювати стратегічні та ризик-менеджментові рішення. Таким чином, FCA прагне зробити управління фондами більш професійним, прозорим і підзвітним.

Не менш вагомим є розділ, присвячений управлінню ризиками та ліквідністю. FCA докладно описує очікування від компаній у цій сфері: наявність чітких внутрішніх політик, проведення регулярних стрес-тестів, сценарне планування та здатність швидко реагувати на кризи. Наголошується, що особливе значення має управління ліквідністю у фондах відкритого типу, які схильні до ризику масового викупу. Нові положення зобов'язують компанії створювати такі механізми управління активами, які дозволять витримати навіть несподівані шоки, захистивши тим самим інтереси дрібних інвесторів. Ці вимоги прямо випливають із уроків глобальної фінансової кризи 2008 року та подій пандемії COVID-19, коли раптовий відтік капіталу створював системні загрози.

Окремим, надзвичайно значущим блоком є питання прозорості та розкриття інформації. FCA у фінальній редакції правил зобов'язує компанії більш детально звітувати перед інвесторами. Це стосується як традиційних аспектів — структури витрат, політики винагород, інвестиційних стратегій, — так і нових напрямів, включно з ESG-показниками. Регулятор підкреслює: інвестор має право знати, як саме управляються його кошти, які ризики бере на себе фонд і як компанія враховує фактори сталого розвитку. Ця вимога відображає глобальний тренд посилення уваги до ESG і робить британський ринок більш сучасним і відповідальним у порівнянні з багатьма іншими юрисдикціями.

Не оминув документ і питання капітальних вимог. FCA прямо говорить, що кожна компанія має забезпечувати достатній рівень власного капіталу для покриття можливих операційних збитків. І хоча для багатьох учасників це означає додаткові фінансові витрати, регулятор доводить, що

це необхідний інструмент довгострокової стабільності. Щоб уникнути надмірного навантаження на невеликі компанії, застосовано принцип пропорційності: вимоги диференціюються залежно від розміру та складності діяльності конкретного суб'єкта. У такий спосіб FCA намагається підтримати баланс між безпекою та життєздатністю бізнесу.

Важливою частиною документа є роз'яснення перехідних положень. FCA усвідомлює, що одномоментне впровадження нових правил може стати шоком для індустрії. Тому регулятор передбачає поетапне введення вимог, чітко визначає часові рамки та навіть допускає певну гнучкість у реалізації окремих стандартів. Це дозволяє компаніям адаптуватися без серйозних ризиків для їхньої фінансової стабільності, а також дає змогу інвесторам поступово звикнути до нових форм звітності. FCA також бере на себе зобов'язання надавати роз'яснення та консультації, щоб знизити регуляторну невизначеність.

У фінальній частині FCA підсумовує очікуваний ефект від впровадження PS25/12. Це насамперед підвищення рівня довіри інвесторів, зміцнення репутації британського ринку як прозорого та стійкого, а також створення більш рівних конкурентних умов для компаній різного масштабу. Крім того, документ має стратегічне значення в контексті глобальної інтеграції: його положення гармонізуються з міжнародними стандартами, але водночас демонструють прагнення Сполученого Королівства вибудовувати власну регуляторну ідентичність після Brexit. У цьому сенсі PS25/12 можна розглядати як крок у формуванні нової моделі фінансового регулювання, яка поєднує глобальні підходи з національними інтересами.

Висновки:

- **Фінансові установи повинні запровадити щоденний контроль за коштами клієнтів, вести план регулювання і бути готовими до швидкого повернення коштів у разі банкрутства.**
  Практичний результат: зменшення часу та витрат при ліквідації компанії та зниження ризику втрати грошей споживачами.
- **Щорічний аудит захисту коштів клієнтів стане обов'язковим для більшості платіжних фірм та установ електронних грошей, що підвищує прозорість та дисципліну ринку.**
  Практичний результат: раніше виявлення порушень і підвищення довіри споживачів та партнерів.
- **Новий щомісячний звіт до FCA дозволить регулятору оперативніше виявляти проблеми, зокрема короткострокові розриви ліквідності.**
  Практичний результат: точковий нагляд, швидше втручання FCA, зниження системних ризиків.
- **Фінансові компанії повинні завчасно планувати страхові чи гарантійні покриття, інакше переходити на метод сегрегації.**
  Практичний результат: уникнення ризиків «різкого переходу», коли клієнтські кошти раптово залишаються без захисту.

SupTech у ПВК/ФТ-нагляді ЄС: нова роль технологій у протидії фінансовим злочинам та становленні AMLA [6]

Документ Європейського банківського органу присвячений огляду стану впровадження та використання інноваційних інструментів наглядових технологій (SupTech) у сфері протидії відмиванню коштів і фінансуванню тероризму в Європейському Союзі. Його підготовка стала логічним продовженням ухвалення у червні 2024 року нового пакету законодавства ЄС з

[6] https://www.eba.europa.eu/sites/default/files/2025-08/2ed3b67d-880b-428d-8282-15689f65b12f/Report%20on%20the%20use%20of%20AMLCFT%20SupTech%20tools.pdf

ПВК/ФТ, який докорінно змінює правові та інституційні підходи до протидії фінансовим злочинам. Одним із ключових елементів цього пакету стало створення нового наднаціонального органу – AMLA, який покликаний координувати діяльність національних регуляторів, забезпечувати узгодженість застосування правил, уніфікацію методології нагляду та сприяти більш ефективній співпраці фінансових розвідок. Впровадження такого органу створює сприятливе підґрунтя для цифрової трансформації нагляду, де SupTech визначається як один із найважливіших інструментів.

У документі зазначено, що попри ранній етап розвитку, використання SupTech швидко поширюється в ЄС. За результатами опитування, проведеного у 2024 році серед 31 компетентного органу з 25 держав-членів і трьох країн-партнерів, загалом зафіксовано близько 60 проєктів і інструментів, що застосовуються для виконання завдань нагляду за ПВК/ФТ. У більшості випадків вони орієнтовані на обробку великих масивів даних, проведення ризик-орієнтованих оцінок, автоматизацію процесів та візуалізацію інформації. При цьому майже половина проєктів уже перебуває у виробничому використанні, тоді як інші знаходяться на стадії розробки чи тестування. Це свідчить про поступове, але впевнене закріплення SupTech як невід'ємної складової сучасного нагляду.

Документ наводить низку прикладів використання SupTech: централізовані системи планування інспекцій, які спрощують аудит і контроль виконання приписів; автоматизовані інструменти оцінки ризиків із застосуванням штучного інтелекту та обробки природної мови; блокчейн-аналітичні платформи для моніторингу транзакцій у сфері криптовалют; комплексні системи управління ризиками, що підтримують координацію між різними органами; інструменти для перевірки доброчесності та придатності керівників фінансових установ, які дозволяють структурувати дані та формувати скорингові оцінки. Усі ці приклади демонструють потенціал SupTech у підвищенні точності ризик-аналізу, зростанні ефективності використання ресурсів і посиленні якості рішень.

Особливу увагу у звіті приділено вигодам від використання SupTech. Серед них покращення якості даних, які стають більш структурованими, систематизованими та придатними для порівняння; підвищення швидкості й глибини аналітичних процесів, що дозволяє наглядовим органам своєчасно виявляти нові загрози та оцінювати адекватність систем контролю у піднаглядних установах; оптимізація ресурсів завдяки автоматизації рутинних завдань; своєчасне виявлення нових тенденцій у сфері відмивання коштів і фінансування тероризму, включно з ризиками, пов'язаними з криптоактивами; покращення співпраці між різними юрисдикціями, що особливо важливо в умовах європейської інтеграції та зростання транскордонних ризиків.

Разом із тим документ висвітлює й низку серйозних викликів. Найбільшою проблемою залишається якість даних – фрагментованість, неповнота та несумісність різних джерел негативно впливають на точність аналітики та ефективність ризик-орієнтованих підходів. Значною перешкодою є також обмежені ресурси, адже багато національних органів стикаються з дефіцитом бюджетів, застарілою IT-інфраструктурою та браком спеціалістів у галузі аналізу даних і штучного інтелекту. Правові ризики залишаються невирішеними: відсутня чітка регламентація питань захисту даних при використанні великих масивів інформації, а також існує невизначеність щодо відповідальності при застосуванні алгоритмічних рішень. Додатково звертається увага на операційні ризики – збої систем, непрозорість алгоритмів і труднощі з поясненням результатів рішень, що може підірвати довіру до нових технологій. У цьому контексті серйозною проблемою є також підзвітність, адже регулятори повинні бути готові обґрунтовувати свої висновки, навіть якщо вони базуються на алгоритмічних моделях, що часто не мають достатньої прозорості. Не менш вагомим викликом є інституційний спротив, брак

цифрової грамотності серед персоналу та побоювання щодо заміни традиційних процесів технологіями.

Попри це, у звіті визначено низку практик, які можуть суттєво полегшити впровадження SupTech. Йдеться про формування цифрової культури та впровадження стратегій управління змінами, що дозволяють зменшити внутрішній спротив і залучити персонал до використання нових підходів; створення систем управління даними та стандартів інтероперабельності для забезпечення сумісності й уніфікації інформаційних потоків; використання синтетичних даних для тестування та навчання алгоритмів без порушення вимог захисту персональної інформації; активну співпрацю з технологічними компаніями, іншими органами та експертами задля обміну досвідом і кращими практиками; впровадження регуляторної пісочниці для експериментального тестування інструментів у безпечному середовищі; створення чітких метрик ефективності, які дозволяють оцінити реальний вплив кожного інструменту на процес нагляду. Важливим є й те, що впровадження має бути орієнтованим на конкретні потреби нагляду, а не зумовленим самою доступністю технологій.

Висновки:

- **SupTech у ПВК/ФТ перебуває на ранній стадії, але швидко розвивається –** майже половина інструментів уже у використанні, що свідчить про системний перехід до цифрового нагляду, хоча більшість органів почуваються лише «помірно готовими».
- **Найбільший потенціал SupTech полягає у підвищенні якості даних, аналітики та ефективності нагляду,** включно з можливістю швидше виявляти нові ризики (особливо у сфері криптоактивів) та підвищувати рівень співпраці між юрисдикціями.
- **Основні бар'єри – слабка якість даних, нестача ресурсів, правова невизначеність і спротив змінам,** які можуть загальмувати масштабне впровадження. Без вирішення цих проблем інноваційні інструменти не принесуть очікуваних результатів.
- **Успіх впровадження залежить від стратегічного та потребо-орієнтованого підходу –** необхідно забезпечити чітке управління даними, інтероперабельність, правові гарантії, навчання персоналу й узгодженість із реальними завданнями нагляду, а також активну координацію на рівні AMLA.

У підсумку Європейський банківський орган констатує, що використання SupTech у сфері ПВК/ФТ перебуває на ранньому етапі, але демонструє значний потенціал. Успіх залежатиме від здатності вирішити проблеми з якістю даних, ресурсами, правовою визначеністю й управлінням ризиками, а також від рівня готовності до інституційної трансформації. Особливо наголошується на важливості координації через AMLA, що дозволить уникнути дублювання зусиль, сприяти розробці сумісних і масштабованих інструментів, а також забезпечити більш тісну співпрацю між наглядовими органами. Таким чином, документ визначає SupTech як ключовий напрям розвитку європейського нагляду, який у перспективі може радикально посилити здатність ЄС протидіяти новим викликам у сфері фінансової злочинності, забезпечуючи технологічну гнучкість, правову захищеність і стратегічну єдність.

Оновлене керівництво FCA щодо політично значущих осіб: пропорційний ризик-орієнтований підхід до PEP у Сполученому Королівстві [7]

Документ, підготовлений Управлінням фінансового нагляду Сполученого Королівства (FCA), є фіналізованим керівництвом, що визначає підхід до політично значущих осіб (PEP) для цілей протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Його структура побудована на базі вимог Money Laundering Regulations 2017 у редакції після змін 2023–2024 років і результатів перегляду практики застосування правил щодо PEP, який було проведено FCA у 2024 році. Документ є логічним продовженням первинного керівництва 2017 року та консультації 2024 року і покликаний уточнити, стандартизувати та водночас зробити більш пропорційним ризик-орієнтований підхід до PEP, членів їхніх родин і відомих близьких осіб. Його головна ідея полягає у балансі між вимогами міжнародних стандартів FATF, превентивним характером регулювання та потребою уникнути надмірного навантаження на установи, зокрема в частині відносин з внутрішніми британськими політичними діячами.

У вступних положеннях FCA наголошує, що політично значуща особа — це не «ризикова особа за замовчуванням», а особа, яка в силу займаної посади може бути більш уразливою до спроб корупційного впливу чи зловживань. Тому посилена перевірка клієнта (EDD) застосовується превентивно, не є ознакою кримінальної поведінки, а спрямована на посилення фінансової стійкості системи. Саме тому FCA ще раз підтверджує ключову зміну у британському праві: всі національні PEP за замовчуванням вважаються низькоризиковими, на відміну від іноземних PEP, які потребують ретельнішої уваги. Водночас для обох категорій вимагається індивідуальна оцінка ризику, що враховує контекст посади, географію, характер фінансового продукту та інші обставини.

У документі детально роз'яснюється, кого слід вважати PEP у британському контексті. Це насамперед глави держав і урядів, міністри та їхні заступники, члени парламентів та аналогічних законодавчих органів включно з парламентами Шотландії, Уельсу та Північної Ірландії, керівники партій, які мають представництво в національних парламентах, судді Верховного Суду, члени вищих судів, керівники центральних банків, вищі офіцери Збройних сил (рівня віце-адмірала, генерал-лейтенанта або маршала авіації), керівники державних підприємств, де держава має контрольний пакет акцій, та керівні органи міжнародних міжурядових організацій (ООН, НАТО тощо). FCA спеціально підкреслює, що до PEP не слід відносити місцевих чиновників, членів муніципальних органів влади, середніх і молодших державних службовців, а також незалежних невиконавчих директорів міністерств. Таким чином, коло осіб максимально звужується до тих, хто дійсно володіє владними повноваженнями, здатними створити масштабні корупційні ризики.

Документ також систематизує підхід до членів сімей PEP та відомих близьких осіб. До сім'ї обов'язково належать подружжя, цивільні партнери, діти та їхні подружжя, батьки і брати/сестри, але у випадках вищого ризику коло може бути розширене, наприклад, до інших родичів. Водночас FCA наголошує, що родич або близька особа самі по собі не є PEP, і до них не слід застосовувати заходи EDD автоматично чи без пропорційності. Вони розглядаються у ширшому контексті можливості бути використаними для обходу фінансового моніторингу. Окремо врегульовано питання декласифікації: після залишення посади особа зберігає статус

[7] https://www.fca.org.uk/publication/finalised-guidance/fg25-3.pdf

PEP ще принаймні 12 місяців, проте члени сім'ї з цього моменту повинні розглядатися як звичайні клієнти, якщо немає інших ризиків.

Особливу увагу FCA приділяє процесу прийняття рішення щодо відносин із PEP. Раніше вимагалося, щоб кожну таку справу схвалював MLRO, але у новій редакції введено більшу гнучкість. Дозволено, аби схвалення здійснював будь-який член старшого менеджменту, який володіє достатніми знаннями та має відповідний рівень авторитету. Це зменшує адміністративне навантаження на MLRO, зберігаючи при цьому вимогу до нагляду та загальної обізнаності MLRO про всі випадки. У документації компанії повинно бути чітко зафіксовано, хто саме уповноважений ухвалювати такі рішення, і цей персонал має пройти відповідне навчання.

У керівництві наведено ознаки, що дозволяють відрізняти нижчий та вищий ризик PEP. Нижчий ризик мають внутрішні PEP у стабільних демократіях, особи без виконавчих повноважень, наприклад, опозиційні парламентарі, а також ті, хто підзвітний у питаннях фінансів та декларацій. Вищий ризик виникає тоді, коли PEP представляє країну з високим рівнем корупції, політичною нестабільністю, слабкими інституціями чи обмеженням свободи преси, а також якщо сама особа контролює масштабні держзакупівлі чи розподіл державних ліцензій і концесій. Так само підвищений ризик пов'язується з невідповідністю стилю життя відомим легальним доходам або наявністю обґрунтованих підозр у фінансових зловживаннях.

Важливою складовою є пояснення, як саме має здійснюватися посилена перевірка. У нижчому ризику достатньо обмежитися використанням доступної інформації, мінімально втручаючись у приватне життя клієнта, рідше переглядати досьє і дозволяти схвалення на середньому рівні менеджменту. У вищому ризику, навпаки, перевірка має бути ретельною, з обов'язковим вивченням джерела статків і коштів, частим моніторингом і схваленням на найвищому рівні керівництва. FCA наголошує, що відмова від відносин можлива лише тоді, коли після оцінки ризику компанія доходить висновку, що ризики неможливо знизити до прийнятного рівня.

Окремі положення документа стосуються довгострокових страхових контрактів, у яких PEP може бути бенефіціаром, та випадків, коли PEP є бенефіціарним власником юридичної особи. FCA уточнює, що компанія не повинна автоматично вважатися PEP, якщо серед її власників є політична особа, окрім випадків, коли ця особа має реальний контроль. Це положення спрямоване на уникнення

Висновки:

- **Національний PEP = нижчий ризик за замовчування.** Всі національні PEP у Сполученому Королівстві та їхні родичі/близькі особи повинні розглядатися як менш ризикові, якщо відсутні інші ризикові фактори. Це означає менше навантаження на фінансові установи та зменшення випадків «де-ріскінгу».
- **Посилення гнучкості у внутрішніх процедурах.** Рішення про відносини з PEP може ухвалювати не тільки MLRO, а й інші старші співробітники із достатнім рівнем повноважень і знань. Це підвищує ефективність управління ризиками та зменшує адміністративний тиск на MLRO.
- **Збалансований ризик-орієнтований підхід.** Фінансові установи мають застосовувати EDD на індивідуальній основі: від обмежених заходів у низькоризикових випадках до поглиблених перевірок у високоризикових (зокрема, при непрозорих джерелах статків, у країнах з високим рівнем корупції чи при великих держзакупівлях).
- **Чітке розмежування кола осіб.** Уточнено, кого саме слід вважати PEP, його сім'єю та близькими особами, з конкретизацією до контексту Сполученого Королівства. Це дозволяє уникати надмірного застосування вимог, мінімізує ризик помилкового віднесення клієнтів до PEP.

безпідставного блокування бізнесу та водночас гарантує, що випадки реального впливу політичних діячів на комерційні структури не залишаться поза увагою.

Загалом документ має системоутворюючий характер, оскільки він одночасно уточнює, кого слід вважати PEP у британських реаліях, встановлює мінімальні та максимальні стандарти перевірки, а також демонструє прагнення до пропорційності у боротьбі з відмиванням коштів і корупцією. FCA уникає формального розширення кола PEP і зосереджується на тих, хто реально створює ризик, чітко розділяє внутрішніх і зовнішніх політичних діячів, врегульовує статус членів сімей та асоційованих осіб і водночас дає установам гнучкість у внутрішніх процедурах. Це керівництво можна розглядати як спробу збалансувати суворість міжнародних стандартів FATF і практичність їх застосування у Сполученому Королівстві, мінімізуючи ризики надмірного тиску на клієнтів та фінансові інституції і зберігаючи основну мету — ефективне управління ризиками відмивання коштів та корупційного впливу.

Звіти окремих інституцій та експертів

Виклики та загрози незаконного обігу вогнепальної зброї та боєприпасів [8]

Документ, підготовлений в межах діяльності Організації американських держав (OAS), презентує результати пілотного дослідження, метою якого було ідентифікувати основні виклики та майбутні загрози, пов'язані з незаконною торгівлею зброєю і боєприпасами у регіоні Америк. Це дослідження є частиною ширшого дослідження з питань обігу зброї, передбаченого резолюцією OAS 2945 (2019), і виконується Секретаріатом з багатовимірної безпеки.

Контекст проблематики визначається тим, що регіон Америк протягом багатьох років демонструє найвищі у світі показники вбивств: за даними ООН, у 2023 році цей показник становив 15 убивств на 100 тисяч населення при світовому середньому 5,8. Водночас близько 67% усіх убивств у регіоні скоєно з використанням вогнепальної зброї, причому половина випадків має прямий зв'язок з діяльністю організованих злочинних груп і банд. Незаконна циркуляція зброї, зокрема її нелегальне виробництво, внутрішньорегіональні потоки і слабкість державних інституцій у сфері контролю, створюють не лише криміногенну небезпеку, а й серйозні наслідки для економіки, політичних свобод і загального рівня безпеки.

Дослідження здійснювалося із використанням методики Delphi — багатораундових консультацій з групою експертів, що дозволило поступово досягти консенсусу щодо визначення найбільш нагальних проблем. Було проведено два етапи опитувань: перший — у цифровій формі, другий — через інтерв'ю та групові сесії. Загалом участь узяли 21 експерт із багаторічним досвідом у питаннях торгівлі зброєю та безпеки.

За підсумками обговорень із 95 визначених проблем 39 були віднесені до категорії високопріоритетних. Вони стосуються широкого спектру вимірів: законодавчого регулювання, виробництва, управління державними арсеналами, внутрішньої та міжнародної торгівлі, контролю кордонів, координації державних інституцій, діяльності приватних охоронних компаній, інформаційних систем, реєстрації зброї, кримінальних розслідувань та міжнародної

[8] https://insightcrime.org/wp-content/uploads/2025/07/Paper_Threats_ENG_v250424-1.pdf

співпраці. Серед ключових викликів особливо виділяються законодавчі прогалини у сфері криміналізації незаконного обігу зброї та обмеження доступу до неї осіб із судимостями за насильницькі злочини, поширення незаконного виробництва, зокрема із застосуванням технологій 3D-друку, відсутність належних протоколів і ресурсів для трасування зброї, слабкий контроль приватних охоронних структур і значні затримки у знищенні вилучених та застарілих арсеналів. Не менш критичною виявилася проблема роз'єднаності та фрагментарності інформаційних систем: дані часто зберігаються у несумісних базах, не обмінюються між відомствами та не піддаються якісному аналізу.

Окремо експерти ідентифікували загрози, що мають перспективний або новітній характер. Вони пов'язані із технологічними інноваціями, такими як виробництво деталей зброї за допомогою 3D-принтерів та поширення міжнародного кустарного виготовлення, що ускладнює контроль за обігом. Значною небезпекою визначено кібератаки на інформаційні системи, ризики злому баз даних та атак типу ransomware, які можуть паралізувати державні механізми обліку і контролю. До загроз також віднесено корупційні практики, коли представники державних органів співпрацюють із кримінальними структурами, а також слабкий рівень обміну інформацією між країнами регіону. Важливо, що багато загроз напряму пов'язані з проблемами захищеного обміну, накопичення та аналізу даних — сфери, які, на думку експертів, можна посилити у короткостроковій перспективі без значних додаткових бюджетних витрат.

Зроблені висновки дозволили структурувати виклики у матрицю, де враховано необхідність ресурсів і час для їх вирішення. Частину завдань, зокрема посилення координації між державними структурами, контроль приватних охоронних компаній і удосконалення комунікації між органами влади, можна реалізувати швидко і відносно недорого. Водночас модернізація інфраструктури на кордонах чи вдосконалення систем управління державними арсеналами вимагатиме суттєвих інвестицій і довшої перспективи.

У підсумку автори документу пропонують низку наступних кроків: перевірку та уточнення вже ідентифікованих проблем і загроз; глибше вивчення їхніх причин для розуміння факторів, які їх породжують; розробку конкретних рішень і заходів протидії на національному та регіональному рівнях; створення дорожніх карт дій, що міститимуть цілі, показники виконання, відповідальних виконавців та чіткі строки. Таким чином, пілотне дослідження не лише окреслило проблематику, але й запропонувало основу для

Висновки:

- **Перегляд і пріоритизація викликів:** З 95 ідентифікованих викликів 39 визнано пріоритетними, включаючи прогалини в законодавстві та слабкий контроль кордонів. Рекомендується переглянути ці пріоритети та вдосконалити інструменти опитування, щоб уникнути паралічу рішень.
- **Короткострокові дії з низькими витратами:** Виклики, такі як недостатня координація між державними органами та виробниками зброї, можна вирішити в короткостроковій перспективі з мінімальними ресурсами, що дозволяє швидко отримати відчутні результати.
- **Фокус на інформаційні загрози:** У чотирьох вимірах (контроль кордонів, системи інформації, кримінальні розслідування, міжнародна торгівля) виявлено брак безпечного обміну даними. Держави можуть оперативно розробити заходи для вирішення цих проблем без значного збільшення бюджету.
- **Розробка планів дій:** На основі причин і рішень пропонується створити національні та регіональні дорожні карти з конкретними цілями, відповідальними сторонами та дедлайнами для ефективного подолання виявлених викликів і загроз.

систематизованої та стратегічної відповіді на виклики незаконного обігу зброї та боєприпасів у регіоні.

Санкції США проти Венесуели: оцінка діяльності Картелю Сонця [9]

Стаття, підготовлена Venezuela Investigation Unit і опублікована InSight Crime, являє собою детальний аналіз нових санкцій, введених урядом США проти так званого "Картелю Сонця" у Венесуелі.

Автор стверджує, що санкції, оголошені 25 липня Офісом з контролю за іноземними активами Міністерства фінансів США (OFAC), базуються на хибному уявленні про природу цієї організації, зображуючи її як ієрархічну структуру, очолювану президентом Ніколасом Мадуро, яка використовує наркотрафік як ідеологічну зброю проти США. Насправді "Картель Сонця" є децентралізованою мережею корупції, де високопоставлені військові та політичні діячі Венесуели отримують прибуток, співпрацюючи з наркоторговцями та забезпечуючи їхній захист, а не діючи за єдиним планом. Санкції включають фінансові обмеження проти Мадуро та інших посадовців, багато з яких уже перебувають під попередніми санкціями, що робить нові заходи малоефективними для них особисто, оскільки їхній доступ до американської фінансової системи вже заблоковано. Однак розширення санкцій на всю організацію дозволяє OFAC ширше таргетувати бізнеси та осіб, які мають фінансові зв'язки з венесуельськими офіційними особами.

Ці санкції були введені невдовзі після обміну в'язнями між США та Венесуелою та через день після того, як Мадуро оголосив про дозвіл компанії Chevron відновити нафтові операції в країні, що вказує на намір президента Дональда Трампа демонструвати жорстку позицію щодо Мадуро, зберігаючи при цьому економічні та дипломатичні відносини. Документ підкреслює, що значні докази підтверджують причетність венесуельських урядовців та військових до наркотрафіку, але останні санкції спотворюють реальну картину діяльності "Картелю Сонця". Зокрема, твердження про те, що Мадуро очолює цю організацію, є надмірним спрощенням – натомість корупція проявляється через використання посадовцями своїх повноважень для захисту наркоторговців, іноді навіть із залученням військової техніки для перевезення наркотиків, хоча частіше їхня роль обмежується забезпеченням безперешкодного проходження вантажів. Мадуро та інші високопосадовці дозволяють таку корупцію, щоб гарантувати лояльність нижчих рангів, але децентралізована структура робить усунення окремих фігур

Висновки:

- **Необхідно оновити аналітичні підходи до санкцій**, зосередившись на конкретних бізнесах і фінансових мережах, пов'язаних із венесуельськими посадовцями, замість загальних позначень організацій.
- **Провести додаткові розслідування** для уточнення ролі Tren de Aragua у наркотрафіку, зосередившись на її основній діяльності (вимагання, торгівля людьми, мігранти), щоб уникнути помилкових асоціацій із "Картелем Сонця".
- **Потрібно розглянути альтернативні дипломатичні стратегії** з Венесуелою, які б враховували децентралізовану природу корупційних мереж, замість ізоляції, що може бути неефективною через стійкість системи.

[9] https://insightcrime.org/news/us-sanctions-mischaracterize-cartel-of-the-suns-venezuela/

неефективним для руйнування всієї мережі.

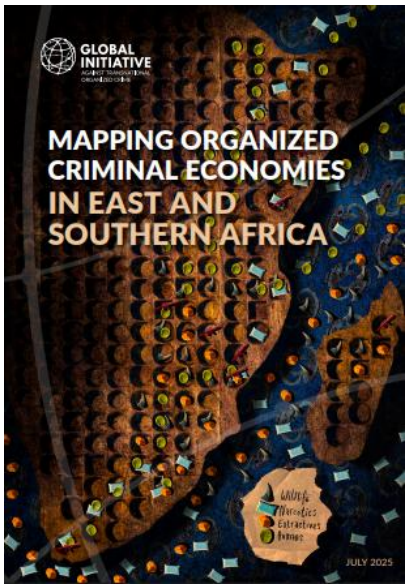
Крім того, документ спростовує ідею, що "Картель Сонця" використовує наркотики як "зброю" для підриву стабільності США, наголошуючи, що діяльність організації керується прагматизмом і прибутком, а не ідеологією.

Наркотики, які надходять із Венесуели на міжнародні ринки, підтримують цю корупційну систему, але їхнє призначення визначається економічною вигодою – вантажі прямують до європейських країн із менш ворожими відносинами з Венесуелою, а також до США, незважаючи на їхній статус ідеологічного "ворога".

Ще одним спростуванням є зв'язок "Картелю Сонця" із венесуельською бандою Tren de Aragua, яку Трамп нещодавно визнав іноземною терористичною організацією. Хоча раніше банда мала політичний захист у Венесуелі, уряд повернув контроль над її базою – в'язницею Токорон – у вересні 2023 року, після чого залишки пов'язаних угруповань стали об'єктами операцій сил безпеки. Частково засекречений меморандум від квітня 2025 року від американських розвідувальних служб вказує на сумніви щодо прямого керівництва Мадуро діяльністю Tren de Aragua, а також на відсутність переконливих доказів того, що банда відіграє значну роль у наркотрафіку до США. Натомість її діяльність більше пов'язана з такими злочинами, як вимагання, торгівля людьми та контрабанда мігрантів.

Таким чином, документ пропонує переосмислення підходів до санкцій, акцентуючи на необхідності точнішого аналізу корупційних мереж та уникнення хибних асоціацій, таких як зв'язок із Tren de Aragua, для розробки більш ефективної політики щодо Венесуели.

Географія організованої злочинності: Незаконні економіки Східної та Південної Африки [10]



Документ від Global Initiative Against Transnational Organized Crime (GI-TOC) є всебічним дослідженням організованої злочинності в регіоні Східної та Південної Африки (ESA), що охоплює 22 країни від Сомалі на півночі до Південної Африки на півдні, а також простягається від узбережжя Індійського океану до Атлантичного. Цей 86-сторінковий звіт, підготовлений командою експертів на чолі з Джулією Станьярд, Майклом МакЛагганом, Ароном Гайманом, Джуліаном Радемейєром, Дженні Айріш-Хобошіане, Метом Гербертом, Джейсоном Елігом, Марсеною Гантер і Лівією Вагнер, базується на польових дослідженнях, літературному огляді та даних Індексу організованої злочинності Африки, підтриманих фінансово Фондом інтегрованої безпеки Сполученого Королівства. Звіт має на меті описати географію чотирьох ключових незаконних ринків — торгівлі наркотиками, дикими тваринами та рослинами, видобутком корисних копалин і торгівлею людьми — а також аналізувати їхню конвергенцію в регіональних хабах.

У вступі підкреслюється, що ESA є стратегічним вузлом для глобальних злочинних мереж, де географічні особливості формують маршрути та точки концентрації незаконної діяльності. Наприклад, героїн з Афганістану через Пакистан і Іран транспортується через Аравійське море та Індійський океан до північного Мозамбіку та Танзанії, де розподіляється на два основні

[10] https://globalinitiative.net/wp-content/uploads/2025/07/Mapping-organized-criminal-economies-in-East-and-Southern-Africa-GI-TOC-July-2025.pdf

потоки: високої інтенсивності для ринків Європи та Австралії та низької для місцевого споживання в містах і селах регіону. Ріг носорога контрабандою перевозиться повітряним шляхом із Йоганнесбурга та Аддіс-Абеби через Дубай, Доху, а іноді Париж і Лондон, щоб заплутати правоохоронців, тоді як слонова кістка відправляється контейнерами з портів Дар-ес-Салам, Нампула та Дурбан до Сінгапуру, Сіануквіля, Хуанпу і Хайфона. Золото, видобуте нелегально в золотих копальнях Квекве в Зімбабве та глибоких шахтах Крюгерсдорпа, Карлтонвіля, Клерксдорпа і Велкому в ПАР, переробляється та відмивається через Дубай, а також масово переправляється через східний кордон ДРК до Руанди, Бурунді, Уганди, Танзанії та ОАЕ.

У північному Мозамбіку та провінції Квазулу-Наталь у ПАР повстанці, пов'язані з "Ісламською державою", беруть участь у злочинних економіках, контрабанді золота, викраденні людей та вимаганні для фінансування. До регіону також залучені міжнародні злочинні мережі з Китаю, Пакистану та Ірану, які співпрацюють із місцевими посередниками в торгівлі наркотиками (метамфетаміном, героїном) та дикими тваринами (абалонами, слоновою кісткою), а також нігерійські та конголезькі синдикати, що координують наркотрафік і фінансові шахрайства з центрами в Йоганнесбурзі.

Методологія дослідження включає три типи хабів: "гарячі точки" з сильною присутністю злочинців, які часто мають політичну підтримку і впливають на регіональну нестабільність; "транзитні пункти" — кордони, аеропорти, порти та коридори для перевезення незаконних товарів; і "зони злочинності" — ширші географічні райони з високою концентрацією незаконної діяльності, такі як конфліктні зони чи місця видобутку. Аналіз базується на даних GI-TOC, Індексу організованої злочинності, який показує зростання злочинності в Східній Африці (середній показник 5,88 у 2023 році) і меншу різноманітність, але значну поширеність у Південній Африці (4,83), де ключовими факторами є слабке державне управління, корупція, бідність, конфлікти та погано контрольовані кордони.

Звіт детально розглядає чотири ринки: торгівлю наркотиками, що зросла як транзитний і споживчий напрямок для героїну, кокаїну та синтетичних препаратів із маршрутами через Мозамбік і Танзанію; незаконну торгівлю дикими тваринами (слонова кістка, ріг носорога, луски панголінів) із хабами в Дар-ес-Саламі та Дурбані; видобуток корисних копалин, зокрема золота в ДРК і Зімбабве, з відмиванням через Дубай; і торгівлю людьми в Розі Африки та Південній Африці, де вразливі групи в Еритреї, Ефіопії, Сомалі, Мозамбіку, Зімбабве та Лесото зазнають експлуатації.

Висновки:

- **Посилення контролю в ключових хабах:** Необхідно терміново покращити скринінг і обладнання в аеропортах (наприклад, Болє, Йоганнесбург) та портах (Дурбан, Дар-ес-Салам), щоб зменшити транзит наркотиків, диких тварин і золота, враховуючи їхню щорічну пропускну спроможність (24 млн пасажирів у Болє та 2,9 млн контейнерів у Дурбані).
- **Міжнародна співпраця:** Рекомендується активізувати координацію між країнами ESA та міжнародними партнерами (наприклад, ОАЕ, ЄС), щоб перервати маршрути контрабанди (героїн через Індійський океан, ріг носорога через Дубай) і відстежувати фінансові потоки відмивання золота.
- **Підвищення стійкості місцевих громад:** Потрібно інвестувати в соціально-економічний розвиток уразливих регіонів (наприклад, Квазулу-Наталь, Сомалі), щоб зменшити залучення місцевих жителів до злочинних мереж, які експлуатують бідність і слабке державне управління.
- **Моніторинг конвергенції:** Ввести регулярний моніторинг хабів із високою конвергенцією (наприклад, Йоганнесбург, Момбаса), щоб запобігти інтеграції наркотрафіку, торгівлі людьми та видобутку в єдині злочинні екосистеми.

Кожен розділ аналізує тенденції, маршрути та "гарячі точки", такі як аеропорт Болє в Ефіопії, який щорічно обробляє 24 мільйони пасажирів, але потерпає від браку обладнання, та порт Дурбан, де через корупцію перевіряється лише мала частина з 2,9 мільйона контейнерів.

Останні розділи зосереджуються на конвергенції злочинних ринків, де хаби, такі як Йоганнесбург і Момбаса, стають центрами кількох видів злочинності, а мережі та брокери сприяють їхній інтеграції в єдину екосистему. Висновки підкреслюють глобальний вплив цих ринків на безпеку та економіку, пропонуючи рекомендації, такі як посилення міжнародної співпраці, інституційної спроможності та моніторингу конвергенції для протидії злочинності в регіоні.

За лаштунками шахрайства: Розслідування щодо використання соціальних платформ [11]

Стаття від OCCRP є всебічним розслідуванням, яке розкриває складні механізми сучасних шахрайських схем, що базуються на скоординованій глобальній мережі сервісних провайдерів. Це дослідження зосереджується на двох масштабних операціях, розкритих у рамках проєкту "Scam Empire": одна базується в Ізраїлі та Європі, а друга — у Грузії. Розслідування детально описує, як професійні шахраї використовують соціальні мережі, спеціалізоване програмне забезпечення та фіктивні компанії для залучення жертв, створення ілюзії довіри та виведення мільйонів доларів із їхніх рахунків, часто залишаючи сліди, які важко відстежити.

Текст розпочинається з огляду ролі кол-центрів — сучасних осередків шахрайства, де маніпулятивні, багатомовні агенти переконують жертв по всьому світу інвестувати у фіктивні фінансові можливості. Ці кол-центри не діють ізольовано, а спираються на екосистему сервісних провайдерів, які сприяють кожному етапу шахрайської схеми — від залучення жертв до виведення грошей — і отримують частку прибутків. Розслідування виділяє три основні фази: залучення жертв, управління схемами та виведення грошей, розкриваючи деталі участі десятків компаній із різних куточків світу.

У першій фазі, "Залучення жертв", описано, як шахраї використовують афілійовані маркетингові компанії, такі як MGA Team (Москва), CRYP (невстановлена юрисдикція), Sierra Media (Болгарія) та Oray Ads (США), для розміщення фішингових оголошень. Ці оголошення обіцяють високі прибутки, часто з підробленими рекомендаціями місцевих знаменитостей, і спрямовані на конкретні аудиторії.

Жертви, які клікають на ці оголошення, потрапляють на лендінгові сторінки, де залишають контактні дані, які потім передаються кол-центрам. Маркетингові компанії заробляють значні суми — наприклад, MGA Team отримала щонайменше $556,850 у 2024 році, а CRYP — майже $850,000 у перші дев’ять місяців 2023 року. Багато з цих компаній приховують свою діяльність через анонімні фіктивні компанії, псевдоніми в зашифрованих чатах і платежі в криптовалюті.

Соціальні платформи, такі як Meta (Facebook, Instagram, WhatsApp) і Google, слугують платформами для розміщення реклами, отримуючи частку прибутків. Незважаючи на політики

[11] https://www.occrp.org/en/investigation/behind-the-scam-how-fraudsters-use-social-media-software-and-shell-companies-to-steal-millions

проти шахрайства, 58% криптовалютних оголошень на Facebook порушують правила компанії, а третина жертв "Scam Empire" згадала Facebook як джерело шахрайських оголошень. Taboola, альтернативна рекламна платформа, також згадується як джерело кампаній, хоча не відреагувала на звернення.

Друга фаза, "Управління схемами", розкриває технологічний бік операцій. Після збору даних жертви швидко отримують дзвінки завдяки програмам, які інтегрують інформацію в бази "лідів". Використовуються CRM-системи, такі як Getlinked.io і PumaTS, які дозволяють зберігати дані про жертв, маніпулювати їхніми "інвестиціями" та контролювати інтерфейси. AnyDesk, програмне забезпечення для віддаленого доступу, допомагає шахраям стежити за діями жертв. Для комунікації використовуються VoIP-сервіси Coperato (отримала понад $1 млн) і Squaretalk (понад $150,000). Адміністративна підтримка забезпечується компаніями, такими як Za Traiding і Saberoni LLC (Грузія), які платять за оренду офісів через проксі-власників, а також Roserit, Amapola, Maximateam і Clear IT (Болгарія), які обробляють зарплати та комунальні витрати, іноді до €19,000 на місяць.

Висновки:

- **Посилення контролю за онлайн-рекламою:** Користувачам рекомендовано уникати кліків на підозрілі інвестиційні оголошення з вигаданими рекомендаціями знаменитостей, а платформам Meta та Google необхідно вдосконалити модерацію, враховуючи, що 58% криптовалютних оголошень на Facebook порушують правила.
- **Моніторинг використання програмного забезпечення:** Компаніям, таким як Getlinked.io, PumaTS і AnyDesk, слід активніше співпрацювати з правоохоронцями, впроваджуючи суворий контроль клієнтів і обмеження доступу до даних жертв, особливо після виявлення маніпуляцій на суму понад $1 млн.
- **Зміцнення банківської безпеки:** Банки (Revolut, Chase UK, Santander, BBVA) та платіжні сервіси (Wise, Wirex) повинні посилити комплаєнс, перевіряючи транзакції на суму понад €4,9 млн, і співпрацювати з владою для запобігання відмиванню грошей.
- **Прозорість проксі-компаній:** Владам рекомендовано перевіряти фіктивні компанії, такі як Selterico SL і Greencode Connection, які переказали мільйони через проксі-рахунки, і вимагати від них розкриття реальних власників для припинення фінансових схем.

Третя фаза, "Виведення грошей", деталізує фінансові механізми. Жертви переводять кошти через цифрові банки, такі як Revolut (598 транзакцій із 5000), Chase UK, Wise, Wirex, а також іспанські Santander і BBVA, які обробили понад €4,9 млн через схему "LWires".

Нерегульовані платіжні провайдери, такі як Bankio/Anywires і Britain Local, забезпечують проксі-рахунки з комісіями 10-17%, створюючи фальшиві документи для обходу банківського контролю. Фіктивні компанії, такі як Selterico SL (Європа), Greencode Connection Limited і Purplesun Limited (Сполучене Королівство), а також Intek Systems Limited (Грузія), використовуються для відмивання грошей, переказуючи мільйони через низку юрисдикцій. Багато компаній заперечують свідоме сприяння шахрайству, посилаючись на обмеження своїх повноважень.

Розслідування підкреслює складність і глобальність цих схем, де легальні бізнеси стають інструментами злочинців, а спеціально створені структури полегшують їхню діяльність. Брак відповідей від багатьох компаній і їхні заяви про співпрацю з правоохоронними органами підкреслюють необхідність ширшого міжгалузевого підходу до боротьби з шахрайством.

Технологічні горизонти 2025: як проривні інновації змінюють бізнес і економіку [12]

Звіт є комплексним аналітичним документом, присвяченим визначенню ключових технологічних напрямів, які формуватимуть глобальну економіку, бізнес-моделі та суспільні трансформації у найближчі роки. Його головна мета полягає в тому, щоб окреслити технології, які вже зараз виходять за межі експериментальної стадії та починають мати системний вплив на корпоративні стратегії, а також ті, які залишаються на горизонті, але вимагають стратегічного спостереження та підготовки до впровадження. Документ структуровано у три великі тематичні блоки: революцію штучного інтелекту, інфраструктурні та обчислювальні фронтири, а також передові інженерні розробки.

У першому блоці, присвяченому штучному інтелекту, McKinsey підкреслює якісно новий етап розвитку — перехід від систем, що працюють як інструменти, до так званого агентського AI (Agentic AI), який здатен діяти автономно, виконувати складні завдання без постійного контролю людини та взаємодіяти між собою і з іншими цифровими системами у багатовекторному середовищі. Такий підхід змінює не лише продуктивність праці, а й структуру бізнесу, створюючи передумови для виникнення нових сервісів, оптимізації операційних процесів і переосмислення ролі людини у виробничих і управлінських ланцюгах. Поряд із цим аналізується традиційний штучний інтелект, що охоплює машинне навчання, генеративні моделі та прикладні кейси у медицині, фінансах, дизайні та управлінні ризиками. Автори наголошують, що ключовим викликом стане баланс між швидкістю впровадження та створенням механізмів контролю, етики і безпеки.

Другий блок зосереджується на так званих обчислювальних і комунікаційних фронтирах, які виступають критичною основою для масштабування інновацій. Тут виокремлено спеціалізовані напівпровідники, що дають змогу обробляти дедалі складніші обсяги даних, та розширену підключеність, яка завдяки 5G і перспективним розробкам 6G створює умови для масового поширення Інтернету речей, автономних систем та інтелектуальних виробничих мереж. Значне місце відводиться хмарним обчисленням та периферійним обчисленням, які забезпечують гнучкість і швидкість інтеграції технологій у реальному часі, дозволяючи компаніям працювати з даними ближче до джерела їх виникнення. У цьому ж контексті розглядаються імерсивні технології, включаючи віртуальну та доповнену реальність, що відкривають нові можливості у навчанні, медицині, індустрії розваг і промисловості. Автори роблять наголос і на критичному аспекті цифрової довіри та кібербезпеки, адже без побудови ефективної архітектури захисту даних та механізмів підтвердження цифрової ідентичності подальше масштабування технологій стане неможливим. Окремим напрямом визначено квантові технології, які попри ранню стадію розвитку вже демонструють потенціал для проривів у галузях матеріалознавства, фармацевтики та фінансового моделювання.

Третій блок присвячено інженерним проривам, які мають довгострокове стратегічне значення. Серед них робототехніка нового покоління, здатна працювати автономно та співпрацювати з людиною в інтегрованих середовищах; мобільність майбутнього, що включає електротранспорт, автономні системи та інфраструктурні рішення для «розумних міст»;

12 https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20top%20trends%20in%20tech%202025/mckinsey-technology-trends-outlook-2025.pdf

біоінженерія, яка розвиває персоналізовану медицину, генні технології та створення нових біоматеріалів; космічні технології, що виходять із суто дослідницької площини в комерційний і оборонний сегмент; а також енергетичні й стійкі технології, де головний акцент робиться на декарбонізації, відновлюваній енергетиці та нових системах зберігання й управління енергією. Автори звіту підкреслюють, що ці напрями потребують не лише приватних інвестицій, але й активної державної політики, міжнародної кооперації та створення умов для довгострокового стратегічного розвитку.

Загалом документ демонструє, що світ входить у фазу, коли окремі технології перестають бути ізольованими інноваціями і починають створювати взаємопов'язані екосистеми, у яких розвиток одного напряму підсилює інші. Це стосується як взаємодії AI з хмарними й квантовими обчисленнями, так і поєднання біоінженерії з робототехнікою чи космічними дослідженнями. McKinsey звертає особливу увагу на ринок висококваліфікованих фахівців: попит на спеціалістів із AI, кібербезпеки, квантових технологій і біоінженерії вже зараз значно перевищує пропозицію, що створює умови для загострення глобальної конкуренції за кадри. Для бізнесу це означає необхідність не лише інвестувати у технології, але й формувати стратегії залучення, навчання та утримання фахівців. Таким чином, Technology Trends Outlook 2025 виступає не лише аналітичним оглядом, а своєрідною дорожньою картою, яка вказує компаніям, урядам та інвесторам на те, які напрями будуть визначати конкурентоспроможність і стійкість у майбутньому, і як варто діяти вже сьогодні, щоб використати нові можливості та мінімізувати ризики.

Висновки:

- **Агентський AI (Agentic AI) стане основним драйвером бізнес-моделей 2025 року:** компанії повинні готуватися до інтеграції автономних систем, що знижують операційні витрати та створюють нові сервіси.
- **Кібербезпека і цифрова довіра стають ключовою умовою інновацій:** без інвестицій у захист даних та нові стандарти довіри до цифрових технологій та їхньої безпеки, компанії не зможуть масштабувати технології.
- **Інфраструктурний фундамент (хмара, периферійні обчислення, напівпровідники, 6G) є критичною передумовою розвитку AI та імерсивних технологій;** державам і бізнесу слід інвестувати у відповідну екосистему вже зараз.
- **4. Технології стійкості (енергія, біоінженерія, космос) виходять у топ стратегічних напрямів,** що вимагає від урядів і корпорацій довгострокового планування та партнерств.

Рекомендовані та навчальні матеріали

«Проста робота, висока зарплата»: розкриття складності примусової праці в Південно-Східній Азії [13]

Humanities & Social Sciences Communications

Стаття авторства Хая Тханя Луонга, опублікована в журналі Humanities and Social Sciences Communications, являє собою перше змішане якісне дослідження, яке розкриває складність шахрайської злочинності, пов'язаної з

[13] https://www.nature.com/articles/s41599-025-05605-1

примусовою працею в'єтнамців (SFVL), організованої китайськими кіберзлочинцями (CCEC) у Південно-Східній Азії.

Дослідження зосереджене на В'єтнамі як ключовому прикладі, детально аналізуючи випадки так званих «pig-butchering» схем які набули поширення під час і після пандемії COVID-19, особливо в Камбоджі. У цих схемах зловмисники використовують соціальні платформи, видаючи себе за рекрутерів, і пропонують фальшиві вакансії з привабливими зарплатами в галузях обслуговування клієнтів, інформаційних технологій та програмування.

Методологія дослідження базується на аналізі змісту десяти відібраних випадків за період із 2018 по 2023 рік та інтерв'ю з дванадцятьма в'єтнамськими поліцейськими різного рангу та досвіду, що дозволяє виявити структуровані злочинні мережі з кількома рівнями, очолювані китайськими синдикатами за участі в'єтнамських та інших спільників. Автор підкреслює складне перехрещення ролей жертв і злочинців у кібершахрайстві, коли жертви піддаються примусу до шахрайських дій під загрозою фізичного насильства та тортур, а також закликає до подальших досліджень у цьому напрямі, зокрема щодо взаємозв'язку між злочинцями та жертвами, торгівлею людьми та технологіями злочинності.

У вступній частині статті, кібершахрайство розглядається як еволюція традиційних видів шахрайства, що стало можливим завдяки розвитку інформаційно-комунікаційних технологій (ІКТ) та соціальних медіа, які забезпечують анонімність і розширюють коло потенційних жертв. Особливу увагу приділено схемам, де зловмисники поступово заробляють довіру жертв через вигадані романтичні чи дружні стосунки, після чого здійснюють фінансову експлуатацію. Цей тип шахрайства набув поширення після заборони онлайн-гемблінгу в Камбоджі у 2019 році та обмежень на подорожі через пандемію COVID-19, що призвело до перепрофілювання готелів і казино в шахрайські центри. У контексті В'єтнаму, де на початку 2024 року нараховувалося понад 78 мільйонів користувачів інтернету та 72 мільйони акаунтів у соціальних мережах, країна виявилася вразливою до CCEC, особливо через співпрацю з місцевими злочинцями. Автор відзначає, що офіційна статистика щодо CCEC у В'єтнамі ще не оприлюднена, що може вказувати на прихований масштаб цих злочинів, а також наголошує на необхідності кримінологічного аналізу "двозначних жертв" — осіб, які одночасно є жертвами та злочинцями.

Методологія дослідження включає три ключові дослідницькі питання: визначення моделей SFVL у В'єтнамі, аналіз зв'язку між кіберзлочинністю та торгівлею людьми в цьому контексті та вивчення методів роботи CCEC. Для цього використано змішаний підхід: аналіз десяти випадків, відібраних з урахуванням географічного розподілу по шести регіонах В'єтнаму (Північний, Дельта Червоної річки, Північно-центральне узбережжя, Центральне нагір'я, Південно-східний регіон та Дельта Меконгу), доповнено змістовним

Висновки:

- **Посилення співпраці правоохоронних органів:** Необхідно налагодити тіснішу співпрацю між в'єтнамськими та іноземними (особливо камбоджійськими та китайськими) правоохоронними органами для збору доказів і переслідування ключових гравців CCEC, враховуючи складність відстеження злочинців через посередників.
- **Освітні кампанії для вразливих груп:** Рекомендується проведення широкомасштабних інформаційних кампаній у сільських та етнічних районах В'єтнаму, щоб підвищити обізнаність про шахрайські схеми з працевлаштуванням і зменшити вразливість жертв.
- **Розширення досліджень:** Потрібно проводити подальші дослідження, зосереджені на перетині ролей жертв і злочинців, зв'язку торгівлі людьми зі злочинністю, пов'язаною з шахрайством, та ролі технологій, використовуючи дані з інших країн Південно-Східної Азії для порівняння.

аналізом супровідних сценаріїв та інтерв'ю з представниками правоохоронних органів. Інтерв'ю тривали від 35 до 55 хвилин, проводилися в'єтнамською мовою, а потім перекладалися англійською для тематичного аналізу. Критерії відбору інтерв'юерів включали географічне охоплення (особливо прикордонні зони з Китаєм, Камбоджею та Лаосом), ранг і досвід (не менше п'яти років), а також баланс між політиками, практиками та академіками. Етичне схвалення отримано від Інституційного комітету з етики та Програми транснаціональних злочинів і конфліктів (США).

Основні результати дослідження розкривають природу CCEC, які експлуатують SFVL, базуючись на тематичному аналізі випадків та інтерв'ю. У десяти випадках ідентифіковано 49 в'єтнамських злочинців і численні жертви, причому в одному випадку (CS9) зафіксовано явне перехрещення ролей жертви та злочинця.

Зловмисники використовують соціальні медіа для рекрутингу, застосовуючи обман, примус і незаконний перетин кордонів, часто через камбоджійських посередників. Жертви, віком від підлітків до дорослих, включають етнічні меншини та жителів сільських районів, приваблених обіцянками високих зарплат. Географія злочинів охоплює різні регіони В'єтнаму, що свідчить про гнучкість і адаптивність мереж CCEC. Автор зазначає, що прямі контакти між в'єтнамськими та китайськими злочинцями рідкісні, а основний зв'язок здійснюється через камбоджійських спільників, що ускладнює роботу правоохоронних органів. Особливу увагу приділено вразливості етнічних груп і необхідності міжнародної співпраці для боротьби з цими транснаціональними злочинами.

Для загального розвитку

Оцінка ризиків клієнтів: Профілювання та виявлення загроз [14]

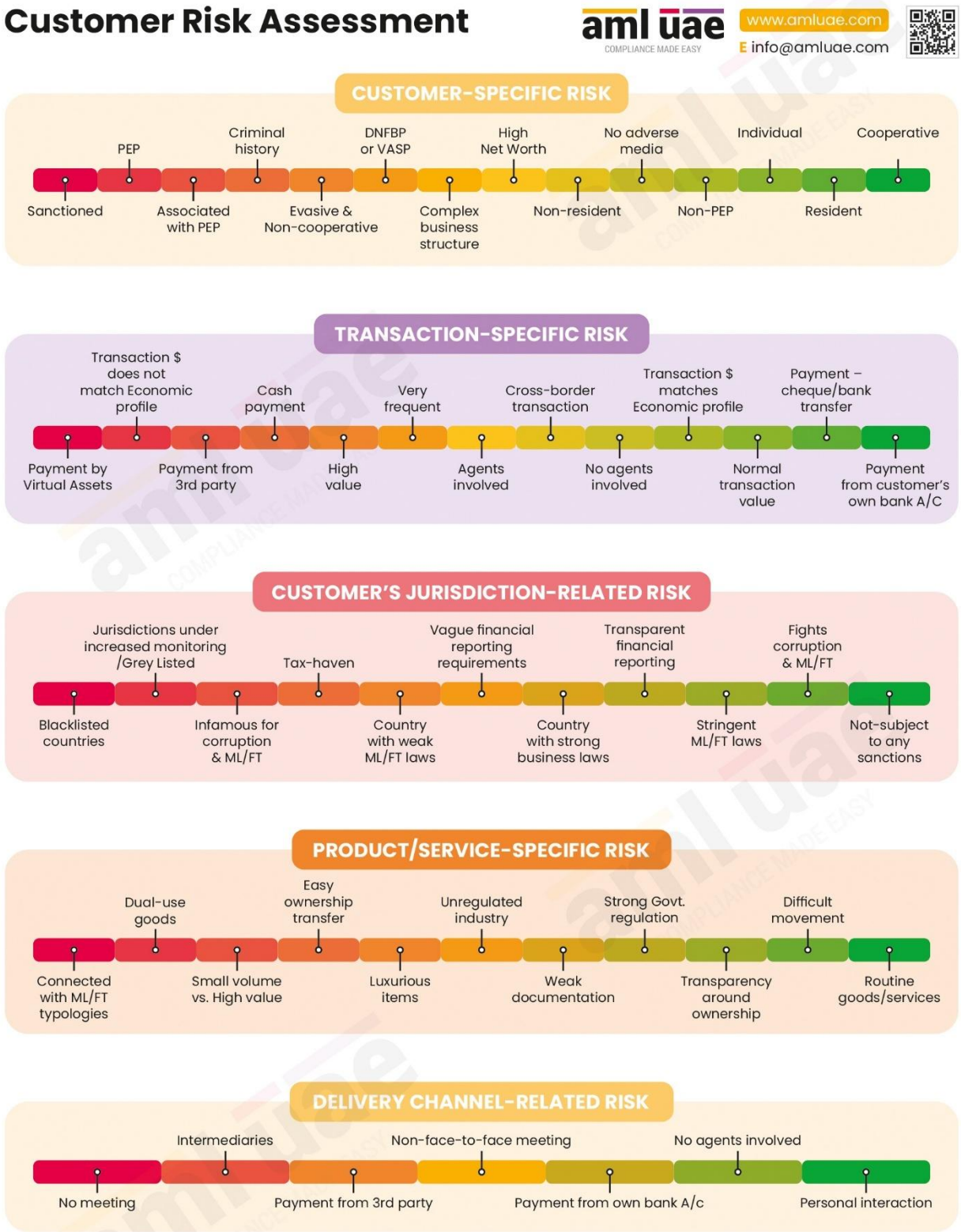
в ОАЕ регуляторні норми з ПВК/ФТ передбачають застосування ризик-орієнтованого підходу для зниження ризику фінансових злочинів. Це означає, що чим вищий ризик, тим суворішими мають бути заходи ПВК. Відповідно, підзвітні суб'єкти зобов'язані проводити оцінку ризиків клієнтів, щоб класифікувати кожного клієнта за категорією ризику: низький, середній, високий або неприйнятний, та впроваджувати методи для запобігання або зниження цих ризиків. Для клієнтів з високим ризиком необхідно застосовувати посилені заходи належної перевірки, тоді як для клієнтів з низьким ризиком достатньо стандартних заходів належної перевірки. Мета цієї оцінки полягає у виявленні ризиків ВК/ФТ, які клієнти становлять для бізнесу, включаючи інтенсивність ризику.

Профілювання ризиків клієнтів може здійснюватися на основі таких основних показників ризику.

По-перше, тип або характер клієнта є критичним фактором. Клієнт, який є кооперативним або резидентом ОАЕ, або не має негативних згадок у ЗМІ, або не є політично значущою особою (PEP), може розглядатися як такий, що має низький ризик. Ризик вважається середнім, якщо клієнт має високий чистий капітал, є нерезидентом та має складну бізнес-структуру. Клієнти, які займаються товарами чи послугами, пов'язаними з поширеними типологіями відмивання коштів, такими як постачальники послуг віртуальних активів (VASP) або визначені нефінансові установи та професії (DNFBP), можуть становити вищий ризик. Клієнт з кримінальним минулим, який уникає співпраці, викликає високу підозру. Ризик є неприйнятно високим, якщо клієнт знаходиться в санкційному списку.

[14] https://amluae.com/portfolio/key-factors-for-customer-risk-assessment-under-aml-regulations/

По-друге, параметри транзакцій також відіграють важливу роль. Якщо клієнт здійснює платіж зі свого власного банківського рахунку, чеком або банківським переказом, такі транзакції можуть розглядатися як безпечні. Якщо вартість транзакції є нормальною для подібного клієнта, враховуючи характер ділової активності, або відповідає економічному профілю клієнта, ризик, що представляє такий клієнт, є нижчим. Транскордонні транзакції або часті транзакції на великі суми становлять середні ризики. Незвично висока сума або повна оплата готівкою може становити вищий ризик фінансового злочину. Клієнти вважатимуться високоризиковими, якщо вони наполягають на оплаті через непов'язаний рахунок третьої особи або використовують віртуальні активи без будь-якого ділового обґрунтування.

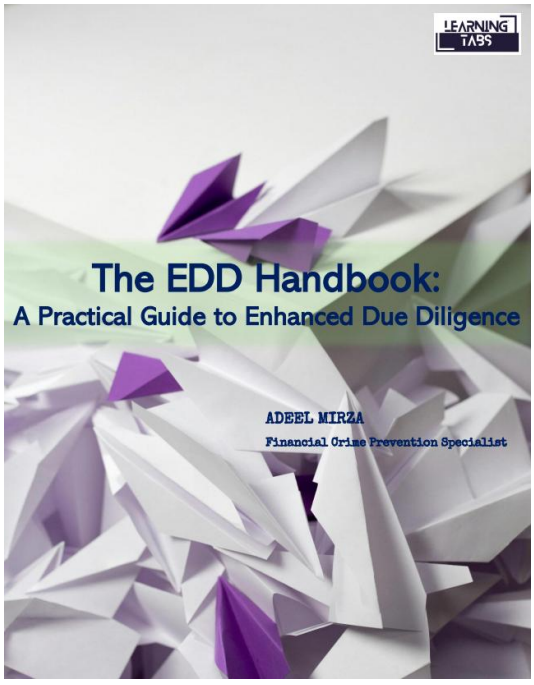


По-третє, одним з критичних елементів профілювання ризиків клієнтів є юрисдикція клієнта. Країна, яка має суворі правила боротьби з фінансовими злочинами, відома своєю боротьбою з корупцією або має прозорі вимоги до фінансової звітності, розглядається як така, що становить нижчий ризик ВК/ФТ для бізнесу. Клієнт з країни або юрисдикції з нечіткими вимогами до фінансової звітності, слабкими законами про відмивання коштів або фінансування тероризму має вищий рівень ризику. Країна, яка виступає офшорною гаванню, відома корупцією та хабарництвом, політичною нестабільністю, внесена до чорного або сірого списку FATF становить підвищений ризик ВК/ФТ.

По-четверте, характеристики продукту або послуг також можуть визначати профіль ризику клієнта. Діяльність з відмивання коштів зазвичай не відбувається у звичайних продуктах, послугах або товарах, які важко переміщувати. Продукт з прозорістю щодо його власності не викликає підозр. Клієнт стає підозрілим, коли він має справу з предметами високої вартості, не веде або майже не веде документацію або пов'язаний з нерегульованою галуззю. Це дуже ризиковано, коли клієнт має товари подвійного призначення або клієнт здійснює серію транзакцій дрібними сумами з товарами або послугами високої вартості, пов'язаними з типологіями фінансових злочинів.

Нарешті, канали доставки та поведінкові риси клієнта також є важливими. Клієнти, які беруть участь у регулярній прямій особистій взаємодії без залучення агентів або здійснюють платежі з власного банківського рахунку, не є підозрілими. Однак ви повинні бути пильними, коли клієнт уникає особистих зустрічей або наполягає на залученні третіх сторін або посередників без будь-якого ділового сенсу.

Довідник EDD: Практичний посібник з посиленої належної перевірки [15]



Посилена належна перевірка (EDD) є більш ретельним та глибоким рівнем перевірки клієнтів, яка застосовується до фізичних осіб, організацій або операцій, що несуть підвищений ризик відмивання коштів, фінансування тероризму або інших фінансових злочинів. Вона виходить за межі стандартної належної перевірки (CDD), вимагаючи додаткової документації, верифікації та пильного контролю для всебічного розуміння особи клієнта, джерела його багатства, ділової діяльності, структури власності та очікуваної операційної поведінки. Основна мета EDD полягає у виявленні та пом'якшенні підвищених ризиків фінансових злочинів шляхом отримання більш детальної, підтвердженої та часто незалежної інформації. Вона забезпечує відповідність нормативним вимогам місцевих та міжнародних законів з ПВК/ФТ, включаючи рекомендації FATF та правила місцевих юрисдикцій. EDD запобігає зловживанню фінансовими системами злочинцями, політично значущими особами (PEP), підсанкційними особами/організаціями або тими, хто діє у зонах високого ризику. Крім того, EDD надає більшу впевненість регуляторам та зацікавленим сторонам у тому, що установа вжила всіх розумних заходів для розуміння профілю та поведінки клієнта, а також дозволяє

[15] https://media.licdn.com/dms/document/media/v2/D4D1FAQGswfphvsKL7w/feedshare-document-pdf-analyzed/B4DZiNfSV8HsAY-/0/1754720453140?e=1756944000&v=beta&t=GICpoK0T2Xo_hVTYjY_AJv98Mks7ZKm9FDtFBaC1hw0

приймати обґрунтовані рішення на основі ризиків при обслуговуванні відносин високого ризику або затвердженні незвичайних чи складних транзакцій. EDD є не одноразовою дією, а безперервним зобов'язанням, особливо для відносин або діяльності, що демонструють червоні прапорці або включають фактори високого ризику. EDD служить критично важливою лінією захисту у системі з ПВК/ФТ фінансової установи, допомагаючи підтримувати цілісність, зменшувати репутаційні та регуляторні ризики та виявляти незаконну фінансову діяльність на ранній стадії.

Посилена належна перевірка обов'язково застосовується, коли клієнт, транзакція або відносини представляють підвищений ризик відмивання коштів, фінансування тероризму, шахрайства або інших фінансових злочинів. EDD є регуляторною вимогою та вимогою управління ризиками, розробленою для пом'якшення ризиків, які не можуть бути адекватно вирішені за допомогою стандартних заходів CDD. EDD повинна спрацьовувати автоматично або за допомогою оцінки на основі ризиків у таких сценаріях високого ризику: клієнти з юрисдикцій високого ризику (наприклад, країни з "сірого/чорного списку" FATF, країни зі слабким контролем за ПВК/ФТ, підсанкційні країни), політично значущі особи (PEP), що зокрема включають глав держав, високопоставлених політиків, суддів, послів, вищих військових посадовців та керівників державних підприємств, а також їхніх членів сім'ї та близьких помічників. EDD також необхідна для клієнтів зі складними юридичними структурами, такими як компанії з багатошаровою власністю, трасти, фонди або офшорні структури, що приховують кінцевого бенефіціарного власника (КБВ), або фіктивні компанії без очевидних ділових операцій. Незвичайні або високоризикові транзакційні моделі, такі як великі або незрозумілі готівкові операції, використання криптовалют, раптові зміни в транзакційній поведінці або структуризація транзакцій для уникнення порогів звітності, також вимагають EDD. До інших тригерів належать негативні згадки у медіа або індикатори негативної репутації, кореспондентські банківські відносини, особливо з установами у високоризикових юрисдикціях, а також юридичні особи з номінальними акціонерами або акціями на пред'явника.

Процес EDD включає шість основних кроків:

1. Оцінка ризику клієнта: Це фундаментальний крок для визначення необхідності EDD, що передбачає систематичну оцінку багатьох факторів ризику, таких як тип клієнта (наприклад, фізична особа, юридична особа, траст, НПО, VASP), географічний ризик (країна проживання, реєстрації, діяльності, офшорні фінансові центри), продукти та послуги (наприклад, приватний банкінг, кореспондентський банкінг, продукти, що забезпечують анонімність) та поведінковий/транзакційний профіль. Після оцінки кожного фактора ризику установа присвоює загальний рівень ризику клієнта (високий, середній, низький).

2. Збір поглибленої інформації: Після класифікації клієнта як високоризикового установа збирає всебічну та незалежно перевірену інформацію. Це включає отримання комплексних документів для перевірки особи (наприклад, ID, підтвердження адреси, дозволи на проживання для фізичних осіб; свідоцтва про реєстрацію, статути, витяги з реєстру для юридичних осіб), детальної інформації про ділову діяльність (наприклад, характер бізнесу, організаційна схема, фінансова звітність), ідентифікацію та верифікацію КБВ, а також документування джерела багатства (SOW) та джерела коштів (SOF). Кращі практики включають запит нотаріально засвідчених копій, використання офіційних реєстрів для підтвердження КБВ та незалежну перевірку документів з оригінальних джерел.

3. Перевірка на предмет несприятливих згадок у медіа та санкцій: Цей крок має на меті виявлення будь-яких відомих або потенційних зв'язків клієнта чи пов'язаної сторони з незаконною діяльністю, репутаційними проблемами або юридичними обмеженнями. Необхідно проводити скринінг санкційних списків (ООН, OFAC, ЄС, національні списки), контрольних списків (Інтерпол, антикорупційні списки, списки фінансування тероризму) та

негативних новин у глобальних та регіональних новинних базах даних, відкритих джерелах та регуляторних діях. Важливо переконатися, що згадки у медіа є актуальними, достовірними та релевантними. У разі виявлення потенційного збігу необхідно призупинити діяльність, провести валідацію, повідомити відділ комплаєнсу та, за необхідності, регуляторам.

4. Проведення виїзної перевірки або відеоінтерв'ю: Для високоризикових клієнтів ці методи є важливими для верифікації легітимності бізнес-операцій та підтвердження особи ключового персоналу. Виїзна перевірка включає відвідування зареєстрованої адреси бізнесу, зустрічі з власниками, спостереження за персоналом, інфраструктурою та наявністю операційних документів. Відеоінтерв'ю проводиться для клієнтів або КБВ, PEP, що не присутні фізично, із запитом на пред'явлення документів, обговорення бізнес-діяльності та спостереження за поведінковими індикаторами. Червоними прапорцями є, наприклад, невідповідність заявленої адреси, відсутність ознак активної діяльності або небажання розкривати деталі бізнесу.

5. Встановлення джерела коштів (SOF) / багатства (SOW): Це центральний стовп EDD, що допомагає фінансовим установам переконатися, що кошти законно отримані та відповідають профілю клієнта. SOF стосується походження конкретних коштів в транзакції, тоді як SOW – походження загального накопиченого багатства клієнта. Для верифікації збираються документи, такі як банківські виписки, податкові декларації, трудові договори, договори продажу активів, документи про спадщину, фінансова звітність для бізнесів. Важливо оцінити правдоподібність і відповідність задекларованих коштів та багатства профілю клієнта. Червоні прапорці включають відмову надавати документи, невідповідності або використання коштів з неперевірених джерел.

6. Посилений поточний моніторинг: EDD не закінчується на започаткуванні відносин; для високоризикових клієнтів необхідні посилені та безперервні заходи моніторингу. Це включає збільшення частоти та глибини моніторингу транзакцій (щоденно, щотижня, в реальному часі), застосування жорсткіших порогових значень для сповіщень та ручні перевірки, а також регулярні переоцінки ризиків (наприклад, кожні 6-12 місяців) та негайної переоцінки при виникненні тригерних подій (зміна власності, негативні згадки у медіа, зміна транзакційної поведінки). Використання технологічних інструментів, таких як поведінкова аналітика та системи динамічної оцінки ризиків, також є ключовим.

Успіх EDD залежить від своєчасного розпізнавання червоних прапорців, таких як відмова або небажання розкривати КБВ, нездатність надати чітку інформацію про джерело коштів/багатства, використання офшорних юрисдикцій без законної економічної мети, складні багатошарові структури власності, зв’язок з високоризикованими юрисдикціями або підсанкційними організаціями, надмірне використання готівки або віртуальних валют, а також часті зміни ключового персоналу або КБВ. Кожен червоний прапорець повинен викликати посилену перевірку та документоване розслідування. Неадекватна EDD може призвести до масштабних репутаційних, регуляторних та фінансових втрат, як показали випадки Danske Bank та Wirecard.

Ваша думка важлива!

1. McKinsey у своєму звіті підкреслює зростання ролі "агентського" штучного інтелекту. Як впровадження таких інструментів може змінити наглядові процеси, і які нові виклики для комплаєнсу у сфері ПВК/ФТ це створює?
2. Яким чином впровадження агентського AI може змінити структуру української економіки та які ризики це створює для ринку праці й етики використання даних?
3. Чи здатне широке застосування штучного інтелекту та блокчейн-аналітики у ПВК/ФТ-нагляді забезпечити реальний прорив у виявленні та запобіганні фінансовим злочинам, чи існує ризик надмірної технологічної залежності від алгоритмів?
4. Згідно з керівництвом FCA , національні політично значущі особи (PEP) у Сполученому Королівстві за замовчуванням вважаються низькоризиковими. Наскільки така модель може бути ефективною в українських реаліях, де корупційні ризики залишаються високими? Чи є інший спосіб забезпечити баланс між ефективним контролем та уникненням надмірного адміністративного тиску?
5. Стаття OCCRP розкриває складну екосистему шахрайства, яка використовує соціальні мережі для обману жертв. Які стратегії мають впровадити фінансові установи та державні органи, щоб захистити найбільш вразливі групи населення, зокрема ВПО та біженців, від онлайн-шахрайства?
6. Яку роль можуть відігравати цифрові платформи, соціальні мережі та месенджери у вербуванні українців для участі в кібершахрайстві, і які механізми протидії має застосовувати держава, щоб знизити ці ризики?
7. Які додаткові заходи можуть впровадити українські банки та платіжні сервіси, особливо ті, що співпрацюють із міжнародними платформами, для виявлення транзакцій, пов'язаних із шахрайськими кол-центрами?
8. Як координувати державні органи та приватний сектор в Україні для боротьби з внутрішньою торгівлею зброєю, особливо в умовах активних бойових дій?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-34

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

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