Методологічний бюлетень

Серійний номер: МінФін-AML-2025-35

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.

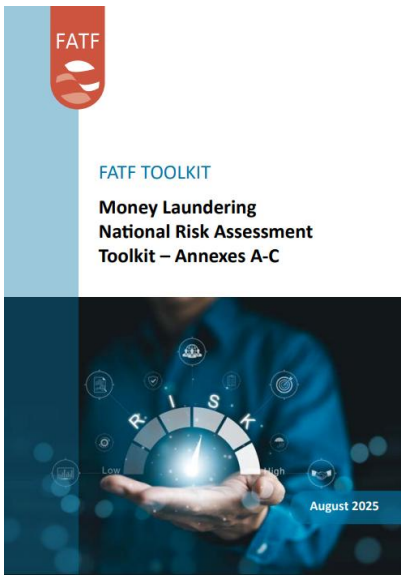
Містить актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

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

Інструментарій для Національної Оцінки Ризиків Відмивання Коштів [1]

АУДІОПЕРЕКАЗ



Представлений документ від FATF є розширеним оновленням до керівництва з Національної оцінки ризиків відмивання коштів. Цей інструментарій не є обов'язковим, тому його слід розглядати як збірник прикладів та передових практик, які можуть полегшити впровадження зобов'язань відповідно до стандартів FATF. Він доповнює та розширює інформацію, викладену в основному документі "ML NRA Guidance", і країни можуть вибірково використовувати матеріали, що є релевантними для їхнього унікального ризику та контексту.

Документ поділений на три додатки:

• Додаток А: "Короткі посібники з оцінки складних сфер оцінки ризиків". Цей додаток розроблено, щоб допомогти країнам впоратися зі складними областями оцінки ризиків, надаючи практичні поради для підвищення ефективності їхніх оцінок

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Money%20Laundering%20National%20Risk%20Assessment%20Toolkit.pdf.coredownload.pdf

ризиків відмивання коштів. Він висвітлює чотири ключові теми, які постійно виявляються складними для оцінки: корупція, віртуальні активи (ВА) та постачальники послуг віртуальних активів (VASP), юридичні особи та правові утворення, а також неформальна економіка. Для кожної з цих сфер надаються рекомендації щодо аналізу контексту країни, ідентифікації загроз та вразливостей, а також рекомендовані джерела даних. Підкреслюється важливість розгляду взаємозв'язків між цими темами, оскільки вони часто перетинаються та можуть посилювати загальний рівень ризику (наприклад, корумповані чиновники можуть використовувати фіктивні компанії або ВА для відмивання коштів, а злочинці можуть зловживати неформальною економікою). Додаток А також включає приклади успішних кейсів з різних країн Глобальної мережі FATF, таких як Індонезія, Малайзія, Франція, Гамбія (для корупції), Люксембург, Південна Африка, Єгипет (для ВА/VASPs), Нова Зеландія, Китай, Туреччина, Нігерія, Йорданія (для юридичних осіб/правових утворень), а також Китай, Індонезія, Ізраїль (для неформальної економіки).

• Додаток В: "Порівняльний аналіз загроз відмивання коштів та їх категоризація, а також категоризація вразливостей". Цей додаток надає узагальнену інформацію про ризики з різних країн, щоб визначити можливі сфери уваги, такі як найпоширеніші предикатні правопорушення та типи відмивання коштів на внутрішньому та міжнародному рівнях. Він служить інструментом для доповнення національних оцінок ризиків та пріоритезації певних поширених предикатних правопорушень, враховуючи транскордонний характер відмивання коштів. У додатку аналізуються основні предикатні правопорушення за даними звітів про взаємну оцінку (MER) та оцінки доходів від злочинів, де шахрайство, корупція, торгівля наркотиками та податкові злочини часто називаються основними. Особлива увага приділяється включенню аналізу наслідків злочинів, таких як людські, соціальні та екологічні збитки, щоб країни могли краще пріоритезувати кримінальні загрози, захищаючи як фінансову систему, так і суспільство в цілому. Додаток також розглядає типи

Висновки:

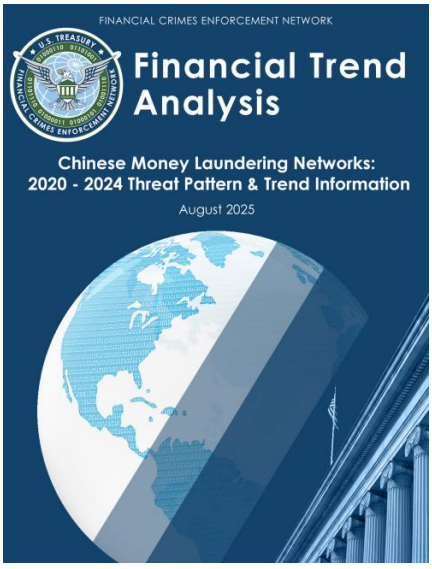
- **Сформуйте Комплексну Національну Оцінку Ризиків (НОР):** Країнам слід активно використовувати цей інструментарій для поглибленої оцінки ризиків ВК у складних сферах, таких як корупція, ВА, юридичні особи/правові утворення та неформальна економіка, адаптуючи надані посібники та тематичні дослідження до свого унікального національного контексту для підвищення ефективності AML-заходів.
- **Пріоритезуйте Аналіз Modus Operandi та Транскордонних Зв'язків:** Для ефективного виявлення та протидії ВК необхідно зосередитися на детальному вивченні способів, якими злочинці відмивають гроші (modus operandi), а також на виявленні та розумінні транскордонних елементів та взаємозв'язків між різними типами злочинності та фінансовими каналами, що дозволить розробити більш цілеспрямовані та ефективні заходи контролю.
- **Враховуйте Соціальні та Екологічні Наслідки Злочинів:** При проведенні НОР не обмежуйтеся лише фінансовими збитками; необхідно оцінювати ширші наслідки предикатних правопорушень, включаючи людські, соціальні та екологічні витрати, щоб забезпечити пропорційний розподіл ресурсів ПВК/ФТ та комплексний захист суспільства від усієї шкоди, спричиненої незаконною діяльністю.
- **Посилюйте Збір Даних та Міжнародну Співпрацю:** Для подолання прогалин у даних та покращення розуміння ризиків країни повинні використовувати різноманітні джерела інформації (наприклад, дані правоохоронних органів, STR, державні закупівлі, секторальні звіти), налагоджувати міжвідомчу координацію та активно брати участь у міжнародному та регіональному обміні інформацією про ризики та типології.

відмивання коштів, зазначаючи, що багато країн недостатньо аналізують складні схеми відмивання коштів у своїх NRA, що може впливати на ефективність розслідувань. Важливим є розуміння modus operandi (способу дії) відмивання коштів, щоб цілеспрямовано розробляти заходи протидії. Він надає всеосяжний перелік факторів загрози та вразливостей, включаючи політичні, економічні, соціальні, технологічні, екологічні та законодавчі чинники (рамки PESTEL), а також секторальні вразливості, щоб допомогти країнам сформувати повну картину ризикового ландшафту.

• Додаток C: "Пакет інструментів НОР (Світовий банк, Міжнародний валютний фонд, Рада Європи)". Цей додаток коротко описує методології, визначення ризиків, концепції властивого та залишкового ризику, оцінку ймовірності та наслідків, а також необхідні вхідні дані та роль кожної організації в процесі оцінки. Він служить орієнтиром для країн, що шукають додаткові ресурси для проведення своїх оцінок ризиків.

Цей документ є надзвичайно корисним для країн, оскільки він надає практичні рекомендації та передові практики для підвищення ефективності їхніх Національних оцінок ризиків відмивання коштів. Він допомагає країнам глибше зрозуміти та оцінити ризики у складних та нових областях, таких як віртуальні активи та неформальна економіка, де часто бракує даних або розуміння. Документ є цінним для розробки цілеспрямованих та пропорційних заходів протидії ВК, оскільки він закликає до аналізу modus operandi та врахування соціальних та екологічних наслідків злочинів, а не лише фінансових втрат. Він служить ресурсом для обміну інформацією та співпраці, пропонуючи зведені дані про регіональні та міжнародні тенденції ризиків, що особливо важливо через транскордонний характер відмивання коштів. Крім того, він надає доступ до методологій та інструментів від провідних міжнародних організацій, таких як Світовий банк, МВФ та Рада Європи, що дозволяє країнам вибирати найбільш відповідні ресурси для своїх потреб. Інструментарій також допомагає підвищити обізнаність як державних органів, так і приватного сектору про регуляторні очікування, типології та індикатори "червоних прапорців", що сприяє кращому виявленню та повідомленню про підозрілу діяльність. Загалом, документ спрямований на забезпечення того, щоб країни могли розвинути пропорційний, заснований на ризиках підхід до своєї системи протидії відмиванню коштів.

FinCEN публікує рекомендації та аналіз фінансових тенденцій щодо китайських мереж відмивання коштів [2] [3]



FinCEN опублікував два документи - Advisory #FIN-2025-A003 та Financial Trend Analysis (FTA) - щодо китайських мереж відмивання коштів (CMLNs), які системно обслуговують мексиканські наркокартелі та інші мережі організованої злочинності, інтегруючи злочинні доходи у фінансову систему США.

Фокус Advisory — дати цілісну картину феномену CMLNs, пов'язаного з картелями, описати провідні типології, навести індикатори підозрілої активності та нагадати про обов'язки банків відповідно до BSA, включно з очікуваною практикою заповнення SAR (із використанням ключового терміна «CMLN-2025-A003» і релевантних чекбоксів) та дотриманням процедур зберігання й надання супровідної документації. Advisory акцентує, що CMLNs — це горизонтально

[2] https://www.fincen.gov/sites/default/files/advisory/2025-08-28/FinCEN-Advisory-CMLN-508.pdf
[3] https://www.fincen.gov/sites/default/files/shared/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf

організовані, фрагментовані мережі професійних відмивачів, побудовані на довірі, які одночасно можуть займатися суміжними злочинними послугами (напр., підробка документів для відкриття рахунків). До складу часто входять чинні та колишні власники паспортів КНР; вони активно вербують представників китайської діаспори, зокрема студентів американських університетів, як грошових мулів, брокерів і кур'єрів. За оцінкою Мінфіну США (NMLRA-2024), CMLNs є однією з найзначніших загроз відмивання для фінсистеми США, а їхня привабливість для картелів зумовлена швидкістю, ефективністю та готовністю брати на себе ризики й втрати.

FTA кількісно підтверджує масштаб явища: 137 153 звіти за BSA від 1 038 установ у 2020–2024 рр., переважно від депозитних установ (85%), відображають підозрілу активність, яку FinCEN асоціює з CMLNs; загальний обсяг підозрілих операцій у датасеті — ≈ $312 млрд, із середнім показником ≈ $2,3 млн на подання та медіаною ≈ $86 тис. CMLNs «підхопили» глобалізацію торгівлі, оминають валютний контроль КНР та системно відмивають доларові доходи картелів через поєднання неформальних каналів і легального бізнесу, маскуючи джерело коштів. Драйвером взаємовигідної моделі є валютні обмеження Мексики (депозит USD у місцевих банках) і КНР (ліміти виведення капіталу громадянами), що стимулює обіг готівкового USD у США, яким CMLNs торгують «у тінь», задовольняючи попит китайських клієнтів на валюту.

Типологічно FinCEN виділяє «дзеркальні трансфери» (mirror transactions) у межах підпільних банківських схем і «peso-обміну», TBML, використання грошових мулів і «дроблення» внесків, а також експлуатацію e-commerce та ринку люксових товарів. У схемах із готівковими мулами нерідко декларуються професії, яким непритаманний великий обіг готівки (студенти, домогосподарки, пенсіонери, некваліфіковані робочі), застосовуються підроблені паспорти КНР для відкриття рахунків; зафіксовано також вербування або проникнення інсайдерів у фінансові установи для підтримки операцій CMLNs. У розрізі TBML, Advisory наводить практичні червоні прапорці: регулярні зарахування з маркетплейсів без відповідних закупівель під товарні залишки; дрібні компанії з необґрунтованими міжнародними переказами; масові вхідні операції P2P із подальшими погашеннями кредиток; диспропорція доходів і видатків у продавців

Висновки:

- **Удосконалити системи моніторингу для виявлення типологій CMLN.** Установи повинні налаштувати сценарії виявлення навколо дзеркальних переказів, аномалій електронної комерції, підозрілих платежів за кредитними картками та рахунків, пов'язаних з низькооплачуваними професіями з непропорційними обсягами транзакцій. Перевірка документів для китайських паспортів повинна бути посилена, щоб зменшити використання підробок.
- **Надавати пріоритет перевірці транзакцій з нерухомістю та касовими чеками.** Підозріла діяльність, пов'язана з об'єднаними коштами, незрозумілими переказами з Китаю та придбанням дорогоцінного майна, повинна послідовно ескалюватися, оскільки вони представляють основні типології відмивання коштів, виділені в Угоді про вільну торгівлю.
- **Посилити дисципліну звітності SAR.** SAR повинні містити відповідні категорії типологій та бути негайно подані з повною супровідною документацією, що гарантує правоохоронним органам ефективне використання розвідувальних даних.
- **Зменшити внутрішні вразливості та експлуатацію грошових мулів.** Установи повинні посилити програми боротьби з інсайдерськими загрозами, покращити перевірку співробітників та розширити моніторинг мереж рахунків, керованих "грошовими мулами", особливо серед студентів та діаспор, на яких спрямовані CMLN.

електроніки/люксових товарів; компанії оболонки з Гонконгу, що пересилають кошти без видимої економічної логіки.

Ринок нерухомості США — ще один ключовий канал інтеграції нелегальних коштів: FTA фіксує 17 389 BSA-звітів на понад $53,7 млрд підозрілої активності у секторі, зокрема через великі готівкові депозити, їх консолідацію, участь третіх осіб і «pooling» коштів; також часто відмічено вхідні перекази з КНР від «родичів», при цьому клієнти не надають підтверджень походження коштів; популярними поясненнями є оплата нерухомості або навчання. У контексті регуляторних бар'єрів у КНР щодо купівлі американської нерухомості FTA описує використання CUBSs і брокерів CMLN для великих платежів.

Окремі супутні злочини та пов'язані сектори ілюструють широту феномена: 1 675 BSA-звітів щодо можливої торгівлі людьми/контрабанди мігрантів; 108 звітів про підозрілі депозити, пов'язані з медичним шахрайством, зловживанням щодо літніх осіб та підозрілою ігровою активністю; 43 звіти (≈ $766 млн) щодо 83 центрів денного догляду за дорослими у Нью-Йорку. Додатково FTA виявляє ≈ 20 282 BSA-звітів (≈ 14% масиву) на ≈ $13,8 млрд, що прямо згадують «китайських студентів»; FinCEN пояснює їхню вразливість до вербування CMLNs потребою мереж у великій кількості рахунків для частих готівкових внесків.

На рівні профілю активності, найтиповішою ознакою, відображеною у FTA, є великі готівкові депозити на рахунки осіб із США з китайськими паспортами без підтвердженого джерела доходів або за умов низькооплачуваних професій; таких подань — ≈ 46 360 (33% датасету) на $33+ млрд.

Узагальнюючи, Advisory/FTA підтверджують: CMLNs — це глобальні, адаптивні мережі, що обслуговують картелі та інші кримінальні еко-системи, агресивно використовуючи торгові, фінансові та побутові канали (від маркетплейсів до титульних компаній у нерухомості), маскуючи походження коштів через багаторівневі й крос-юрисдикційні схеми; ключова роль фінансового сектору — раннє виявлення типових патернів, належне документування та проактивний обмін даними, що забезпечує корисну для правоохоронців фінрозвідку.

Ставлення громадян до корупції в ЄС у 2025 році [4]

Документ є масштабним соціологічним дослідженням, проведеним у 27 країнах Європейського Союзу, яке відображає сприйняття громадянами поширеності корупції, її впливу на щоденне життя, довіри до державних інституцій та готовності повідомляти про корупційні випадки. У звіті представлено детальну статистику за демографічними та соціально-професійними групами, а також простежено ключові закономірності. Більшість громадян ЄС (69%) вважають корупцію широко поширеною, при цьому найбільший рівень занепокоєння демонструють ті, хто має фінансові труднощі, безробітні та ті, хто безпосередньо стикався або був свідком корупції. У молодших вікових групах рівень занепокоєння нижчий, тоді як громадяни старшого віку та менш освічені частіше оцінюють корупцію як всеохопну проблему.

Ставлення до корупції у повсякденному житті є амбівалентним: лише 30% громадян ЄС відчувають її

[4] https://europa.eu/eurobarometer/surveys/detail/3361

безпосередній вплив, тоді як 64% вважають, що корупція існує, але не зачіпає їх напряму. Найвищий рівень відчуття особистої ураженості мають ті, хто зазнає регулярних фінансових труднощів або має досвід власного зіткнення з корупційними практиками. Цікаво, що толерантність до корупційних дій у суспільстві низька: 64% респондентів вважають її абсолютно неприйнятною, хоча 30% визнають певний рівень терпимості залежно від ситуації.

Громадяни чітко визначають сфери найбільшої корупційної вразливості. Політичні партії, національні та місцеві політики, чиновники, що розподіляють тендери, та посадові особи, які видають дозволи на будівництво чи бізнес, очолюють список інституцій, де хабарництво й зловживання владою вважаються поширеними. Водночас поліція, митні органи, система охорони здоров'я та навіть банки сприймаються як сектори, де корупція також має місце, хоч і меншою мірою.

У динаміці останніх років 44% громадян ЄС вважають, що рівень корупції зріс, тоді як лише 9% вважають, що він знизився. Це формує загальний песимістичний фон щодо ефективності державних заходів. Більшість респондентів (73%) погоджуються, що корупція існує на національному рівні, 70% – на місцевому, а 66% вважають, що хабарі та використання особистих зв'язків часто є найпростішим способом отримати послуги. Близько 77% погоджуються, що надмірна взаємозалежність бізнесу та політики неминуче веде до корупції, а 65% переконані, що фаворитизм і хабарництво шкодять конкуренції.

Надзвичайно важливим є низький рівень довіри до ефективності антикорупційних заходів. Дві третини громадян вважають, що гучні справи про корупцію не переслідуються належним чином, а 61% вважають, що заходи протидії не застосовуються неупереджено. Лише 32% респондентів погоджуються, що існує достатня кількість успішних вироків, здатних відлякувати потенційних порушників. Це підриває загальне відчуття справедливості та впевненість у верховенстві права.

Ще один критичний аспект стосується готовності повідомляти про корупцію. Лише 5% громадян ЄС протягом останнього року особисто стикалися з корупційними випадками, але навіть серед них рівень повідомлення надзвичайно низький: тільки 20% зробили офіційні звернення. Основні причини небажання повідомляти включають складність доказування, переконання у безкарності винних, страх перед репресіями та відсутність знань, куди саме звертатися. Лише 44% респондентів знають, куди слід скаржитися у випадку корупції, і найбільшу довіру серед органів викликає поліція (61%), тоді як спеціалізовані антикорупційні агентства, медіа чи омбудсмени отримують значно нижчі показники довіри.

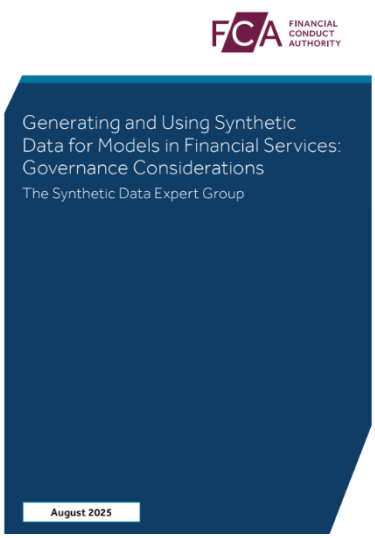
В Україні тенденції є подібними до результатів ЄС, але з більш вираженою інтенсивністю. За даними опитування Transparency International Ukraine (2023), 88% українців вважають корупцію широко поширеною, що вище за середній показник ЄС у 69%. Так само українці вважають політичні партії, суди та правоохоронні органи найбільш корумпованими. Рівень недовіри до здатності держави ефективно

Висновки:

- **Поширене сприйняття корупції:** у ЄС 69% громадян вважають корупцію широко поширеною.
- **Низька довіра до інституцій:** більшість респондентів у ЄС вважають, що справи високопосадової корупції не переслідуються належним чином, а заходи застосовуються упереджено.
- **Недостатня готовність до повідомлення:** лише 20% громадян ЄС, які стикалися з корупцією, заявили про неї.
- **Ключові сфери ризику:** в ЄС найбільш вразливими до корупції вважаються політичні партії, сфера державних закупівель та дозвільні органи, що вимагає посилення прозорості, цифровізації та незалежного контролю.

переслідувати високопосадову корупцію ще вищий, ніж у ЄС, що зумовлено системними проблемами. Водночас, на відміну від багатьох країн ЄС, в Україні рівень громадянської активності та використання антикорупційних інструментів є вищим, що дає підстави для формування позитивної динаміки у довгостроковій перспективі.

Використання синтетичних даних: як побудувати довіру та безпечні рамки у фінансовій сфері [5]



Документ, підготовлений Synthetic Data Expert Group (SDEG) при FCA у серпні 2025 року, є підсумковим аналітичним звітом, що систематизує практичний досвід, теоретичні напрацювання та ключові виклики, пов'язані зі створенням і використанням синтетичних даних у фінансовому секторі. Центральним завданням звіту є не лише описати потенційні можливості цієї технології, а й висвітлити аспекти врядування, управління ризиками, прозорості, етики та довіри, без яких широке впровадження синтетичних даних у практику фінансових інститутів залишатиметься обмеженим. Відправною точкою аналізу є визнання того факту, що сучасні фінансові послуги функціонують на основі даних, і хоча це відкриває нові можливості для інновацій та автоматизації, водночас це створює серйозні ризики, пов'язані з конфіденційністю, нерівним доступом та можливими викривленнями результатів прийняття рішень. Синтетичні дані, визначені як штучно створені набори, що відтворюють статистичні властивості реальних даних без включення персонально ідентифікаційної інформації, постають як інструмент, здатний знизити ці ризики та підтримати розвиток інновацій. FCA через діяльність SDEG намагалася виробити підходи, які дозволять перетворити синтетичні дані на надійний та масштабований механізм підтримки фінансових технологій.

У вступній частині документ окреслює історію становлення тематики у Великій Британії: від ініціативи DataSprint 2020 року, яка дозволила регулятору та ринку спільно випробувати перші підходи до генерації синтетичних даних, до запуску Digital Sandbox та подальших консорціумів, у тому числі проєкту з протидії відмиванню коштів (ПВК) із залученням FCA, Alan Turing Institute, Plenitude та Napier AI. Ці ініціативи продемонстрували практичну значущість синтетичних даних для оцінки ефективності систем моніторингу, тестування алгоритмів та побудови прототипів у безпечному середовищі. Водночас зібраний досвід підтвердив необхідність розроблення рамкових підходів до врядування та вироблення спільних стандартів, адже 31% учасників Call for Input 2022 прямо заявили про потребу регуляторних настанов, стандартів або рамок врядування для забезпечення довіри до таких рішень.

Подальші розділи звіту детально висвітлюють, як організаціям оцінювати власну готовність до запуску синтетичних проєктів. Тут акцент зроблено на важливості трьох фундаментальних складових: наявності структур врядування, які охоплюють контрольні процеси, ролі та механізми ескалації; чіткої ідентифікації ролей та відповідальності між учасниками, включно з юридичними, технічними та етичними функціями; підтримки наскрізної документації і механізмів постійного моніторингу. Автори наголошують, що будь-який проєкт із синтетичними даними має починатися з визначення його мети і конкретного завдання, яке він покликаний вирішити, наприклад посилення конфіденційності, забезпечення доступності даних чи

[5] https://www.fca.org.uk/publication/corporate/synthetic-data-models-financial-services-governance.pdf

підвищення якості тренування моделей. Для цього необхідно проводити оцінку цінності й ризику, зіставляючи потенційні переваги із витратами та ймовірними загрозами, а також враховувати регуляторні, етичні й правові аспекти ще на стадії планування.

Окрему увагу звіт приділяє процесу генерації синтетичних даних, де головними викликами визначено аудитованість, захист приватності та управління упередженістю. Підкреслюється, що вибір методології (генеративно-змагальні нейронні мережі (GAN)s, агенто-орієнтовані підходи, статистичні моделі) не є суто технічним, а потребує балансування між точністю, корисністю та конфіденційністю. При цьому кожен крок процесу має супроводжуватися документацією і створенням «ланцюга доказів», що дозволяє відслідковувати прийняті рішення, використані припущення і результати валідації. Для мінімізації ризиків реідентифікації рекомендуються комплексні підходи до тестування приватності, включно з red teaming (група експертів, що імітує дії потенційного зловмисника з метою тестування вразливостей системи, процесів чи даних), застосуванням K-anonymity чи L-diversity (методи захисту приватності у наборах даних), аналізом ризиків кореляції з зовнішніми наборами даних та використанням диференційної приватності. Проте автори підкреслюють, що додаткові шари захисту, як-от внесення шуму, можуть знижувати якість і корисність даних, отже необхідне балансування залежно від кінцевої мети. Щодо упередженості, наголошується на необхідності ідентифікації потенційних упереджень у вихідних наборах, формування чіткої стратегії щодо їх корекції чи збереження, а також документування усіх рішень і компромісів, зроблених у процесі.

Висновки:

- **Необхідність інтеграції синтетичних даних у вже існуючі рамки управління ризиками та етики:** їх застосування має спиратися на принципи AI Ethics та Model Risk Management, з особливим фокусом на прозорість, відповідальність і запобігання дискримінації.
- **Приватність і упередженість — ключові ризики:** навіть у відсутності персональних даних залишається ризик реідентифікації або відтворення історичних упереджень. Тому потрібне комплексне тестування і регулярний моніторинг протягом усього життєвого циклу.
- **Якість синтетичних даних оцінюється через їх корисність для конкретного застосування, а не лише через статистичну подібність до реальних даних.** Для цього застосовуються порівняльне оцінювання продуктивності, TSTR і залучення доменних експертів.
- **Будування довіри — критичний фактор впровадження:** організації мають документувати і пояснювати, навіщо та як застосовується синтетичний набір, які були компроміси, які заходи захисту реалізовані. Це є основою не лише для внутрішньої довіри, але й для зовнішнього регуляторного та суспільного прийняття.

Далі документ зосереджується на використанні синтетичних даних у моделях машинного навчання та аналітиці. Синтетичні набори можуть застосовуватися як тренувальні, тестові чи валідаційні дані, але їхня якість має оцінюватися не лише за статистичною подібністю до реальних, а насамперед у контексті завдань, які вони виконують. У цьому сенсі ключовими підходами виступають порівняльне оцінювання продуктивності та метод Train-Synthetic-Test-Real (TSTR), які дозволяють визначити, наскільки модель, навчена на синтетичних даних, здатна узагальнювати й ефективно працювати з реальними. Особливе значення надається аналізу пояснювальності та чутливості ознак: наскільки адекватно модель, тренована на синтетичних даних, ідентифікує та інтерпретує ключові ознаки, і чи не виникає надмірної залежності від вузького набору змінних, що може свідчити про низьку достовірність синтетичного набору. У фінансовому секторі, де ці моделі можуть впливати на рішення щодо кредитування, шахрайських

транзакцій чи клієнтської сегментації, наслідки таких викривлень можуть мати суттєвий вплив на справедливість і надійність результатів.

У висновковій частині наголошено, що довіра до синтетичних даних є передусім завданням врядування, а не лише технічного вдосконалення алгоритмів. Вона формується через прозорість у прийнятті рішень, постійний моніторинг, міждисциплінарну співпрацю, обов'язкову документацію, аудит і готовність пояснити як внутрішнім, так і зовнішнім стейкхолдерам, чому та як використовуються синтетичні дані, які компроміси були прийняті та які гарантії захисту реалізовано. FCA підкреслює, що розвиток спільних підходів і продовження співпраці між регулятором, бізнесом, академічним середовищем і суспільством є вирішальними для формування зрілого екосистемного підходу до синтетичних даних. Таким чином, документ окреслює синтетичні дані не як технічний інструмент із гарантованими перевагами, а як складну технологію, ефективність якої залежить від здатності організацій інтегрувати її у врядувальні структури, етичні стандарти та регуляторні вимоги, забезпечуючи баланс між інноваціями, безпекою та суспільною довірою.

Пропорційність і ризик-орієнтований підхід у нових змінах до MLRs Великої Британії [6]

Документ є комплексною відповіддю уряду Великої Британії на проведену у 2024 році консультацію щодо вдосконалення ефективності положень Money Laundering Regulations (MLRs), що встановлюють обов'язки для широкого кола фінансових і нефінансових організацій у сфері запобігання та протидії відмиванню коштів і фінансуванню тероризму. У вступі підкреслюється, що ефективна система ПВК/ФТ є ключовою для збереження цілісності фінансової системи, захисту інвестиційної привабливості країни та виконання міжнародних зобов'язань у рамках FATF. Документ розкриває чотири головні напрями змін, що стали результатом консультації: підвищення пропорційності та ефективності перевірки клієнтів, зміцнення координації між учасниками системи, уточнення сфери дії та питань реєстрації, а також реформа Trust Registration Service (TRS).

Перший блок стосується належної перевірки клієнів (CDD) та посиленої перевірки клієнтів (EDD), які становлять ядро всієї системи ПВК/ФТ. Уряд визнає, що частина норм була нечіткою, а вимоги надмірними або непропорційними. Тому запроваджується низка змін. Уточнюються тригери проведення CDD для нефінансових установ (зокрема для арт-дилерів, агентів з нерухомості, торговців високовартісних товарів), щоб уникнути дублювання між поняттям «бізнес-відносин» та порогами вартісних транзакцій. Планується внесення коректив у регуляції для забезпечення більшої чіткості, тоді як деталізація має відображатися у галузевих керівництвах. Особлива увага приділяється перевіркам джерела походження коштів: уряд залишає формулювання «де це необхідно», але прагне посилити роз'яснення та надати приклади для конкретних секторів, щоб зменшити неоднозначність застосування. Уточнено й положення щодо випадків, коли особи діють від імені клієнта: визнано, що звичайні працівники компанії, які здійснюють транзакції від імені свого роботодавця, не повинні підпадати під процедури повної перевірки, на відміну від агентів чи представників з довіреностями. Значним кроком є інтеграція цифрових технологій ідентифікації, що отримали державну підтримку і стандартизацію в рамках Data (Use and Access) Act 2025, із

[6] https://assets.publishing.service.gov.uk/media/6878c1b42bad77c3dae4dd25/MLRs_Consultation_Response.pdf

запровадженням акредитації цифрових провайдерів та їх сертифікації. Також передбачено законодавчий виняток із загальних вимог для неплатоспроможних банків, коли під час масового переходу клієнтів в інші банки затримки у верифікації могли б спричинити економічні ризики: у таких випадках банки зможуть відкривати рахунки з відтермінованою ідентифікацією, але під наглядом FCA. Щодо EDD, ключові зміни стосуються уточнення, що обов'язкова посилена перевірка застосовується лише до «незвично складних» транзакцій, а не до будь-яких складних за своєю природою, тоді як вимога для «незвично великих» операцій залишається. Це дозволяє уникати надмірної перевірки у секторах, де більшість угод є складними за визначенням, наприклад у нерухомості чи корпоративних операціях. Крім того, у частині високоризикових країн змінюється підхід: EDD буде обов'язковим лише для країн зі списку FATF Call for Action (Іран, КНДР, М'янма), тоді як країни з Increased Monitoring List враховуватимуться у ризик-оцінках, але без автоматичного застосування EDD. Це є більш ризик-орієнтованим підходом і дозволяє концентрувати ресурси на напрямках, найбільш небезпечних для фінансової системи Великої Британії. Важливим є і рішення щодо зведених клієнтських рахунків: замість прив'язки до спрощеної перевірки клієнта пропонуються окремі правила, що мають спростити доступ до таких рахунків при одночасному забезпеченні належних захисних механізмів.

Другий блок стосується зміцнення координації системи та обміну інформацією. Консультація показала необхідність розширення механізмів інформаційної взаємодії між наглядовими органами та іншими державними інституціями. Зокрема, до переліку органів у Regulation 52 буде включено уповноважених з розгляду скарг на фінансових регуляторів (FRCC) для підвищення прозорості нагляду FCA. Також уряд передбачає уточнення можливостей FCA у розкритті конфіденційної інформації, зокрема стосовно криптовалютних компаній. Значним кроком є внесення Companies House до переліку обов'язкових партнерів для кооперації із наглядовими органами, що має посилити контроль за корпоративними структурами та їхніми бенефіціарами у рамках реформи, закріпленої в Economic Crime and Corporate Transparency Act 2023. Водночас уряд вирішив не вводити прямого зобов'язання щодо обов'язкового врахування національної оцінки ризиків (НОР) у ризик-оцінках компаній, оскільки це вже є усталеною практикою, але наголосив на необхідності оновлення НОР та роз'яснювальних матеріалів.

Третій блок стосується сфери застосування та реєстраційних питань. Усі пороги у валютних сумах у MLRs будуть переведені з євро на фунти стерлінгів за принципом 1:1, що усуває адміністративну плутанину після виходу Великої Британії з ЄС. Одним із найбільш важливих нововведень є поширення регуляцій на продаж «off-the-shelf» компаній (компанії, які готові до використання) Trust and Company Service Providers, що закриває серйозну прогалину у системі, оскільки раніше під час перепродажу компанії CDD не застосовувалося. Значна увага приділена криптовалютному сектору: планується гармонізація регулювання між MLRs та FSMA, щоб уникнути подвійної реєстрації, забезпечити чіткі механізми зміни у структурі власності та узгодити підходи до перевірки на відповідність вимоам доброчесності та професійної придатност. Це означає, що криптосервісні компанії будуть ліцензуватися виключно за FSMA, а їхні власники перевірятимуться за єдиними стандартами. Передбачено також вимогу належної перевірки контрагентів для криптокомпаній, у відповідності до стандартів FATF (рекомендації 13 та 15).

Четвертий блок присвячений Trust Registration Service. Визнається суттєва прогалина у регулюванні: іноземні трасти без британських довірчих власників (trustee), які володіли нерухомістю, придбаною до жовтня 2020 року, не підлягали реєстрації. Тепер уряд поширює на них вимогу обов'язкової реєстрації та включає у систему обміну даними, забезпечуючи можливість доступу третіх сторін за критерієм «законний інтерес». Також уніфікуються правила для трастів, що виникають після смерті, зокрема шляхом надання дворічного пільгового періоду для їхньої реєстрації, щоб зменшити адміністративне навантаження у складний час. Шотландські трасти із застереженням про спадкування (Scottish survivorship destination trusts)

будуть виключені з-під реєстраційних вимог як низькоризикові. Водночас запроваджується звільнення за принципом de minimis для дрібних трастів із невеликим обсягом активів і доходів, що дозволить знизити бюрократичний тиск на малозначні структури, включаючи локальні спортивні клуби. Окремо ухвалено рішення виключити податок на гербовий збір при операціях з цінними паперами зі списку «відповідних податків», які автоматично спричиняли реєстрацію трасту, оскільки це призводило до надмірного навантаження навіть за незначних інвестицій у британські акції.

Завершальна частина документа містить додаткові уточнення, серед яких узгодження положень MLRs з FSMA Exemption Order щодо суверенних фондів, уточнення визначення страхових установ із виключенням перестрахувальних контрактів як низькоризикових для ВК/ФТ, а також підготовка до впровадження повного пакету змін через новий підзаконний нормативно-правовий акт. Уряд наголошує, що всі ці зміни спрямовані на баланс між зниженням адміністративних витрат для бізнесу, посиленням таргетованого ризик-орієнтованого підходу та зміцненням здатності системи запобігати відмиванню коштів, фінансуванню тероризму й уникненню санкцій. Таким чином, реформа MLRs відображає курс Великої Британії на більш розумне, сучасне й скоординоване регулювання, яке відповідає як національним ризикам, так і міжнародним зобов'язанням.

Висновки:

- **Фокус EDD на високих ризиках.** Відтепер обов'язкова посилена перевірка застосовуватиметься лише до «Call for Action» країн FATF та до «незвично складних» транзакцій. Це знижує адміністративні витрати та концентрує ресурси на найнебезпечніших ризиках.
- **Посилення прозорості трастів.** Усі іноземні трасти, які володіють британською нерухомістю (незалежно від дати придбання), підлягатимуть реєстрації в TRS і потрапляють під механізм «законного інтересу». Це закриває ключову прогалину у боротьбі з прихованою власністю.
- **Гармонізація регулювання криптовалют.** Запроваджується узгодження між MLRs і FSMA, що усуває дублювання вимог і робить процедури «перевірки на відповідповідність вимогам доброчесності та професійної придатності» для власників криптокомпаній більш ефективними, одночасно вводячи вимогу належної перевірки контрагентів.
- **Цифрова ідентифікація та зведених рахунків.** Запуск державних стандартів цифрової ідентифікації та спрощення доступу до зведених клієнтських рахунків мають зробити процедури у сфері ПВК більш сучасними, технологічними та практичними.

Звіти окремих інституцій та експертів

Звіт робочої групи з питань державно-приватного партнерства та віртуальних активів в Україні [7]

Звіт Цільової групи з державно-приватного партнерства та віртуальних активів в Україні, підготовлений Оксаною Ігнатенко та Гретою Баркаускене з Королівського об'єднаного інституту оборонних досліджень (RUSI), підкреслює критичну необхідність України врегулювати ринок віртуальних активів (ВА) у контексті її вступу до ЄС та боротьби з фінансовими злочинами. У липні 2025 року RUSI та Центр фінансової доброчесності скликали зустріч Цільової групи, в якій взяли участь близько п'ятдесяти представників державного та приватного секторів України, а

[7] https://static.rusi.org/ukraine-ppps-taskforce-second-report-august-2025.pdf

також міжнародні експерти. Основна увага приділялася аналізу чинної нормативно-правової бази, пов'язаних ризиків, незаконної діяльності та міжнародного досвіду, з метою розробки рекомендацій для підтримки регулювання та розвитку безпечного ринку ВА в Україні.

Україна, як частина процесу вступу до ЄС, повинна імплементувати 69 реформ відповідно до Плану Механізму підтримки України, включаючи гармонізацію законодавства щодо ВА з законодавством ЄС, що має бути завершено до кінця 2025 року як частина ширших заходів протидії відмиванню коштів. Одночасно, Україна повинна забезпечити належну імплементацію Рекомендації 15 FATF, яка вимагає від країн оцінювати та пом'якшувати ризики ВК/ФТ, пов'язані з ВА та постачальниками послуг віртуальних активів (VASP). Україна отримала лише часткову відповідність у 2020 році від FATF, і є побоювання, що її рейтинг може бути знижений у майбутній оцінці MONEYVAL вже у 2027 році.

Спроби регулювання ринку ВА в Україні почалися ще у 2018 році. Хоча Закон України «Про віртуальні активи» № 2074-IX був прийнятий у лютому 2022 року, він так і не набрав чинності через нерозв'язані питання оподаткування та відсутність змін до Податкового кодексу. Між 2022 та 2023 роками було розроблено два проєкти законів – один від Національної комісії з цінних паперів та фондового ринку (НКЦПФР) з інтеграцією стандартів ЄС Markets in Crypto Assets Regulation (MiCA), а інший від Міністерства цифрової трансформації, що поєднував існуюче законодавство з положеннями MiCA. Ці проєкти викликали дискусії, але залишилися не ухваленими, залишаючи сектор неврегульованим. Новий законопроєкт № 10225-д, поданий до парламенту 24 квітня 2025 року, об'єднує попередні пропозиції та вводить ключові зміни для регулювання ринку ВА відповідно до міжнародних стандартів, включаючи вимоги до ліцензування платформ (капітал, прозорість, стандарти KYC) та процедури звітності для транзакцій ВА. Він також надає чіткі класифікації та визначення типів ВА, таких як криптоактиви, токени електронних грошей (EMTs) та токени, прив'язані до активів (ARTs), повністю узгоджені зі стандартами MiCA, хоча експерти висловили сумніви щодо запропонованих класифікацій.

Ключовим невирішеним питанням залишається призначення відповідального регулятора. Пропонується двохетапна модель регулювання: Національний банк України (НБУ) контролюватиме банки, що беруть участь у транзакціях з ВА, та регулюватиме EMTs, тоді як інший регулятор (ймовірно, НКЦПФР) наглядатиме за криптобіржами та іншими VASPs. Міжнародні експерти застерігають, що традиційні банківські регуляції не завжди ефективно застосовні до швидкозмінного криптосектору, що створює ризик регулятивного арбітражу. Франція наводиться як приклад успішної двохетапної моделі. Парламент України визначить регулятора при прийнятті законопроєкту, і критично важливо забезпечити узгодженість, ясність та функціональну відповідність регулятивного нагляду для розвитку ринку.

Серед поточних викликів регулювання ВА в Україні обговорювалося питання податкової амністії, адже Національна оцінка ризиків України визначила криптоактиви як високий ризик ВК/ФТ, що робить спрощену податкову амністію нездійсненною. Зростає кількість судових справ, пов'язаних з ВА, але правова невизначеність зберігається через непослідовні рішення та нечіткі процедури. Експерти наголосили на необхідності підвищення обізнаності та навчання суддів та правоохоронців. Також була висловлена стурбованість щодо фрагментованої політичної волі та відсутності чіткої міжвідомчої координації, що є перешкодою для подальшого прогресу.

У питанні відповідності MiCA, експерти зауважили, що її складність може гальмувати інновації та створювати навантаження на малі фірми. Оскільки Україна ще не є членом ЄС, вона має можливість прийняти більш поступовий та адаптований підхід. Учасники пропонували надати

юридичний статус таким видам діяльності, як кредитування, запозичення та торгівля деривативами, які виходять за рамки MiCA, для розвитку інфраструктури ліквідності та створення нових джерел доходу. Регулювання стейблкоїнів може бути спрощено шляхом об'єднання EMTs та ARTs в єдину категорію, обмеження емісії регульованими фінансовими установами та дозволу виплат для підтримки ліквідності. Економічні потреби України наразі можуть суперечити логіці правових актів ЄС, і країна повинна надавати пріоритет стабільності, навіть якщо це означає тимчасове відхилення від MiCA.

Законодавство повинно бути гнучким, на високому рівні, щоб охоплювати майбутні розробки, як це успішно продемонстровано в ОАЕ з їхнім спеціалізованим регулятором та регулятивними «пісочницями». На відміну від Молдови, яка спочатку заборонила VASPs, Україна повинна збалансувати ефективний контроль з практичною імплементацією, щоб уникнути корупції та організованої злочинності, включаючи прозорий процес ліцензування та чіткі інструкції для правоохоронних органів. Реєстрація першого VASP в Україні є ключовою для демонстрації готовності до регулювання перед MONEYVAL та зупинки відтоку українських VASPs за кордон.

Віртуальні активи несуть як універсальні ризики (обмежена відстежуваність, непослідовний нагляд, слабкий захист споживачів, складність перевірки джерел коштів, незворотність транзакцій, погане управління гаманцями), так і специфічні для України ризики. До останніх належать значна діяльність позабіржових (OTC) платформ, які використовуються для обходу міжнародних санкцій, включаючи закупівлю компонентів подвійного призначення для російських збройних сил та гібридну війну, наприклад, розповсюдження синтетичних наркотиків через Telegram. Україна також розглядається як потенційний хаб для відмивання криптофондів іноземними акторами, особливо російськими розвідувальними службами, через її географічне положення, вразливості військового часу та недосконале законодавство. Крім того, обмеження НБУ на міжнародні перекази після вторгнення призвели до зростання схем з «дропами» (грошовими мулами), які, за оцінками, коштують державному бюджету близько 1 мільярда гривень (24 мільйони доларів) на місяць.

Для пом'якшення ризиків, VASPs використовують інструменти блокчейн-аналітики та комерційні засоби для належної перевірки клієнтів (CDD) та постійного моніторингу, хоча їх якість та сумісність варіюються, і вони не завжди є надійними доказами в суді. Традиційні фінансові установи часто уникають співпраці з криптосектором, але можуть розробити найкращі практики, такі як опитувальники KYC та CDD, за зразком Вольфсберзької групи. Необхідно вдосконалити обмін інформацією між приватним та державним секторами, особливо з правоохоронними органами, оскільки поточні обмеження захисту даних перешкоджають своєчасному звітуванню.

Державно-приватні партнерства (PPP) є перспективною сферою для підвищення ефективності боротьби з фінансовими злочинами в Україні, зокрема шляхом спільної розробки оцінок ризиків. Поточна Національна оцінка ризиків України 2022 року щодо ВА є неглибокою і не відображає секторних загроз, а також не повною мірою залучає правоохоронні органи та інші ключові зацікавлені сторони. Для покращення аналітичних можливостей державі потрібен прямий доступ до первинних даних, включаючи розвідку з відкритих джерел та дані обмінних платформ. Міжнародний досвід, такий як Europol Financial Intelligence Public Private Partnership (EFIPPP) та литовський AML Center, демонструє успішні моделі співпраці для обміну фінансовою розвідкою та вирішення проблем, таких як Travel Rule. Литва, наприклад, активно інтегрує VASPs, навіть якщо більшість з них ще не отримали повних ліцензій, що свідчить про необхідність залучення криптосектору до діяльності PPP. Україні слід прийняти сфокусовану стратегію відповідності, починаючи з найважливіших вимог і поступово розширюючись, одночасно залучаючи міжнародних партнерів.

Загалом, учасники зустрічі дійшли висновку, що законодавство не є передумовою для негайних практичних дій, особливо через PPP, для виявлення та пом'якшення незаконної діяльності. Водночас, Україні потрібне цілеспрямоване та добре розроблене законодавство, адаптоване до її контексту, щоб уникнути регулятивного застою.

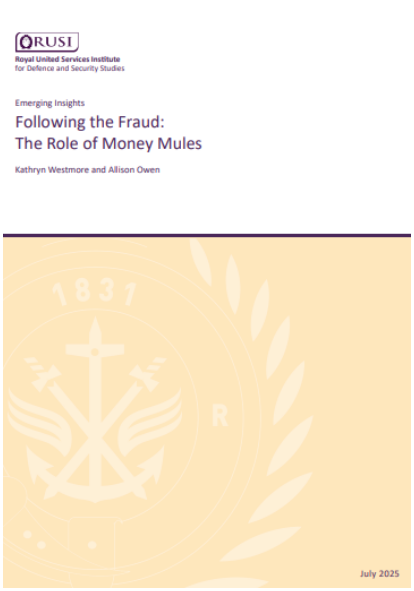
Висновки:

- **Негайне посилення правозастосування та оперативних заходів проти незаконної діяльності з ВА:** Незважаючи на відсутність комплексного законодавства, Україна повинна негайно використовувати наявні інструменти та досвід для боротьби з незаконною діяльністю, пов'язаною з ВА. Це включає: 1) Запровадження цільових стратегій правозастосування проти позабіржових (OTC) операцій, які використовуються для обходу санкцій, фінансування російських військових та поширення синтетичних наркотиків; 2) Інвестиції у розслідування блокчейну та покращення координації між фінансовими установами та правоохоронними органами для відстеження транскордонних потоків; 3) Підвищення обізнаності та навчання суддів та співробітників правоохоронних органів, щоб забезпечити послідовність та обґрунтованість рішень у справах, що стосуються ВА; 4) Використання комерційних рішень для зміцнення можливостей інституцій щодо ефективного відстеження транзакцій з ВА.
- **Прийняття цільового та гнучкого законодавства щодо віртуальних активів з фокусом на економічні потреби та міжнародні стандарти:** Україні вкрай необхідне спеціалізоване законодавство щодо ВА, яке було б адаптоване до її поточного контексту та дозволяло уникнути регулятивної стагнації. Практичні дії включають: прискорене прийняття законопроєкту № 10225-д або подібного законодавства; визначення чітких регуляторів; надання правового статусу діяльності, що виходить за рамки MiCA та спрощення регулювання стейблкоїнів.
- **Зміцнення PPP та розробка якісних, орієнтованих на дані оцінок ризиків:** Для ефективного протидії ВК/ФТ в секторі ВА Україні потрібно покращити співпрацю та обмін інформацією. Ключові дії: 1) Спільна розробка поглиблених оцінок ризиків, що включають секторальні загрози ВА, залучаючи правоохоронні органи та інших ключових стейкхолдерів; 2) Забезпечення прямого доступу регуляторів та правоохоронних органів до сирих даних від провайдерів блокчейн-аналітики, а також ширшого спектру джерел; 3) Створення дорожньої карти зацікавлених сторін для PPP, що сприятиме обміну знаннями та інформацією, а також допоможе зрозуміти потреби кожного учасника для ефективної співпраці.

Відстежуючи шахрайство: Роль грошових мулів [8]

Документ, підготовлений Кетрін Вестмор і Еллісон Овен із Королівського об'єднаного інституту оборонних і безпекових досліджень (RUSI) у липні 2025 року за фінансової підтримки Lloyds Banking Group, є ґрунтовним аналітичним дослідженням ролі "грошових мулів" у відмиванні грошей, отриманих від шахрайства з авторизованими платіжними дорученнями (APP fraud) у Великій Британії. Ця праця підкреслює, що шахрайство, яке становить понад 40% усіх злочинів у країні, щорічно завдає економіці збитків на суму, що перевищує £200 мільярдів, і спричиняє значний емоційний та психологічний тиск на жертв, що робить його потенційною загрозою національній безпеці через підрив верховенства права та загрозу стабільності фінансового сектору.

[8] https://static.rusi.org/following-the-fraud-the-role-of-money-mules.pdf



Автори зазначають, що Велика Британія тривалий час є привабливим напрямком для шахраїв, а зростання APP-шахрайства, коли жертви обманом змушені переказувати гроші на рахунки, контрольовані злочинцями через "грошових мулів", стало особливо помітним протягом останнього десятиліття. Дослідження базується на детальному аналізі даних транзакцій від Lloyds Bank за період із червня по серпень 2024 року на загальну суму £7,2 млн, а також на огляді матеріалів за 2016–2024 роки та інтерв'ю з вісьмома експертами з правоохоронних органів та індустрії, що дозволяє глибоко дослідити механізми переміщення коштів з рахунків мулів.

Дослідження виявило, що нові учасники платіжної системи, такі як цифрові банки та платіжні компанії, отримують непропорційно велику частку транзакцій від "грошових мулів", зокрема одна фірма забезпечила 20% усіх подальших переказів через систему Faster Payments, що вказує на слабкість у контролі фінансових злочинів у цих установах і підкреслює нагальну потребу в посиленні регуляторних заходів. Основним методом переказу коштів залишаються Faster Payments, які становлять 57% усіх вихідних транзакцій, хоча значна частина коштів (19%) витрачається через дебетові картки, а 10% знімається готівкою в банкоматах або відділеннях банків. Автори підкреслюють, що кошти зазвичай затримуються на рахунках мулів лише від 15 хвилин до години — 28% залишають рахунок протягом 15 хвилин, а 53% — протягом години, що робить відстеження надзвичайно складним і вимагає негайної співпраці між правоохоронцями та приватним сектором для ідентифікації шахрайств у реальному часі. Більшість рахунків (60%) мають вік понад рік, а 20% старші за п'ять років, що дозволяє маскувати шахрайську діяльність під легітимні операції, ускладнюючи виявлення підозрілої активності.

Висновки:

- **Посилення регулювання нових платіжних компаній:** Нові учасники платіжної системи, такі як цифрові банки, отримують непропорційно велику частку транзакцій від "грошових мулів" (20%). Рекомендується впровадити жорсткіші регуляторні заходи для підвищення контролю за фінансовими злочинами в цих установах.
- **Швидка реакція на переміщення коштів:** 28% коштів залишають рахунки мулів протягом 15 хвилин, а 53% — протягом години. Необхідно налагодити тісну співпрацю між правоохоронними органами та банками для реального часу ідентифікації шахрайств і швидкого повернення коштів.
- **Розширення ініціатив обміну даними:** Різноманітні методи переміщення коштів (Faster Payments, дебетові картки, готівка) вимагають залучення всіх учасників платіжної екосистеми, включаючи менші фірми та постачальників криптовалют, до програм обміну даними для запобігання та виявлення шахрайства.
- **Використання старих рахунків:** Близько 60% рахунків мають вік понад рік, що ускладнює виявлення шахрайства. Рекомендується вдосконалити моніторинг довгострокових рахунків для своєчасного виявлення підозрілої активності.

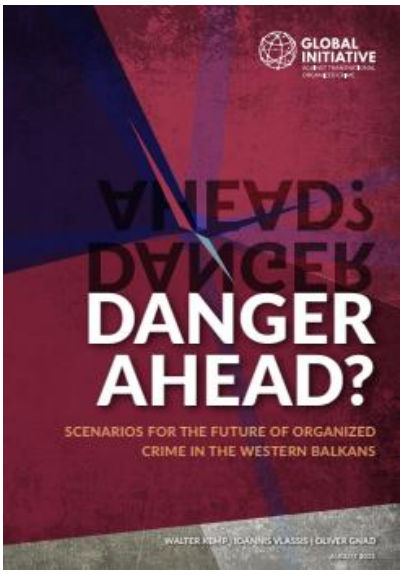
Методологія дослідження включає огляд статистики від UK Finance, Payment Systems Regulator, Office for National Statistics та інших джерел, а також аналіз анонімізованих даних від Lloyds Bank, де враховувалися типи платежів, їх призначення, вік власників рахунків та самих рахунків. Інтерв'ю проводилися з експертами, окрім представників Lloyds Bank, щоб мінімізувати упередженість, хоча автори визнають, що дані від одного банку дають лише часткову картину транзакційних потоків і потребують подальшого дослідження для

узагальнення тенденцій у ширшій платіжній екосистемі. Дослідження також детально описує типовий шлях APP-шахрайства, яке зазвичай починається за межами фінансової системи, зокрема на онлайн-платформах (70% випадків у 2024 році) або через телекомунікаційні послуги (16%), де жертви піддаються соціальній інженерії, щоб переказати гроші на рахунки мулів, які можуть бути як свідомими, так і несвідомими учасниками злочинів. Ці мули рекрутуються через фальшиві оголошення про роботу, примус (наприклад, жертви торгівлі людьми) або експлуатацію (жертви романтичних шахрайств), що підкреслює різноманітність методів залучення.

Основна мета роботи — підтримувати політичний фокус на боротьбі зі шахрайством у Великій Британії та сприяти розробці цільових заходів для максимального впливу на злочинні мережі, включаючи залучення менших платіжних фірм і постачальників криптовалют до ініціатив обміну даними. Автори наголошують на транснаціональному характері шахрайства, де понад 75% випадків пов'язані з іноземними злочинцями, а 47% випадків у 2021 році включали співпрацю між британськими та закордонними учасниками, що робить проблему ще більш складною. Дослідження описує, як злочинні мережі використовують мулові рахунки для швидкого переміщення коштів, часто протягом кількох хвилин, що ускладнює їх повернення жертвам. Зокрема, дані показують, що лише 15% коштів залишаються на рахунках мулів після 24 годин, що підтверджує необхідність негайних дій.

Крім того, робота підкреслює, що більшість рахунків є старими, що дозволяє злочинцям уникати підозр, а використання нових технологій, таких як штучний інтелект, усе більше посилює ефективність атак шахраїв. Автори рекомендують розширити моніторинг довгострокових рахунків, покращити швидкість реагування банківських систем і залучити всі сегменти платіжної екосистеми до спільних зусиль із запобігання шахрайству. Це дослідження є лише початковим етапом, який потребує подальших досліджень для оцінки ширших тенденцій, але вже пропонує практичні рекомендації щодо посилення контролю, швидкої реакції та розширення співпраці для запобігання та виявлення шахрайства, зберігаючи актуальність проблеми в політичному та суспільному дискурсі.

Небезпека попереду: сценарії майбутнього організованої злочинності на Західних Балканах [9]



Документ підготовлений Global Initiative Against Transnational Organized Crime (GI-TOC), є всебічним аналітичним дослідженням, яке спрямоване на прогнозування розвитку організованої злочинності у Західних Балканах протягом наступного десятиліття, до 2035 року. Цей звіт використовує метод стратегічного огляду, щоб надати глибокий аналіз можливих траєкторій розвитку злочинних мереж та ринків у регіоні, який історично характеризується складними геополітичними, економічними та соціальними умовами. Автори прагнуть не лише описати потенційні сценарії, а й підготувати зацікавлені сторони до проактивних дій, спрямованих на зменшення шкоди від організованої злочинності через розуміння майбутніх викликів та можливостей.

У вступній частині документа підкреслюється критична потреба у відході від реактивного підходу до управління сучасними

[9] https://globalinitiative.net/wp-content/uploads/2025/08/Walter-Kemp-Ioannis-Vlassis-and-Oliver-Gnad-Danger-ahead_-Scenarios-for-the-future-of-organized-crime-in-the-Western-Balkans-GI-TOC-August-2025.pdf

загрозами та перехід до стратегічного планування. Автори пояснюють, що злочинці та ринки демонструють високу адаптивність, швидко реагуючи на нові можливості, тоді як правоохоронні органи та політики часто зосереджуються на вирішенні поточних проблем. Щоб подолати цей розрив, стратегічний огляд пропонується як інструмент, який допомагає подолати когнітивні упередження, сприяє колективному мисленню та дозволяє заглянути за горизонт поточних подій.

Майбутнє розглядається як множинне явище, формуючись під впливом мега-трендів, таких як технологічні інновації та геополітична конкуренція, а також випадкових подій та свідомих рішень. Автори наголошують на важливості критичного мислення для оцінки припущень та підготовки до неочікуваних змін, посилаючись на історичні приклади, такі як теракти 11 вересня, фінансова криза, пандемія COVID-19 та війна в Україні, які кардинально змінили глобальний ландшафт.

Методологія дослідження ґрунтується на поділі майбутнього на три горизонти: ближчий (3–5 років), середній (10–20 років) та далекий (20–50 років), з акцентом на середньострокову перспективу до 2035 року. Ближче майбутнє визначається як відносно передбачуване, формуючись на основі попередніх рішень та подій, тоді як середнє майбутнє залежить від взаємодії мега-трендів, ключових драйверів змін та ресурсів, що додає йому вищу ступінь невизначеності. Аналіз базується на PESTEL-рамці (політичні, економічні, соціальні, технологічні, екологічні та правові фактори), яка дозволяє ідентифікувати мега-тренди (наприклад, повороти геополітики, зміна клімату), звичайні тренди (міграція, зростання туризму) та слабкі сигнали (автономний AI, використання дронів). Ця структура допомагає визначити, як ці фактори можуть впливати на організовану злочинність у регіоні, пропонуючи детальний огляд потенційних ризиків та можливостей.

Історичний огляд організованої злочинності у Західних Балканах підкреслює її еволюцію, пов’язану з геополітичними зрушеннями після розпаду Югославії, економічною нестабільністю та зовнішніми впливами. Цей контекст слугує базою для семи сценаріїв, які представляють різні шляхи розвитку: "Criminal States" (кримінальні держави), де злочинність інтегрується в державні структури; "Fortress Europe" (фортеця Європа), що фокусується на впливі міграційних бар’єрів; "Breaking Bad" (злочинний злам), який описує трансформацію злочинних ринків; "Techtonic Shifts" (технологічні зсуви), що досліджує вплив технологій; "Rent-a-mob" (найманий натовп), де розглядається використання організованих груп; "Scarcity Markets" (ринки дефіцитів), пов’язані з експлуатацією ресурсів через кліматичні зміни; та "Crime is

Висновки:

- **Розробка системи раннього попередження:** Урядам та правоохоронним органам Західних Балкан необхідно до кінця 2026 року створити централізовану систему моніторингу слабких сигналів, таких як автономний AI чи дрони, з регулярними звітами кожні три місяці для своєчасного реагування на нові загрози до 2035 року.
- **Посилення міжнародної співпраці:** Країни регіону мають до 2027 року підписати угоди з ЄС та Europol про обмін даними та гармонізацію регулювання криптовалют і боротьби з корупцією, щоб зменшити можливості для відмивання грошей злочинними групами.
- **Інвестиції в адаптацію до кліматичних змін:** Уряди повинні до 2028 року виділити не менше 10% бюджетів на розвиток інфраструктури, стійкої до посух та повеней, щоб запобігти виникненню ринків дефіциту, які можуть бути експлуатовані злочинцями.
- **Освіта та підвищення обізнаності:** Проведення щорічних кампаній з підвищення цифрової грамотності серед 50% населення до 2030 року допоможе зменшити вразливість до кіберзлочинності та маніпуляцій у соціальних мережах.

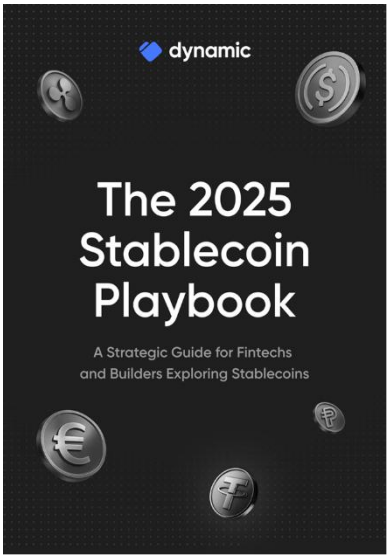
Elsewhere" (злочинність в іншому місці), що передбачає переміщення злочинних операцій за межі регіону. Кожен сценарій супроводжується аналізом ключових гравців — від злочинних груп до урядів та міжнародних організацій — та їхніх стратегій і інтересів.

Документ також детально аналізує драйвери змін, використовуючи PESTEL-аналіз для виділення геополітичних (повороти геополітики, конфлікти), економічних (криптовалюти, іноземні інвестиції), соціальних (ідентичність, нерівність доходів), технологічних (кібербезпека, синтетичні наркотики), екологічних (кліматичні катастрофи) та правових (регулювання криптовалют) трендів.

Слабкі сигнали, такі як автономний AI чи використання дронів, підкреслюють необхідність моніторингу для своєчасного реагування. Аналіз стейкхолдерів допомагає визначити, хто виграє або програє від цих змін, наголошуючи на ролі злочинних мереж, корумпованих чиновників та міжнародних партнерів.

Завершальна частина пропонує практичні рекомендації, включаючи створення системи раннього попередження для відстеження слабких сигналів, посилення міжнародної співпраці з ЄС та організаціями, такими як Europol, для боротьби з корупцією та регулювання криптовалют, а також інвестиції в інфраструктуру, стійку до кліматичних ризиків, та підвищення цифрової грамотності населення. Ці заходи спрямовані на зменшення шкоди від організованої злочинності та стимулювання проактивних стратегій у регіоні та за його межами.

Глобальна роль стейблкоїнів у фінансовій екосистемі 2025 року [10]



Документ є комплексним посібником, який систематизує знання та практичні рекомендації щодо впровадження стейблкоїнів у фінансових продуктах і сервісах. Його основна мета полягає в тому, щоб допомогти фінтех-командам, розробникам і продуктовим менеджерам орієнтуватися у швидкозмінному середовищі, розуміти як технічні, так і регуляторні нюанси роботи зі стейблкоїнами та ефективно інтегрувати їх у різні бізнес-моделі. Автори наголошують, що стейблкоїни перестали бути інструментом вузького криптоспільнотного використання і дедалі більше перетворюються на елемент глобальної фінансової інфраструктури. Якщо раніше вони асоціювалися переважно зі спекуляціями на ринку цифрових активів, то сьогодні стейблкоїни активно застосовуються у виплатах заробітної плати, транскордонних переказах, B2B-платежах, роздрібній торгівлі, заощадженнях, а також у сфері ліквідності та обслуговування нео-банківських платформ. Така еволюція перетворює їх на інструмент, здатний вирішувати проблеми високої вартості транскордонних переказів, низької швидкості здійснення міжнародних платежів та валютної нестабільності, особливо в країнах, що розвиваються.

У документі докладно пояснюється, що фундаментальні параметри вибору стейблкоїнів визначають подальшу долю продукту і його прийняття користувачами, партнерами та регуляторами. Йдеться насамперед про три ключові фактори: хто є емітентом і чи має він належний рівень репутації, прозорості та підзвітності; який обрано дизайн токена, зокрема чи базується його стабільність на фіатних резервах, алгоритмічних моделях або мультиколатеральному забезпеченні; а також на якій блокчейн-мережі випущено токен, що

[10] https://marketing-site-assets.dynamic.xyz/Dynamic_2025_Stablecoin_Playbook.pdf

безпосередньо впливає на вартість і швидкість транзакцій, масштабованість та рівень безпеки. Вдале поєднання цих елементів знижує технічні, юридичні й репутаційні ризики, а помилки у виборі можуть зруйнувати довіру і зробити продукт нежиттєздатним.

Окрема увага у звіті приділяється інфраструктурі, необхідній для впровадження стейблкоїнів у бізнес-моделі. Сюди належать інтеграції з цифровими гаманцями, суб'єктами платіжної інфраструктури, зокрема процесинговими центрами та платіжними шлюзами, інструментами управління ліквідністю, рішеннями для ПВК/KYC та комплаєнсу, а також системами аудиту резервів. Автори підкреслюють, що без надійної та прозорої інфраструктури, яка забезпечує і регуляторні вимоги, і зручність для кінцевого користувача, навіть добре розроблений продукт може втратити конкурентоспроможність. Стабільність та довіра користувачів базуються не тільки на самій монеті, але й на екосистемі, яка дозволяє безпечно, швидко й прозоро користуватися нею у щоденних фінансових операціях.

Важливим блоком документа є аналіз регуляторного середовища. Автори нагадують, що у світі немає єдиного універсального підходу до регулювання стабільних монет, однак спостерігається загальна тенденція до формування чіткіших правил. У Європейському Союзі вже набули чинності норми регламенту MiCA, які встановлюють вимоги до емітентів, резервів і прозорості. У США триває розробка спеціального законодавства для стейблкоїнів, де ключовими залишаються питання ліцензування, банківського нагляду та захисту інвесторів. У країнах, що розвиваються, регулятори акцентують увагу на валютному контролі та захисті споживачів. Це створює нерівномірне середовище, в якому компанії змушені адаптуватися залежно від юрисдикції, але водночас воно стає більш передбачуваним і дозволяє будувати довгострокові бізнес-стратегії.

Фінальна частина посібника присвячена стратегіям для фінтехів і розробників. Автори рекомендують чітко визначати першочергові сегменти використання стейблкоїнів — чи то платежі, чи транскордонні перекази, чи нео-банкінг — і тестувати продукти на конкретних нішевих ринках, де потреба у дешевих і швидких транзакціях є найбільшою. Водночас підкреслюється, що побудова партнерств із банками, платіжними провайдерами та глобальними мережами є критичною для масштабування й виходу на міжнародний рівень. Для досягнення довготривалої життєздатності продуктів компаніям потрібно впроваджувати комплаєнс-практики, ефективні ПВК/KYC-рішення та забезпечувати аудит резервів, оскільки лише поєднання інноваційності та відповідності вимогам регуляторів здатне гарантувати довіру користувачів і відкривати доступ до ширших ринків.

Таким чином, документ формує бачення стабільних монет як нового покоління фінансових інструментів, які поєднують криптографічні технології з реальними економічними потребами, виступають ефективною альтернативою традиційним

Висновки:

- **Стейблкоїни вийшли за межі криптосфери** — вони вже використовуються у зарплатних проєктах, міжнародних розрахунках і споживчих платежах; компаніям варто інтегрувати їх у продукти для ринків, де потрібні дешеві та швидкі транзакції.
- **Три критичні фактори вибору:** емітент, дизайн токена та базовий блокчейн. Від них залежать надійність, регуляторна сумісність і довіра клієнтів.
- **Регуляторне середовище стає ключовим бар'єром і драйвером:** необхідно враховувати вимоги MiCA (ЄС), законодавчі ініціативи США та локальні режими валютного контролю.
- **Успішна стратегія виходу на ринок** передбачає поетапне тестування, побудову партнерств і впровадження комплаєнс-рішень (ПВК/KYC, аудит резервів), що мінімізує ризики та відкриває шлях до масштабування.

банківським платіжним системам і дають фінтех-компаніям можливість створювати гнучкі, масштабовані та глобально релевантні сервіси.

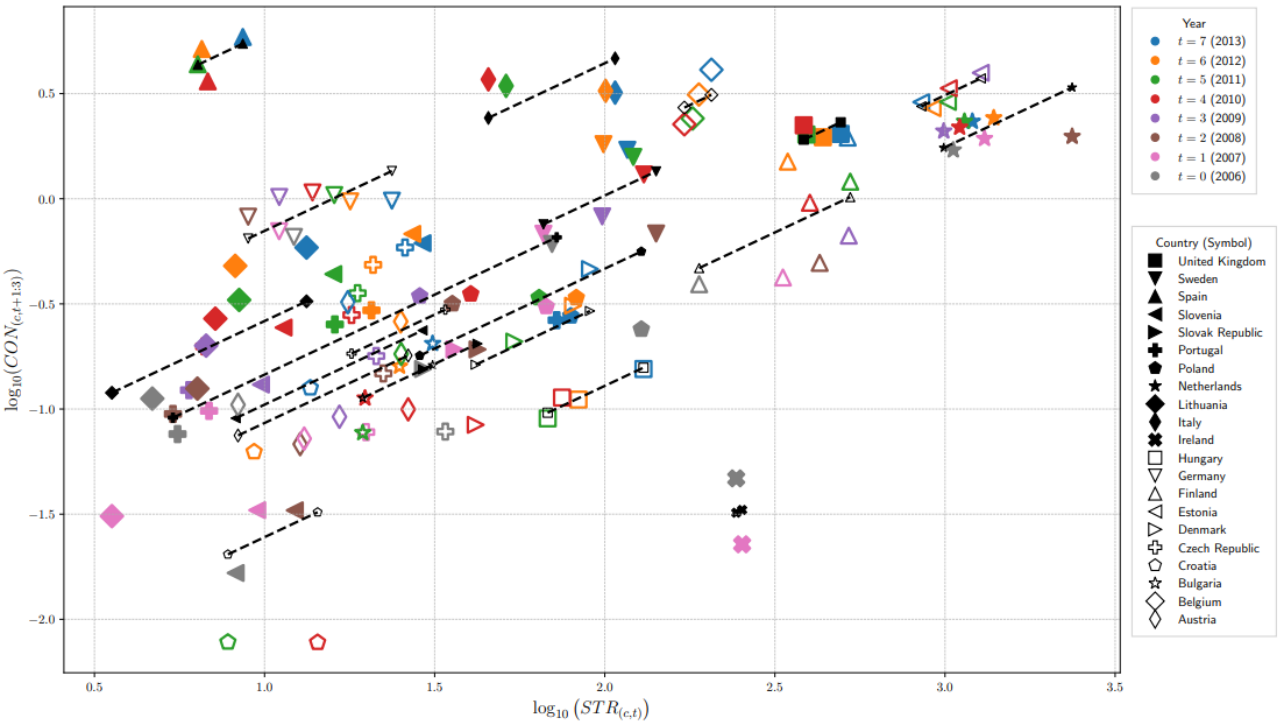
Рекомендовані та навчальні матеріали

Чи призводить збільшення кількості STR до збільшення кількості вироків за відмивання коштів? [11]

Згідно з дослідженням, проведеного Расмусом Інгеманном Туффвесоном Єнсеном, Себастіаном Холмбі Хансеном та Калле Йоганнесом Роузом, було детально проаналізовано взаємозв'язок між обсягом повідомлень про підозрілі транзакції (STR) та результативністю боротьби з відмиванням коштів, вимірюваною кількістю судових вироків. Автори використали дані з різних публічних джерел, включаючи Європол, Світовий банк, Міжнародний валютний фонд та Європейський довідник статистики злочинності, що охоплюють період з 2006 по 2016 рік по країнах Європейського Союзу.

Для аналізу дослідники застосували регресійні моделі, які дозволили оцінити, наскільки зміни в одному показнику (кількість STR) пов'язані зі змінами в іншому (кількість вироків). Важливим етапом було використання логарифмічного перетворення даних, що дозволило лінеаризувати взаємозв'язок і краще виявити залежності. Спочатку було використано звичайний метод найменших квадратів, який показав існування позитивного, але сублінійного взаємозв'язку. Це означає, що хоча зростання кількості STR і супроводжується зростанням кількості вироків, кожен наступний звіт додає все менше до загального результату. Це явище отримало назву «ефект фальшивої тривоги» (crying wolf effect): надмірна кількість звітів, багато з яких можуть бути низької якості, перевантажує фінансові розвідки та правоохоронні органи, чиї ресурси для розслідування є обмеженими. Це призводить до зниження ефективності їх роботи та "розпилення" зусиль на менш значущі випадки.

Ключовим моментом дослідження стало включення до аналізу моделей з фіксованими ефектами. Ці моделі дозволили контролювати неспостережувані, специфічні для кожної країни

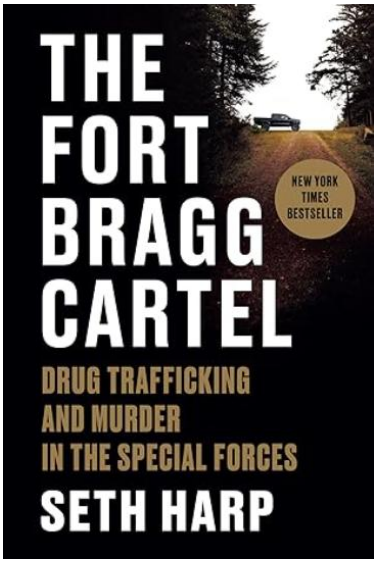


[11] https://arxiv.org/pdf/2508.18932

фактори, такі як відмінності в законодавстві, правовій системі та ефективності роботи органів влади. Найбільш важливим стало врахування часового фактора. Коли до моделі були додані змінні, що відображають загальний часовий тренд, статистична значущість зв'язку між кількістю STR та вироків повністю зникла. Цей висновок свідчить про те, що виявлена кореляція є хибною (spurious correlation), а не причинно-наслідковою. Автори припускають, що обидва показники зростали одночасно під впливом певного прихованого, спільного фактора — ймовірно, посилення політичного, суспільного та регулятивного тиску, який спонукав фінансові інститути до більш активного подання звітів, а правоохоронні органи — до більш інтенсивного розслідування та покарання за відмивання коштів. Таким чином, кількість звітів не є провідною причиною зростання кількості вироків.

Результати дослідження мають важливі наслідки для світової політики боротьби з відмиванням коштів, оскільки ставлять під сумнів усталений підхід, що зосереджується на кількісних показниках. **Автори стверджують, що фокус регуляторів і наглядових органів має зміститися з кількості поданих звітів на те, як ці звіти використовуються фінансовими розвідками та правоохоронними органами. Ключовою метою має стати підвищення якості звітів та ефективності їх обробки, а не просто збільшення їх обсягу.**

Шокуюча історія елітних американських військових, що стали наркобаронами [12]



Книга Сета Гарпа видана Penguin Random House занурює читача у шокуючу історію злочинної змови всередині Спільного командування спеціальних операцій США (JSOC) на базі Форт-Брегг, Північна Кароліна, де елітні військові, такі як оператори Delta Force та SEAL Team Six, організували власний наркокартель. На відміну від попередніх розкриттів, таких як книга Альфреда МакКоя "The Politics of Heroin in Southeast Asia" (1972), яка висвітлювала співпрацю ЦРУ з опіумними мережами у В'єтнамі, чи звіту Керрі (1989) про кокаїнові операції в Нікарагуа, ця книга фокусується на внутрішній злочинності американських військ, що робить її особливо резонансною.

Спочатку книга розкриває історичний контекст створення JSOC у пізних 1970-х роках як альтернативи ЦРУ, коли Конгрес посилив нагляд за розвідкою, дозволяючи Білому дому проводити таємні операції з мінімальним контролем. Під час війни з терором JSOC проводив інтенсивні операції за циклом F3EAD (Find, Fix, Finish, Exploit, Analyze, Disseminate), захоплюючи документи та жорсткі диски після вбивств, що сприяло розвитку передових технологій стеження, подібних до зображених у "1984" Оруелла. Оператори мали доступ до значних ресурсів, таких як готівка для інформаторів та військові стимулятори, як-от декстроамфетамін (Adderall), що, за словами колишнього підрядника IT Джордана Терреллa, створювало ситуацію, де "немає даних, до яких вони не можуть дістатися". Ця відсутність нагляду, як стверджує Гарп, породила культуру безкарності, яка стала ґрунтом для злочинів.

Перша половина книги складається з окремих історій про недисциплінована поведінку ветеранів JSOC, таких як вбивство сержанта 1-го класу Марка Лешікара Вільямом Лавінем у березні 2018 року під час сп'яніння від наркотиків у Дісней Ворлд. Лавінь, який уникнув покарання через військову юстицію, зізнався другу, що вбив дитину на війні, що відобразило глибокі психологічні травми від 14 ротацій. Командир штабу Delta Force скаржився, що проблемних солдатів, включаючи звинувачених у злочинах, переводили на письмову роботу,

[12] https://www.amazon.com/exec/obidos/ASIN/0593655087/reasonmagazinea-20/

що загрожувало дисципліні. Ці випадки підкреслюють, як тривалі бойові дії та доступ до наркотиків, таких як Adderall, сприяли деградації моральних принципів.

Друга половина книги розкриває деталі картелю, очолюваного екс-інтендантом Тімоті Дюмасом і колишнім поліцейським Фредді Вейном Гауфом. Гауф, який розповів про свої злочини з федеральної в'язниці, створив наркобізнес у стилі "Breaking Bad", переправляючи кілограми кокаїну через свій передмістський будинок під виглядом торгівлі вживаними побутовими приладами. Його мережа включала місцевих мафіозі, пуерто-риканських контрабандистів, мексиканський картель Los Zetas (заснований дезертирами спецпризначенців, навчених у Форт-Брегу) та навіть колишнього бійця "Ісламської держави", якого представив Дюмасу один із працівників Гауфа. Дюмас, який намагався викрити ширшу мережу контрабанди опіатів з Афганістану, передав Гауфу USB-накопичувач із компроматом, який той назвав "страховкою" та "серйозно інкримінуючим матеріалом". У грудні 2020 року Дюмас і Лавінь були вбиті в лісі поблизу Форт-Брегга, а поліція заарештувала місцевого злочинця, хоча свідки сумніваються в його винуватості, натякаючи на змову.

Інші резонансні справи включають зникнення солдата Енріке Романа-Мартінеса у травні 2020 року під час кемпінгу, чия голова з'явилася на пляжі через кілька днів Це вбивство досі не розкрите. З 2020 по 2023 рік 12 солдатів Форт-Брегга були вбиті або звинувачені у вбивствах, що призвело до прізвиська Фейєтвілля як "Фаталвілля". Гауф, який як поліцейський використовував процедуру цивільної конфіскації для вилучення готівки, був звільнений, що спонукало його до злочинів. Лавінь і Гауф уникали покарань завдяки "хлоп'ячій культурі" Північної Кароліни, де ветерани в уніформі часто уникали суду. Судові документи натякають, що Гауф мав компромат на правоохоронців, включаючи матеріали сексуального характеру.

Після вбивства Дюмаса та Лавінема, ФБР і Департамент внутрішньої безпеки розслідували мережу Гауфа, але USB-накопичувач, конфіскований поліцією Вінстон-Сейлема, виявився порожнім, що підозріло. Гарп стверджує, що безкарність JSOC, викликана його статусом "воїнської касти", є коренем проблеми, і пов'язує ці явища з "поверненням війни додому". Він закликає до переосмислення підходу до нагляду за елітними військами, наголошуючи, що поки Америка тримає JSOC вище закону, деякі воїни зловживатимуть привілеями.

Інші новини

Чи є «екстремальна перевірка» наступним підходом до захисту від санкцій? [13]

Стаття авторства Ніка Гендерсона-Mayo, опублікована в журналі Corporate Compliance Insights, пропонує детальний аналіз сучасних викликів у сфері комплаєнсу в умовах швидких геополітичних змін.

Автор, директор з навчання та контенту компанії VinciWorks, стверджує, що традиційна розширена перевірка (Enhanced Due Diligence, EDD), розроблена за рекомендаціями Financial Action Task Force (FATF), більше не відповідає реаліям, де санкційні режими змінюються щомиті. Наприклад, Захід послаблює санкції проти Сирії, тоді як Росія та Іран створили складні механізми ухилення, включаючи тіньові економіки поза SWIFT, а арт-ринок і люксові товари стають каналами для відмивання грошей, зокрема для сирійських воєначальників та фінансів Хезболли. Сирія ілюструє швидке зняття десятирічних санкцій, попри

[13] https://www.corporatecomplianceinsights.com/is-extreme-due-diligence-next-sanctions-defense/

присутність режиму, пов’язаного з хімічною зброєю та тероризмом, що відкриває двері для турецьких забудовників, за якими можуть ховатися санкційні діячі.

Автор наголошує на ролі криптовалют, таких як Tether, які дозволяють переказувати кошти за секунди, уникаючи традиційного контролю, тоді як нові міксери, як-от Tornado Cash, ускладнюють відстеження. У відповідь на це пропонується концепція "екстремальної перевірки" (Extreme Due Diligence, EXDD) — проактивний підхід, який виходить за межі юридичних вимог EDD. EXDD передбачає не просто перевірку одного рівня власників, а повне картування ланцюжка власності, детальний аналіз джерел фінансування, субпідрядників та їхніх бенефіціарів, із припущенням найгіршого сценарію, доки не буде доведено зворотне. Це вимагає інвестування в аналітику блокчейнів, відстеження гаманців і співпраці з місцевими партнерами для побудови динамічних профілів ризиків.

Стаття також звертає увагу на Дубай, який став притулком для капіталів російських олігархів та іранських посередників, які інвестують у нерухомість і люксові активи. Росія використовує двосторонні угоди та цифровий рубль, а Іран — мережу підставних фірм у Дубаї, Гонконгу та Туреччині, утворюючи систему, яку важко відстежити.

Криптовалюти додають анонімності, з 40% незаконних транзакцій, пов’язаних із санкційними юрисдикціями. EXDD пропонується як єдиний спосіб протистояти таким загрозам, замінюючи статичні списки санкцій активним аналізом. Автор підкреслює, що провали в комплаєнсі вже не є лише юридичним ризиком, а стають екзистенційною загрозою, особливо в умовах, коли компанії змушені працювати в Сирії поряд із санкційними гравцями, такими як Росія та Іран, чиї екосистеми ухилення випереджають регуляції.

Таємна система виплат ХАМАС: як організація підтримує зарплати та лояльність [14]

Новинна стаття від BBC детально розкриває, як рух ХАМАС, попри значне послаблення своєї військової спроможності та тиск на політичне керівництво після майже двох років відкритої війни, продовжує виплачувати зарплати державним службовцям у секторі Газа.

Стаття описує секретну касову систему, за якою 30 000 цивільних службовців отримують зарплати на загальну суму 7 мільйонів доларів (£5,3 млн). Кожен із них отримує приблизно 300 доларів щотижня, що становить лише 20% від їхньої «довоєнної» зарплати. Ця недостатня сума викликає невдоволення серед прихильників ХАМАС через високий рівень інфляції, коли, наприклад, кілограм борошна коштує до 80 доларів через дефіцит продуктів, спричинений, за словами гуманітарних агентств, ізраїльськими обмеженнями.

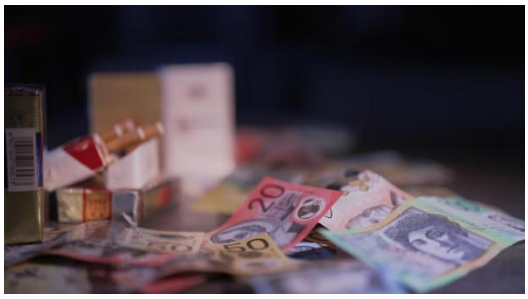
Процес отримання зарплати є складним і небезпечним через відсутність функціональної банківської системи в Газі. Службовці, від поліцейських до податкових чиновників, отримують зашифровані повідомлення з інструкціями відвідати певне місце для "зустрічі з другом за чаєм", де їм передають гроші в закритих конвертах. Ці операції регулярно зазнають атак ізраїльських сил, які намагаються зірвати фінансову діяльність ХАМАС. Наприклад, один із працівників Міністерства релігійних справ ХАМАС розповів про ризик бути вбитим під час таких виплат, а вчителю Алаа, який утримує сім’ю з шести осіб, видали пошкоджені банкноти, з яких лише частина була придатною до використання.

[14] https://www.bbc.com/news/articles/c1kz42j92jmo

Фінансування ХАМАС базується на попередніх накопиченнях — близько 700 мільйонів доларів готівкою та сотні мільйонів шекелів, захованих у тунелях під керівництвом Яхії Сіварра та його брата Мохаммеда, які загинули від рук ізраїльських сил. Крім того, ХАМАС використовує податки на торгівлю, продаж цигарок за цінами в 100 разів вищими за довоєнні (до 170 доларів за пачку), а також підтримку з Катару, Ірану та 10% бюджету забороненого Єгипетського мусульманського братства. Незважаючи на знищення фінансової інфраструктури, включаючи вбивство Ісмаїла Бархума, глави фінансів ХАМАС, у березні 2025 року, організація продовжує виплачувати кошти.

Стаття також наголошує на соціальному напруженні: ХАМАС розподіляє продуктові набори лише серед своїх прихильників через ротаційні комітети, що викликає обурення серед населення, яке страждає від голоду. Мешканці, як-от вдова Нісрін Халед, звинувачують ХАМАС у нерівному розподілі допомоги та провалі забезпечення базових потреб перед атакою 7 жовтня 2023 року, що призвела до війни. Ізраїль звинувачує ХАМАС у крадіжці гуманітарної допомоги під час перемир'я, що організація заперечує, хоча джерела BBC підтверджують ці факти.

Приватні банкомати як тіньовий канал відмивання коштів: австралійські розслідування нелегальної тютюнової торгівлі та прогалини нагляду у сфері ПФК[15] [16]



Дві серії журналістських розслідувань ABC Australia у червні та серпні 2025 року висвітлили одну із найменш контрольованих, але критично небезпечних сфер фінансової інфраструктури — використання приватних банкоматів у магазинах, пов'язаних із нелегальною торгівлею тютюновими виробами. Першим об'єктом розслідування стала компанія Next Payments, майже наполовину контрольована фінансовим гігантом Macquarie Group, яка встановлювала власні банкомати у торгових точках, де вже фіксувалися випадки продажу контрабандних сигарет і нелегального тютюну. Журналісти виявили, що низка цих банкоматів працювала у магазинах, власники яких мали судимості або прямі зв'язки зі справами про нелегальну торгівлю та відмивання коштів. Особливо тривожним виявився механізм так званих self-filled ATMs — банкоматів, які завантажуються готівкою самими власниками, а не банками чи сертифікованими інкасаторами. Це створює надзвичайно зручний канал для «очищення» готівкових доходів від незаконної торгівлі, адже походження грошей залишається непрозорим і практично не піддається фінансовому моніторингу. Ситуація загострюється тим, що в Австралії приватні банкомати взагалі не підпадають під регулювання у сфері ПВК/ФТ, тоді як у багатьох юрисдикціях такі схеми давно закриті шляхом запровадження вимог у сфері ПВК до операторів банкоматів. Під тиском фактів і суспільного резонансу Next Payments була змушена видалити понад сорок банкоматів зі «сумнівних» точок продажу, а компанія EFTEX відмовилася від обслуговування таких транзакцій, фактично заблокувавши можливість їх подальшої експлуатації у звичних схемах.

Через кілька місяців аналогічна історія повторилася з NCR Atleos, одним із найбільших світових постачальників банкоматів, який оперує брендом Cashzone. Журналістське розслідування з'ясувало, що десятки їхніх банкомтів стояли у тютюнових магазинах Брісбена, Дарвіна та

[15] https://www.abc.net.au/news/2025-08-21/ncr-atleos-removing-machines-suspected-illegal-tobacco-stores/105680294

[16] https://www.abc.net.au/news/2025-06-18/macquarie-group-next-atm-illegal-tobacco-trade/105399234

Сіднея, також пов'язаних із нелегальним продажем тютюну й вейпів. І тут було зафіксовано схожу модель використання: власники магазинів самостійно завантажували в банкомати готівку, що унеможливлювало прозору трасуваність походження коштів та створювало ідеальне середовище для відмивання. Деякі з торгових точок уже були відомі правоохоронцям і мали фігурантів із судимостями, але це не завадило встановленню та використанню банкоматів. Після викриття компанія NCR Atleos оголосила про видалення понад п'ятдесяти пристроїв, підкреслюючи, що це лише один відсоток їхньої мережі, але водночас визнавши необхідність перегляду політики розміщення та перевірки партнерів. Експерти у сфері фінансової безпеки, зокрема з Macquarie University Financial Integrity Hub, наголосили, що ситуація засвідчила наявність системної прогалини у регулюванні, яка відкриває шлях до масштабного використання банкоматів для відмивання доходів від злочинної діяльності.

Поєднання цих двох розслідувань показало загальнонаціональну проблему: приватні банкомати в Австралії стали своєрідним «сліпим кутом» для органів фінансового моніторингу, де відсутність нагляду у сфері ПВК збігається з високою концентрацією нелегальних грошових потоків у сфері торгівлі тютюновими виробами. Сам факт, що одразу дві великі компанії — одна локальна із підтримкою великого банку, інша транснаціональна — опинилися в центрі скандалу, свідчить про масштабність і системність ризиків. Видалення десятків банкоматів є лише реактивним заходом, тоді як експерти вимагають структурних змін: від запровадження обов'язкової реєстрації операторів банкоматів і звітності про завантаження готівки до встановлення прямих обов'язків у сфері ПВК і належної взаємодії з фінансовою розвідкою та правоохоронними органами. Ці події не лише висвітлили вразливість австралійської фінансової системи, а й стали яскравим прикладом того, як відсутність регуляторного контролю у ніші, що здається другорядною, може бути використана для масштабного обігу «брудних грошей» і посилення організованої злочинності.

Для загального розвитку

Tornado Cash: Де приватність і санкції зіштовхуються [17]

Стаття, написана національним експертом з безпеки Вільямом Джонсом, пропонує глибоке занурення у складні взаємодії між технологіями, фінансовою приватністю та санкційними заходами через аналіз протоколу Tornado Cash.

Цей протокол, розроблений як інструмент для змішування криптовалютних транзакцій, дозволяє користувачам депонувати криптовалюту на фіксовані адреси та виводити її з інших адрес, ефективно маскуючи джерело коштів і забезпечуючи підвищений рівень анонімності. На піку своєї популярності, що припав на 2022 рік, Tornado Cash демонстрував щомісячні надходження в розмірі $400–550 мільйонів, із значною частиною — 30–40% — пов'язаною з незаконною діяльністю, зокрема масштабними кібератаками, такими як злом Ronin Bridge. Ця статистика підкреслює як потенціал протоколу для захисту приватності, так і його вразливість до зловживань з боку кримінальних елементів.

Юридичний контекст, висвітлений у статті, розкриває драматичні правові наслідки використання Tornado Cash. У серпні 2022 року Міністерство фінансів США через Офіс контролю за іноземними активами (OFAC) ввело санкції проти протоколу, звинувативши його в відмиванні понад $7 мільярдів, включно з активами, викраденими Північною Кореєю через групу Lazarus. Ці дії призвели до арешту співзасновників Алексія Перцева та Романа Шторма. Перцев був засуджений до 64 місяців ув'язнення (апеляція в процесі), тоді як Шторм, якого судили в Окружному суді Південного округу Нью-Йорка, був визнаний винним у змові з метою ведення

[17] https://www.btcpolicy.org/articles/tornado-cash-where-code-privacy-and-sanctions-collide

бізнесу з передачі грошей без ліцензії. Проте присяжні не дійшли згоди щодо звинувачень у відмиванні грошей та порушенні санкцій, що відображає складність правового трактування децентралізованих технологій. Захист Шторма наполягав, що публікація відкритої кодової бази є захищеним актом свободи слова відповідно до Першої поправки до Конституції США, а суддя у справі заборонив згадувати санкції, що суттєво послабило позицію обвинувачення щодо національної безпеки. У березні 2025 року нова адміністрація скасувала ці санкції, що стало поворотним моментом і викликало нові дебати про доцільність регулювання децентралізованого програмного забезпечення як форми вираження.

Аналіз даних у документі детально досліджує вплив санкцій на діяльність Tornado Cash. Після їх введення в серпні 2022 року обсяги транзакцій різко впали на 85%, а потоки незаконних коштів зменшилися на 75%. Однак пропорція незаконної діяльності зросла через ще значніший спад легітимного використання, що вказує на обмежену ефективність санкцій у децентралізованих екосистемах. Скасування санкцій у 2025 році призвело до швидкого повернення легальних користувачів, різкого зростання вартості рідного токена TORN майже вдвічі протягом кількох днів і пожвавлення підтримки засновників через пожертви. Ці ринкові реакції, за словами автора, відображають не лише спекулятивний інтерес, але й ширшу впевненість індустрії в легітимності та попиті на приватність, яку пропонує протокол, особливо після зняття юридичної невизначеності. Джонс зазначає, що це підкріплює аргументи захисників, які, посилаючись на патову ситуацію з присяжними у справі Шторма, стверджують, що протоколи приватності самі по собі не є злочинними.

Стаття також присвячує значну увагу законним аспектам використання протоколів приватності, таких як Tornado Cash. Серед прикладів — захист особистих фінансів (наприклад, журналісти, які отримують гонорари анонімно, щоб уникнути публічного розкриття своєї фінансової історії), анонімне благодійництво (підтримка чутливих або спірних ініціатив, таких як цивільні свободи в авторитарних режимах, без ризику переслідування), комерційна конфіденційність (захист транзакцій бізнесу, наприклад, DAO, від конкурентів або маніпуляцій на ринках DeFi) та приватне голосування в децентралізованих організаціях (забезпечення анонімності для уникнення тиску під час суперечливих рішень). Окрему увагу приділено використанню в авторитарних режимах, де приватність дозволяє активістам, наприклад, представникам дисидентських спільнот, отримувати фінансову підтримку без загрози розкриття. Ці приклади підкреслюють універсальність і соціальну значущість таких інструментів.

Висновки:

- **Оцінка ефективності санкцій:** Санкції проти Tornado Cash значно зменшили обсяги транзакцій (на 85%) і незаконні потоки (на 75%), однак пропорція незаконної діяльності зросла через більший спад легітимного використання. Рекомендується переглянути підходи до регулювання децентралізованих екосистем, враховуючи їхню стійкість до традиційних санкцій.
- **Повернення легальних користувачів:** Після скасування санкцій у березні 2025 року легальні користувачі повернулися, а токен TORN зріс у ціні вдвічі, що вказує на попит на приватність.
- **Законні випадки використання:** Приватність через Tornado Cash підтримує фінансову конфіденційність, благодійництво, комерційні інтереси та захист у авторитарних режимах. Слід просувати політики, які балансують приватність із можливостями цільового контролю за незаконною діяльністю.
- **Лідерство США у криптоінноваціях:** Інтеграція криптовалют, таких як Bitcoin і стейблкоїни, може зміцнити роль долара та експортувати демократичні цінності. Рекомендується інвестувати в розробку криптоінфраструктури, що відповідає принципам свободи та безпеки.

У заключній рефлексії автор наголошує, що принцип приватності, яка не має бути підозрілою, глибоко резонує з американськими цінностями індивідуальної свободи, конституційних гарантій і свободи вираження. США, за його словами, мають багаторічну історію захисту цих принципів як всередині країни, так і на міжнародній арені, і підтримка фінансових інструментів приватності може зміцнити цю ідентичність у цифрову епоху.

Джонс пропонує стратегічне бачення, де приватність у криптовалютній інфраструктурі стає шансом для економічного лідерства США. Він пропонує інтегрувати технології, такі як Bitcoin як децентралізований резерв, стейблкоїни як програмоване розширення долара та інші цифрові активи, такі як Ethereum, як основу для глобальної торгівлі. Ці інструменти, за його думкою, можуть експортувати демократичні ідеали свободи, стійкості та інновацій, демонструючи, що фінансова інновація та громадянські свободи можуть співіснувати. Такий підхід, на його думку, дозволить США не лише зберегти вплив долара, але й очолити світову цифрову економіку, показуючи приклад балансу між контролем і свободою.

Майбутнє комплаєнсу: як технології і культура ПВК/ФТ змінюють боротьбу з фінансовими злочинами [18]

Документ присвячений системному аналізу ролі культури дотримання вимог у сфері протидії відмиванню коштів і фінансуванню тероризму та розповсюдження зброї масового знищення. Автори підкреслюють, що сама по собі наявність законів чи регулятивних актів ще не гарантує їх ефективного виконання, оскільки правові норми без внутрішнього прийняття і вбудування в щоденну діяльність організацій залишаються лише формальними приписами. Тому створення культури ПВК/ФТ постає як стратегічний інструмент, який поєднує формальні зобов'язання із реальною поведінкою керівництва, співробітників та всієї бізнес-структури.

На початку документа роз'яснюється сутність поняття культури комплаєнсу у сфері ПВК/ФТ, яка визначається як сукупність спільних цінностей, вірувань і стандартів етичної поведінки, що формують відповідальне ставлення організації до своїх обов'язків у межах національного та міжнародного режиму протидії відмиванню коштів і фінансуванню тероризму. Така культура пронизує всі рівні управління, починаючи від ради директорів і топменеджменту та закінчуючи рядовими працівниками, і стає невід'ємною частиною ідентичності компанії. Вона відображається у рішеннях, процедурах, продуктах, послугах і навіть у взаєминах із клієнтами та партнерами.

Подальший виклад присвячено ключовим компонентам, без яких неможливо побудувати ефективну культуру комплаєнсу. Насамперед це лідерство і беззастережна підтримка з боку керівництва, яке має задавати тон своїми діями, схвалювати та контролювати процес проведення комплексної оцінки ризиків (EWRA), затверджувати політики та процедури, визначати схильність до ризиків компанії, ініціювати незалежні аудити й реагувати на появу нових типологій і червоних прапорців. Другою складовою є етичні стандарти, що включають прозорість, доброчесність, підзвітність і довіру, оскільки без них навіть найкращі інструкції перетворюються на формальні документи без реального впливу. Важливими є також розробка чітких і зрозумілих політик та процедур, що визначають ролі й відповідальність кожного учасника процесу, а також систематичне навчання персоналу. Автори наголошують, що лише

[18] https://amluae.com/wp-content/uploads/2025/08/AML-CFT-Compliance-Culture-eBook-N.pdf

через обізнаність і підготовку співробітники здатні вчасно розпізнати ризики, прийняти правильні рішення й діяти відповідно до духу закону, а не лише до його букви.

Розділ про значення культури комплаєнсу показує, що вона має мультиплікативний ефект. По-перше, вона сприяє утвердженню доброчесності в організації та робить дотримання вимог природним елементом внутрішнього середовища. По-друге, формує довіру клієнтів, партнерів і регуляторів, зміцнює бренд та імідж. По-третє, допомагає своєчасно адаптуватися до змінних регуляторних вимог, оскільки самі закони у сфері ПВК/ФТ постійно оновлюються відповідно до нових загроз і схем злочинців. У підсумку компанія, яка впроваджує таку культуру, не лише виконує юридичні приписи, а й отримує конкурентну перевагу на ринку.

Окремий блок документа розкриває роль культури у протидії відмиванню коштів і фінансуванню тероризму через превентивні та детективні заходи. До превентивних належать чіткі внутрішні політики, функціонування інституту офіцера з питань ПВК/ФТ, застосування ризик-орієнтованого підходу, проведення належної перевірки клієнтів (CDD/KYC), скринінг на санкції та негативні медіа, постійний моніторинг транзакцій, а також обов'язкове звітування про підозрілі операції. Детективний блок акцентує на використанні сучасних технологій і аналітики даних для виявлення аномалій у поведінці клієнтів і транзакціях, проведенні аудитів і перевірки стану системи для виявлення прогалин, а також на активній ролі співробітників як першої лінії захисту. Пильність персоналу, правильна організація каналів повідомлень і співпраця з регулятором дозволяють вчасно реагувати на загрози й запобігати реалізації злочинних схем.

Далі автори розглядають методологію побудови сильної культури комплаєнсу, протиставляючи її слабкій. Сильна культура базується на проактивності, достатньому фінансуванні, стратегічному баченні комплаєнсу як інвестиції, чітких процедурах, регулярних перевірках і ефективній комунікації між усіма рівнями організації. Слабка ж культура характеризується формальним підходом, відсутністю ресурсів, реактивністю, неактуальними процедурами та непрозорими каналами комунікації, що зрештою робить систему вразливою для обходу вимог.

Важливе місце у тексті відведено викликам, із якими стикаються організації. Серед них суперечність між прагненням до швидкого зростання прибутку та дотриманням етичних норм, опір працівників, які не завжди усвідомлюють свій внесок у боротьбу з відмиванням коштів, висока вартість упровадження сучасних технологій і навчання, а також складність у постійному відстеженні динамічних регуляторних вимог. Автори переконують, що саме лідерство й правильне донесення цінностей комплаєнсу до колективу здатні трансформувати виклики на можливості, а витрати — на інвестиції, що приносять дивіденди у вигляді репутації, довіри та уникнення штрафів.

Заключні розділи спрямовані у майбутнє і показують, як технології, такі як штучний інтелект, машинне навчання та великі дані, здатні радикально змінити культуру комплаєнсу, зробивши її більш швидкою, точною та економічною. Вони автоматизують перевірку клієнтів, санкційний скринінг, аналіз поведінкових моделей, а також сприяють створенню більш прозорої і контрольованої системи. Водночас зазначається, що розвиток міжнародної співпраці та посилення глобальних регуляторних стандартів вимагають від організацій ще більшої гнучкості та здатності до адаптації. Підтримання сильної культури можливе лише через постійне вдосконалення, регулярні перевірки, навчання персоналу та відданість лідерів.

Фінальний акцент робиться на переході від формального «обов'язку» до інтегрованої «ідентичності», коли принципи ПВК/ФТ стають органічною частиною бізнес-моделі, формуючи не лише юридичну, але й етичну основу діяльності. Автори підсумовують, що культура комплаєнсу повинна стати щитом і мечем одночасно — інструментом захисту бізнесу та зброєю у боротьбі зі злочинними практиками, які загрожують фінансовій стабільності та безпеці суспільства.

Ваша думка важлива!

1. Документ висвітлює зростання використання приватних банкоматів та грошових мулів як інструментів для відмивання готівки, отриманої від незаконної торгівлі. Які інноваційні технологічні рішення або методи, крім традиційного моніторингу транзакцій, можуть допомогти фінансовим установам ефективно виявляти та протидіяти таким схемам у режимі реального часу?
2. Звіт про ставлення громадян до корупції вказує на низьку довіру до державних інституцій та ефективності антикорупційних заходів. Як, на вашу думку, можна використати інструменти ПВК/ФТ, щоб підвищити суспільну довіру та зробити боротьбу з корупцією ефективною?
3. Як український уряд може адаптувати міжнародний досвід регулювання приватності у сфері віртуальних активів, враховуючи потреби з ПВК та одночасну підтримку фінансової свободи громадян у цифровій економіці?
4. Яким чином технологічні інновації, такі як використання дронів, можуть стати основними інструментами організованої злочинності в Україні?
5. Які ризики для фінансової стабільності можуть виникнути у разі масового переходу населення та бізнесу на використання CBDC, і які саме інструменти – законодавчі, технологічні чи регуляторні – можуть бути ефективними для їх мінімізації в українських реаліях?
6. Як збалансувати потребу в інноваціях і розвитку штучного інтелекту у фінансовому секторі з необхідністю суворого дотримання норм захисту персональних даних і запобігання дискримінаційним результатам рішень?
7. Як балансувати між економічним зростанням, потребою у швидкому розвитку фінансових технологій та необхідністю підтримувати високу культуру ПВК/ФТ в Україні, щоб уникнути ризику використання фінансової системи для ВК/ФТ?

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-2025-35

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].