Методологічний бюлетень

Серійний номер: МінФін-AML-2026-30

Липень 2026

“Прогрес неможливий без змін, а ті, хто не може змінити мислення, не здатні змінити нічого!”

Бернард Шоу

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

Децентралізовані фінанси під прицілом FATF [1]

Децентралізовані фінанси (DeFi) стрімко еволюціонували від нішевої технологічної екосистеми до значущого сегменту глобального фінансового ландшафту.

Згідно зі звітом FATF, за 2026 рік загальна заблокована вартість активів у протоколах DeFi досягла 86,6 мільярдів доларів США, що демонструє приріст приблизно на 85% порівняно з 2023 роком. Хоча цей показник залишається відносно невеликим у порівнянні із загальною капіталізацією ринку віртуальних активів, динаміка зростання та збільшення участі інституційних інвесторів, постачальників послуг віртуальних активів та інших регульованих суб'єктів суттєво підвищують актуальність DeFi у контексті глобальних фінансових ризиків. Особливу занепокоєність викликає той факт, що цей сектор все частіше використовується для відмивання коштів, фінансування тероризму та розповсюдження зброї масового знищення, що вимагає негайного переосмислення регуляторних підходів.

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/targeted-report-decentralised-finance-2026.pdf.coredownload.pdf

DeFi представляє собою сукупність фінансових послуг, що реалізуються через самовиконувані смарт-контракти на блокчейн-платформах без традиційних фінансових посередників. Користувачі можуть зберігати кошти у своїх гаманцях та безпосередньо взаємодіяти з протоколами, які програмно забезпечують виконання складних фінансових операцій, включаючи торгівлю, обмін, кредитування, запозичення та управління активами. Ключовою особливістю є автоматизація на основі смарт-контрактів, що дозволяє здійснювати миттєві транскордонні операції без участі традиційних фінансових інституцій. Усі транзакції записуються публічно на блокчейні, хоча зазвичай на псевдонімній основі, що створює ілюзію прозорості при одночасному ускладненні ідентифікації реальних учасників.

Екосистема DeFi вирізняється низкою унікальних характеристик, які водночас створюють як інноваційні можливості, так і суттєві вразливості. Відкритий код більшості протоколів дозволяє будь-кому перевіряти, повторно використовувати та відтворювати базовий код, що прискорює створення подібних рішень, але також полегшує зловмисникам пошук вразливостей. Композиційна архітектура, де різні протоколи можуть безперешкодно взаємодіяти один з одним, створює ефективний механізм для легальних користувачів, проте зловмисники використовують цю ж функцію для переміщення коштів на безпрецедентній швидкості через численні DeFi-рівні, нерегульовані офшорні VASP та позабіржових брокерів. Алгоритмічні ринкові механізми, такі як автоматичні маркет-мейкери, пули ліквідності та кредитні протоколи з алгоритмічним регулюванням відсоткових ставок, функціонують без втручання регульованих посередників, що ускладнює моніторинг традиційними інструментами комплаєнсу.

Особливу загрозу становить функція участі, яка дозволяє будь-кому з блокчейн-гаманцем отримувати доступ до фінансових послуг без належної перевірки клієнта. Це відкритий, необмежений доступ створює суттєві ризики відмивання коштів, оскільки злочинці можуть псевдонімно входити в екосистему та використовувати її складність для приховування незаконних потоків. Крім того, залежність від оракулів - сторонніх джерел даних, які надають смарт-контрактам зовнішню інформацію про ціни активів та відсоткові ставки - створює додаткові вразливості, оскільки слабкі місця в дизайні або управлінні оракулами можуть бути використані для маніпуляцій та шахрайських дій.

Принципово важливо розуміти, що стандарти FATF є технологічно нейтральними та застосовуються до будь-якої фізичної або юридичної особи, яка надає фінансові послуги. Ключовий документ - оновлені рекомендації 2021 року - чітко визначає, що DeFi-структури підпадають під дію Рекомендації 15 у випадках, коли фізична або юридична особа здійснює контроль або достатній вплив над структурою. Однак на практиці більшість юрисдикцій у Глобальній мережі FATF стикаються зі значними труднощами в ідентифікації та регулюванні DeFi-структур, що діють на їхній території. Ці складнощі зумовлені транскордонним характером DeFi, відсутністю чітких юрисдикційних якорів, обмеженою технічною експертизою наглядових органів та проблемами розмежування між децентралізованою технологією та потенційно централізованим управлінням.

Згідно з даними звіту, переважна більшість юрисдикцій (132 з 142) не ідентифікували жодної структури, що діє на їхній території, лише чотири країни впровадили вимоги ліцензування та реєстрації, і лише дві фактично застосували ці вимоги. Особливо показовим є те, що лише 26 з 142 юрисдикцій провели оцінку ризиків, пов'язаних з DeFi. Це свідчить про системну проблему у застосуванні Рекомендації 15 до DeFi-структур, що включає недостатнє розуміння складних структур управління, труднощі з ідентифікацією осіб, які здійснюють контроль, та проблеми застосування регуляторних або примусових заходів до структур, що підпадають під дію стандартів, але не виконують відповідних вимог.

Звіт пропонує принципово важливе розмежування трьох категорій DeFi-структур на основі їхніх систем управління та контролю.

Перша категорія - централізовані структури, які мають ідентифікованих контролерів або осіб, що здійснюють достатній вплив, таких як адміністратори, власники токенів управління,

розробники або інвестори. Важливо підкреслити, що структури, які в маркетингових цілях позиціонують себе як повністю децентралізовані, можуть на практиці залишатися централізованими, і саме вони підпадають під дію стандартів FATF і повинні регулюватися.

Друга категорія - централізовані структури, де контролери не можуть бути легко ідентифіковані через псевдонімність або інші фактори. Такі структури також підпадають під дію стандартів FATF, хоча наглядові органи можуть стикатися з практичними труднощами в застосуванні регуляторних заходів. У випадках, коли регулювання не може бути ефективно застосоване, такі структури слід розглядати як нерегульовані і застосовувати до них ті ж заходи пом'якшення, що й до повністю децентралізованих структур.

Третя категорія - повністю децентралізовані структури, де жодна особа не підтримує контроль або не здійснює достатнього впливу. Такі структури випадають зі сфери дії стандартів FATF і зазвичай не регулюються, хоча вони все одно створюють значні ризики, які потребують альтернативних заходів пом'якшення на основі ризиків. Ключовий висновок полягає в тому, що стандарти FATF застосовуються до перших двох категорій, причому вирішальне значення має функціональний підхід, який зосереджується на діяльності, що здійснюється, а не на тому, як структура себе позиціонує.

Найбільш складною проблемою є визначення "контролю або достатнього впливу" в DeFi-структурах. Звіт пропонує вичерпний перелік індикаторів, розділених на ончейн- та офчейн-показники, які можуть допомогти юрисдикціям у цьому процесі.

До ончейн-індикаторів належать: наявність оновлюваних контрактів, проксі-патернів або функцій аварійного вимкнення, особливо якщо такі повноваження зберігаються за конкретною особою або групою; право на одностороннє встановлення або зміну ключових параметрів протоколу, включаючи ліміти ризику, комісії, винагороди та коефіцієнти забезпечення; можливість вибору, налаштування або зміни джерел даних оракулів; виключний або домінуючий контроль над ключами розгортання та критичними залежностями контрактів; потоки комісій та прибутків на конкретні адреси; концентрація токенів управління та голосуючої влади, що дозволяє невеликій кількості учасників визначати результати управління.

Офчейн-індикатори включають: призначення підписантів для управлінських або адміністративних рішень; контроль над публічними веб-інтерфейсами та мобільними додатками; наявність корпоративних структур, таких як компанії, фонди або операційні компанії, які наймають ключових розробників, володіють правами інтелектуальної власності або управляють казначействами; визначення пріоритетів розробки, контроль над випусками або управління критичною офчейн-інфраструктурою; контроль над офіційним брендингом, публічними повідомленнями, документацією та освітніми матеріалами. Важливо підкреслити, що існування кількох контролерів, які керують різними компонентами DeFi-структури, саме по собі не усуває та не зменшує зобов'язань щодо боротьби з відмиванням коштів та фінансуванням тероризму.

Зловмисники все активніше експлуатують характеристики та вразливості DeFi-структур, причому ці ризики значно посилюються там, де ефективне регулювання відсутнє або недостатньо впроваджене. Шахраї та організатори фінансових пірамід використовують DeFi-протоколи для створення складних схем омани, часто маскуючи їх під легітимні інвестиційні можливості. Показовим прикладом є схема SafeMoon Token, яка залучила понад два мільйони інвесторів при капіталізації понад 9 мільярдів доларів, але насправді була шахрайською схемою, де творці приховано зберігали контроль над ліквідністю, дозволяючи їм виводити величезні суми для особистої вигоди. Інший випадок - платформа Forsage, яка позиціонувалася як легітимна DeFi-інвестиція, а насправді була схемою Понці, що діяла на кількох блокчейнах, де творці контролювали гаманці верхнього рівня, які заробляли найбільше без необхідності інвестувати власні кошти.

Професійні мережі відмивання грошей та транснаціональна організована злочинність використовують DeFi для складних багаторівневих операцій приховування походження коштів. Ці мережі використовують витончені техніки, включаючи фрагментацію коштів та переміщення їх через численні гаманці перед маршрутизацією через децентралізовані біржі, крос-чейн містки, міксери та свопи, створюючи багатошарову обфускацію за допомогою швидких автоматизованих транзакцій та стрибків між блокчейнами. Після тривалого процесу нашарування кошти консолідуються та виводяться у фіатну валюту через централізовані біржі зі слабким контролем або неліцензованих позабіржових брокерів.

Особливу загрозу становлять групи, пов'язані з КНДР, які проводять все більш складні кібератаки на DeFi-структури для фінансування діяльності з розповсюдження зброї. У квітні 2026 року дві великі атаки на DeFi-платформи, приписувані КНДР, склали приблизно 76% річних втрат від інцидентів зламу віртуальних активів. Перша атака на Drift Protocol - велику децентралізовану біржу безстрокових ф'ючерсів на Solana - призвела до втрати 285 мільйонів доларів. Друга атака на KelpDAO призвела до втрат приблизно 292 мільйони доларів через експлуатацію недоліку в дизайні мосту LayerZero. Ці інциденти демонструють критичні вразливості, а також зростаючу витонченість атак, спрямованих на DeFi-структури.

Звіт містить комплексні рекомендації для юрисдикцій щодо ефективного впровадження Рекомендації 15 до DeFi-структур. Першочерговим кроком є проведення належної оцінки ризиків, інтегрованої в національні, секторальні або галузеві оцінки ризиків. Ця оцінка повинна визначати характер та матеріальність ризиків, пов'язаних з DeFi, включаючи ступінь внутрішнього впливу, транскордонні виміри та потенційні вразливості, що виникають з операцій, управління та використання DeFi-структур. Важливо, що звіт наголошує на пропорційному підході: юрисдикції з більш значною DeFi-активністю повинні виділяти більше ресурсів на розуміння, нагляд та розробку підходів до пом'якшення ризиків, тоді як країни з обмеженим впливом повинні присвячувати менше ресурсів, зосереджуючись на моніторингу ринкових тенденцій та нових типологій.

Ключовим елементом є встановлення чітких стандартів для визначення контролерів DeFi-структур. Юрисдикції повинні застосовувати функціональний підхід, оцінюючи, хто фактично контролює або впливає на різні аспекти структури, а не покладаючись виключно на інформацію, надану самою структурою, або маркетингові терміни, що описують ступінь децентралізації. У випадках, де контролери існують, але не можуть бути ідентифіковані, наглядові органи повинні тісно співпрацювати з іншими суб'єктами, які можуть володіти додатковою інформацією, включаючи відповідні внутрішні органи, іноземних колег через механізми міжнародного співробітництва та приватний сектор, включаючи компанії з аналітики блокчейну.

Юрисдикції повинні впроваджувати вимоги ліцензування або реєстрації для централізованих DeFi-структур. Як мінімум, структури, контрольовані юридичними особами, повинні бути ліцензовані або зареєстровані в юрисдикції створення, тоді як у випадках, коли контролер є фізичною особою, така особа повинна бути ліцензована або зареєстрована в юрисдикції місця ведення бізнесу або проживання. Наглядові органи також повинні встановити чіткі стандарти для аудитів смарт-контрактів, заохочувати вбудовування засобів контролю боротьби з відмиванням коштів безпосередньо в смарт-контракти, посилювати нагляд за провайдерами та операторами оракулів, а також сприяти прозорості в структурах управління DeFi.

Особливу увагу приділено взаємодії між DeFi-структурами та регульованими фінансовими установами та VASP. Фінансові установи та VASP, що взаємодіють з DeFi-структурами, повинні проводити оцінку ризиків продуктів та вживати відповідних заходів для управління та пом'якшення ризиків. При роботі з централізованими DeFi-структурами вони повинні проводити належну перевірку клієнта щодо структури, визначаючи, чи ліцензована та зареєстрована вона та чи підлягає адекватному нагляду. У випадках з централізованими структурами, де контролери не можуть бути легко ідентифіковані, та повністю децентралізованими структурами, фінансові установи та VASP повинні застосовувати

відповідні заходи до кінцевих користувачів структури, включаючи перевірку особи та постійний моніторинг цілісності та безпеки протоколу. Важливо, що регуляторні та наглядові органи можуть розглядати більш гнучкий підхід, де повністю децентралізовані структури впроваджують ефективні заходи пом'якшення ризиків на рівні протоколу.

Транскордонний характер DeFi вимагає безпрецедентного рівня міжнародного співробітництва. Обмін інформацією між юрисдикціями є фундаментальним для ідентифікації централізованих DeFi-структур, які можуть діяти без відповідної реєстрації або ліцензії. Наглядові органи повинні максимально використовувати існуючі механізми міжнародного співробітництва, такі як Багатосторонній меморандум про взаєморозуміння IOSCO, для обміну даними про нові ризики, результати розслідувань та заходи правозастосування. Ефективний обмін інформацією між підрозділами фінансової розвідки відіграє ключову роль у виявленні транскордонних ризиків, пов'язаних з DeFi, причому досвід Глобальної мережі FATF показує, що обмін операційним та стратегічним аналізом може підтримувати виявлення нових способів зловживання DeFi-структурами та зусилля з відстеження коштів.

Правоохоронні органи повинні тісно співпрацювати з наглядовими органами, підрозділами фінансової розвідки та іншими компетентними органами через спільні операційні процедури, міжвідомчий доступ до пропрієтарних платформ аналітики блокчейну та тимчасові відрядження персоналу. Спеціалізовані міждисциплінарні цільові групи можуть підтримувати розслідування, враховуючи високотехнологічний та транскордонний характер DeFi-структур, інтегруючи різноманітний досвід підрозділів фінансової розвідки, кіберзлочинності та фінансових наглядачів.

Блокування та повернення коштів, пов'язаних з незаконною діяльністю в DeFi, створює як операційні, так і регуляторні проблеми. Ефективний підхід полягає у зосередженні зусиль на суміжних компонентах екосистеми віртуальних активів, здатних застосовувати механізми блокування або відхилення, включаючи емітентів стейблкоїнів, забезпечених фіатними валютами, VASP як кастодіальні кінцеві точки та DeFi-інтерфейси, що інтегрують певні інструменти комплаєнсу.

Публічно-приватні партнерства відіграють вирішальну роль у вирішенні ризиків, пов'язаних з DeFi, забезпечуючи структурований обмін інформацією, спільний операційний аналіз та спільне розуміння нових ризиків та регуляторних вимог. Ці партнерства особливо цінні для допомоги органам влади у виявленні характеристик, особливостей управління та структур контролю DeFi-структур, розробці глибшого розуміння того, як програмуються та розгортаються протоколи та смарт-контракти, а також для сприяння розробці та впровадженню заходів боротьби з відмиванням коштів та децентралізованих рішень ідентифікації.

Висновки:

- **DeFi стрімко зростає, але залишається "сірою зоною":** Загальна заблокована вартістьактивів у DeFi сягнула $86,6 млрд, однак 92% юрисдикцій (132 з 142) досі не ідентифікували жодного DeFi-регулювання на своїй території, а лише 4 країни впровадили ліцензування.
- **Ключовий критерій – "контроль", а не декларації про "децентралізацію":** FATF наголошує: стандарти застосовуються до будь-якої DeFi-структури, де є ідентифіковані контролери (розробники, власники токенів управління, адміністратори), навіть якщо вона визначає себе як децентралізована.
- **DeFi активно використовується для фінансових злочинів:** Зловмисники використовують DeFi для складного багаторівневого відмивання через міксери та мости між блокчейнами.
- **Вимога до піднаглядних установ – посилений контроль за ризиками DeFi:** Банки, фінансові установи та VASP, які взаємодіють з DeFi, зобов'язані проводити оцінку ризиків, належну перевірку клієнтів та впроваджувати додаткові заходи моніторингу.

Звіт FATF демонструє, що DeFi продовжує стрімко розвиватися і має потенціал відіграти важливу роль у майбутній глобальній фінансовій системі. Його технологічні особливості створюють як можливості для фінансових інновацій, так і суттєві ризики відмивання коштів, фінансування тероризму та розповсюдження зброї. Ці ризики посилюються широко поширеними помилковими уявленнями про "децентралізацію", стійкими регуляторними прогалинами та зростаючим використанням DeFi-структур кіберзлочинцями, шахраями, професійними відмивачами грошей та мережами фінансування розповсюдження, включаючи використання передових інструментів штучного інтелекту.

Стандарти FATF вже забезпечують рамки для вирішення цих ризиків, але їх впровадження залишається значно недостатнім. Більшість юрисдикцій досі не ідентифікували DeFi-структури, що діють на їхній території, не оцінили їхні ризики та не застосували Рекомендацію 15 до структур, що кваліфікуються як VASP. Ключовим викликом є визначення осіб, які здійснюють контроль або достатній вплив над DeFi-структурами. Юрисдикції повинні прийняти функціональний, заснований на ризиках підхід до ідентифікації контролерів, застосування вимог ліцензування/реєстрації та нагляду за DeFi-структурами. Влада повинна посилити розслідувальні та правозастосовні спроможності, включаючи аналітику блокчейну, операційну співпрацю та публічно-приватні партнерства.

Для структур, які є повністю децентралізованими та випадають зі сфери дії стандартів, юрисдикції повинні використовувати альтернативні заходи пом'якшення ризиків, спрямовані на суміжні регуляторні точки доступу, такі як емітенти стейблкоїнів, VASP та інтерфейси прикладного рівня. Ці альтернативні заходи можуть бути скориговані там, де повністю децентралізовані структури впроваджують адекватні заходи пом'якшення ризиків.

В кінцевому підсумку, ефективне пом'якшення ризиків, пов'язаних з DeFi, вимагатиме скоординованих глобальних дій, прозорих практик управління, інноваційних рішень комплаєнсу та постійної взаємодії між регуляторами, правоохоронними органами та приватним сектором. Без таких заходів швидка еволюція DeFi, яка має потенційні переваги для модернізації платежів, ризикує створити зростаючу регуляторну асиметрію, полегшуючи юрисдикційний арбітраж та сприяючи масштабному незаконному фінансуванню, що може підірвати цілісність світової фінансової системи.

Глобальна імплементація стандартів FATF щодо віртуальних активів: прогрес, системні прогалини та нові ризики [2]

Сьоме цільове оновлення FATF щодо імплементації міжнародних стандартів у сфері віртуальних активів і постачальників послуг у сфері криптопослуг (VASP) оцінює прогрес держав у виконанні Рекомендації 15 FATF та відповідної Пояснювальної записки. Документ охоплює проведення оцінок ризиків, формування національних режимів регулювання, ліцензування або реєстрацію VASP, здійснення ризик-орієнтованого нагляду, виконання правила переказу інформації – Travel Rule, а також реагування на нові ризики ВК/ФТ/ФР, пов’язані зі стейблкоїнами, некастодіальними гаманцями, офшорними провайдерами та децентралізованими фінансами. Основний висновок FATF полягає в тому, що держави поступово вдосконалюють законодавство, однак між формальним запровадженням вимог і їх практичним застосуванням залишається істотний розрив. Юрисдикції дедалі частіше проводять оцінки ризиків і ухвалюють необхідні норми, але повільніше переходять до реальних перевірок, виявлення неліцензованих провайдерів, застосування санкцій та заморожування незаконних віртуальних активів.

[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/7th-targeted-update-on-implementation-fatf-standards-vas-vasps-2026.pdf.coredownload.pdf

Аналітична база звіту охоплює відповіді 147 юрисдикцій, серед яких 38 членів FATF і 109 членів регіональних органів за типом FATF, матеріали Контактної групи FATF з питань віртуальних активів, а також результати 149 взаємних оцінок і звітів про прогрес, опублікованих станом на квітень 2026 року. FATF наголошує, що результати опитування є самооцінкою держав і не проходили незалежної перевірки. Крім того, 58 із 205 юрисдикцій глобальної мережі FATF не відповіли на опитування, тому для цілей аналізу організація виходила з припущення, що вони не досягли прогресу у виконанні Рекомендації 15. Наведені дані, таким чином, характеризують загальну динаміку, але не завжди дають змогу оцінити реальну ефективність національних систем.

За результатами взаємних оцінок рівень технічної відповідності Рекомендації 15 дещо покращився, проте залишається недостатнім. Із 149 оцінених юрисдикцій лише одна повністю відповідає встановленим вимогам. Частка юрисдикцій, які переважно відповідають Рекомендації 15, зросла з 29% у 2025 році до 34% у 2026 році, тоді як частка тих, що відповідають частково, зменшилася з 50% до 43%. Водночас 22% юрисдикцій усе ще не відповідають вимогам. Найсуттєвіші недоліки стосуються оцінювання ризиків і застосування ризик-орієнтованого підходу, виявлення осіб, які фактично здійснюють діяльність VASP, практичного виконання Travel Rule, здійснення ефективного нагляду та міжнародного співробітництва.

У сфері оцінювання ризиків зафіксовано помітний формальний прогрес. У 2026 році 86% респондентів, або 124 зі 145 юрисдикцій, повідомили про проведення оцінки ризиків ВК/ФТ/ФР, пов'язаних із віртуальними активами та VASP, порівняно із 76% у 2025 році. Проте лише 48 зі 149 оцінених юрисдикцій повністю або переважно виконують критерій 15.3 щодо оцінювання ризиків і застосування ризик-орієнтованого підходу. Отже, результати оцінок нерідко не трансформуються у конкретні наглядові пріоритети, плани перевірок, розподіл ресурсів і цільові заходи мінімізації ризиків. FATF рекомендує оцінювати не лише постачальників послуг, створених або фізично присутніх у державі, а всю фактичну експозицію юрисдикції до крипторинку. Це має охоплювати іноземних VASP, які обслуговують резидентів, емітентів стейблкоїнів, контрольовані механізми DeFi, однорангові перекази, некастодіальні гаманці, нові технології та способи переміщення активів між блокчейнами.

Більшість держав уже визначила загальний підхід до регулювання сектору. У 2026 році 89% опитаних юрисдикцій повідомили, що вирішили, яким чином вони регулюватимуть віртуальні активи та VASP. Із 144 респондентів 66% дозволяють відповідну діяльність, 8% застосовують часткову заборону, 15% – повну заборону, а 11% ще не визначилися. За часткової заборони держави найчастіше обмежують використання віртуальних активів як засобу платежу, але дозволяють їх придбання, зберігання, інвестування або торгівлю в межах контрольованого режиму. Додаткові обмеження можуть поширюватися на конфіденційні криптоактиви, послуги підвищення анонімності, майнінг або зберігання активів.

FATF застерігає, що повна заборона діяльності VASP не усуває ризиків автоматично. Такий підхід допускається стандартами, але може створити додаткові вразливості, якщо держава не здатна виявляти приховану або транскордонну діяльність, ідентифікувати операторів незаконних сервісів і застосовувати до них санкції. Із 21 юрисдикції, які повідомили про повну заборону VASP, 16 уживали наглядових або правоохоронних заходів проти незаконних провайдерів. Проте реалізація таких режимів залишається нерівномірною, а лише одна юрисдикція із заборонним підходом повністю виконала вимоги FATF щодо оцінювання ризиків.

У сфері ліцензування також існує розрив між законодавством і практикою. Серед 130 юрисдикцій, які не забороняють або не планують забороняти діяльність VASP, 73%, або 95 держав, запровадили вимогу щодо їх ліцензування чи реєстрації. Водночас лише 58%, або 76 юрисдикцій, фактично видали ліцензію чи зареєстрували хоча б одного провайдера. Ще 19 мають відповідне законодавство, але не здійснили жодної реєстрації, а 17 перебувають у

процесі його ухвалення. Показово, що п’ять із 50 юрисдикцій, які визнали сектор віртуальних активів високоризиковим, досі не запровадили чинної вимоги щодо ліцензування або реєстрації VASP.

Серед 95 юрисдикцій із режимом ліцензування або реєстрації 81% повідомили про проведення наглядових перевірок, а 71% – про застосування примусових, адміністративних чи інших наглядових заходів. Водночас FATF виявила суперечності у відповідях, оскільки деякі держави заявили про проведення перевірок, хоча фактично не ліцензували жодного VASP. Головною практичною проблемою залишається виявлення осіб, які надають криптопослуги без необхідного дозволу. Для цього наглядовим органам необхідно використовувати не лише офіційні реєстри, а й блокчейн-аналітику, інформацію підрозділів фінансової розвідки, банків і платіжних установ, відкриті джерела, рекламу, мобільні застосунки та дані про цифрову інфраструктуру.

Значний нормативний прогрес відбувся в імплементації Travel Rule, яке поширює вимоги Рекомендації 16 FATF щодо прозорості платежів на перекази віртуальних активів. Правило зобов’язує VASP і фінансові установи отримувати, зберігати та безпечно передавати встановлену інформацію про ініціатора й одержувача переказу. У 2026 році 83% відповідних респондентів, або 91 зі 109 юрисдикцій, повідомили про ухвалення такого законодавства, порівняно із 73% у 2025 році. Проте 60% держав, які вже запровадили Travel Rule, ще не здійснювали пов’язаних із ним наглядових або правозастосовних заходів. Отже, законодавче закріплення правила поки не гарантує реального передавання інформації між VASP, перевірки її повноти та реагування на перекази з відсутніми або недостовірними даними. FATF вважає це серйозною проблемою, оскільки ефективність Travel Rule залежить від його послідовного та узгодженого застосування на глобальному рівні.

Окрему увагу у звіті приділено офшорним VASP, які обслуговують клієнтів за межами держави своєї реєстрації або фізичного розташування. Якщо такий провайдер зареєстрований у юрисдикції зі слабким режимом ПВК/ФТ/ФРЗМЗ, ризики поширюються на всі країни, у яких він пропонує послуги. Деякі офшорні VASP цілеспрямовано залучають користувачів у державах, де вони не мають ліцензії, використовуючи соціальні мережі, зашифровані месенджери, партнерські програми та місцеву рекламу. Окремі провайдери можуть рекомендувати користувачам застосовувати VPN або надавати неправдиві відомості для обходу територіальних обмежень.

Додатковий ризик створюють вкладені схеми, за яких офшорний VASP отримує доступ до ліквідності, торгівлі або каналів введення та виведення фіатних коштів через рахунок у ліцензованого місцевого VASP чи фінансової установи. При цьому офшорний провайдер може видавати себе за звичайного роздрібного клієнта, хоча фактичні обсяги його операцій значно перевищують типові показники. Для виявлення таких схем FATF рекомендує поєднувати блокчейн-аналітику, інформацію з відкритих джерел, повідомлення про підозрілі операції, аналіз фіатних каналів і дані міжнародних партнерів.

Дедалі більше держав застосовує до офшорних VASP діяльнісний підхід, за якого обов’язок отримати місцеву ліцензію виникає через фактичне надання послуг резидентам, навіть за відсутності формальної присутності в країні. Ознаками такої діяльності можуть бути цілеспрямована реклама, залучення місцевих клієнтів і використання національної платіжної інфраструктури. До провайдерів, які відмовляються виконувати вимоги, можуть застосовуватися публічні попередження, видалення застосунків із цифрових магазинів, обмеження доступу до місцевої фінансової системи, адміністративні санкції та кримінальне переслідування. Ефективність таких заходів залежить від взаємодії наглядових органів, підрозділів фінансової розвідки, правоохоронних і податкових органів, а також від міжнародного співробітництва.

У частині ризиків FATF констатує «індустріалізацію» шахрайства з використанням віртуальних активів. Організовані злочинні угруповання використовують масштабні шахрайські центри, фіктивні інвестиційні платформи, соціальну інженерію, некастодіальні

гаманці, позабіржових брокерів і платіжні шлюзи. Такі операції діють транскордонно та генерують багатомільярдні доходи. Як приклад наведено фінансовий конгломерат у Камбоджі, який, за даними компетентних органів, упродовж серпня 2021 – січня 2025 року відмив щонайменше 4 млрд доларів США. Та сама інфраструктура використовувалася пов'язаними з КНДР суб'єктами для відмивання активів, викрадених унаслідок кібератак, частина яких могла спрямовуватися на програми зброї масового знищення та балістичних ракет.

Іншим прикладом є операція Borrelli, у межах якої компетентні органи Іспанії за підтримки Європолу та органів Естонії, Франції і США припинили діяльність міжнародної мережі криптоінвестиційного шахрайства. За оцінкою слідства, через неї було відмито близько 460 млн євро, одержаних від понад 5 000 потерпілих. Віртуальні активи в цій схемі одночасно були способом залучення потерпілих, предметом фіктивного інвестування та каналом відмивання незаконних доходів.

Звіт показує зближення ризиків організованої злочинності, відмивання коштів, фінансування тероризму, фінансування розповсюдження, ухилення від санкцій і кіберзлочинності. Різні незаконні суб'єкти дедалі частіше використовують спільну інфраструктуру: глобальні біржі, офшорних VASP, позабіржових брокерів, стейблкоїни, некастодіальні гаманці, мости між блокчейнами та DeFi-протоколи. Тому FATF рекомендує розглядати ці загрози не ізольовано, а через виявлення спільних посередників, технологічних компонентів і повторюваних моделей переміщення активів.

Додатковим фактором ризику стає штучний інтелект. Злочинці можуть використовувати синтетичні профілі та підроблені відеоматеріали для соціальної інженерії, а інструменти штучного інтелекту – для пошуку вразливостей смартконтрактів і підготовки атак на DeFi-протоколи та кросчейн-інфраструктуру. Після викрадення активи можуть швидко переміщуватися через стейблкоїни, децентралізовані біржі, мости й декілька VASP, що ускладнює їх відстеження та заморожування. FATF розглядає штучний інтелект як чинник, здатний прискорювати та масштабувати різні етапи шахрайства, кібератак і відмивання коштів.

Значна частина ризиків пов'язана зі стейблкоїнами, привабливість яких для незаконних суб'єктів пояснюється стабільною вартістю, ліквідністю та швидкістю транскордонних переказів. FATF описує випадок створення власного стейблкоїна, який позиціонувався як несприйнятливий до заморожування активів і незалежний від регуляторного контролю. Його запуск став реакцією на заморожування стороннім емітентом понад 29 млн доларів США на гаманці, пов'язаному з підозрілою діяльністю. Цей випадок демонструє ризик створення інфраструктури, у якій навмисно відсутня технічна можливість виконувати вимоги про блокування, заморожування або вилучення активів. FATF рекомендує поширювати вимоги ПВК/ФТ/ФР на емітентів стейблкоїнів, якщо вони відповідають визначенню VASP, та забезпечувати технічну спроможність виконувати законні рішення компетентних органів.

Однорангові перекази через некастодіальні гаманці FATF розглядає як структурну прогалину системи ПВК/ФТ/ФР, оскільки вони здійснюються без регульованого посередника, відповідального за належну перевірку клієнта, виконання Travel Rule та повідомлення про підозрілі операції. Хоча перекази у публічних блокчейнах доступні для перегляду, псевдонімність адрес і використання складних ланцюгів гаманців ускладнюють установлення фактичних учасників. Із 66 юрисдикцій, які оцінили цей ризик, 88% визнали його високим, але лише 23% держав збирають та аналізують ринкові показники щодо масштабів таких операцій. FATF рекомендує застосовувати посилену перевірку до операцій із некастодіальними гаманцями підвищеного ризику та використовувати блокчейн-аналітику для виявлення дроблення сум, швидкого переміщення активів і взаємодії з ризиковими адресами.

Найменш розвиненою сферою залишається регулювання DeFi. Лише 18% юрисдикцій оцінили пов'язані з ними ризики, а ще 9% проводять таку оцінку. Хоча 31% держав стверджують, що їхні заходи мінімізації ризиків поширюються на DeFi, лише чотири запровадили відповідні

вимоги щодо ліцензування або реєстрації, дві фактично ліцензували чи зареєстрували такі механізми, і тільки одна повідомила про застосування заходів впливу. FATF розмежовує механізми з ідентифікованими контролерами, формально децентралізовані механізми, які фактично мають осіб із достатнім контролем або впливом, і справді децентралізовані системи. Стандарти FATF поширюються на перші дві категорії, тоді як ризики справді децентралізованих систем мають мінімізуватися за допомогою альтернативних ризик-орієнтованих заходів.

Висновки:

- **Перетворити оцінку ризиків на наглядовий план.** Юрисдикціям необхідно пов'язати встановлені ризики зі списком наглядових пріоритетів, категоризацією VASP, періодичністю перевірок, розподілом ресурсів і конкретними заходами впливу. Сам факт проведення оцінки ризиків більше не може вважатися достатнім результатом.
- **Пріоритетом має бути фактична видача ліцензій, перевірка виконання вимог, виявлення неліцензованої діяльності та застосування санкцій.** Особливу увагу слід приділити 60% юрисдикцій, які ухвалили Travel Rule, але ще не здійснювали відповідного нагляду або правозастосування.
- **Розширити контроль за транскордонною криптоінфраструктурою.** Регуляторні режими повинні охоплювати офшорних VASP, які фактично обслуговують резидентів, а VASP і банки мають виявляти вкладені рахунки, маскування провайдерів під роздрібних клієнтів та операції з некастодіальними гаманцями, стейблкоїнами, мостами й DeFi підвищеного ризику.
- **Для України завершити перехід від нормативної підготовки до повноцінного нагляду.** Необхідно завершити режим авторизації VASP, визначити компетентний наглядовий орган і його повноваження, установити вимоги до емітентів стейблкоїнів і контрольованих DeFi-механізмів, розпочати ризик-орієнтовані перевірки та створити процедури оперативного відстеження, заморожування й конфіскації незаконних віртуальних активів.

Для державного сектору FATF визначає пріоритетами комплексне оцінювання ризиків, створення дієвого режиму ліцензування, проведення виїзних і безвиїзних перевірок, контроль виконання Travel Rule, виявлення неліцензованої діяльності та застосування ефективних санкцій. Окреме значення має посилення внутрішнього, міжнародного та публічно-приватного співробітництва, включно зі створенням каналів швидкого обміну інформацією та операційних механізмів для відстеження, заморожування, арешту й конфіскації незаконних віртуальних активів.

Приватному сектору рекомендовано створити повноцінні системи ПВК/ФТ/ФР, забезпечити практичне виконання Travel Rule, оцінювати ризики стейблкоїнів, некастодіальних гаманців, офшорних VASP і DeFi та використовувати інструменти блокчейн-аналітики. Контрольні механізми мають охоплювати належну перевірку клієнта, перевірку адрес і гаманців, моніторинг транзакцій, застосування переліків заборонених, а за необхідності й дозволених адрес, а також можливість оперативно блокувати або заморожувати активи.

До оновленої таблиці юрисдикцій із матеріально значущою діяльністю VASP включено країни, на які припадає понад 0,25% світового обсягу торгівлі віртуальними активами, або держави, що входять до 30 юрисдикцій із найвищими показниками володіння чи використання таких активів. Сукупно вони охоплюють приблизно 97% світового ринку. Включення до таблиці не свідчить ані про підвищений ризик, ані про рівень відповідності стандартам, а лише відображає матеріальне значення відповідного ринку.

Україну також включено до цього переліку. За наведеною у звіті самооцінкою, Україна провела оцінку ризиків віртуальних активів і VASP, не застосовує їх повної заборони та імплементувала Travel Rule. Водночас законодавче врегулювання ліцензування або реєстрації VASP і застосування до них заходів ПВК/ФТ перебуває у процесі. На момент опитування не повідомлено про практичні наглядові перевірки, заходи впливу або запровадження окремих вимог до емітентів стейблкоїнів. Рейтинг України за Рекомендацією 15 визначено як «частково відповідає», однак він ґрунтується на оцінці 2020 року та може не відображати подальших змін.

Загалом документ демонструє, що основною проблемою глобальної імплементації Рекомендації 15 є вже не лише відсутність законодавства, а недостатня практична ефективність установлених вимог. Нерівномірність національного регулювання створює можливості для регуляторного арбітражу та перетворює юрисдикції зі слабким наглядом на точки входу до глобальної фінансової системи. Тому FATF переносить акцент із формального ухвалення норм на досягнення конкретних результатів: фактичне ліцензування VASP, проведення перевірок, виконання Travel Rule, виявлення незаконних провайдерів, застосування санкцій, оперативний обмін інформацією та повернення незаконних віртуальних активів.

Штучний інтелект: Нова ера ризиків для фінансової стабільності [3]

Світ фінансів вступив у нову еру, де штучний інтелект (ШІ) стає не просто інструментом ефективності, а ключовим фактором, що перевизначає саму природу ризиків та загроз.

Документ Міжнародного валютного фонду (МВФ) є глибоким аналізом цієї трансформації, яка ставить під сумнів усталені підходи до регулювання та нагляду. Основна теза, яку проводять автори полягає в тому, що найбільша загроза для фінансової стабільності полягає не в появі принципово нових видів кібератак, а в драматичному масштабуванні вже існуючих загроз. ШІ діє як каталізатор, що прискорює швидкість, частоту та широту виявлення й експлуатації вразливостей, перетворюючи операційні слабкості в загальновживаному програмному забезпеченні, хмарних сервісах та інших спільних технологіях на системні події.

Сучасна фінансова система, з її глибокою взаємопов'язаністю та покладанням на спільну цифрову інфраструктуру, є надзвичайно вразливою до цього нового класу загроз. Банки, керуючі активами, страхові компанії, платіжні системи та ринкові інфраструктури все більше покладаються на спільні хмарні платформи, операційні системи, програмне забезпечення з відкритим кодом та мережі. Ця спільна архітектура, хоч і забезпечує ефективність, створює критичну корельовану вразливість. Коли вразливість виявляється в такому спільному компоненті, ШІ дозволяє зловмисникам ідентифікувати та атакувати її одночасно в багатьох установах у стислі терміни. Як наслідок, те, що раніше могло бути ізольованим інцидентом, тепер може викликати ланцюгову реакцію збоїв, які швидко поширюються між фірмами, секторами та юрисдикціями. Останні інциденти, такі як збій в системі TARGET у лютому 2025 року або технічні проблеми з системою RTGS/CHAPS Банку Англії у 2023 році, яскраво демонструють, як операційні збої можуть мати системні наслідки, і ШІ значно підсилює цю ймовірність.

Ключовим аспектом аналізу є подвійна природа (dual-use) технологій ШІ в кібербезпеці. Одні й ті ж інструменти, які допомагають захисникам виявляти аномалії, проводити тестування на проникнення та автоматично перевіряти код, можуть бути використані зловмисниками для створення складніших атак. ШІ не просто автоматизує окремі етапи атаки, як-от створення фішингових листів або сканування вразливостей. Сучасні передові моделі ШІ, як демонструє випадок з моделлю Claude Mythos компанії Anthropic, здатні до автономного виконання багатоетапних кібероперацій – від виявлення вразливостей до розробки експлойтів та

[3] https://www.imf.org/-/media/files/publications/imf-notes/2026/english/insea2026005.pdf

виконання повної послідовності атаки без безперервного втручання людини. Цей перехід до машинної швидкості атаки зменшує час реагування захисників до мінімуму. Якщо раніше середній час для горизонтального переміщення зловмисника в мережі ("breakout time") міг обчислюватися годинами або днями, то з використанням ШІ, за даними CrowdStrike, він скоротився до 29 хвилин, а в деяких випадках – до лічених секунд.

Така динаміка підриває традиційний баланс між нападом і захистом. Зловмисники отримують можливість діяти швидше та масштабніше, використовуючи вразливості, які раніше могли залишатися непоміченими роками. Показовим є той факт, що модель Mythos, яка не навчалася спеціально для кібератак, продемонструвала здатність виявляти тисячі критичних вразливостей нульового дня (zero-day) у всіх основних операційних системах та веб-браузерах, включаючи 27-річну помилку в стеку TCP протоколу OpenBSD. Це підкреслює важливе спостереження: передові кіберможливості можуть виникати як "побічний ефект" загального вдосконалення моделей, роблячи процес їхнього контролю та регулювання надзвичайно складним.

У відповідь на ці виклики міжнародне співтовариство та національні регулятори починають перебудовувати свої підходи. МВФ відіграє центральну роль через свій нагляд, технічну допомогу та аналітичну роботу, включаючи програму оцінки фінансового сектора (FSAP). Рада з фінансової стабільності (FSB) визначила кіберризики, пов'язані з ШІ, як одну з ключових вразливостей, закликаючи до посилення моніторингу та оцінки адекватності політик. Міжнародна організація комісій з цінних паперів (IOSCO) у своєму консультаційному документі 2025 року визначила кібербезпеку як найвищий ризик, пов'язаний з ШІ на ринках капіталу, а також наголосила на ризику концентрації від невеликої кількості постачальників хмарних послуг та розробників ШІ. На національному рівні підходи відрізняються: від горизонтального регулювання в ЄС (включаючи Закон про ШІ та DORA) до секторально-орієнтованих стратегій у Великій Британії та США, але всі вони визнають необхідність посилення контролю над третіми сторонами, управління моделями та кіберстійкістю.

Висновки:

- **Головна загроза – швидкість і масштаб, а не нові види атак.** ШІ не створює принципово нових кібератак, але катастрофічно прискорює виявлення та експлуатацію вразливостей, перетворюючи ізольовані інциденти на системні кризи.
- **Критична вразливість – концентрація та взаємопов'язаність.** Фінансова система надзвичайно вразлива через спільну хмарну інфраструктуру, програмне забезпечення та невелику кількість глобальних постачальників ШІ-послуг.
- **Наявні регуляторні інструменти стрімко застарівають.** Сучасні бенчмарки безпеки втрачають інформативність, а управління передовими системами залишається переважно добровільним, що створює небезпечний розрив між технологіями та наглядом.
- **Оборона має стати такою ж швидкою, як і напад.** Ключ до стійкості – не лише в запобіганні, а в технічних заходах для обмеження "радіусу вибуху" (blast radius), швидкому реагуванні, посиленому нагляді за третіми сторонами та міжнародній координації.

Однак аналіз МВФ виявляє низку критичних прогалин у поточній регуляторній архітектурі.

По-перше, це "насичення бенчмарків" – стандартні тести безпеки ШІ швидко стають неінформативними. Коли передова модель, як-от Mythos, досягає 100% на стандартному бенчмарку Cybench, цей показник втрачає будь-яку сигнальну цінність для наглядових органів. Це створює ризик, що регулятори та фірми покладатимуться на недостовірні оцінки, недооцінюючи реальні можливості моделей, які мають значення для фінансової стабільності.

По-друге, загострюється глобальна нерівність у сфері безпеки. Країни з ринками, що розвиваються (EMDEs), мають таку ж експозицію до глобальної спільної інфраструктури, але часто не мають ні ресурсів, ні технічного потенціалу для впровадження сучасних систем захисту, що робить їх більш вразливими та може стати новим каналом глобальної фінансової фрагментації.

По-третє, зберігається значний розрив у сфері управління (governance). Управління передовими системами ШІ залишається переважно добровільним та контролюється самими розробниками, чого явно недостатньо, коли на карту поставлена фінансова стабільність.

Враховуючи це, автори документу пропонують сім ключових політичних рекомендацій. Головний акцент зміщується з простого запобігання атакам на здатність системи стримувати та локалізувати збитки. По-перше, необхідно оновлювати нагляд за кіберризиками, інтегруючи сценарії машинного виявлення вразливостей та корельовану експлуатацію спільних технологій у моніторинг фінансової стабільності. По-друге, критично важливо посилити нагляд за третіми сторонами, особливо за великими постачальниками хмарних послуг та ШІ, враховуючи ризики концентрації та відсутності замінників. По-третє, необхідно розширювати міжсекторальну координацію, оскільки фінансовий сектор є лише частиною ширшої критичної інфраструктури, і збої в енергетиці чи телекомунікаціях можуть мати каскадний вплив. По-четверте, слід оновлювати симуляційні навчання (стрес-тести), щоб вони враховували не лише операційні, але й макрофінансові наслідки, такі як вплив на ліквідність, маржинальні вимоги та ринкове забезпечення. По-п'яте, запровадження стандартизованих вимог до розкриття інформації про інциденти допоможе покращити обізнаність та швидкість реагування. По-шосте, необхідно зміцнювати міжнародну координацію управління ШІ, щоб уникнути фрагментації та забезпечити спільні стандарти безпеки. І нарешті, регулятори та наглядові органи повинні створити спеціалізований потенціал для моніторингу передових ШІ, інвестуючи в кадри та технології.

На завершення, аналітичний документ МВФ окреслює новий ландшафт фінансової стабільності, де кіберзагрози, підсилені штучним інтелектом, стають першочерговим ризиком. Відповідь на цей виклик не може бути поетапною або зосередженою виключно на окремих фірмах. Вона вимагає системної, цілісної та міжнародно-скоординованої стратегії, в основі якої лежить здатність не лише захищатися, але й швидко відновлюватися після неминучих інцидентів, обмежуючи їхню руйнівну силу.

Штучний інтелект змінює правила гри, і час для адаптації регуляторних та операційних рамок стискається так само швидко, як і час на реагування на кібератаки. Затримка в цих діях може коштувати стабільності всієї глобальної фінансової системи.

Ефективні публічно-приватні партнерства у сфері ПВК/ФТ: від обміну інформацією до спільного управління ризиками [4]

Документ, підготовлений Егмонтською групою та її Робочою групою з обміну інформацією, містить практичну модель створення та розвитку публічно-приватних партнерств (ППП) у сфері протидії відмиванню коштів, фінансуванню тероризму та пов’язаним предикатним злочинам. Вихідною тезою документа є те, що сучасні злочинні мережі навмисно використовують фрагментованість фінансової системи, проводячи операції через різні установи, юридичні особи, юрисдикції, види активів і платіжні канали. Унаслідок цього жоден окремий учасник системи не володіє повною картиною злочинної діяльності. Державні органи мають слідчі, наглядові та аналітичні повноваження, тоді як приватні установи володіють актуальними даними про операції, поведінку клієнтів, внутрішні моделі ризику та результати роботи систем моніторингу. Поєднання цих можливостей дозволяє зменшити системні

[4] https://egmontgroup.org/wp-content/uploads/2026/07/Effective-PPPs-Practical-Guidance-Report.pdf

прогалини, перейти від реактивного подання повідомлень до координованого запобігання ризикам та забезпечити спільне визначення найбільш суттєвих загроз.

Публічно-приватне партнерство розглядається не як консультаційний майданчик, а як системний механізм забезпечення стійкості національної архітектури ПВК/ФТ. До державної частини партнерства можуть входити підрозділи фінансової розвідки, правоохоронні й наглядові органи, прокуратура, профільні міністерства, податкові та митні органи й служби безпеки. Приватний сектор можуть представляти фінансові установи, постачальники послуг, пов'язаних із віртуальними активами, визначені нефінансові установи та професії, неприбуткові організації, а за потреби – технологічні компанії, наукові установи, оператори соціальних мереж і телекомунікаційні компанії. Склад учасників має визначатися відповідно до конкретних ризиків і необхідної експертизи. Наприклад, для роботи з відмиванням коштів через торгівлю доцільно залучати митні органи й фахівців із торговельного фінансування, а для аналізу ризиків віртуальних активів – профільних постачальників послуг і спеціалістів із блокчейн-аналітики.

Перед запуском ППП необхідно оцінити інституційну спроможність, готовність учасників, рівень операційної зрілості та стабільність політичної підтримки. Оскільки партнерство є довгостроковим механізмом, його функціонування може залежати від зміни керівництва, реформування державних органів, оновлення законодавства й перегляду національних пріоритетів. Тому рекомендується поетапний підхід: спочатку зосередитися на стратегічному обміні, типологіях і формуванні спільного розуміння ризиків, а після зміцнення довіри, правової визначеності й технічної спроможності переходити до контрольованого обміну операційною інформацією.

Однією з основних передумов функціонування ППП є чітка правова основа. Учасники повинні розуміти, яку інформацію дозволено передавати, кому, з якою метою, на якій правовій підставі та за яких процедурних умов. Відсутність визначеності може призвести або до неправомірного розкриття конфіденційних відомостей, або до надмірно обережної поведінки, за якої учасники фактично уникають змістовного обміну. Правова визначеність може забезпечуватися поєднанням законодавчих змін, офіційних роз'яснень, меморандумів про взаєморозуміння, стандартизованих процедур і гарантій захисту добросовісних учасників від відповідальності. Меморандум не створює нових повноважень, але може визначати межі партнерства, категорії інформації, правила конфіденційності, порядок доступу, відповідальність учасників і процедури вирішення спорів.

Особливе значення мають положення про «безпечну гавань», які захищають приватні установи від цивільно-правової, регуляторної чи іншої відповідальності за добросовісне передавання інформації відповідно до встановлених правил. Без таких гарантій комплаєнс-підрозділи можуть обмежувати участь через ризик судових позовів, санкцій або репутаційних наслідків. Водночас учасники повинні не лише мати формальне право передавати інформацію, а й сприймати механізм ППП як юридично безпечний та інституційно підтримуваний.

Значна увага приділяється захисту персональних даних. Документ наголошує, що відповідні вимоги не перешкоджають співпраці, якщо вони вбудовані в конструкцію партнерства. Для цього потрібно визначити конкретну та законну мету обробки, правову підставу, мінімально необхідний обсяг даних, строки зберігання, порядок видалення та коло осіб, які матимуть доступ. Під час стратегічного аналізу перевага має надаватися анонімізованим або псевдонімізованим відомостям. Персоніфікована інформація може передаватися лише за наявності обґрунтованої операційної потреби та чіткої правової підстави. Доцільно застосовувати рольовий доступ і вести журнали аудиту, які фіксують, хто, коли та до яких даних отримував доступ. Раннє залучення органу із захисту персональних даних може посилити легітимність партнерства й довіру його учасників.

Стратегічною основою ППП мають бути національні та секторальні оцінки ризиків, стратегічна аналітика ПФР, оцінки загроз правоохоронних органів, наглядові огляди, аналіз ризиків обходу санкцій, міжнародні типології та результати взаємних оцінок FATF і

регіональних органів за типом FATF. Виявлені ризики необхідно перетворювати на конкретні напрями роботи. Для цього рекомендується затверджувати річний або дворічний план із переліком пріоритетних загроз, відповідальними учасниками, строками та очікуваними результатами. Такими результатами можуть бути типологічний звіт, оновлені індикатори ризику, рекомендації щодо моніторингу або зміни наглядових підходів. Формальна матриця ймовірності та впливу може використовуватися для визначення пріоритетів, але остаточне рішення має враховувати професійне судження експертів.

Важливою умовою стійкості ППП є політична та інституційна підтримка. Вона надає партнерству легітимності, забезпечує представників необхідними повноваженнями, дозволяє виділяти ресурси та сприяє безперервності роботи після зміни керівництва. Партнерство доцільно закріпити в національній стратегії ПВК/ФТ, рішенні уряду, міністерському мандаті або рішенні керівних органів відповідних установ. Кожна сторона повинна призначити постійних контактних осіб, закріпити функції ППП у їхніх посадових обов'язках і забезпечити аналітичну, технічну та адміністративну підтримку. За можливості рекомендується створити невеликий секретаріат. На стратегічному рівні мають бути представлені керівники з реальними повноваженнями, а в тематичних робочих групах – профільні фахівці.

Запропонована структура управління передбачає стратегічний керівний рівень, операційні робочі групи та технічну групу з питань даних. Керівний рівень визначає цілі, пріоритети, показники ефективності, склад учасників і правила поширення результатів. При цьому необхідно узгодити різні інституційні інтереси. ПФР може прагнути отримувати більш ранні та змістовні сигнали, наглядові органи – підвищити якість систем внутрішнього контролю, правоохоронні органи – посилити доказову цінність інформації, а приватні установи – отримати чіткіші індикатори та пропорційні регуляторні очікування. Ці інтереси можуть бути різними, але їх слід об'єднати навколо спільної мети зменшення системного ризику.

Одним із найважливіших напрямів роботи ППП є розроблення типологій. Типологія повинна не просто описувати злочинну схему, а пояснювати механізм її функціонування, поведінкові аномалії, використані регуляторні або операційні прогалини, можливі індикатори та обмеження чинних систем виявлення. ПФР може надавати узагальнені закономірності й результати стратегічного аналізу, наглядові органи – інформацію про недоліки внутрішнього контролю, правоохоронні органи – відомості про слідчі та доказові проблеми, а приватні установи – анонімізовані приклади й практичні спостереження щодо проявів схем у реальних операціях. Результатом мають бути практичні матеріали, придатні для вдосконалення систем моніторингу, навчання працівників, підготовки повідомлень і визначення напрямів нагляду.

Індикатори ризику повинні ґрунтуватися на реальних типологіях і описувати передусім поведінкові закономірності, а не лише формальні характеристики. Доцільно розрізняти основні та контекстуальні індикатори, щоб одинична ознака не спричиняла автоматичного висновку про підозрілість. Перед упровадженням індикатори необхідно перевіряти разом із приватними установами на предмет доступності даних, можливості технічного застосування та ймовірності надмірної кількості хибнопозитивних спрацювань. Надто широкі індикатори можуть стимулювати захисне звітування, тобто подання значної кількості формальних повідомлень із низькою аналітичною цінністю. Тому метою ППП має бути не збільшення кількості повідомлень, а підвищення їх якості, релевантності й зв'язку з реальними загрозами.

Обмін операційною інформацією щодо конкретних осіб, компаній, мереж або операцій може значно підвищити здатність системи до раннього виявлення та припинення злочинної діяльності, але водночас створює найбільші правові та репутаційні ризики. Його метою не повинно бути передавання приватним установам слідчих функцій або створення неофіційних «чорних списків». Отримана інформація має використовуватися для посиленого моніторингу й самостійного оцінювання ризику, а не для автоматичного припинення ділових відносин. Партнерство не повинно створювати фактичний санкційний режим поза встановленими законом процедурами.

Операційна взаємодія може включати термінове адресне передавання інформації за наявності ризику швидкого переміщення активів, повідомлення характеристик конкретної мережі без розкриття всіх ідентифікаторів або структуровані запити компетентних органів, за якими установи перевіряють власні дані. Для кожної форми необхідно встановити правову підставу, мету, коло одержувачів, порядок використання, зберігання та подальшого поширення інформації. Доступ повинен надаватися лише уповноваженим особам, а передавання третім сторонам – заборонятися без дозволу джерела інформації.

Технічна безпека ППП не обмежується використанням шифрування. Вона має охоплювати класифікацію інформації за рівнем чутливості, багатофакторну автентифікацію, рольовий доступ, журнали аудиту, кібербезпековий моніторинг, строки зберігання, безпечне видалення та процедури реагування на витік. Необхідно визначити, хто управляє цифровою платформою, надає доступ і контролює його використання. Працівники мають регулярно проходити підготовку, оскільки навіть захищена система може бути скомпрометована через необережне поводження з інформацією.

Документ розрізняє стратегічну, операційну та гібридну моделі ППП. Стратегічна модель передбачає обмін агрегованими або анонімізованими даними, типологіями, тенденціями та секторальними оцінками. Вона охоплює широке коло учасників і має менші правові ризики, однак її результати готуються та впроваджуються повільніше. Операційна модель передбачає швидке адресне передавання інформації про конкретні ризики й може сприяти заморожуванню активів або започаткуванню розслідувань, але потребує вузького кола учасників і суворих гарантій. Гібридна модель поєднує широке поширення стратегічних матеріалів, контрольований обмін тактичними сигналами та обмежене передавання чутливої операційної інформації. Вона дозволяє узгодити швидкість реагування, масштаб охоплення та необхідний рівень конфіденційності.

Технології можуть перетворити ППП із консультаційного майданчика на масштабовану систему колективного аналізу. Захищені платформи дозволяють створювати спільні бібліотеки типологій та індикаторів, стандартизувати повідомлення, документувати доступ і зберігати інституційну пам’ять. Технології підвищення конфіденційності, зокрема захищені багатосторонні обчислення та федеративне навчання, можуть допомагати виявляти спільні закономірності без передавання повних первинних даних. Штучний інтелект може застосовуватися для аналізу тенденцій і групування поведінкових індикаторів, але лише за умови прозорості, пояснюваності, людського контролю та збереження провідної ролі професійного судження.

Автори також звертають увагу на нерівність спроможностей учасників. Великі фінансові установи можуть мати спеціалізовані аналітичні підрозділи та сучасні технології, тоді як невеликі установи, фінтех-компанії або нефінансові суб’єкти можуть володіти значно меншими ресурсами. Щоб партнерство не стало залежним від найбільших учасників, доцільно застосовувати різні рівні участі, пропонувати базові й розширені варіанти реалізації рекомендацій, проводити спільне навчання та використовувати доступні технічні рішення. Установи з більшою спроможністю можуть виконувати складніші аналітичні завдання, але це не повинно надавати їм непропорційного впливу на діяльність ППП.

Довіра формується завдяки чіткому розподілу ролей, однаковому ставленню до учасників, конфіденційності, взаємності внесків, прозорості прийняття рішень і практичним результатам. Участь у ППП не повинна надавати окремим установам регуляторних переваг або привілейованого доступу до інформації. Державні органи мають надавати приватним установам змістовний зворотний зв’язок щодо якості повідомлень і актуальних загроз, а приватні установи – повідомляти про практичні труднощі застосування індикаторів та недоліки систем виявлення. Одне неправомірне розкриття конфіденційної інформації може зруйнувати довіру, яка формувалася роками, тому правила використання та подальшого поширення відомостей мають суворо дотримуватися.

Партнерство повинно залишатися гнучким і здатним швидко реагувати на нові способи обходу санкцій, використання децентралізованих фінансів, синтетичні ідентичності, нові форми шахрайства та інші загрози. Щонайменше раз на рік необхідно переглядати пріоритети, передбачити процедури термінового скликання учасників і створювати тимчасові тематичні групи для виконання конкретних завдань. Водночас усі зміни цілей, складу або моделі обміну повинні бути задокументовані та затверджені керівним рівнем. Гнучкість не має послаблювати базові принципи законності, пропорційності, конфіденційності, справедливості та підзвітності.

Ефективність ППП рекомендується оцінювати за його операційним і стратегічним впливом, удосконаленням системи ПВК/ФТ та внутрішнім станом самого партнерства. Операційними результатами можуть бути підвищення якості повідомлень про підозрілі операції, скорочення часу реагування, виявлення взаємопов'язаних індикаторів, заморожування активів або започаткування розслідувань. Стратегічними результатами є використання напрацювань ППП у національній та секторальних оцінках ризиків, наглядових рекомендаціях і політиці ПВК/ФТ. Системне вдосконалення має проявлятися у зменшенні обсягу низькоякісного звітування, покращенні моніторингу та більшій узгодженості очікувань ПФР, наглядових органів і суб'єктів звітування. Стан партнерства оцінюється за сталістю участі, виконанням домовленостей, збалансованістю внесків і рівнем довіри. Оцінювання повинно використовуватися для адаптації та вдосконалення, а не для покарання або рейтингування учасників.

Висновки:

- **Створення ППП необхідно починати з формалізації правової та управлінської основи.** До запуску партнерства слід визначити допустимі категорії інформації, правові підстави її передавання, правила доступу, строки зберігання, відповідальність учасників, захист добросовісного обміну та процедури реагування на витоки.
- **Діяльність партнерства має бути безпосередньо прив'язана до оцінених ризиків і вимірюваних продуктів.** Доцільно затверджувати річний або дворічний план, у якому кожному пріоритетному ризику відповідають робоча група, відповідальні учасники, строки та конкретний результат.
- **Найбільш практичною для зрілих систем є гібридна модель обміну.** Стратегічні типології та загальні індикатори можуть поширюватися серед широкого кола суб'єктів, тактичні сигнали – серед визначених секторів, а персоніфікована операційна інформація – лише через захищені канали серед уповноважених учасників.
- **ПФР має виконувати роль аналітичного інтегратора, а не одноосібного адміністратора партнерства.** Його ресурси слід спрямовувати на виявлення міжсекторальних зв'язків, формування типологій, пріоритизацію ризиків і зворотний зв'язок щодо повідомлень.

Майбутній розвиток ППП пов'язується з транскордонною співпрацею, особливо у протидії обходу санкцій, використанню віртуальних активів, кіберзумовленому шахрайству, відмиванню коштів через торгівлю та діяльності професійних мереж відмивання. Як приклад такого механізму згадується Публічно-приватне партнерство Європолу з обміну фінансовою розвідувальною інформацією (EFIPPP). Транскордонні партнерства потребують авторитетного координатора, узгодженої структури управління, належної правової основи та багаторівневого порядку доступу. Стратегічні типології можуть поширюватися серед широкого кола учасників, тактичні сигнали – у контрольованому середовищі, а високочутлива операційна інформація – через усталені канали ПФР або правоохоронних органів. Також визнається зростання ролі приватно-приватного обміну, який може допомогти поєднати

окремі фрагменти схем, виявлені різними установами, але потребує чітких правових і конфіденційних гарантій.

ПФР відводиться роль аналітичного інтегратора та довіреного посередника між приватним сектором, наглядовими й правоохоронними органами. Завдяки доступу до повідомлень різних секторів ПФР може виявляти міжінституційні зв'язки, перетворювати розрізнені дані на типології та визначати пріоритетні ризики. Його роль характеризується як primus inter pares – «перший серед рівних»: ПФР забезпечує аналітичне й координаційне спрямування, але не повинно домінувати над іншими учасниками або підміняти їхні повноваження. З огляду на обмежені ресурси ПФР його участь має зосереджуватися на функціях, у яких воно створює унікальну цінність: міжсекторальному аналізі, виявленні пов'язаних схем, пріоритизації загроз і наданні зворотного зв'язку. Адміністративне та технічне забезпечення доцільно покладати на секретаріат або інших учасників.

Загалом документ представляє публічно-приватне партнерство як інтегрований механізм управління ризиками, результативність якого визначається не кількістю зустрічей або підготовлених матеріалів, а реальним впливом на якість фінансової розвідки, виявлення й припинення злочинних схем, системи внутрішнього контролю, наглядові пріоритети та державну політику. Найбільш адаптивною є гібридна модель, що поєднує широке поширення стратегічних знань із контрольованим обміном тактичною та операційною інформацією. Вирішальними передумовами її ефективності залишаються правова визначеність, політична підтримка, чіткий розподіл ролей, захист конфіденційності, взаємність, достатня спроможність учасників і постійне оцінювання практичних результатів.

Банківське обслуговування небанківських надавачів платіжних послуг: ризики, прозорість платежів і контроль фінансових злочинів [5]

Документ Вольфсберської групи формує комплексну ризик-орієнтовану основу для управління ризиками фінансових злочинів, що виникають у відносинах між фінансовими установами та небанківськими надавачами платіжних послуг. Керівництво розвиває попередні напрацювання Вольфсберської групи у сфері кореспондентських банківських відносин і прозорості платежів, зокрема стандарти прозорості платежів 2023 року та роз'яснення щодо ролей і відповідальності учасників платіжного ланцюга 2024 року. Воно також ураховує зміни до Рекомендації 16 FATF, ухвалені в червні 2025 року з метою підвищення прозорості та безпеки транскордонних платежів шляхом забезпечення повноти й точності інформації про платника та отримувача коштів.

Під небанківськими надавачами платіжних послуг у документі розуміється широкий спектр суб'єктів, які забезпечують переказ коштів, не маючи банківської ліцензії. До них можуть належати оператори грошових переказів, сторонні платіжні процесори, фінтех-компанії та установи електронних грошей. Рекомендації також можуть використовуватися для оцінювання інших учасників платіжного ринку, зокрема надавачів послуг з ініціювання платежів та послуг з надання інформації про рахунки. Водночас керівництво не поширюється на компанії, які займаються виключно обміном готівкової валюти або переведенням чеків у готівку, технологічні компанії, що лише надають програмне забезпечення і не беруть участі в русі коштів, операції, які здійснюються на підставі банківської ліцензії, підприємства, що проводять виключно власні господарські платежі, а також суб'єктів, діяльність яких обмежується наданням послуг у сфері віртуальних або криптоактивів.

Підготовка керівництва зумовлена суттєвою трансформацією світового платіжного середовища. Небанківські надавачі платіжних послуг забезпечують швидші, дешевші та зручніші платежі, але водночас значною мірою залежать від банків та інших фінансових установ. Їм необхідні банківські рахунки, доступ до локальних і міжнародних платіжних

[5] https://db.wolfsberg-group.org/assets/354d12bd-b2db-4a39-993c-03a14ffd94a9/Wolfsberg_Guidance_NonBankPSP_2026_1.pdf

систем, можливість здійснювати розрахунки, агрегувати платежі та проводити транскордонні перекази. У результаті один платіж може проходити через кількох посередників, різні платіжні інструменти, рахунки та юрисдикції. Фінансова установа, яка обслуговує небанківського надавача, нерідко бачить лише окремий етап такого платежу й може не мати повної інформації про первинного платника, кінцевого отримувача, економічну мету операції та всіх учасників платіжного ланцюга. Ситуацію додатково ускладнює відсутність міжнародно узгоджених вимог до ліцензування, регулювання та нагляду за небанківськими надавачами, через що однакові за змістом послуги в різних країнах можуть підпадати під неоднакові нормативні вимоги.

В основу запропонованої системи покладено ризик-орієнтований підхід, забезпечення прозорості платежів і комплексне управління ризиками. Глибина належної перевірки та інтенсивність моніторингу мають визначатися з урахуванням конкретної бізнес-моделі небанківського надавача, характеру його клієнтської бази, географії діяльності, видів платіжних інструментів і структури руху коштів. Особлива роль відводиться прозорості платіжних повідомлень. Небанківський надавач, який виступає платіжним надавачем платника, повинен забезпечити внесення до платіжного повідомлення повної і точної інформації про платника та отримувача. Посередники повинні зберігати й передавати ці дані без змін, а також виявляти операції з відсутньою або неповною інформацією відповідно до законодавства відповідної юрисдикції. Фінансова установа, зі свого боку, повинна розуміти не лише формальний статус небанківського надавача, а й фактичний зміст його діяльності, склад клієнтів, рух коштів та ефективність контрольних механізмів.

Діяльність небанківських надавачів у документі умовно поділяється на три основні категорії. Перша охоплює платіжні послуги для юридичних осіб, зокрема внутрішні та транскордонні перекази, управління коштами та валютно-обмінні операції для корпорацій, малих і середніх підприємств, фінансових установ та інших небанківських надавачів полуг. Друга категорія включає перекази між фізичними особами, які можуть здійснюватися через банківські рахунки, платіжні картки, електронні гаманці, однорангові платформи або інші цифрові рішення. У межах цієї категорії важливо розрізняти повністю цифрові моделі та моделі, пов’язані з готівкою, оскільки вони характеризуються різними рівнями простежуваності коштів. Третя категорія охоплює еквайринг торговців, за якого небанківський надавач забезпечує приймання карткових та інших платежів за товари або послуги, акумулює кошти покупців і здійснює розрахунки з торговцями чи постачальниками.

Один небанківський надавач послуг може одночасно працювати за кількома моделями, пропонувати клієнтам рахунки або електронні гаманці, платіжні й валютно-обмінні платформи, фізичні та віртуальні картки. Він також може діяти від імені інших ліцензованих надавачів послуг, які, своєю чергою, обслуговують власних клієнтів. Це створює вкладені відносини, за яких банк фактично обробляє операції клієнтів, з якими не має безпосередніх відносин і щодо яких не проводив належної перевірки. Тому банку недостатньо знати загальну назву послуги: необхідно встановити, які продукти фактично пропонуються, кому вони надаються, як фінансуються, які платіжні канали використовуються, хто здійснює перевірку клієнтів і які сторони відповідають за санкційний скринінг та моніторинг операцій.

Окремо розглядається модель Banking-as-a-Service, або «банківські послуги як сервіс», за якої небанківський надавач послуг використовує власну технологічну платформу для пропонування клієнтам банківських продуктів, зокрема рахунків, кредитних послуг або випущених банком платіжних карток. Залучення клієнта, збір і зберігання ідентифікаційних даних та інформації про операції при цьому можуть здійснюватися через платформу небанківського надавача послуг. Залежність банку від даних і технологічної інфраструктури зовнішньої компанії посилює значення управління ризиками третіх сторін, контролю якості інформації та можливості банку отримати доступ до необхідних відомостей.

Іншою моделлю співпраці є спонсорований рахунок, за якого небанківський надавач послуг отримує доступ до платіжної системи, використовуючи ліцензію фінансової установи-

спонсора. Така конструкція може сприяти швидкому виходу на новий ринок, але не звільняє банк від відповідальності за діяльність, що проводиться через його рахунки. Фінансова установа повинна чітко визначити допустимі види операцій, установити межі використання рахунку, перевірити контрольне середовище небанківського надавача послуг та забезпечити постійний нагляд за відповідною діяльністю.

Важливою складовою документа є класифікація платіжних потоків на власні, платежі третіх осіб та агреговані, неттовані або пакетні платежі. Власними є операції, які небанківський надавач здійснює від свого імені, наприклад виплата заробітної плати або розрахунки з іншими фінансовими установами. Такі платежі зазвичай мають нижчий рівень ризику, оскільки банк не зазнає безпосереднього впливу діяльності клієнтів небанківського надавача. Проте деякі компанії можуть класифікувати як управління ліквідністю операції, що фактично є попереднім фінансуванням майбутніх виплат клієнтам або третім особам. Така практика здатна приховувати реальний характер платежів і створювати невраховану експозицію банку до ризиків операцій третіх осіб.

Платежі третіх осіб проводяться небанківським надавачем від імені його клієнтів. У цьому випадку банк опосередковано зазнає ризиків, пов’язаних із клієнтською базою небанківського надавача послуг, навіть не маючи прямих відносин із відповідними платниками й отримувачами. За своїм змістом такі відносини можуть бути подібними до кореспондентських банківських відносин, оскільки фінансова установа покладається на належну перевірку та контроль, які здійснює її клієнт. Тому банк повинен розуміти склад портфеля клієнтів небанківського надавача послуг, їхню географію, види діяльності та характер підтримуваних платежів. Залежно від нормативних вимог і структури операцій також може виникати необхідність відкриття окремого рахунку для захисту коштів клієнтів.

Найбільше проблем із прозорістю створюють агреговані, неттовані або пакетні платежі, коли значна кількість окремих операцій об’єднується в один, часто транскордонний, переказ. Модель «один платник – багато отримувачів», характерна, наприклад, для масової виплати заробітної плати, зазвичай має нижчий рівень ризику. Натомість моделі «багато платників – один отримувач» та особливо «багато платників – багато отримувачів» істотно ускладнюють визначення реальних сторін окремих операцій. Банк може бачити лише загальну суму агрегованого переказу, не отримуючи структурованих даних про кожного платника, отримувача та призначення відповідних платежів. Це знижує ефективність санкційного скринінгу та моніторингу підозрілої діяльності й посилює залежність банку від системи контролю небанківського надавача послуг.

До основних загроз у таких відносинах належать недостатня прозорість платежів, ризик порушення санкційних обмежень, ризик відмивання коштів і ризик шахрайства. Недостатня прозорість виникає через використання кількох платіжних каналів, інструментів, посередників та юрисдикцій, унаслідок чого банк обробляє лише окрему частину операції. Санкційний ризик пов’язаний із можливістю участі підсанкційних осіб або юрисдикцій, а також із фінансуванням операцій щодо товарів чи послуг, які підпадають під обмеження. У пакетних платежах банк може не бачити окремих сторін і тому вимушений покладатися на санкційний контроль небанківського надавача послуг, ефективність якого може залежати від якості регулювання та нагляду в його юрисдикції.

Ризик відмивання коштів посилюється, коли фінансова установа не має достатньої інформації про походження коштів, первинного платника, економічну мету операції та кінцевого отримувача. Ризик шахрайства зростає через те, що окремі небанківські надавачі не мають традиційних тривалих відносин із клієнтами та достатнього масиву історичних поведінкових даних. Фрагментація платіжного процесу між кількома учасниками може призводити до того, що жоден із них не бачить повної картини діяльності клієнта, а шахрайські операції виявляються із запізненням.

Для управління відповідними загрозами фінансовим установам рекомендовано проводити посилену перевірку небанківських надавачів послуг. Якщо один надавач послуг здійснює

кілька видів діяльності, до відносин повинні застосовуватися вимоги, що відповідають найбільш ризиковому виду послуг. Стандартні анкети доцільно доповнювати спеціально адаптованими питаннями щодо бізнес-моделі, руху коштів, платіжних коридорів, способів фінансування, клієнтських сегментів, партнерів, агентів та системи протидії фінансовим злочинам.

Належна перевірка не повинна завершуватися після встановлення ділових відносин. Ураховуючи швидкість розвитку фінтех-компаній, банки мають проводити постійне переоцінювання ризиків. Підставами для позапланового перегляду можуть бути негативна інформація, зміна власників, інциденти у сфері фінансових злочинів, зміна ліцензійного статусу, запровадження нових продуктів або платіжних потоків, залучення додаткових посередників та вихід на нові ринки.

Під час оцінювання бізнес-моделі необхідно визначити види послуг, частку транскордонних операцій, способи фінансування, наявність клієнтів-нерезидентів, використання партнерських мереж та агентів. До підвищеного ризику належать готівка, грошові перекази, передплачені картки та інші способи фінансування, які складно простежити. Транскордонні операції також розглядаються як більш ризикові через участь різних юрисдикцій, неоднакові нормативні вимоги, складнішу структуру платежів і потенційну експозицію до санкцій, корупції, шахрайства та інших фінансових злочинів.

Використання партнерів та агентів потребує чіткого розподілу обов'язків щодо ПВК, санкційного контролю та належної перевірки клієнтів. Банк має з'ясувати, хто проводить ідентифікацію та верифікацію клієнтів, хто контролює операції, здійснює санкційний скринінг, розслідує попередження та подає повідомлення про підозрілі операції. Небанківський надавач послуг повинен забезпечувати належний нагляд за агентами, особливо якщо вони безпосередньо залучають клієнтів або виконують контрольні функції, а також перевіряти необхідність їх реєстрації чи ліцензування.

Ліцензійний статус небанківського надавача послуг необхідно співвідносити з його фактичною діяльністю. Фінансова установа має перевірити, чи охоплює ліцензія всі послуги, що підтримуються банком, чи дозволяє вона здійснювати транскордонну діяльність, чи потрібні окремі дозволи у відповідних країнах та чи правомірно використовуються механізми визнання ліцензії в інших юрисдикціях. Географічне оцінювання повинно охоплювати не лише країну реєстрації небанківського надавача, а й місцезнаходження його материнської компанії, клієнтів, торговців, агентів, партнерів, інших залучених надавачів і кінцевих отримувачів коштів.

Ризик-прийнятність небанківського надавача послуг щодо клієнтів повинна узгоджуватися з ризик-апетитом фінансової установи. Якщо небанківський надавач послуг обслуговує категорії клієнтів, види діяльності або юрисдикції, які банк не готовий підтримувати, сторони повинні обмежити відповідні платіжні потоки. Якщо такого обмеження недостатньо для зменшення ризику, банк має відмовитися від установлення відносин або припинити їх.

Оцінювання системи управління ризиками фінансових злочинів має охоплювати кваліфікацію та досвід керівників комплаєнс-функції, достатність персоналу, участь вищого керівництва, порядок ескалації проблем, роботу профільних комітетів і здатність контрольної системи масштабуватися відповідно до зростання бізнесу. Необхідно аналізувати процедури ідентифікації та верифікації клієнтів, установлення кінцевих бенефіціарних власників, присвоєння рівнів ризику, періодичного оновлення даних і застосування посилених заходів до високоризикових клієнтів.

Окремої уваги потребують управління ризиками третіх сторін, оцінювання нових продуктів, використання операційних лімітів і моніторинг фактичного використання послуг. Фінансова установа повинна з'ясувати, чи застосовує небанківський надавач геолокаційний контроль, зокрема перевірку IP-адрес, для виявлення та блокування доступу з підсанкційних юрисдикцій. Перевірка систем скринінгу має охоплювати санкційні переліки, політично

значущих осіб, внутрішні контрольні списки та негативну інформацію, а також джерела даних, частоту перевірок, перелік пов'язаних осіб і порядок опрацювання потенційних збігів.

Висновки:

- **Банкам необхідно оцінювати не лише самого небанківського надавача послуг, а весь платіжний ланцюг:** реальних платників і отримувачів, партнерів, агентів, способи фінансування та всі залучені юрисдикції.
- **Для агрегованих і вкладених платежів слід встановлювати посилені вимоги до прозорості:** отримувати деталізовані дані про базові операції, перевіряти дотримання Рекомендації 16 FATF та документувати розподіл обов'язків щодо ПВК, санкційного скринінгу і моніторингу.
- **Періодична перевірка має доповнюватися моніторингом подій:** зміна власності, ліцензії, продуктів, партнерів, платіжних коридорів, обсягів операцій або поява регуляторних порушень повинні автоматично спричиняти переоцінку ризику.
- **Якщо ризик-апетит небанківського надавача послуг не узгоджується з ризик-апетитом банку, необхідно обмежити конкретні потоки або припинити відносини:** наявність ліцензії сама по собі не є достатнім підтвердженням прийнятності ризику.

Платіжний санкційний скринінг оцінюється з урахуванням рівня його автоматизації, проведення в режимі реального часу, якості використовуваних технологій, застосування нечіткого пошуку, переліку перевірюваних полів платіжного повідомлення та санкційних списків. Щодо моніторингу підозрілої діяльності банк повинен оцінювати використання ручних і автоматизованих процедур, характер сценаріїв виявлення, кількість сформованих попереджень, наявність невирішених справ, швидкість їх опрацювання, порядок ескалації та достатність ресурсів.

Використання машинного навчання і штучного інтелекту для протидії відмиванню коштів, санкційного контролю, виявлення шахрайства або проведення розслідувань потребує належного управління. Фінансова установа має встановити, чи забезпечено незалежне оцінювання відповідних моделей, їхню пояснюваність, результативність і належний нагляд, а також чи має персонал достатній рівень компетентності для контролю автоматизованих рішень.

Важливим джерелом інформації є управлінська звітність небанківського надавача послуг. Вона повинна дозволяти оцінити накопичені затримки в моніторингу операцій або оновленні даних клієнтів, невиконані рекомендації внутрішнього чи зовнішнього аудиту, результати регуляторних перевірок і стан реалізації планів усунення недоліків. Банку необхідно розуміти першопричини виявлених проблем і переконатися, що заплановані заходи не лише усувають поточні недоліки, а й знижують імовірність їх повторення.

Перевірка також повинна охоплювати механізми забезпечення повноти платіжної інформації відповідно до Рекомендації 16 FATF, системи протидії шахрайству, відстеження IP-адрес і пристроїв, виявлення підроблених документів, порядок розслідування та подання повідомлень про підозрілі операції. Додатковими компонентами системи контролю є внутрішній або зовнішній незалежний аудит, заходи протидії хабарництву та корупції, регулярне навчання працівників і комплексне оцінювання ризиків фінансових злочинів на рівні підприємства.

Під час визначення загального рівня ризику рекомендується враховувати тривалість роботи небанківського надавача послуг, його історію дотримання вимог, попередні заходи впливу з боку регуляторів і спроможність управляти ризиками в період швидкого розвитку. До новостворених компаній можуть застосовуватися частіші перегляди та додаткові заходи перевірки, включаючи отримання результатів зовнішнього аудиту. Стратегія розвитку надавача послуг також має аналізуватися наперед, оскільки запуск нових продуктів, вихід на

нові ринки та різке збільшення клієнтської бази повинні супроводжуватися пропорційним розширенням комплаєнс-функції.

Особливу роль документ відводить аналізу активності за рахунком небанківського надавача послуг. Його метою є виявлення не лише окремих підозрілих операцій, а й ширших змін у поведінці клієнта, зокрема різкого збільшення обсягів платежів, появи нових платіжних коридорів, високоризикових клієнтів або юрисдикцій, неочікуваних вкладених відносин чи погіршення прозорості платіжних повідомлень. Результати такого аналізу мають використовуватися під час періодичного перегляду ризикового профілю небанківського надавача послуг.

У додатку наведено приклади платіжних потоків різної складності. Вони охоплюють прості цифрові перекази між фізичними особами, вкладені транскордонні перекази за участю локального і глобального небанківських надавачів, еквайринг торговців, транскордонний еквайринг із залученням кількох надавачів та складну модель електронного гаманця. Остання передбачає можливість поповнення гаманця готівкою через агентську мережу, банківським переказом, платіжною карткою або з іншого електронного гаманця, а також подальше використання коштів для переказів, оплати товарів і послуг або зняття готівки. Наведені схеми демонструють, що зі збільшенням кількості посередників, платіжних інструментів, способів фінансування та юрисдикцій зменшується прозорість для банку й посилюється його залежність від системи контролю небанківського надавача послуг.

Загальний висновок документа полягає в тому, що співпраця фінансових установ із небанківськими надавачами послуг є важливою для розвитку дешевших, швидших, доступніших і безпечніших платежів, однак вона повинна ґрунтуватися на всебічному розумінні конкретної бізнес-моделі та кожного підтримуваного платіжного потоку. Наявність ліцензії або формальне проходження стандартної перевірки не є достатніми підставами для визнання ризику прийнятним. Якщо встановлені ризики неможливо належним чином зменшити, особливо в умовах обмеженої наскрізної прозорості платежів, фінансова установа повинна запровадити додаткові контрольні заходи, обмежити окремі продукти, клієнтські категорії чи платіжні коридори або відмовитися від установлення чи продовження відповідних ділових відносин.

Штучний інтелект і відкриті фінанси: нові можливості, ризики та регуляторні компроміси [6]

Аналітичний документ ОЕСР досліджує взаємозв’язок між двома ключовими напрямами цифрової трансформації фінансового сектору – впровадженням штучного інтелекту та розвитком механізмів обміну фінансовими даними. Автори наголошують, що поєднання цих технологій створює нові можливості для підвищення ефективності, персоналізації фінансових послуг, розвитку конкуренції та фінансової інклюзії, але водночас посилює ризики, пов’язані із захистом персональних даних, дискримінацією, непрозорістю автоматизованих рішень, кібербезпекою, ринковою концентрацією та визначенням відповідальності. Метою документа є встановлення умов, за яких штучний інтелект може безпечно, відповідально та масштабовано застосовуватися в екосистемах відкритих фінансів.

Відкриті фінанси визначаються як система надання доступу до фінансових даних клієнтів, їх передачі та повторного використання різними постачальниками фінансових послуг через захищені цифрові канали та за згодою клієнта. Ця концепція розширює відкритий банкінг, оскільки охоплює не лише платіжні рахунки, а й заощадження, кредити, пенсійне забезпечення, страхування та інвестиції. У перспективі до відповідної системи можуть бути включені нефінансові відомості, зокрема дані про оплату комунальних послуг, використання

[6] https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/07/artificial-intelligence-and-open-finance_409e7c69/eb511c3c-en.pdf

телекомунікаційних сервісів та операції електронної комерції. У результаті відкриті фінанси можуть забезпечувати доступ до комплексного цифрового фінансового профілю особи або підприємства.

Спільною основою відкритих фінансів і штучного інтелекту є дані. Відкриті фінанси створюють інфраструктуру для їх захищеного й стандартизованого обміну, тоді як штучний інтелект забезпечує інструменти для аналізу та перетворення цих даних на практично корисні висновки. Взаємозв'язок має двосторонній характер: відкриті фінанси надають моделям ширші, різноманітніші й актуальніші набори інформації, а штучний інтелект допомагає очищувати, структурувати, узгоджувати та аналізувати отримані дані. Якість результатів залежить не лише від їх обсягу, а й від актуальності, репрезентативності, унікальності та відповідності конкретному сценарію використання. Синтетичні дані можуть доповнювати реальні, однак моделі, навчені виключно на синтетичних наборах, можуть бути менш стійкими до реальних умов і маніпулятивного впливу.

Однією з основних переваг такого поєднання є можливість гіперперсоналізації фінансових продуктів і послуг. Отримуючи доступ до інформації про доходи, витрати, боргові зобов'язання, заощадження, інвестиції та фінансові цілі клієнта, моделі штучного інтелекту можуть формувати точніші рекомендації щодо інвестування, накопичення, управління боргами, страхування або пенсійного планування. Використання даних, які оновлюються в режимі реального часу, дає змогу автоматизованим консультантам адаптувати рекомендації до поточного фінансового становища та потреб конкретної особи.

Значний потенціал ОЕСР пов'язує з розширенням фінансової інклюзії. Традиційні системи кредитного скорингу не завжди можуть належно оцінити осіб або малі та середні підприємства, які не мають тривалої кредитної історії чи достатнього забезпечення. Аналіз ширшого кола фінансових і нефінансових даних може сформувати повніше уявлення про їхню платоспроможність і розширити доступ до кредитування. Водночас збільшення кількості даних саме собою не гарантує справедливого результату: якщо інформація є нерепрезентативною або відображає історичну нерівність, модель може відтворювати чи посилювати дискримінаційні практики.

Штучний інтелект також може сприяти розвитку конкуренції та інновацій. Зменшення інформаційної асиметрії між традиційними фінансовими установами й новими учасниками ринку знижує бар'єри для фінтех-компаній та інших постачальників послуг. Це створює умови для розвитку агрегаторів рахунків, платформ управління особистими фінансами, автоматизованих консультантів і віртуальних помічників. На операційному рівні штучний інтелект може автоматизувати введення, перевірку, звіряння та перетворення даних, виявляти невідповідності й приводити інформацію з різних джерел до уніфікованих форматів. У результаті краще структуровані дані підвищують якість моделей, а штучний інтелект, своєю чергою, покращує якість та сумісність даних у системі відкритих фінансів.

Важливу роль у цьому процесі відіграють інтерфейси прикладного програмування, які забезпечують безперервний обмін інформацією між учасниками фінансової екосистеми. Оновлення даних у режимі реального часу є особливо важливим для систем виявлення шахрайства, оперативного оцінювання ризиків, контролю платежів і моніторингу фінансового стану клієнтів. Водночас технічної інфраструктури недостатньо – необхідне управління даними, пристосоване до використання штучного інтелекту. Воно має охоплювати машиночитані стандарти, простежуваність походження даних, версійність, відтворюваність результатів, безперервний моніторинг, аудиторські журнали та контроль не лише первинної інформації, а й похідних об'єктів, створених моделями.

Як приклад такого підходу наведено Банк Кореї, який перетворив понад 1,4 млн внутрішніх документів і публічних звітів на стандартизований формат JSON. Загалом первинне оброблення охопило приблизно 3 млн документів, після чого було усунуто дублювання та відфільтровано персональні дані. Банк також розробив інституційну онтологію, яка встановлює зв'язки між підрозділами, документами, наборами даних і рівнями їх захисту. Це

дозволяє відстежувати походження інформації та визначати, хто, як і для яких цілей її використовує.

Практичний потенціал відкритих фінансів показано на прикладі Бразилії. Основними чинниками розвитку бразильської моделі стали обов'язкова участь фінансових установ і небанківських фінансових посередників, взаємність обміну даними, участь приватного сектору у формуванні стандартів кібербезпеки та широкий спектр сценаріїв використання. Наприкінці 2024 року понад 60 млн осіб у Бразилії надали дозвіл на передачу своїх даних. Центральний банк країни визначив 139 сценаріїв використання відкритих фінансів, із яких 90 стосувалися обміну даними, а 49 – ініціювання платежів. У першій половині 2025 року близько 35 млн клієнтів користувалися рішеннями, які об'єднували інформацію про рахунки, картки та інвестиції. Завдяки передачі даних середній час відкриття рахунку скоротився з 32 годин до 2 годин 10 хвилин. Відкриті фінанси також сприяли персоналізації кредитних та інвестиційних пропозицій, автоматизації платежів і розвитку інструментів управління фінансами підприємств.

Поряд із перевагами поєднання відкритих фінансів і штучного інтелекту посилює ризики, властиві обом сферам. Одним із них є надмірна залежність споживачів від автоматизованих рекомендацій. Клієнти можуть не розуміти обмежень або методології моделі, але сприймати її висновки як об'єктивні й безпомилкові. Особливо небезпечним це є під час використання складних інвестиційних продуктів. Поширення автоматизованих інтерфейсів і чат-ботів також може поглибити цифрове виключення літніх людей, населення сільських територій та осіб із низьким рівнем фінансової або цифрової грамотності, особливо якщо доступ до підтримки з боку людини скорочується.

Важливою проблемою є ризик упередженості та дискримінації. Моделі можуть відтворювати закономірності, закладені в історичних даних, або визначати захищені характеристики особи за непрямими показниками. Особи з обмеженим цифровим слідом або ті, які відмовилися від передачі інформації, можуть оцінюватися як більш ризикові та отримувати менш вигідні умови. У страхуванні це може проявлятися як «премія за приватність», коли клієнт сплачує більше через небажання надавати детальні дані. Обмежена пояснюваність складних моделей ускладнює виявлення дискримінаційних результатів і надання зрозумілого обґрунтування таких рішень, як відмова у кредиті або страховому покритті.

Ще одним ризиком є використання даних поза первинною метою, для якої клієнт надав згоду. Наприклад, інформація, отримана для оцінювання кредитоспроможності, може надалі застосовуватися для маркетингового профілювання. Ітеративний характер розроблення моделей ускладнює контроль, оскільки дані можуть повторно використовуватися в наступних циклах навчання та доопрацювання системи. Тому принципи обмеження мети, мінімізації даних, конфіденційності за проєктуванням, підзвітності та обмеження строків зберігання мають бути вбудовані в архітектуру відповідних систем. Практичним інструментом можуть стати інформаційні панелі управління згодою, через які користувачі зможуть переглядати, змінювати або відкликати надані дозволи.

Розширення обміну фінансовою інформацією також збільшує ризики витоків і кібератак. У відкритій екосистемі дані передаються між багатьма установами та постачальниками, що розширює поверхню потенційних атак. Порушення безпеки може розкрити комплексний фінансовий профіль особи та сприяти персоналізованому шахрайству або створенню синтетичних ідентичностей. Для зменшення таких ризиків можуть застосовуватися федеративна аналітика, оброблення зашифрованих даних, диференційна приватність і докази з нульовим розголошенням. Водночас технічні рішення не можуть замінити належного правового та організаційного контролю.

Документ також визначає низку регуляторних компромісів. Прагнення використовувати більші обсяги інформації для підвищення точності моделей може суперечити принципу мінімізації даних. Отримання нової згоди на кожному етапі оброблення може ускладнювати масштабування моделей, тоді як надто широка згода послаблює контроль споживача. Вимоги

щодо локалізації даних посилюють національний нагляд, але одночасно підвищують витрати, обмежують транскордонний обмін і можуть знижувати якість моделей. Передача інфраструктури зовнішнім постачальникам скорочує частину витрат, проте створює залежність від третіх сторін і ризики недостатнього контролю за обробленням інформації.

Окрему увагу приділено великим технологічним компаніям. Вони вже володіють значними масивами поведінкових, комерційних і транзакційних даних, тому доступ до фінансової інформації може додатково посилити їхню конкурентну перевагу. Особливо проблемними є системи без взаємності, у яких фінансові установи зобов'язані передавати дані технологічним компаніям, але не отримують еквівалентного доступу до їхньої інформації. Водночас повне виключення таких компаній із відкритих фінансів може послабити конкуренцію та інновації. ОЕСР підтримує збалансований підхід, заснований на взаємності, рівних конкурентних умовах, контролі концентрації, належній перевірці постачальників, аудиторських правах і наявності стратегій їх заміни.

Окрема частина документа присвячена теоретичному сценарію поширення агентного штучного інтелекту – систем, здатних самостійно планувати, виконувати й коригувати дії та взаємодіяти із зовнішніми інструментами. У поєднанні з даними відкритих фінансів такі системи могли б перейти від реактивного обслуговування до проактивного управління фінансами: виявляти надлишок коштів, пропонувати погашення заборгованості, коригувати інвестиційні портфелі, прогнозувати майбутні потреби та управляти ліквідністю підприємств.

Висновки:

- **Необхідно інтегрувати управління даними та моделями штучного інтелекту.** Фінансовим установам необхідно забезпечити простежуваність походження, передачі, трансформації та повторного використання даних, документувати версії моделей, проводити перевірки на упередженість і зберігати аудиторські журнали рішень.
- **Доцільно забезпечити реальний контроль споживача.** Згода має бути конкретною, усвідомленою та керованою. Рішення з істотними фінансовими наслідками повинні супроводжуватися зрозумілим поясненням, можливістю оскарження і доступом до людського розгляду.
- **Потрібно управляти ризиками технологічної концентрації.** Участь великих технологічних і хмарних постачальників доцільно регулювати на основі взаємності доступу до даних, належної перевірки, аудиторських прав, постійного моніторингу, оцінювання концентрації та реалістичних стратегій заміни або виходу.
- **Необхідно проводити міжвідомче та міжнародне оцінювання екосистем відкритих фінансів.** Фінансовим регуляторам, органам із захисту даних і конкурентним органам необхідно спільно перевірити чинні механізми обміну даними на сумісність із використанням штучного інтелекту, визначити прогалини у відповідальності та сформувати пропорційні ризик-орієнтовані вимоги.

Проте повністю автономні фінансові агенти поки залишаються експериментальною технологією. Їх поширення ускладнює визначення відповідальності між розробником, постачальником, фінансовою установою та користувачем. Існують ризики невідповідності цілей системи інтересам клієнта, поступового розширення її повноважень, неправомірного використання даних і втрати людського контролю. Масове одночасне виконання автоматизованих операцій також може впливати на ліквідність установ і створювати системні наслідки. Тому рішення, що істотно впливають на права та фінансовий стан клієнтів, повинні залишатися зрозумілими, оскаржуваними й виправними, а людський контроль – центральним елементом управління.

У підсумку ОЕСР наголошує на необхідності узгодити системи управління відкритими фінансами та штучним інтелектом на основі пропорційного ризик-орієнтованого підходу. Необхідними елементами є чіткий розподіл відповідальності, механізми відшкодування шкоди й оскарження рішень, контроль упередженості, пояснюваність моделей, простежуваність використання даних, належна кібербезпека та усвідомлена згода клієнтів. Автори рекомендують посилити співпрацю між фінансовими регуляторами, органами захисту персональних даних, конкурентними органами та установами, відповідальними за політику у сфері штучного інтелекту. Загальний висновок документа полягає в тому, що переваги поєднання штучного інтелекту й відкритих фінансів можуть бути реалізовані лише за наявності довіри, надійного управління, ефективного нагляду та збереження людської відповідальності за фінансові рішення.

Злочинна екосистема Південно-Східної Азії: нові масштаби та механізми транснаціональної організованої злочинності [7]

Доповідь Управління ООН з наркотиків і злочинності (УНЗ ООН) аналізує трансформацію регіонального злочинного середовища після попередньої оцінки 2019 року. Центральна теза документа полягає в тому, що організовану злочинність більше не можна розглядати як сукупність відокремлених ринків. Незаконний обіг наркотиків, шахрайство з використанням кіберзасобів, незаконні онлайн-азартні ігри, торгівля людьми, злочини проти довкілля, контрабанда тютюнових виробів і зброї функціонують у межах спільної фінансової, цифрової та логістичної інфраструктури. Одні й ті самі мережі використовують спільні маршрути, компанії, професійних сприячів злочинної діяльності, корупційні зв'язки й механізми відмивання коштів, унаслідок чого Південно-Східна Азія перетворилася на один із ключових центрів глобальної транснаціональної злочинності.

Дослідження охоплює держави – члени АСЕАН (Асоціації держав Південно-Східної Азії) та пов'язані з ними країни Східної і Південної Азії та Океанії. Воно ґрунтується на офіційних даних правоохоронних, митних, фінансових і регуляторних органів, статистиці вилучень, матеріалах кримінальних проваджень, фінансовій розвідувальній інформації, базах УНЗ ООН, академічних дослідженнях і перевірених відкритих джерелах. Для оцінювання збитків від шахрайства враховувався значний рівень неповідомлення про такі злочини, а вартість наркоринків визначалася на основі даних про поширеність споживання, ціни, чистоту речовин, вилучення та результати аналізу стічних вод. Водночас наведені показники є орієнтовними, оскільки приховані злочинні ринки неможливо виміряти з абсолютною точністю.

Основною структурною зміною став перехід від локальних угруповань до технологічно розвинених і географічно розподілених мереж. Їхні керівники, виконавці, цифрова інфраструктура, фінансові потоки та активи розміщуються у різних юрисдикціях, що зменшує ефективність окремих національних операцій. Злочинні організації дедалі більше працюють за моделлю «злочинність як послуга», пропонуючи відмивання коштів, конвертацію криптоактивів, підроблення документів, постачання шкідливого програмного забезпечення, продаж викрадених даних, організацію перевезень, вербування людей і корупційний захист.

УНЗ ООН виділяє чотири рівні злочинної організації. Перший становлять керівники, які приховують активи через корпоративні структури, номінальних власників і декілька юрисдикцій. Другий охоплює оперативних координаторів, відповідальних за логістику, фінансові потоки та корупційні домовленості. Третій складається з виконавців – вербувальників, кур'єрів, грошових мулів, технічних фахівців та осіб, примусово залучених до злочинної діяльності. Четвертий рівень утворюють професійні та інші сприячі: юристи, бухгалтери, оператори підпільних банківських систем, конвертери криптоактивів, постачальники технологій, корумповані посадовці й недержавні збройні формування. Такі

[7] https://www.unodc.org/roseap/uploads/documents/Publications/2026/TOCTA_South-East_Asia_2026.pdf

сприячі часто обслуговують декілька злочинних організацій, тому їх виявлення може мати більший системний ефект, ніж затримання окремих виконавців.

Важливим поняттям документа є «злочинні прямі іноземні інвестиції» – вкладення коштів злочинного походження у нерухомість, казино, готельні комплекси, платіжні установи, цифрові платформи та підприємства у спеціальних економічних зонах. Такі інвестиції забезпечують відмивання коштів, корпоративне прикриття, політичний вплив і доступ до місцевої інфраструктури. Доходи переміщуються через компанії-оболонки, номінальних директорів, грошові мули, підпільні банківські мережі та криптоактиви, після чого інтегруються в легальну економіку. Додаткові можливості для приховування особи, активів і бенефіціарного контролю можуть створювати програми громадянства за інвестиції.

Корупція розглядається як структурна умова існування злочинної екосистеми. Вона охоплює прикордонний і митний контроль, міграційні процедури, ліцензування казино, реєстрацію компаній, нагляд за інвестиціями та спеціальними економічними зонами, доступ до правоохоронних баз і втручання у кримінальні провадження. Поєднання слабкого місцевого управління, непрозорого інвестування, обмеженого контролю бенефіціарної власності та недостатньої присутності держави дозволяє окремим прикордонним територіям і спеціальним економічним зонам перетворюватися на захищені осередки злочинної діяльності.

Золотий трикутник залишається основним регіональним центром виробництва наркотиків. Сукупна річна роздрібна вартість ринків метамфетаміну, героїну та кетаміну, пов'язаних із постачанням із Південно-Східної Азії, оцінюється у 75–109,7 млрд доларів США. Метамфетамін формує приблизно 70 % цього обсягу – 48,1–74,8 млрд доларів. Попри рекордні вилучення, зниження цін і збереження високої чистоти речовини свідчать про надзвичайно значну пропозицію. Ринок кетаміну оцінено у 2,7–7,2 млрд доларів, а його вилучення у 2025 році досягли рекордних 52,5 тонни у Східній і Південно-Східній Азії. Паралельно відновлюється опіатна економіка: виробництво опію в М'янмі у 2025 році оцінено в 1 010 тонн, а його національна економічна вартість – у 641 млн–1,05 млрд доларів.

Найсуттєвішою новою загрозою автори називають індустріалізацію шахрайства з використанням кіберзасобів. Великі шахрайські центри у прикордонних районах і спеціальних економічних зонах Камбоджі, Лаоської Народно-Демократичної Республіки та М'янми функціонують як повноцінні злочинні підприємства з технічним персоналом, вербувальниками, охороною, фінансовими підрозділами та міжнародними каналами відмивання коштів. Сукупні збитки від шахрайства у Східній і Південно-Східній Азії, Австралії та Новій Зеландії у 2025 році оцінюються у 88,3–114,1 млрд доларів. Закриття окремих комплексів переважно призводить до переміщення операторів, оскільки без одночасного переслідування керівників, фінансистів, професійних сприячів і каналів відмивання коштів злочинна інфраструктура швидко відновлюється.

Криптоактиви, зокрема USDT у мережі TRON (блокчейн-платформі, що використовується, зокрема, для швидких переказів криптоактивів із порівняно низькими комісіями), забезпечують швидкі транскордонні розрахунки поза традиційною банківською системою. Зашифровані платформи використовуються для комунікації та функціонування незаконних ринків, генеративний штучний інтелект – для автоматизації шахрайства, створення переконливого контенту різними мовами та синтезу голосу й відео, а супутниковий інтернет дозволяє злочинним центрам діяти у віддалених районах. Поширюється також продаж конфіденційних відомостей про пересування людей, готельні записи та інформацію з правоохоронних баз, що допомагає злочинцям контролювати потерпілих і уникати затримання.

Незаконні онлайн-азартні ігри та шахрайство розглядаються як взаємопов'язані етапи спільного злочинного бізнесу. Після обмеження діяльності офшорних грального операторів частина казино, готелів, технічних платформ і платіжних мереж була переорієнтована на шахрайські операції. Глобальний оборот незаконних ставок оцінюється у 340 млрд–1,7 трлн

доларів на рік. У 2025 році китайськомовні мережі з відмивання коштів провели через 1 799 активних криптогаманців приблизно 16,1 млрд доларів незаконних коштів.

Висновки:

- **Необхідно зосередити зусилля не лише на розкритті окремих злочинів, а й на ліквідації фінансової, цифрової та організаційної інфраструктури, яка забезпечує діяльність злочинних мереж.** Правоохоронним органам і підрозділам фінансової розвідки необхідно спільно встановлювати організаторів, фінансистів, фахівців, які сприяють діяльності злочинних мереж, корупційні зв'язки, корпоративні структури та цифрові платформи, що одночасно обслуговують кілька злочинних ринків.
- **Паралельне фінансове розслідування доцільно зробити стандартною процедурою.** Від початку кожного значного розслідування слід відстежувати стейблкоїни й інші криптоактиви, мережі грошових мулів, неформальні перекази, компанії-оболонки, номінальних власників, нерухомість і транскордонні інвестиції з подальшим арештом, конфіскацією та поверненням активів.
- **Необхідно закрити системні зони вразливості.** Пріоритетними заходами мають стати перевірка бенефіціарної власності та джерел інвестицій, посилений нагляд за казино, спеціальними економічними зонами й прикордонними анклавами, а також незалежний антикорупційний контроль органів ліцензування, митниці, міграційних і правоохоронних органів.
- **Доцільно створити технологічно спроможну та скоординовану систему реагування.** Державам необхідні сумісні інформаційні системи, єдині аналітичні стандарти, захищені канали обміну даними, блокчейн-аналітика, цифрова криміналістика та механізми співпраці з фінансовим і технологічним сектором.

Торгівля людьми дедалі частіше здійснюється з метою примусового залучення потерпілих до шахрайства. У злочинних центрах регіону Меконгу виявлено осіб щонайменше з 80 країн і територій. Це ускладнює розмежування між професійними учасниками злочинних мереж та людьми, яких примусили вчиняти правопорушення. Тому УНЗ ООН наголошує на необхідності системної ідентифікації потерпілих і їх перенаправлення до механізмів захисту, а не автоматичного кримінального переслідування. Онлайн-експлуатація дітей також пов'язана із шахрайськими центрами, незаконними платформами, криптоактивами та неформальними системами передавання коштів або їхнього економічного еквівалента, що потребує спеціалізованої цифрової криміналістики й співпраці з технологічними компаніями.

Злочини проти довкілля охоплюють незаконну торгівлю об'єктами дикої природи, мінеральними ресурсами, електронними та іншими відходами. Вони часто вбудовані у легальні торговельні ланцюги, а соціальні мережі та інтенсивні морські перевезення спрощують продаж і переміщення незаконних товарів. Контрабанда тютюнових виробів щороку генерує мільярдні доходи, частина яких може надходити недержавним збройним формуванням. Незаконний обіг зброї, своєю чергою, посилює можливості злочинних організацій контролювати території, персонал і потерпілих.

Важливим транзитним районом є морський трикутник Сулу–Селебес між Індонезією, Малайзією та Філіппінами. Інтенсивний законний рух суден дозволяє приховувати перевезення наркотиків, зброї, об'єктів дикої природи та потерпілих від торгівлі людьми. Злочинці використовують супутниковий зв'язок, безпілотні апарати, системи відстеження суден, рахунки підставних осіб і криптоактиви, а їхні фінансові операції перетинаються з інфраструктурою незаконних азартних ігор та шахрайських центрів.

У підсумку УНЗ ООН закликає перейти від протидії окремим злочинам до системного руйнування спільної злочинної інфраструктури. Для цього необхідно гармонізувати законодавство, розвивати розслідування на основі розвідувальної інформації та проводити паралельні фінансові розслідування від початку кримінального провадження. Особливу увагу слід приділяти керівникам, фінансистам, фахівцям, які сприяють діяльності злочинних мереж, корупційним зв'язкам, криптоактивам, компаніям-оболонкам, нерухомості та іншим активам. Документ також рекомендує підвищити прозорість бенефіціарної власності, посилити контроль іноземних інвестицій і спеціальних економічних зон, удосконалити цифрову криміналістику та блокчейн-аналітику, а також забезпечити постійний міжнародний обмін інформацією і належний захист потерпілих.

Звіти окремих інституцій та експертів

Цифровий слід: як журналісти розслідують криптовалютні схеми [8]

Криптовалюти стали невід'ємною частиною сучасної фінансової системи, але разом із легітимними транзакціями вони відкрили широкі можливості для злочинців, корупціонерів та шахраїв, які використовують їх для анонімного переміщення коштів через кордони, оминаючи традиційну банківську систему. За даними ФБР, лише у Сполучених Штатах річні збитки від криптовалютних злочинів сягають сотень мільйонів доларів, що робить розслідування криптовалютних транзакцій критично важливим інструментом для сучасної журналістики, спрямованої на підзвітність влади та бізнесу.

У 2025 році Міжнародний консорціум журналістів-розслідувачів (ICIJ) очолив масштабне розслідування "Coin Laundry", присвячене "брудним" грошам у криптовалюті. Цей проєкт виявив чотири ключові складові успіху в аналізі блокчейну для журналістів. По-перше, дослідники здобули базові знання про використання загальнодоступних інструментів аналізу криптовалют для отримання попередніх результатів. По-друге, вони навчилися знаходити криптовалютні адреси. По-третє, команда здебільшого обійшла стороною великі аналітичні фірми, натомість залучивши десятки незалежних експертів із відстеження криптовалют, які допомогли підтвердити та розширити попередні висновки. По-четверте, журналісти опанували методику отримання масивів даних через API від Arkham Intelligence та Tronscan – двох безкоштовних інструментів для дослідження блокчейну, що дозволило аналізувати криптовалютні транзакції у великих масштабах.

Блокчейн є децентралізованим розподіленим цифровим реєстром, який зберігає інформацію в комп'ютерній мережі та зазвичай містить повну історію транзакцій. Криптоактиви існують виключно в цифровому просторі й використовуються для торгівлі, інвестицій та придбання товарів. Дані про транзакції зберігаються у файлах, відомих як "блоки", які хронологічно додаються до "ланцюга", утворюючи блокчейн. Існують різні види криптовалют: біткоїн (BTC), ефіріум (ETH), тезер (USDT) тощо. Деякі з них, як-от біткоїн, функціонують лише у власному блокчейні, тоді як інші, наприклад тезер, можуть працювати на кількох блокчейнах одночасно. Коли журналіст розслідує криптовалютні операції, він обов'язково має перевірити, яку саме криптовалюту було використано та на якому блокчейні відбулася транзакція, оскільки це критично важливо для конвертації вартості у традиційні валюти, особливо враховуючи високу волатильність багатьох криптоактивів.

Центральне місце в розумінні криптовалютних розслідувань займають так звані гаманці – цифрові інструменти для зберігання та управління криптоактивами. Користувачі можуть отримати гаманець через реєстрацію на біржі, яка контролює його від імені клієнта, або створити самокерований гаманець, доступ до якого має лише власник. Такі гаманці мають публічні та приватні ключі. Публічний ключ подібний до номера банківського рахунку – він видимий у даних транзакцій, записаних у блокчейні, і саме цей рядок літер та цифр

[8] https://gijn.org/resource/reporters-guide-to-investigating-cryptocurrency/

використовується в санкційних списках. Приватний ключ, натомість, схожий на пароль і залишається невидимим, оскільки той, хто ним володіє, фактично контролює пов'язану з ним криптовалюту.

Журналісти можуть знаходити криптовалютні адреси в різноманітних джерелах: поліцейських звітах, судових документах, санкційних списках, скаргах до фінансових регуляторів, а також через спілкування з жертвами шахрайства або їхніми адвокатами, які часто мають виписки про транзакції із зазначенням адреси, на яку було надіслано криптовалюту жертви. Криптокористувачі можуть публікувати свої адреси в соціальних мережах для збору коштів, і це ще один спосіб пов'язати криптоактивність із незаконними коштами – прикладом є адреси, використані для підтримки війни росії проти України. Також адреси можна отримати при конвертації готівки в криптовалюту через спеціалізовані пункти обміну.

У розслідуванні "Coin Laundry" ICIJ досліджував транзакції між централізованими біржами та компанією Huione Group з Камбоджі, яку американська влада звинуватила в переміщенні коштів для операторів скам-центрів та північнокорейських хакерів. Адреси Huione було знайдено у китайськомовних квартальних фінансових звітах компанії. Централізовані біржі – це торговельні платформи, які використовують власні гаманці для збору та об'єднання депозитів користувачів. Багато з цих гаманців публічно ідентифіковані біржами в періодичних звітах про резерви, і блокчейн-експлорери позначають такі гаманці як власність бірж. Це допомогло журналістам перевірити приналежність гаманців і проаналізувати транзакції між адресами біржових гаманців та зібраними адресами, пов'язаними зі злочинністю.

Важливим аспектом методології стало зосередження на вхідних потоках – транзакціях, спрямованих до рахунків централізованих бірж, а не на вихідних. Цей вибір був зумовлений тим, що вхідні та вихідні потоки необхідно кількісно оцінювати окремо, оскільки діяльність усередині централізованих бірж відбувається поза ланцюгом, у так званому off-chain просторі, і не видима в блокчейн-записах. Усередині біржі криптовалюта з різних джерел може змішуватися, тому неможливо зробити остаточні висновки про вихідні потоки на основі вхідних. Кожна транзакція має відправника та отримувача, і ключове завдання розслідувача – з'ясувати, хто вони, та перевірити свої висновки за допомогою експертів.

ICIJ значною мірою покладався на безкоштовний блокчейн-експлорер Arkham Intelligence, навчаючи партнерів користуватися цим інструментом. Процес базового відстеження криптовалют включає кілька кроків: ідентифікацію адреси гаманця, вибір сукупності транзакцій для аналізу (наприклад, адреси отримувачів або адреси відправників), фокусування на релевантному для історії періоді, вибір напрямку потоку (вхідний або вихідний), увагу до уникнення дублювання сум та описування лише обсягу надісланого або отриманого за певний період, а також обов'язкову перевірку результатів із незалежним експертом.

Блокчейн-експлорери часто ідентифікують власників адрес, але ця інформація не завжди надійна – наприклад, у одному з розслідувань адреса, позначена як власність біржі HTX, фактично використовувалася іншою біржею Kyrrex. Тому завжди необхідно залучати експерта для верифікації отриманих даних і ретельно добирати формулювання для опису транзакційної активності. Важливо також з обережністю ставитися до статистичних даних, які публікують великі криптоаналітичні платформи на кшталт Chainalysis та TRM Labs, оскільки в міру виявлення нових адрес, пов'язаних із санкціями, шахрайством або відмиванням грошей, до підрахунків додається новий транзакційний обсяг, тому не слід безпосередньо порівнювати новий звіт із результатами попереднього року, а краще пояснювати, що йдеться про мінімальну оцінку, яка, ймовірно, зростатиме.

Окремої уваги заслуговує робота з жертвами шахрайства, що потребує терпіння та розуміння – постраждалі можуть відчувати сором або збентеження через те, що їх ошукали, і не бажати розголосу. Деякі з них після першого шахрайства зверталися до приватних детективів або фірм, які обіцяли повернути вкрадені кошти, але ставали жертвами повторного шахрайства. Жертви часто плутаються в послідовності подій, оскільки шахрайські схеми можуть тривати місяцями, протягом яких їх переконують, що гроші вкладаються в законні інвестиції.

Створення хронології допомагає журналістам розплутати ланцюг подій і надати важливий контекст для аналізу активності криптогаманця. Жертви часто зберігають детальні записи про діяльність шахраїв, зокрема криптовалютні адреси, використані зловмисниками, які можна знайти в повідомленнях, електронних листах та інших документах. Деякі з них мають квитанції про транзакції, здійснені через криптомати, або скріншоти застосунків, які також містять адреси гаманців. У деяких випадках вони мають звіти про відстеження, підготовлені експертами в межах судових проваджень, що допомагає перехресно перевірити висновки.

ICIJ також виявив криптовалютні адреси через запити на публічну інформацію. Багато юрисдикцій за замовчуванням вилучають такі адреси з публічних документів, але не всі. Наприклад, штат Флорида, як виявилося, дозволяє розкривати повні криптовалютні адреси в публічних записах, і ICIJ отримав адреси в скаргах споживачів та поліцейських звітах саме з цього штату.

У процесі розслідування ICIJ викрив глобальну мережу так званих касових пунктів (cash desks) та кур'єрських служб, які дозволяють анонімно виводити величезні суми криптовалюти в готівку поза контролем фінансових регуляторів та правоохоронних органів. Поліція та прокуратура повідомили, що ці сервіси значно ускладнюють відстеження або повернення вкрадених коштів, оскільки вони часто використовують невідомі владі адреси гаманців, і слід у блокчейні зникає. Журналіст ICIJ інтегрувався з незалежним дослідником Річардом Сандерсом, який подорожує світом, збираючи розвіддані про ці вразливі для зловживань криптосервіси. Сандерс обмінює криптовалюту в касах по всьому світу, щоб збирати адреси гаманців для правоохоронних органів. Журналісти також можуть отримувати цифрові квитанції з криптоадресами, здійснюючи особисті транзакції.

Для дослідження криптоматів корисним ресурсом є вебсайт Coin ATM Radar, який містить фізичні адреси терміналів у США та інших країнах. ICIJ використав скрейпінг цього сайту для отримання адрес компанії Bitcoin Depot. Журналісти можуть використовувати Coin ATM Radar для пошуку магазинів із криптоматами, зв'язуватися з власниками телефоном або відвідувати їх особисто. У досвіді ICIJ власники та менеджери магазинів часто охоче обговорювали проблеми, пов'язані з цими терміналами. Для пошуку жертв шахрайства з криптоматами корисними ресурсами є федеральні та місцеві судові записи США, зокрема архів CourtListener, де можна шукати за назвою компанії, а також Docket Alarm для справ на рівні штатів. Цивільні позови часто містять набагато більше інформації, зокрема імена жертв, і адвокати в таких справах часто охоче діляться знаннями, включаючи адреси гаманців. Запити про публічну інформацію до агентств із захисту прав споживачів можуть надати безліч скарг на конкретні компанії, включаючи інформацію про гаманці та деталі того, як компанії реагували на скарги.

Великі аналітичні фірми, такі як Chainalysis і Elliptic, іноді надають провідним виданням звіти, що описують незаконні потоки коштів, але ці фірми зазвичай дуже зайняті й мають безліч міркувань, які слід враховувати. Тому ICIJ обрав інший шлях – культивування стосунків з окремими експертами з відстеження криптовалют, які могли розширити висновки та перевірити їх. Оскільки блокчейн є загальнодоступним, журналісти могли залучити кількох експертів для відтворення та перевірки результатів.

Комплаєнс-офіцери та колишні працівники криптокомпаній, які бачили процес зсередини, часто мотивовані розповідати про проблеми, з якими вони стикалися. LinkedIn є найкращим ресурсом для виявлення колишніх співробітників, але їхні імена можна знайти також у Facebook, Twitter (X), корпоративних документах та прес-релізах. Особливо цінними виявилися академічні експерти, які зіграли ключову роль у розслідуванні діяльності Володимира Охотнікова, звинуваченого у фінансових шахрайствах та створенні пірамід. Експерти проаналізували смарт-контракти, що лежать в основі його платформи Meta Whale, і виявили схожість із Forsage – криптоплатформою, яка була центром звинувачень у США. Розслідування також спиралося на криптотранзакції, судові документи з Грузії та інших країн, банківські записи та корпоративні документи компаній, використаних Охотніковим.

Технологія блокчейн створює терабайти даних, які потребують значної обчислювальної потужності для обробки, і відстеження криптотранзакцій може швидко стати непосильним завданням. Для проєкту "Coin Laundry" ICIJ зосередився на діяльності трьох гаманців, пов'язаних із Huione Group, на блокчейні TRON, аналізуючи суми, надіслані в тезері (USDT) – стейблкоїні, вартість якого прив'язана до долара США, що значно спрощує обчислення вартості. Аналіз охоплював період із листопада 2023 по липень 2025 року для біржі Binance та з лютого по липень 2025 для OKX. У випадку Binance аналізована активність відбулася після визнання компанією провини в 2023 році та сплати штрафу в розмірі 4 мільярдів доларів за те, що тодішня міністр фінансів США Джанет Єллен назвала "умисними порушеннями, які дозволили грошам надходити до терористів, кіберзлочинців і осіб, які вчиняють насильство над дітьми".

Висновки:

- **Блокчейн є водночас інструментом анонімності та слідства**: хоча криптовалюти дозволяють приховувати особистість користувачів, кожна транзакція назавжди записується в публічний реєстр.
- **Ключовим джерелом для розслідувань є криптовалютні адреси**, які журналісти можуть знаходити в судових документах, поліцейських звітах, скаргах до регуляторів, через інтерв'ю з жертвами шахрайства, а також за допомогою запитів на публічну інформацію.
- **Залучення незалежних експертів є критично важливим для верифікації даних:** великі аналітичні фірми мають обмежені ресурси та власні інтереси.
- **Аналіз великих масивів даних через API безкоштовних інструментів** (Arkham Intelligence, Tronscan) дозволяє самостійно кількісно оцінювати криптовалютні потоки без залежності від дорогих комерційних платформ, що робить методику доступною з обмеженим бюджетом.

Команда ICIJ використовувала дані, загальнодоступні через API Arkham Intelligence та Tronscan. Експортовані дані показували транзакції в USDT, надіслані від Huione Group на адреси, позначені Arkham як депозитні адреси Binance та OKX. Дослідники верифікували ці позначки, аналізуючи потоки коштів від цих адрес до так званих "гарячих гаманців", які використовуються біржами для управління депозитами та виведенням коштів.

У глобальному контексті розслідування охопило багато країн. В Африці, у Кенії, Africa Uncensored досліджував, як шахрайство трансформувалося у фальшиві криптоінвестиції, що використовували довіру та місцеві мережі. В Азії The Indian Express висвітлював розслідування криптобірж індійською владою та "мега-криптошахрайства" за участі індійських операторів, а також показав, як відсутність законодавчої бази залишає майже 120 мільйонів індійських інвесторів незахищеними від фінансового шахрайства. У Південній Америці CONNECTAS разом із Vistazo та El Espectador деталізували багатомільйонну криптоінвестиційну схему в Еквадорі та Колумбії, що обіцяла легкі гроші інвесторам. Журналісти встановили, що 176 мільйонів у щонайменше 36 різних криптовалютах було втрачено ще до того, як прокуратура змогла арештувати кошти на рахунках, і підтвердили, що збитки простежуються до Binance, де зареєстровано кілька гаманців організаторів схеми.

У Північній Америці CBC News, Toronto Star та La Presse досліджували зростання послуг обміну криптоактивів в Канаді та те, як будь-хто може використати їх для переказу криптовалюти на іноземний нерегульований гаманець, а потім отримати десятки тисяч доларів готівкою анонімно. CNN та ICIJ виявили, що мережа магазинів Circle K заробила мільйони, здаючи площу під криптомати, попри зростаючі докази того, що ці машини відіграють ключову роль у міжнародних шахрайських схемах.

У Європі кілька медіа досліджували зв'язки між президентом США Трампом та криптоіндустрією, включаючи L'Espresso в Італії та Suddeutsche Zeitung у Німеччині. De Tijd і

Knack виявили, що Binance припинила співпрацю з бельгійською поліцією та судовими органами в кримінальних розслідуваннях, а інші великі біржі також створювали бар'єри для європейських правоохоронців. Het Financieele Dagblad висвітлював справу 25 нідерландських жертв, які позиваються до криптобіржі, зареєстрованої на Карибах, через нездатність належно захистити користувачів від шахраїв. На Близькому Сході Shomrim досліджував активність адрес гаманців, пов'язаних із ХАМАС та Іраном, та їхні зв'язки з великими біржами.

Таким чином, розслідування криптовалютних транзакцій відкриває нову еру для журналістів, озброюючи їх інструментами для викриття фінансових злочинів, які традиційно залишалися непоміченими. Поєднання технічних знань, наполегливості у пошуку адрес, роботи з експертами та використання сучасних інструментів аналізу даних дозволяє розкривати схеми, які раніше здавалися непроникними.

Ключовим є розуміння того, що блокчейн, попри свою анонімність, залишає цифровий слід, який при правильному підході може стати потужним джерелом журналістських розслідувань та притягнення до відповідальності тих, хто використовує криптовалюту для незаконної діяльності.

Корупція у секторі гуманітарної допомоги: основні типології, ризики та механізми протидії [9]

Дослідження Міжнародної антикорупційної академії (IACA) присвячене системному аналізу корупційних практик, які виникають під час фінансування, організації, реалізації та контролю гуманітарних проєктів. Воно становить перший етап дослідницького проєкту IACA, започаткованого у 2024 році з метою формування методологічної основи для розроблення, впровадження та оцінювання програм доброчесності й антикорупційного комплаєнсу в гуманітарних організаціях. Актуальність роботи пов’язана зі зростанням глобальних гуманітарних потреб унаслідок збройних конфліктів, економічної нестабільності, пандемій і природних катастроф, що супроводжується швидкою мобілізацією значних фінансових та матеріальних ресурсів і, відповідно, посиленням ризику їх привласнення, неналежного використання або незаконного перенаправлення.

Автори наголошують, що гуманітарний сектор часто помилково сприймається як менш уразливий до корупції через його неприбутковий характер і суспільно корисну місію. Проте така презумпція доброчесності може послаблювати внутрішній контроль і перешкоджати відкритому обговоренню порушень. Корупція не лише зменшує обсяг допомоги, що доходить до кінцевих отримувачів, але й підриває довіру донорів, завдає репутаційної шкоди гуманітарним організаціям і може спричинити скорочення або зупинення фінансування. Дослідження ґрунтується на аналізі відкритих джерел, практичних кейсів, експертних інтерв’ю, законодавства, кодексів поведінки та програм доброчесності гуманітарних організацій.

У документі виділено три основні групи операторів гуманітарної допомоги: міжурядові організації, державні агенції розвитку та неурядові гуманітарні організації. Вони можуть реалізовувати проєкти самостійно або через місцевих партнерів, підрядників і постачальників. Багаторівнева структура гуманітарних операцій ускладнює контроль за рухом коштів та розподілом відповідальності. Найбільш уразливими визначено внутрішнє управління організаціями, взаємодію з донорами, відбір виконавчих партнерів і постачальників, відносини з державними органами, контроль виконання проєктів та безпосередню взаємодію з отримувачами допомоги.

Автори застосовують широке розуміння корупції, яке охоплює зловживання владою, усі форми хабарництва, привласнення й розтрату коштів, фінансове шахрайство, відмивання

[9] https://www.iaca.int/media/attachments/2026/07/16/iaca_typologies-of-corruption-in-the-humanitarian-aid-sector_research-paper.pdf

коштів, підроблення документів, торгівлю впливом, порушення закупівельних процедур, конфлікти інтересів, переслідування викривачів та інші форми неправомірного використання службового становища. Підкреслюється, що частина цих практик є типовою для державного і приватного секторів, проте умови гуманітарної діяльності створюють специфічні ризики, пов'язані з терміновістю операцій, роботою в зонах конфлікту, слабкістю місцевих інституцій, взаємодією з фактичними органами влади та критичною залежністю отримувачів від допомоги.

У сфері внутрішнього управління корупція може починатися з призначення лояльних або недостатньо компетентних працівників через непотизм, патронаж, підкуп чи торгівлю впливом. Надалі такі працівники сприяють незаконним платежам, відбору визначених постачальників та обходу внутрішнього контролю. Фінансові зловживання здійснюються через завищені зарплати й необґрунтовані премії, фіктивні звіти про витрати, неправдиві рахунки та пряме викрадення коштів. Приклад GiveDirectly у Демократичній Республіці Конго показав, що навіть цифрові грошові перекази залишаються вразливими: працівники використали спрощену процедуру реєстрації SIM-карт та перенаправили близько 900 тис. доларів, унаслідок чого допомогу не отримали понад 1 700 сімей. Це підтверджує, що технологічні рішення не замінюють незалежної верифікації та розподілу повноважень.

Закупівлі й відбір третіх сторін визначено одним із найбільш ризикових напрямів. Необхідність швидко придбавати великі обсяги товарів і послуг часто призводить до спрощення стандартних процедур. Корупційні схеми включають витік конфіденційної інформації, формування умов тендера під певного учасника, обмеження конкуренції, змову постачальників, приховані конфлікти інтересів, відкати та вибір компаній, пов'язаних із керівниками організації. Після укладення контракту ціна може завищуватися, до рахунків включаються фіктивні витрати, оплачуються ненадані послуги або постачаються товари неналежної якості. Показовим є випадок International Rescue Committee, працівники якого у змові з турецькими постачальниками маніпулювали закупівлями для гуманітарної операції щодо Сирії. У 2021 році організація погодилася сплатити уряду США приблизно 6,9 млн доларів для врегулювання претензій щодо закупівельного шахрайства.

Відносини між донорами та виконавцями є вразливими через нерівність фінансових можливостей. Організації, які прагнуть отримати фінансування, можуть перебільшувати власну спроможність, фальсифікувати дані про діяльність чи потреби отримувачів, приховувати неналежне управління коштами або пропонувати працівникам донорських установ неправомірну вигоду. Водночас представники донорів можуть вимагати хабарі чи використовувати вплив на розподіл коштів в особистих інтересах. Аналогічні ризики існують під час відбору місцевих партнерів, особливо якщо не перевіряються їхня репутація, структура власності, зв'язки з посадовими особами та реальна спроможність виконати проєкт. Окремо наголошується на ризику використання гуманітарних і благодійних організацій для відмивання коштів або фінансування тероризму, що потребує застосування пропорційних ризик-орієнтованих заходів ПВК/ФТ.

Значні ризики виникають під час взаємодії з державними органами, оскільки від посадових осіб часто залежать митне оформлення вантажів, отримання дозволів, доступ до територій та безпека персоналу. У зонах конфлікту або країнах зі слабкими інституціями посадовці можуть вимагати неправомірну вигоду за пропуск гуманітарного вантажу, доступ до постраждалих районів чи забезпечення охорони. Гуманітарні працівники при цьому можуть опинятися перед складною дилемою, коли відмова від платежу затримує критично необхідну допомогу або створює загрозу для персоналу. Тому організаціям необхідно заздалегідь визначати процедури реагування, канали термінової ескалації та правила ухвалення рішень у таких ситуаціях.

Органи влади також можуть привласнювати гуманітарні ресурси, продавати їх на ринку або розподіляти серед визначених груп для зміцнення політичного впливу. В Ефіопії у 2023 році було виявлено масштабне відведення продовольчої допомоги, до якого, за наведеними у документі даними, були причетні державні та регіональні структури. Допомогу відновили

після запровадження біометричної верифікації отримувачів, незалежного моніторингу та усунення місцевих урядових комітетів від розподілу продовольства. В Уганді біометрична перевірка показала, що заявлена кількість біженців була завищена приблизно на 300 тис. осіб, що використовувалося для залучення додаткового міжнародного фінансування. Ці випадки підтверджують необхідність незалежного формування та регулярної перевірки реєстрів отримувачів.

Контроль виконання контрактів є не менш важливим, ніж прозоре проведення закупівель. Типовими порушеннями є викрадення допомоги та її продаж на нелегальному ринку, подання неправдивих звітів про розподіл, завищення транспортних та інших витрат, оплата ненаданих послуг і прийняття неякісних робіт. Такі схеми часто потребують співпраці працівників гуманітарних організацій, місцевих партнерів, підрядників, корумпованих посадовців та іноді організованих злочинних груп. Справи щодо розкрадання допомоги в Сомалі, привласнення грантових коштів у Малі та втрати близько 5 млн доларів, призначених для протидії спалаху Еболи у Західній Африці, демонструють системний характер відповідних ризиків. Реконструкція індонезійської провінції Ачех після цунамі також показала, що неналежний технічний контроль може призвести до використання неякісних матеріалів і необхідності ремонту або перебудови сотень об’єктів.

Особливо небезпечними є зловживання під час безпосередньої взаємодії з отримувачами гуманітарної допомоги. Працівники й посередники контролюють доступ до продовольства, житла, грошових виплат, працевлаштування, статусу біженця та переселення, тоді як отримувачі перебувають у залежному становищі. Цей дисбаланс може використовуватися для вимагання грошей, послуг або інших особистих вигод. Можливість подання скарги часто обмежується страхом помсти, припиненням допомоги або залежністю від того самого працівника, на якого подається повідомлення. Тому механізми повідомлення повинні бути незалежними, конфіденційними, доступними різними мовами та зрозумілими для людей із різним рівнем освіти.

Висновки:

- **Антикорупційний контроль необхідно поширити на весь цикл гуманітарного проєкту.** Перевірка має охоплювати не лише закупівлю, а й призначення персоналу, відбір донорів і партнерів, ідентифікацію отримувачів, фактичне постачання, якість робіт та кінцевий розподіл допомоги.
- **Закупівлі й виконання контрактів потребують посиленого ризик-орієнтованого моніторингу.** Практичними заходами мають стати перевірка пов’язаності постачальників із працівниками, незалежне зіставлення цін, розподіл повноважень, підтвердження фактичного постачання та фінансово-технічний аудит.
- **Для роботи у зонах конфлікту потрібні заздалегідь визначені протоколи реагування на вимагання неправомірної вигоди.** Організація повинна надати персоналу чіткі сценарії дій, цілодобові канали ескалації та контакти уповноважених центральних органів, одночасно враховуючи безпеку працівників і необхідність безперервного надання допомоги.
- **Канали повідомлення мають бути доступними не лише персоналу, а й партнерам та отримувачам допомоги.** Їх ефективність залежить від конфіденційності, незалежного розгляду, захисту від помсти, зрозумілої процедури реагування та регулярного інформування про права і способи подання скарг.

За результатами дослідження автори рекомендують створювати комплексні ризик-орієнтовані програми доброчесності й антикорупційного комплаєнсу, які охоплюватимуть увесь цикл гуманітарного проєкту. Вони мають включати перевірку персоналу і третіх сторін, розподіл повноважень, урегулювання конфліктів інтересів, прозорі закупівлі, незалежне порівняння

цін, фінансовий та технічний аудит, перевірку фактичного постачання, контроль якості й моніторинг кінцевого розподілу допомоги. Штучний інтелект та інші технології можуть застосовуватися для виявлення аномальних платежів, дубльованих рахунків, завищених цін і концентрації контрактів у пов'язаних постачальників, проте вони повинні доповнювати, а не замінювати незалежний контроль.

Організації також повинні встановлювати чіткі правила щодо подарунків і гостинності, заздалегідь повідомляти свої антикорупційні вимоги відповідним органам влади та навчати працівників діяти у випадках вимагання неправомірної вигоди або виникнення загрози безпеці. Доцільно визначати в центральних органах влади, поліції, митній службі або підрозділах внутрішньої безпеки цілодобові контактні пункти для оперативного реагування на корупційні інциденти. Окремого значення набувають механізми повідомлення про порушення: недостатньо лише створити гарячу лінію – працівники, партнери й отримувачі повинні знати порядок розгляду скарг, строки реагування, можливі наслідки та способи захисту заявника від помсти.

Таким чином, документ розглядає корупцію в гуманітарному секторі як системний ризик, що супроводжує весь шлях допомоги – від залучення коштів і призначення персоналу до закупівлі, транспортування та передачі ресурсів кінцевим отримувачам. Ефективна протидія потребує не лише розслідування окремих випадків, а й інтегрованої системи запобігання, контролю, захисту викривачів, незалежного аудиту та співпраці з компетентними органами. Належний антикорупційний комплаєнс при цьому має розглядатися не як перешкода для оперативного надання допомоги, а як необхідна умова того, щоб гуманітарні ресурси своєчасно та в повному обсязі доходили до людей, для яких вони призначені.

Рекомендовані матеріали

43-й Кембриджський міжнародний симпозіум з економічної злочинності [10]

Кембриджський міжнародний симпозіум з економічної злочинності, організований під егідою Центру геополітики Кембриджського університету, є унікальним явищем у світі боротьби з фінансовими злочинами. Він вирізняється своїм масштабом, глибиною аналізу та, що найголовніше, прагматичною спрямованістю.

Симпозіум збирає понад 600 експертів з більш ніж 100 країн, представляючи унікальне поєднання практичного досвіду та академічної думки. До участі залучені не лише науковці, але й безпосередні виконавці – співробітники правоохоронних органів, регулятори, судді, дипломати, представники розвідки, комплаєнс-офіцери та політики. Такий склад учасників перетворює симпозіум на дієвий майданчик для вироблення реальних рішень та налагодження міжнародної співпраці, що є критично важливим для боротьби зі злочинами, які часто не знають державних кордонів.

Основна тема 43-го симпозіуму, що відбудеться 23-30 серпня 2026 року – «Повернення активів та верховенство права: від риторики до результатів» – акцентує увагу на одній з найбільш проблемних ланок у ланцюгу протидії економічній злочинності. Визнаючи, що стратегії, спрямовані на блокування та конфіскацію злочинних доходів, є наріжним каменем у стримуванні та дезорганізації злочинних мереж, організатори констатують парадоксальну реальність: практичні результати, особливо у вимірі реально вилучених коштів та майна, залишаються доволі скромними.

Програма заходу критично оцінює ефективність поточних підходів, визнаючи, що витрати, ризики та незручності, пов'язані з комплаєнсом та іншими заходами, не завжди мають

10 https://static1.squarespace.com/static/5c3312b1d274cbf1e812027c/t/6a5f36dfd5f8cb18773074de/1784624863742/2026+Symposium+Programme+%283.3%29.pdf

очевидний економічний сенс. Це питання стає особливо гострим, коли мова йде про криптовалюти та інші цифрові активи, які суттєво ускладнюють процеси ідентифікації, блокування та конфіскації.

У відповідь на ці виклики, програма симпозіуму демонструє системний підхід, який виходить за межі суто карного переслідування. Значну увагу приділено альтернативним стратегіям, зокрема використанню інструментів цивільного права, таким як конфіскація на підставі непоясненого багатства (unexplained wealth orders) та цивільна конфіскація (non-conviction based forfeiture). Ці механізми дозволяють діяти більш гнучко, не чекаючи винесення вироку у кримінальній справі, що часто є тривалим та складним процесом. Наприклад, обговорення на панелях з тематикою «No place to hide: the extraterritorial reach of US civil forfeiture» (Сховатися ніде: екстериторіальна дія цивільної конфіскації у США) та «Unexplained wealth – so what?» (Непояснене багатство – і що з того?), безпосередньо торкаються практичних аспектів застосування цих інструментів, їхньої ефективності та викликів, пов'язаних з міжнародним визнанням та виконанням таких рішень.

Особливу увагу в програмі симпозіуму приділено новітнім викликам, які ставлять перед системою цифрові технології. Робочі групи та панельні дискусії, присвячені криптовалютам («Crypto assets – the criminal and regulatory law», «Controversies in crypto and blockchain», «Crypto markets, illicit finance and asset recovery»), свідчать про глибоке усвідомлення того, що цифрові активи стали невід'ємною частиною сучасного фінансового ландшафту та інструментом для злочинців. Обговорення стосуються не лише ризиків, але й можливостей, які надають технології аналізу блокчейну для відстеження транзакцій. Водночас піднімаються питання шахрайства з використанням штучного інтелекту, кіберзлочинності та таких схем, як романтичне шахрайство, які демонструють симбіоз сучасних технологій та маніпуляцій людською психікою.

Окрім технологічних аспектів, на симпозіумі розглядається ширший контекст, який впливає на корупцію та незаконні фінансові потоки. Це, зокрема, секція, присвячена «Geopolitical strategic corruption and illicit finance» (Геополітична стратегічна корупція та незаконні фінанси). В рамках цього напрямку аналізується, як глобальна політична напруженість, санкційний режим та конкуренція між державами впливають на методи та масштаби корупції. Обговорюються питання, пов'язані з використанням інвестицій для досягнення стратегічних геополітичних цілей, що часто суперечить принципам прозорості та верховенства права. Це свідчить про те, що боротьба з економічною злочинністю більше не є виключно технічним чи правовим питанням, а стає невід'ємною частиною міжнародної політики та безпеки.

Важливим аспектом, який відрізняє цей захід, є його інклюзивність та зосередженість на практичних рішеннях. Окрім пленарних засідань, програма містить численні майстер-класи, аналітичні групи (think tanks) та закриті робочі сесії за правилами Chatham House, що сприяє відвертому та неформальному обміну досвідом. Серед тем цих сесій – питання комплаєнсу, ефективності боротьби з відмиванням грошей, роль аудиторів, податкові механізми, проблеми офшорних центрів, а також вирішення конфліктів. Спеціальні програми, присвячені геополітичній корупції, боротьбі з вимаганням з використанням програм-вимагачів (ransomware) та відновленню активів, свідчать про те, що організатори намагаються охопити найактуальніші проблеми.

На завершення варто зазначити, що 43-й Кембриджський симпозіум – це знакова подія, яка задає вектор розвитку міжнародної співпраці у боротьбі з економічною злочинністю. Зосередившись на практичній ефективності повернення активів, він виходить за межі звичайної риторики, пропонуючи майданчик для конструктивного діалогу між провідними світовими експертами. Він демонструє перехід від реактивних методів до проактивних, інтегрованих стратегій, які поєднують традиційне карне право, цивільно-правові інструменти, передові технології та глибоке розуміння геополітичних процесів.

Беззаперечним є те, що такі заходи є критично необхідними для посилення глобальної архітектури фінансової безпеки та захисту інституцій від зловживань, сприяючи переходу від благородних намірів до конкретних результатів.

Інші новини

Прозорість та кібербезпека в умовах геополітичного протистояння [11]

У сучасному цифровому світі, де кібербезпека стала наріжним каменем національної безпеки, а питання конфіденційності даних виходить на перший план, довіра до постачальників програмного забезпечення є критичним фактором.

Розслідування, проведене OCCRP та його партнерами, виявило тривожні факти щодо іспанського менеджера паролів Passwork, який позиціонує себе як суто європейський продукт, однак, як з'ясувалося, має глибокі технологічні та історичні зв'язки з російською компанією-аналогом, що проходить державну сертифікацію в інтересах оборонного відомства рф. Ця ситуація демонструє, як комерційний маркетинг може суперечити реальному стану речей, створюючи потенційно небезпечні вразливості для європейських державних установ, університетів та підприємств, які є клієнтами цього сервісу.

Іспанська компанія Password Europe S.L., яка володіє продуктом Passwork, наполегливо наголошує на своєму європейському походженні, використовуючи гасла на кшталт «Європейська компанія, створена для довіри» та бейдж «Зроблено в ЄС». На веб-сайті компанії наголошується на її незалежності, прозорості та відсутності зв'язків з будь-якими неєвропейськими суб'єктами, включно з росією. Проте, журналістське розслідування доводить зворотне.

Виявляється, що програмне забезпечення Passwork було розроблено двома російськими співзасновниками – Іллею Гарахом та Андрієм П'янковим, які досі залишаються причетними до діяльності непрозорої компанії, зареєстрованої в Об'єднаних Арабських Еміратах, що, своєю чергою, постачає іспанському продукту оновлення. Цей ланцюжок – від Архангельська до Фінляндії, потім до ОАЕ та Іспанії – створює заплутану корпоративну структуру, яка ускладнює визначення реального власника та контролера даних, що є неприпустимим для продукту, який використовується для зберігання ключів до цифрової інфраструктури державних установ.

Критичним аспектом цієї історії є той факт, що російська версія Passwork, яка використовує ідентичний логотип та практично таку саму кодову базу, пройшла сертифікацію у Федеральній службі з технічного та експортного контролю (ФСТЕК), підрозділі Міністерства оборони російської федерації, а також у ФСБ. Ця сертифікація передбачала глибокий аналіз вихідного коду програмного забезпечення з метою виявлення «вразливостей або недекларованих можливостей», що на практиці означає пошук потенційних бекдорів.

Експерти, опитані OCCRP, одностайні у своїй думці: така процедура, проведена російськими державними аудиторами, надає москві безпрецедентний рівень розуміння внутрішньої архітектури продукту. Враховуючи спільне походження кодової бази та синхронізований графік випуску оновлень між російською та іспанською версіями, будь-яка вразливість, виявлена в російському продукті, з високою ймовірністю існує і в європейському аналозі. Це створює ситуацію, коли компетентні органи рф можуть мати інсайдерську інформацію про слабкі місця системи безпеки, якою користуються європейські державні структури.

Окремої уваги заслуговує механізм оновлення програмного забезпечення, який, на думку фахівців з кібербезпеки, є одним з найефективніших векторів атак. У випадку з Passwork оновлення для іспанської компанії постачаються з ОАЕ через компанію, керовану одним з

[11] https://www.occrp.org/en/investigation/european-password-manager-shares-origins-and-updates-with-state-certified-russian-firm

російських співзасновників. Ця структура абсолютно непрозора, а хто саме контролює конвеєр оновлень, залишається невідомим. Експерт Дональд Ортманн проводить паралелі з гучним кібернападом на SolarWinds, коли зловмисники через скомпрометоване оновлення отримали доступ до мереж тисяч організацій. З огляду на те, що російський продукт сертифікований ФСТЕК, існує цілком реальний ризик того, що державні органи рф, володіючи інформацією про код, могли б або ініціювати впровадження шкідливого коду на етапі підготовки оновлень, або використовувати знайдені вразливості для проведення цілеспрямованих атак на європейські установи. «Нульове знання» архітектури, на яке посилається CEO іспанської компанії Александр Мунтян, не є панацеєю, адже навіть найкраща модель шифрування може бути скомпрометована на етапі оновлення або через вбудовані «закладки» на рівні коду, що є основною метою перевірок ФСТЕК.

Найбільше занепокоєння викликає реакція клієнтів та сама позиція керівництва Passwork Europe. Коли OCCRP зв'язався з близько 30 клієнтами, зазначеними на сайті Passwork, з'ясувалося, що майже жоден з них не знав про російське коріння продукту або про його сертифікацію в росії. Ірландські державні установи, які використовують Passwork, повідомили, що не ідентифікували жодних ризиків, однак визнали, що отримана інформація є новою і вимагає серйозного перегляду. Інша група компаній, які фігурували на сайті Passwork як клієнти, включно з Enel Group та Deutsche Post, взагалі заявили, що не використовують цей продукт. Це свідчить про вкрай низький рівень належної перевірки (due diligence) з боку клієнтів, які довіряють критичну інфраструктуру продукту з непрозорою структурою власності. CEO Мунтян, хоч і заперечує активну співпрацю з російською компанією, визнає спільне походження кодової бази та підтверджує, що оновлення надходять від еміратської компанії, пов'язаної з російськими засновниками. Його аргументи про те, що код «відкритий для аудиту» клієнтами, виглядають неспроможними в умовах, коли самі клієнти не обізнані про існування ризиків, а AI-інструкції на сайті, які однозначно стверджували про відсутність російських зв'язків, були поспішно видалені одразу після перших запитань журналістів.

Ця ситуація підіймає фундаментальне питання довіри у сфері кібербезпеки. Як зазначає експерт Берт Губерт, у таких сервісах немає середнього шляху: ви або довіряєте вендору повністю, або ні. «Ви не можете сказати: я не довіряю постачальнику, але я довіряю програмному забезпеченню», – наголошує він. Надання державному органу країни-агресора, яка проводить активні гібридні та кібероперації проти європейських держав, доступу до вихідного коду продукту, який використовують європейські держустанови, є грубим прорахунком або ж свідомою недбалістю. Аналіз засвідчує, що «розрив» між європейською та російською версіями є «поверховим» – вони отримують оновлення майже одночасно, мають ідентичні інструкції користувача, а їхні скрипти інсталяції збігаються на сотні рядків. Це свідчить про те, що, попри юридичне розділення компаній, технологічно вони залишаються надзвичайно близькими, що унеможливлює будь-які запевнення про незалежність європейського продукту від російського впливу.

Таким чином, випадок Passwork – це не просто історія про комерційну недобросовісність, а яскравий приклад того, як відсутність прозорості та належного контролю у сфері критичної інформаційної інфраструктури може перетворити звичайний інструмент на потенційний канал для реалізації загроз національній безпеці цілих держав.

Як штучний інтелект трансформує ландшафт злочинів проти дітей [12]

Сучасний цифровий світ, який відкриває безпрецедентні можливості для комунікації, творчості та розвитку, водночас стає дедалі більш небезпечним простором для найбільш вразливих членів суспільства – дітей.

[12] https://globalinitiative.net/analysis/abuse-at-scale-artificial-intelligence-is-reshaping-child-sexual-exploitation/

Технологічний прогрес, зокрема стрімкий розвиток штучного інтелекту, парадоксальним чином обертається новими викликами для системи глобальної безпеки, створюючи інструменти, які зловмисники використовують із загрозливою ефективністю.

Штучний інтелект кардинально змінює економіку та доступність виробництва протиправного контенту. Якщо раніше створення матеріалів сексуального характеру з участю дітей вимагало безпосереднього контакту з жертвою або доступу до архівів реальної експлуатації, що несло високі ризики викриття, то сьогодні генеративні моделі дозволяють продукувати такі матеріали практично з повітря, використовуючи лише публічно доступні зображення. Масштаби цього явища вражають: за оцінками експертів, щонайменше 1,2 мільйона дітей уже стали жертвами використання їхньої зовнішності для генерування контенту сексуального характеру за допомогою штучного інтелекту.

Існує небезпечна ілюзія, що поява синтетичних матеріалів може знизити рівень реальної експлуатації дітей, оскільки зловмисники отримають можливість задовольняти свої потреби без безпосереднього контакту з жертвами. Однак емпіричні дані та аналітичні висновки правоохоронних органів свідчать про прямо протилежну тенденцію. Синтетичний контент не замінює реальну експлуатацію, а скоріше діє як каталізатор, розширюючи коло потенційних правопорушників і створюючи додаткові стимули для злочинних мереж. Доступність інструментів штучного інтелекту знижує поріг входження у цю сферу, залучаючи нових осіб, які раніше не мали технічних навичок або сміливості для вчинення таких злочинів.

Масштаб цієї загрози найпереконливіше демонструють результати нещодавніх міжнародних правоохоронних операцій, які виявили раніше небачені форми організованої злочинної діяльності. Операція "Камберленд" 2025 року, яка об'єднала зусилля правоохоронців із 19 країн під егідою Європолу, стала першим в історії випадком ліквідації транснаціональної мережі, яка спеціалізувалася виключно на розповсюдженні контенту сексуального характеру, створеного штучним інтелектом. В рамках цієї операції було ідентифіковано майже 300 користувачів по всьому світу, що свідчить про глобальний характер проблеми.

Однією з ключових особливостей нової хвилі злочинності є те, що виробництво та розповсюдження матеріалів сексуального характеру з участю дітей дедалі більше переймає операційні методи, характерні для інших форм кіберзлочинності. Зловмисники активно використовують соціальні мережі для пошуку потенційних жертв та створення фальшивих ідентичностей, зашифровані комунікаційні канали для обміну матеріалами та анонімні платіжні системи для отримання прибутку. Це створює ситуацію, коли традиційні методи розслідування, орієнтовані на фізичні докази та прямі контакти між злочинцем і жертвою, стають все менш ефективними. Хоча багато комерційних платформ штучного інтелекту впроваджують захисні механізми для запобігання створенню шкідливого контенту, дослідники та правоохоронці неодноразово демонстрували, що ці захисти можна легко обійти.

Особливо серйозну загрозу становлять відкриті моделі штучного інтелекту з відкритим вихідним кодом, які дозволяють будь-якому користувачеві отримати доступ до їхньої архітектури та модифікувати її відповідно до власних потреб. Саме на основі таких моделей зловмисники створюють спеціалізовані інструменти, які перетворюють звичайні фотографії на компрометуючі матеріали. Ці інструменти стають дедалі більш досконалими, створюючи додаткові труднощі для правоохоронців, які мають відрізнити синтетичний контент від реального.

Ця тенденція ідеально вписується у ширшу картину трансформації організованої злочинності, окреслену в нещодавніх звітах Європолу. Штучний інтелект не створює абсолютно нових кримінальних ринків, але він суттєво прискорює існуючі, розширюючи їхні масштаби, підвищуючи ефективність та стійкість, а також ускладнюючи їх виявлення та припинення. Фінансова інфраструктура, що забезпечує ринок матеріалів сексуального характеру з участю дітей, стає дедалі більш витонченою та нагадує практики інших кіберзлочинних ринків. Хоча близько половини ідентифікованих транзакцій не перевищують 100 доларів США, що зумовлено низькою собівартістю та масштабністю виробництва, оператори все частіше

переходять до абонентських моделей бізнесу, забезпечуючи стабільні потоки доходу. Біткоїн залишається популярним засобом платежу, але мережі також конвертують виручку в криптовалюти з підвищеною конфіденційністю, такі як Monero, які дозволяють швидко обмінювати активи з мінімальними вимогами до верифікації клієнтів. Ці фінансові практики значно ускладнюють відстеження та перекриття незаконних грошових потоків.

Успіх правоохоронних операцій під керівництвом Європолу демонструє, що транскордонна співпраця може бути ефективною навіть у таких складних умовах, проте ці ж операції виявили критичну прогалину в системі правосуддя. Значним бар'єром для ідентифікації як правопорушників, так і жертв стало встановлення походження або достовірності вилучених матеріалів, особливо у випадках, коли контент створений штучним інтелектом. Судові експерти стикаються з необхідністю розрізняти реальні та синтетичні зображення, що стає дедалі складнішим завданням у міру вдосконалення технологій. Правова база, що регулює контент сексуального характеру з участю дітей, створений штучним інтелектом, залишається вкрай нерозвиненою, і Європол офіційно зазначив, що координація операції через 19 країн за відсутності національного законодавства була надзвичайно складною для слідчих. Це свідчить про те, що міжнародне право та національні законодавства не встигають за темпами технологічного прогресу, створюючи юридичний вакуум, який активно використовують злочинці.

Ситуація загострюється регуляторною невизначеністю на рівні Європейського Союзу, де тимчасове відступлення від Регламенту про електронну приватність, яке дозволяло технологічним компаніям на добровільній основі сканувати певні комунікації на наявність контенту сексуального характеру з участю дітей, закінчилося в квітні 2026 року. Хоча в липні того ж року Європейський Парламент продовжив дію цього тимчасового режиму з певними поправками, включаючи захист наскрізного шифрування комунікацій, переговори щодо постійної правової бази тривають і досі.

Деякі уряди розпочали реагувати на зростання контенту сексуального характеру з участю дітей, створеного штучним інтелектом, пропонуючи цільове законодавство, що свідчить про політичну волю вирішити цю проблему. Австралія, Сполучені Штати, Сполучене Королівство та Європейський Союз висунули або впровадили заходи, які криміналізують створення такого контенту або обмежують використання систем штучного інтелекту для цих цілей. Рада Європи зробила конкретні кроки, криміналізувавши створення, зміну та поширення генерованих штучним інтелектом матеріалів сексуального характеру з участю дітей відповідно до своїх конвенцій. Проте, за винятком нещодавніх поправок до Закону ЄС про штучний інтелект, які вводять вимоги прозорості для контенту, створеного штучним інтелектом, і мають набути чинності в грудні 2026 року, більшість законодавчих ініціатив все ще перебувають на стадії розробки. Правоохоронні органи продовжують працювати в межах правових рамок, які не були розроблені з урахуванням синтетичних матеріалів, що призводить до ситуації, коли злочинці діють на випередження, а законодавці лише наздоганяють їх, часто зі значним запізненням.

Вирішення цієї багатогранної проблеми вимагає комплексного підходу, що поєднує технологічні інновації, правові реформи та міжнародну співпрацю. Інтеграція принципів безпеки за замовчуванням та заходів захисту дітей у системи штучного інтелекту на етапі їх розробки є критично важливою для мінімізації можливостей зловживання. Технологічні компанії мають нести більшу відповідальність за свої продукти, особливо моделі з відкритим кодом, які можуть бути легко адаптовані для шкідливих цілей. Правоохоронні органи потребують додаткових ресурсів, спеціалізованого навчання та доступу до передових технологій для виявлення та розслідування злочинів, скоєних за допомогою штучного інтелекту. Міжнародне співробітництво має бути поглиблене та систематизоване, щоб забезпечити швидкий обмін інформацією та координацію дій між різними юрисдикціями. Водночас необхідно знайти баланс між захистом дітей та забезпеченням конфіденційності комунікацій, що є особливо складним завданням в умовах широкого використання наскрізного шифрування.

Штучний інтелект змінює методи сексуальної експлуатації дітей, проте жертви залишаються тими ж – вразливими дітьми, чиї права, гідність та майбутнє опиняються під загрозою. Ця технологічна революція, яка несе стільки обіцянок для людства, також демонструє свою темну сторону, де інновації стають зброєю.

Щоб гарантувати, що прогрес не сприятиме подальшому розквіту організованої злочинності, системи захисту мають бути такими ж проактивними та адаптивними, як і злочинні мережі, які експлуатують нові технології. Це вимагає не лише технічних рішень, але й фундаментальної зміни підходу до регулювання, правоохоронної діяльності та суспільної свідомості, адже боротьба за безпеку у цифровому світі є одним із найважливіших викликів нашого часу, від вирішення якого залежить не лише сьогодення, але й майбутнє цілих поколінь.

Ваша думка важлива!

1. Як вирішити проблему "регуляторного арбітражу", коли DeFi-протоколи свідомо реєструються в юрисдикціях з м'якшим регулюванням, але надають послуги українським резидентам через веб-інтерфейси українською мовою?
2. Які реальні інструменти та юридичні механізми має Україна для блокування або примусового аудиту використання підсанкційного (або пов'язаного з підсанкційними особами) програмного забезпечення у державних інформаційних системах?
3. Як Україні забезпечити належний антикорупційний контроль за гуманітарною допомогою, не створюючи надмірних процедурних перешкод для благодійних та гуманітарних організацій в умовах війни?
4. Наскільки результативною може бути боротьба з організованою злочинністю без паралельного виявлення корупційних зв’язків, фінансових потоків і професійних учасників, які надають злочинним мережам спеціалізовані послуги?
5. Які практичні кроки має здійснити Україна, щоб перейти від формального законодавчого врегулювання ринку віртуальних активів до ефективного ліцензування, ризик-орієнтованого нагляду та застосування санкцій до порушників?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-30

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

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