Методологічний бюлетень

Серійний номер: МінФін-AML-2026-10

Березень 2026

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

Томас Карлайл

Мета

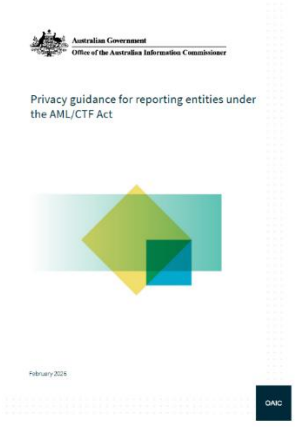
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Від формального комплаєнсу до системного управління даними у сфері ПВК/ФТ [1]



Документ, підготовлений Офісом Уповноваженого з питань інформації Австралії (OAIC), є комплексним нормативно-методичним роз’ясненням щодо взаємодії режиму протидії відмиванню коштів і фінансуванню тероризму (ПВК/ФТ) із законодавством про захист персональних даних в Австралії. Його ключова мета полягає у формуванні чіткої інституційної рамки, яка забезпечує одночасне та узгоджене виконання вимог Anti-Money Laundering and Counter-Terrorism Financing Act 2006 та Privacy Act 1988, включаючи обов’язкове дотримання Australian Privacy Principles (APPs) при здійсненні клієнтської перевірки, моніторингу, звітності та зберігання інформації.

[1] https://www.oaic.gov.au/__data/assets/pdf_file/0021/261336/OAIC-Guide-to-privacy-for-reporting-entities-under-the-AML-CTF-Act.pdf

Документ має стратегічне значення у зв'язку з розширенням сфери ПВК/ФТ-регулювання. Починаючи з 31 березня 2026 року змінюються вимоги до чинних підзвітних суб'єктів (так звані Tranche 1 entities), а з 1 липня 2026 року регулювання у сфері ПВК/ФТ поширюється на нові категорії суб'єктів (Tranche 2), серед яких — ріелтори, суб'єкти господарювання, які здійснюють торгівлю дорогоцінними металами і дорогоцінним камінням, юристи, бухгалтери, провайдери трастових та корпоративних послуг. Особливо принциповим є положення, за яким навіть малі підприємства, що зазвичай не підпадають під дію Privacy Act через обсяг річного обороту, стають повноцінними суб'єктами режиму захисту персональних даних у тій частині діяльності, яка пов'язана з виконанням обов'язків у сфк=ері ПВК/ФТ. Таким чином, статус у сфері ПВК/ФТ автоматично активує застосування норм про захист персональних даних щодо відповідних процесів.

Центральною концепцією документа є принцип пропорційності та вимога обмеження збору персональної інформації лише тим обсягом, який є об'єктивно необхідним для досягнення законної мети та виконання функцій суб'єкта, включаючи зобов'язання у сфері ПВК/ФТ. Це об'єктивний тест: організація повинна бути здатною обґрунтувати, що конкретний обсяг інформації був необхідним, а не просто бажаним чи зручним. Особливо наголошується, що законодавство у сфері ПВК/ФТ не надає суб'єктам необмеженого права на масовий або превентивний збір інформації без об'єктивної необхідності. Збір даних на етапі онбордингу клієнта допустимий лише тоді, коли суб'єкт обґрунтовано дійшов висновку, що взаємодія може включати надання визначеної послуги у розумінні законодавства у фері ПВК/ФТ. Документ детально аналізує приклади, коли проведення клієнтської перевірки є виправданим навіть до фактичного надання послуги, а також ситуації, коли такий збір буде надмірним і не відповідатиме критерію необхідності.

Окрему увагу приділено роботі з чутливою інформацією, яка охоплює дані про політичні переконання, членство у професійних або політичних асоціаціях, кримінальну історію, здоров'я, генетичну інформацію та біометричні дані. Біометрична інформація прямо визначається як чутлива інформація і підлягає підвищеному рівню захисту. Її збір допускається лише за наявності чіткої законодавчої підстави або за умови отримання згоди особи, причому в контексті ПВК/ФТ згода зазвичай вважається необхідною перед застосуванням біометричної ідентифікації. Це створює баланс між ефективністю цифрової верифікації та захистом фундаментальних прав особи.

Важливим нововведенням є пряма рекомендація не зберігати повні копії посвідчень особи (паспортів, водійських посвідчень) після набрання чинності реформами 2026 року. AML/CTF Act більше не вимагає зберігати скан-копії документів; достатньо зберігати лише релевантні реквізити, такі як ім'я, дата народження, адреса, номер документа, дата закінчення дії, тип документа, а також інформацію про здійснену верифікацію та оцінку ризику ВК/ФТ Це суттєво зменшує «обсяг накопичених персональних даних» організацій і знижує ризик формування «концентрованого масиву чутливих даних, що становить підвищений ризик» масивів персональних даних, які можуть стати мішенню для кіберзлочинців.

Документ детально регламентує використання та розкриття персональної інформації. Загальне правило полягає в тому, що інформація може використовуватися для первинної мети збору — виконання обов'язків у сфері ПВК/ФТ. Використання для вторинних цілей можливе лише за наявності винятків або згоди особи. Водночас AML/CTF Act створює правову підставу для обов'язкового розкриття інформації, зокрема під час подання повідомлення про підозрілу діяльність до AUSTRAC, виконання вимог щодо передачі інформації про платників і отримувачів або реагування на офіційні запити. Однак діють суворі обмеження, пов'язані з положеннями про конфіденційність та забороною розголошення факту повідомлення або проведення перевірки (заборона інформування клієнта), які можуть обмежувати навіть реалізацію права особи на доступ до своїх персональних даних.

Особливий блок присвячено транскордонній передачі інформації. Якщо персональні дані передаються за кордон, суб'єкт зобов'язаний вжити розумних заходів для забезпечення того, щоб іноземний отримувач дотримувався Australian Privacy Principles. Загальне правило полягає в тому, що суб'єкт залишається відповідальним за порушення, допущені іноземним контрагентом, якщо не застосовується виняток, наприклад коли розкриття прямо передбачене законом. Таким чином, режим екстериторіальної відповідальності фактично стимулює впровадження належного договірного та процедурного контролю.

Значний обсяг документа присвячено кібербезпеці та реагуванню на витоки даних. Суб'єкти у сфері ПВК/ФТ акумулюють значні масиви чутливої персональної інформації, що об'єктивно підвищує як ризик кіберінцидентів, так і ймовірність подальшого використання викрадених даних для обходу процедур фінансового моніторингу. Рекомендовано впроваджувати багатофакторну автентифікацію, регулярне оновлення програмного забезпечення, ведення журналів обліку доступу до інформації, контроль привілеїв користувачів та мати формалізований «План реагування на порушення безпеки персональних даних». Застосовується режим обов'язкового повідомлення про порушення безпеки персональних даних, який зобов'язує суб'єкта інформувати наглядовий орган і відповідних осіб у випадку інциденту з високим ризиком шкоди, за винятком ситуацій, коли таке повідомлення суперечить нормам щодо збереження конфіденційності або забороні розголошення факту подання повідомлення про підозрілу діяльність.

Документ також розглядає право особи на доступ до персональної інформації та її виправлення. Суб'єкт повинен реагувати на запити протягом розумного строку, зазвичай 30 календарних днів, однак доступ не може надаватися, якщо це суперечить законодавству у сфері ПВК/ФТ, зокрема положенням про нерозголошення або заборону попередження клієнта про розслідування. У разі відмови суб'єкт повинен надати письмове повідомлення із зазначенням загальних підстав, але без розкриття інформації, яка може створити ризик порушення закону.

Окремо регламентовано питання аутсорсингу. Перед залученням третіх осіб суб'єкт повинен провести належну перевірку, переконатися у наявності політик захисту даних, передбачити контрактні гарантії, механізми контролю та зобов'язання щодо видалення даних після завершення співпраці. Підкреслюється, що як підзвітні суб'єкти, так і їх уповноважені агенти несуть

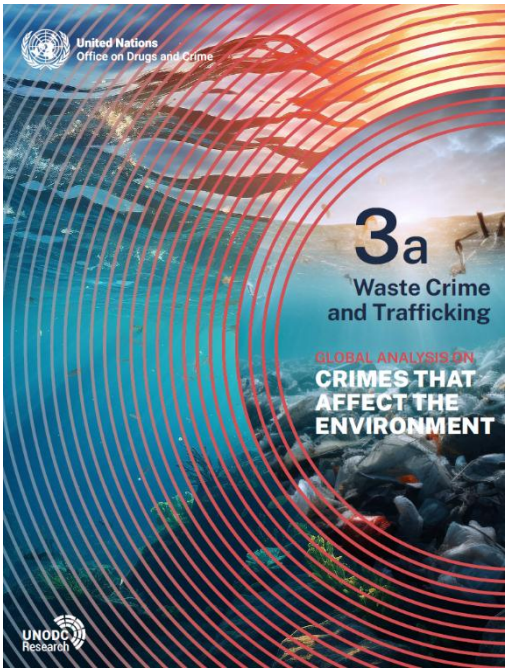
Висновки:

- **Інтеграція вимог у сфері ПВК/ФТ та захисту персональних даних є обов'язковою для всіх підзвітних суб'єктів, включаючи малий бізнес.** Організаціям необхідно переглянути свої програми у сфері ПВК/ФТ та інтегрувати в них політики захисту персональних даних, призначити відповідальних осіб та оновити внутрішні процедури.
- **Принцип мінімізації даних повинен бути реалізований на практиці.** Слід обмежити зберігання повних копій ID-документів, переглянути анкети CDD та усунути надлишкові поля збору інформації, впровадити чіткі строки зберігання та процедури знищення даних.
- **Кібербезпека стає елементом управління ризиками ВК/ФТ.** Необхідно впровадити багаторівневий контроль доступу, ведення журналів обліку, багатофакторну автентифікацію та формалізований план реагування на інциденти, оскільки витік KYC-інформації може бути використаний для обходу фінансового моніторингу.
- **Транскордонна передача та аутсорсинг потребують підвищеного контролю.** Суб'єкти повинні проводити належну перевірку третіх осіб, включати в договори положення про захист даних і забезпечувати аудит виконання зобов'язань, оскільки відповідальність може зберігатися за основним суб'єктом.

відповідальність за дотримання Privacy Act при обробці персональної інформації для цілей у сфері ПВК/ФТ.

У цілому документ формує системну модель інтеграції режиму ПВК/ФТ із режимом захисту персональних даних, засновану на принципах мінімізації даних, пропорційності, ризик-орієнтованого підходу та підзвітності. Він демонструє, що ефективність ПВК/ФТ не може досягатися за рахунок надмірного або неконтрольованого збору інформації, а навпаки — потребує чіткої системи управління обробкою даних, належного рівня кіберстійкості та збалансованого поєднання обов'язків фінансового моніторингу з гарантіями права на приватність.

Тіньовий ринок відходів: масштаби, механізми та виклики міжнародній безпеці [2]



Аналітичний звіт UNODC є комплексним дослідженням транснаціональної злочинності у сфері поводження з відходами та незаконного їх переміщення, яке розглядає проблему у взаємозв'язку з глобальною економікою, екологічною безпекою, корпоративною відповідальністю та діяльністю організованих злочинних груп. Документ формує системне бачення незаконного обігу відходів як структурного явища сучасної глобалізованої економіки, а не як ізольованого екологічного правопорушення.

У центрі дослідження перебуває економічна природа відходів як специфічного об'єкта злочину. На відміну від більшості нелегальних товарів, відходи первинно мають негативну вартість, оскільки їх власник зобов'язаний оплачувати витрати на збирання, транспортування, обробку та утилізацію. Саме ця особливість створює парадоксальну економічну мотивацію: незаконна діяльність стає способом мінімізації витрат, а у випадку певних категорій відходів — ще й джерелом прибутку через вилучення цінних компонентів, зокрема металів або дорогоцінних елементів у складі електронних відходів. Автори демонструють, що глобальний легальний ринок управління відходами у 2024 році оцінювався приблизно у 1,2 трильйона доларів США, що свідчить про його стратегічну вагу для світової економіки та водночас пояснює привабливість цього сектору для кримінальних структур.

Значна увага приділяється правовому контексту, насамперед Базельській конвенції про контроль за транскордонними перевезеннями небезпечних відходів та їх видаленням. Конвенція встановлює обов'язок криміналізувати незаконний обіг небезпечних відходів, однак її мандат зосереджений переважно на транскордонному вимірі, залишаючи поза повним регулюванням внутрішні національні схеми незаконного поводження з відходами. Звіт підкреслює, що хоча більшість держав криміналізували відповідні правопорушення, практична ефективність правозастосування залишається нерівномірною, а санкції часто не мають достатнього стримувального ефекту, особливо у випадку великих комерційних операторів.

Аналітичний блок, присвячений масштабам та потокам, демонструє складну та багатовекторну географію переміщення відходів. Хоча традиційно вважається, що незаконні відходи рухаються з країн із високим рівнем доходу до країн із низьким рівнем доходу, емпіричні дані вказують на

[2] https://www.unodc.org/documents/data-and-analysis/Crimes%20on%20Environment/Waste_Crime/ECR_3a.Waster_Crime_and_Trafficking.pdf

значний обсяг внутрішньорегіональних потоків, зокрема в межах Європи. Водночас автори наголошують на суттєвій проблемі дефіциту даних поза європейським регіоном, що створює географічне викривлення статистики та унеможливлює точну оцінку глобального обсягу незаконного обігу. Особливо проблематичною є ситуація з електронними відходами, які є одним із найшвидше зростаючих потоків, тоді як лише незначна частка їх обробляється екологічно безпечним способом.

Окремий розділ присвячено структурі учасників, залучених до незаконних операцій. Звіт розмежовує ролі виробників відходів (осіб, діяльність яких призводить до утворення відходів), посередників і брокерів, логістичних операторів та кінцевих отримувачів і переробників. У багатьох випадках злочинні схеми реалізуються через поєднання легальних і нелегальних структур, що ускладнює виявлення та доведення умислу. Організовані злочинні групи активно використовують компанії-оболонки, фіктивні документи, транзитні юрисдикції та фрагментацію ланцюга постачання для розмивання відповідальності. Документ підкреслює, що значна частина справ пов'язана з корпоративними суб'єктами, які або свідомо порушують вимоги законодавства, або використовують паралельні нелегальні операції поряд із легальним бізнесом.

Схеми незаконного обігу відходів включають декласифікацію небезпечних відходів як безпечних, фальсифікацію ліцензій і митних документів, маркування відходів як уживаних товарів, змішування небезпечних та не небезпечних матеріалів, використання транзитних країн для ускладнення маршруту та створення видимості легальності. Внутрішні злочини охоплюють незаконне захоронення, спалювання, зберігання без дозволів і використання відходів у будівельних роботах без дотримання екологічних стандартів. Така складність ланцюга управління відходами, поєднана з різними класифікаційними підходами, створює значні труднощі для кримінального переслідування.

Документ приділяє суттєву увагу основним причинам та факторам, що стимулюють злочинну діяльність. Головним мотивом визначено економічну вигоду, яка виникає внаслідок високої вартості легальної утилізації та наявності ринку вторинної сировини. Підвищення екологічних стандартів, запровадження нових регуляторних вимог і зростання обсягів відходів парадоксально можуть розширювати можливості для нелегальної діяльності за відсутності належного контролю. Додатковими факторами є корупція, слабкість інституцій, низькі штрафи, нестача спеціалізованих знань у правоохоронних органів і

Висновки:

- **Летальне політичне насильство є структурною, а не випадковою проблемою.** Необхідно створити централізовану державну систему моніторингу політично мотивованих злочинів із інтеграцією даних поліції, прокуратури та фінансової розвідки для раннього виявлення ескалації конфліктів.
- **Найвищий ризик концентрується на муніципальному рівні.** Потрібні цільові програми захисту місцевих депутатів і активістів у зонах земельних та ресурсних конфліктів, включаючи механізми превентивної охорони та спеціалізовані прокурорські підрозділи.
- **Домінування вогнепальної зброї та контрактних виконавців свідчить про існування організованого ринку насильства.** Політика контролю зброї має поєднуватися з фінансовими розслідуваннями, відстеженням підозрілих транзакцій та аналізом платіжних потоків, пов'язаних із замовленням убивств.
- **Політичні кризи та виборчі цикли потребують спеціальних режимів безпеки.** У періоди підвищеної політичної напруги необхідне посилення захисту кандидатів і активістів, а також міжвідомчі превентивні заходи для запобігання насильницькій ескалації.

відсутність ефективної координації між екологічними регуляторами та органами кримінальної юстиції.

Соціальні та екологічні наслідки незаконного обігу відходів описуються як багатовимірні та довгострокові. Незаконні полігони та несанкціоноване спалювання призводять до значних витрат на очищення територій, шкоди здоров'ю населення та деградації екосистем. Особливо вразливими є країни з низьким рівнем доходу, де небезпечні відходи часто обробляються в неформальному секторі без належних засобів захисту, що створює ризики отруєння важкими металами, канцерогенами та іншими токсичними речовинами. Таким чином, економічні вигоди злочинців трансформуються у зовнішні витрати для суспільства.

У частині, присвяченій реагуванню, автори аналізують міжнародні механізми співпраці, зокрема мережу ENFORCE у межах Базельської конвенції, та підкреслюють необхідність гармонізації законодавства, посилення корпоративної відповідальності та підвищення ефективності санкцій. Особлива увага приділяється проблемі обмежених ресурсів для перевірки контейнерів, недостатній кількості спеціалізованих підрозділів та слабкій інтеграції інформаційних систем між державами. Документ також наголошує на необхідності розвивати механізми відстеження відходів від моменту їх утворення до кінцевої утилізації, що є ключовим інструментом запобігання нелегальним потокам.

У підсумку звіт формує концептуальну модель, у межах якої незаконний обіг відходів постає як складний транснаціональний феномен, що поєднує екологічні правопорушення, організовану злочинність, фінансові злочини та корупцію. Він демонструє, що без інтегрованого підходу, який поєднує кримінальне переслідування, фінансові розслідування, корпоративну відповідальність і міжнародну координацію, масштаби проблеми зростатимуть разом із глобальним ринком управління відходами. Документ позиціонує боротьбу з незаконним обігом відходів як невід'ємну складову ширшої стратегії забезпечення екологічної безпеки, економічної доброчесності та верховенства права у глобальному вимірі.

Ризики відмивання коштів і фінансування тероризму у транзакціях зі стейблкоїнами: висновки цільового звіту FATF [3]

Документ FATF є спеціалізованим аналітичним дослідженням, спрямованим на вивчення ризиків відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення (ВК/ФТ/ФР), що виникають у зв'язку з використанням стейблкоїнів та некастодіальних криптовалютних гаманців, зокрема у транзакціях типу peer-to-peer. У документі розглядається розвиток глобальної екосистеми стейблкоїнів, їх роль у криптоекономіці та зростаючій взаємодії з традиційною фінансовою системою, а також аналізуються загрози, вразливості та практичні заходи протидії незаконному використанню таких інструментів.

Звіт виходить із того, що за останнє десятиліття стейблкоїни стали одним із ключових інструментів криптовалютного ринку. Починаючи з появи перших стейблкоїнів, прив'язаних до долара США, у 2014 році, їх кількість та економічне значення різко зросли. Станом на 2025 рік у світі перебувало

[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf

в обігу понад 250 стейблкоїнів із сукупною ринковою капіталізацією понад 300 млрд доларів США, а їх щоденні торгові обсяги перевищували обсяги операцій із біткоїном. Стейблкоїни становлять значну частку всіх транзакцій у мережах блокчейну, що відображає їх центральну роль у криптоекономіці, особливо як засобу розрахунків і збереження вартості. Основну частину ринку формують централізовані фіатно-забезпечені стейблкоїни, переважно прив'язані до долара США, тоді як криптовалютно-забезпечені та алгоритмічні стейблкоїни займають значно меншу частку ринку.

Документ детально пояснює природу та функціонування стейблкоїнів, визначаючи їх як різновид віртуальних активів, що має механізм стабілізації ціни шляхом прив'язки до певного референтного активу, найчастіше фіатної валюти. У звіті розглядаються різні моделі стейблкоїнів, зокрема забезпечені активами, забезпечені іншими криптоактивами та алгоритмічні моделі, які підтримують стабільність вартості через програмні механізми регулювання пропозиції. Незалежно від технічної моделі, FATF розглядає стейблкоїни як віртуальні активи, а суб'єкти, що надають послуги з їх обігу, можуть підпадати під визначення постачальників послуг віртуальних активів або фінансових установ відповідно до стандартів FATF.

У звіті також описується структура екосистеми стейблкоїнів та ролі її ключових учасників. До них належать емітенти стейблкоїнів, які випускають і погашають токени та управляють стабілізаційними механізмами; кастодіани резервів, що зберігають активи, які забезпечують стейблкоїни; криптобіржі та інші постачальники послуг віртуальних активів, які забезпечують торгівлю, обмін і зберігання таких активів; платіжні сервіси та карткові мережі, які інтегрують стейблкоїни у платіжну інфраструктуру; а також провайдери аналітики блокчейнів, що аналізують транзакційні дані для виявлення ризиків незаконної діяльності. Окремим елементом екосистеми є некастодіальні криптогаманці, у яких користувачі самостійно контролюють свої приватні ключі і можуть здійснювати транзакції без участі посередників.

Значна частина звіту присвячена аналізу сучасної ситуації та загроз, пов'язаних із використанням стейблкоїнів. FATF констатує, що стейблкоїни дедалі частіше використовуються у схемах відмивання коштів, фінансування тероризму та обходу санкцій. Згідно з аналітичними оцінками, у 2025 році стейблкоїни становили переважну частку незаконних криптовалютних транзакцій. Їх популярність серед злочинців пояснюється поєднанням кількох характеристик: стабільності вартості, високої ліквідності, можливості швидких міжнародних переказів і сумісності з різними блокчейн-мережами. Ці властивості дозволяють злочинцям використовувати стейблкоїни як зручний інструмент для переміщення незаконних коштів між різними юрисдикціями та фінансовими системами.

У документі детально описуються різні категорії загрозливих учасників, які використовують стейблкоїни. Серед них виділяються державні кіберзлочинні групи, пов'язані з КНДР, які активно використовують криптоактиви для фінансування програм озброєнь і обходу міжнародних санкцій. Зокрема, згадуються випадки масштабних крадіжок криптоактивів, після яких викрадені кошти проходили складний процес відмивання через численні гаманці, міксери та децентралізовані біржі, після чого конвертувалися у стейблкоїни та обмінювалися на фіатні кошти через позабіржових брокерів. Аналогічні механізми використовуються іранськими структурами для фінансування закупівлі військових технологій та підтримки союзних збройних груп. У звіті також підкреслюється роль стейблкоїнів у діяльності організованих злочинних угруповань, зокрема у наркоторгівлі, де вони використовуються для розрахунків за прекурсори синтетичних наркотиків, а також для відмивання доходів від незаконної діяльності.

Окремий розділ присвячений використанню стейблкоїнів у схемах фінансування тероризму. Терористичні організації все частіше застосовують стейблкоїни для збору пожертв і переказу коштів між своїми структурами, використовуючи соціальні мережі, зашифровані месенджери та

онлайн-платформи. Донорів заохочують надсилати кошти на змінні адреси криптогаманців, після чого кошти розбиваються на численні невеликі транзакції і проходять через кілька посередників або децентралізованих платформ, що ускладнює їх відстеження. Така тактика дозволяє фінансовим мережам терористичних організацій продовжувати функціонувати навіть після блокування окремих адрес або платформ.

Звіт також аналізує ключові вразливості екосистеми стейблкоїнів. Однією з головних проблем є транскордонний характер цих активів, що дозволяє емітентам та посередникам працювати з юрисдикцій зі слабким регулюванням або недостатнім наглядом. Це створює умови для регуляторного арбітражу, коли компанії обирають юрисдикції з мінімальними вимогами до фінансового моніторингу. Іншою проблемою є складні схеми багатостороннього випуску стейблкоїнів, у яких кілька емітентів із різних країн беруть участь у створенні одного активу, що ускладнює визначення відповідальності та координацію між регуляторами.

Особливо серйозною вразливістю визнаються транзакції peer-to-peer через некастодіальні гаманці. Такі операції здійснюються без участі постачальників послуг віртуальних активів або фінансових установ, а тому не підпадають під стандартні вимоги щодо належної перевірки клієнтів, моніторингу транзакцій та подання повідомлень про підозрілі операції. Хоча транзакції у публічних блокчейнах є видимими, вони залишаються псевдонімними і не містять інформації про реальних власників гаманців. Додаткові труднощі створює використання таких методів маскування, як часта зміна адрес гаманців, дроблення транзакцій, використання міксерів і переміщення коштів між різними блокчейн-мережами.

У документі також підкреслюється, що певна частина транзакцій у криптовалютних екосистемах відбувається поза блокчейном. Наприклад, перекази між клієнтами однієї криптобіржі можуть здійснюватися у внутрішніх облікових системах платформи без відображення у публічному блокчейні. Це означає, що правоохоронні органи та підрозділи фінансової розвідки не мають прямого доступу до всієї інформації про такі операції і залежать від співпраці з відповідними платформами.

Друга частина звіту зосереджена на практиках зниження ризиків незаконного використання стейблкоїнів. FATF наголошує на необхідності повної імплементації стандартів щодо

Висновки:

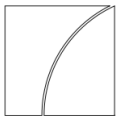
- **Стейблкоїни стали основним інструментом незаконних криптовалютних операцій.** За оцінками аналітики блокчейнів, у 2025 році близько 84% незаконних транзакцій з криптоактивами здійснювалися саме у стейблкоїнах, що потребує посилення регуляторного контролю за емітентами та постачальниками послуг віртуальних активів.
- **P2P-транзакції через некастодіальні гаманці є найбільшою регуляторною прогалиною у системі ПВК/ФТ.** Такі операції здійснюються без участі регульованих посередників і тому не підпадають під вимоги щодо ідентифікації клієнтів, моніторингу транзакцій та подання повідомлень про підозрілі операції.
- **Державні та кримінальні суб'єктми активно використовують стейблкоїни для обходу санкцій і фінансування злочинної діяльності.** Зокрема, групи, пов'язані з КНДР та Іраном, застосовують стейблкоїни для відмивання викрадених криптоактивів, закупівлі військових компонентів та фінансування програм озброєнь.
- **Емітенти стейблкоїнів можуть відігравати ключову роль у протидії фінансовим злочинам через технологічні механізми контролю.** Використання функцій заморожування активів, знищення токенів, формування переліку дозволених адрес, формування переліку заборонених адрес та інструментів аналітики блокчейну дозволяє блокувати активи, пов'язані з незаконною діяльністю, і підтримувати розслідування правоохоронних органів.

постачальників послуг віртуальних активів, передбачених Рекомендацією 15, включаючи ліцензування або реєстрацію таких суб'єктів, застосування процедур належної перевірки клієнтів, моніторинг транзакцій, виконання санкційних вимог та подання повідомлень про підозрілі операції. Особливу роль відіграє ефективний нагляд за криптобіржами та іншими посередниками, оскільки саме вони є ключовими точками контролю у системі фінансового моніторингу криптоактивів.

Звіт також звертає увагу на потенціал технологічних механізмів контролю, які можуть застосовувати емітенти стейблкоїнів. Завдяки програмованості смарт-контрактів емітенти можуть впроваджувати функції заморожування або блокування активів, створювати списки дозволених або заборонених адрес, обмежувати обсяги транзакцій та виконувати інші заходи, спрямовані на зменшення ризиків незаконної діяльності. Використання таких інструментів у поєднанні з аналітикою блокчейнів дозволяє швидше виявляти підозрілі транзакції та реагувати на запити правоохоронних органів.

У підсумку документ підкреслює, що стрімке зростання ринку стейблкоїнів створює нові виклики для глобальної системи протидії відмиванню коштів і фінансуванню тероризму. Водночас ці виклики можуть бути подолані через поєднання ефективного регулювання, міжнародної координації, використання сучасних технологічних інструментів моніторингу та активної співпраці між державним і приватним секторами. Таким чином, звіт формує стратегічне бачення того, як система ПВК/ФТ/ФР повинна адаптуватися до нової фінансової реальності, у якій стейблкоїни відіграють дедалі важливішу роль.

Від готівки до криптоактивів: послідовний регуляторний підхід до незаконних платежів [4]



Документ Банку міжнародних розрахунків (BIS) є фундаментальним методологічним трактатом, який концептуалізує та переосмислює ефективність архітектури ПВК/ФТ в умовах безпрецедентної еволюції глобального платіжного ландшафту. Автори дослідження, застосовуючи глибинний політекономічний підхід, відходять від традиційного технологічного детермінізму, пропонуючи натомість аналітичну парадигму «відмінності за дизайном» (difference by design). Ця методологія класифікує платіжні інструменти не за їхньою формою (фіатні, електронні чи криптографічні), а за наявністю або відсутністю ідентифікованих посередників — підзвітних суб'єктів — у ланцюгу створення та підтвердження транзакції. Дослідження постулює, що саме ці посередники виконують критичну інституційну функцію «гейткіперів», на яких покладається регуляторний тягар здійснення належної перевірки клієнтів (CDD), безперервного транзакційного моніторингу та інформування підрозділів фінансової розвідки (ПФР) про підозрілі операції (STR). Відповідно, інструменти з високим рівнем посередництва, такі як депозити комерційних банків та електронні гроші, структурно забезпечують найвищу ймовірність виявлення незаконних операцій, тоді як інструменти без посередників, зокрема готівка, офлайн-версії цифрових валют центральних банків (CBDC) та некастодіальні (self-hosted) криптогаманці, створюють асиметричні ризики для фінансової безпеки через їхню архітектурну непрозорість.

[4] https://www.bis.org/publ/bppdf/bispap166.pdf

Центральним концептом, що пояснює динаміку переміщення незаконних капіталів у цьому багатополярному платіжному середовищі, є «ефект водяного ліжка» (waterbed effect). Згідно з цією поведінковою моделлю, зловмисники діють як високораціональні економічні агенти, котрі постійно реоптимізують свої стратегії на основі аналізу витрат і вигод. Якщо регуляторний тиск посилюється в одному сегменті — наприклад, через впровадження суворіших стандартів KYC у традиційному банківському секторі або на кастодіальних криптобіржах, — злочинна активність не зникає, а миттєво «виштовхується» в найменш контрольовані зони платіжної екосистеми. Цей ефект регуляторного арбітражу системно підриває ефективність ізольованих секторальних реформ, доводячи неможливість подолання відмивання коштів без наскрізного бачення всієї сукупності фінансових каналів. Автори наголошують, що в умовах зростання попиту на приватність, перетікання користувачів до нерегульованих інструментів може бути зумовлене не лише злочинним умислом, але й легітимним бажанням захистити персональні дані. Цей компроміс між інформаційною приватністю та вимогами фінансової безпеки є однією з найскладніших юридичних і політичних дилем, оскільки ПВК/ФТ за своєю природою вимагає «обмеженої приватності» (bounded privacy) як суспільного блага для захисту цілісності ринків.

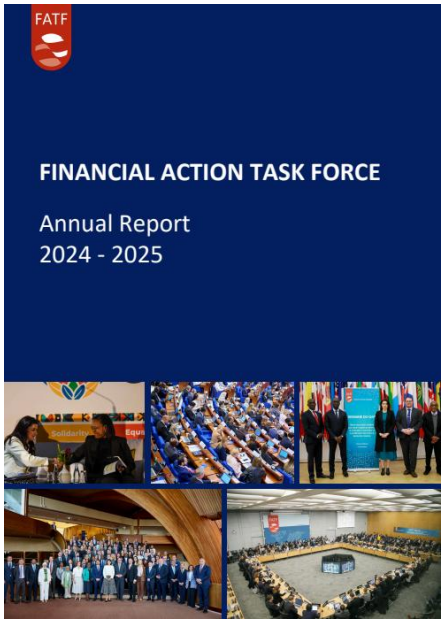
Для нейтралізації ризиків регуляторного арбітражу документ пропонує впровадження дворівневої регуляторної логіки, що спирається на принципи Lex Generalis та Lex Specialis. Рівень Lex Generalis вимагає встановлення уніфікованих, базових вимог комплаєнсу для всіх платіжних інструментів, що архітектурно передбачають участь ідентифікованих посередників. Це означає, що комерційні банки, емітенти електронних грошей та провайдери кастодіальних криптопослуг (CASP) повинні підпорядковуватися ідентичним стандартам моніторингу та звітності, що усуває стимули для переміщення брудних коштів між різними типами регульованих установ. Водночас, рівень Lex Specialis застосовується до дезінтермедійованих інструментів, де імплементація стандартних правил FATF є технічно неможливою. У цьому контексті регуляторні зусилля мають бути сконцентровані на «точках дотику» — інтерфейсах конвертації, де анонімні активи (наприклад, готівка або токени з некастодіальних гаманців) входять у контрольовану фінансову систему або виходять з неї. Крім того, специфічні заходи мають включати встановлення жорстких жорстких кількісних лімітів на зберігання та проведення транзакцій для інструментів без посередників, аналогічно до існуючих у багатьох країнах обмежень на готівкові розрахунки.

Висновки:

- **Управління ризиками комплаєнсу в епоху Web3 вимагає від суб'єктів фінансового моніторингу переходу до архітектурно-орієнтованого підходу:** ступінь ризику інструменту визначається не його технологічною формою, а здатністю протоколу забезпечити наявність відповідального посередника-гейткіпера.
- **Для нівелювання «ефекту водяного ліжка» наглядові органи мають перенести фокус уваги на аудит «точок дотику»**, розробивши спеціалізовані критерії EDD для операцій конвертації між некастодіальними гаманцями та регульованими рахунками у фіатній валюті.
- **Національним регуляторам необхідно імплементувати концепцію Lex Specialis під час проектування режимів регулювання стейблкоїнів**, превентивно закладаючи в їхні смарт-контракти алгоритмічні ліміти на обсяг анонімних транзакцій та загальні баланси утримання для мінімізації привабливості цих інструментів для тіньової економіки.
- **Централізація нагляду на наднаціональному рівні (за прикладом створення AMLA) стає критичною умовою для подолання регуляторного арбітражу**, оскільки децентралізований крипто-ринок легко обходить локальні бар'єри, вимагаючи гомогенного правозастосування на континентальних масштабах.

Як практичний полігон для тестування цієї концептуальної моделі, автори здійснюють глибокий розбір еволюції регуляторної бази Європейського Союзу, що кульмінувала у масштабній реформі архітектури ПВК/ФТ. Документ аналізує Регламент про ринки криптоактивів (MiCAR), який ліквідував тривалий правовий вакуум, перетворивши європейських постачальників послуг з криптоактивів на повноцінних суб'єктів первинного фінансового моніторингу. Окрему увагу приділено створенню Європейського органу з питань протидії відмиванню коштів (AMLA) та переходу від директив до Регламенту про ПВК (AMLR), який діє як закон прямої дії, усуваючи фрагментацію національних законодавств, що раніше активно експлуатувалася транснаціональними криміналними мережами. У контексті інновацій документ детально розглядає розробку правової рамки для цифрового євро. Аналітики BIS проводять чітку межу між онлайн-CBDC, що функціонуватиме через традиційних посередників з повним збереженням аудиторського сліду, та офлайн-CBDC, яка призначена для імітації приватності готівки у безконтактних транзакціях. Запровадження офлайн-версії цифрового євро є найбільш ризикованим елементом з точки зору ПВК/ФТ, оскільки цифровий формат позбавлений фізичних обмежень готівки (вага, обсяг), що робить його ідеальним інструментом для контрабанди капіталу. Саме тому розробка офлайн-CBDC супроводжується жорсткими дебатами щодо вбудованих технологічних обмежень балансу та інтеграції елементів криптографічної простежуваності, що залишаються недоступними для комерційних банків, але можуть бути розкриті за рішенням суду.

Річний звіт FATF (2024-2025): Стратегічні пріоритети, оцінка глобальних ризиків та нові стандарти [5]



Річний звіт FATF за 2024-2025 роки є важливим документом, що підбиває підсумки першого року головування Елізи де Анда Мадразо та фіксує зсув організації від моніторингу технічної комплаєнтності до оцінки реальної операційної ефективності національних систем ПВК/ФТ/ФР. Звіт розгортається навколо чотирьох фундаментальних стратегічних пріоритетів, які формують глобальний порядок денний. Першим пріоритетом є радикальне підвищення ефективності процесу взаємного оцінювання (peer review) через запуск нового, п'ятого раунду перевірок, який фокусується на більш жорстких строках, посиленому ризик-орієнтованому підході (РОП) та глибинному аудиті результативності діяльності правоохоронних органів. Другим напрямком є зміцнення Глобальної мережі, що об'єднує понад 200 юрисдикцій і покриває 99% світового ВВП, з особливим акцентом на інституційну підтримку держав із низьким потенціалом через регіональні органи за типом FATF (FSRB). Третій пріоритет стосується посилення імплементації стандартів у таких складних доменах як прозорість бенефіціарної власності та механізми конфіскації і повернення активів, паралельно з мінімізацією непередбачуваних наслідків, таких як невиправданий «де-рискінг» НПО. Четвертий пріоритет передбачає проактивне реагування на технологічні зрушення у фінансах, зокрема повноцінне охоплення віртуальних активів та модернізацію стандартів платіжної прозорості.

[5] https://www.fatf-gafi.org/content/dam/fatf-gafi/annual-reports/fatf-annual-report-2024-2025.pdf.coredownload.pdf

Документ оприлюднює деталізовані та тривожні статистичні дані щодо ефективності глобальної протидії складним схемам фінансування розповсюдження зброї масового знищення та ухилення від міжнародних санкцій, що базуються на звіті FATF від червня 2025 року. Аудит виявив критичну слабкість світової системи: лише 16% оцінених держав продемонстрували високий або суттєвий рівень ефективності у впровадженні цільових фінансових санкцій (ЦФС) відповідно до резолюцій Ради Безпеки ООН. Деконструкція архітектури санкційного обходу виявила глибоку інтеграцію цих процесів у легальну світову торгівлю та фінансову систему. Близько 80% ідентифікованих схем використовують складні багаторівневі корпоративні структури (підставні компанії-оболонки) у різних юрисдикціях для приховування КБВ. Вражає те, що 80% випадків пов'язані з торговельними маніпуляціями — фальсифікацією супровідних документів, приховуванням товарів подвійного призначення та маніпуляціями з митною вартістю, що підкреслює фундаментальну важливість моніторингу відмивання коштів через торгівлю (TBML). Крім того, понад 70% операцій здійснюються через формальні банківські канали із застосуванням багаторівневих кореспондентських рахунків, 66% транзакцій супроводжуються професійними посередниками (юристами, постачальниками трастових послуг, логістичними брокерами), а кожен четвертий випадок (25%) включає використання віртуальних активів для розриву фінансового сліду.

Компонент схеми ухилення від санкцій / ФР	Частота використання у досліджених кейсах (%)	Характеристика вразливості в системі ПВК/ФТ/ФР
Підставні компанії-оболонки	~80%	Непрозорість корпоративних реєстрів та використання номінальних директорів.
Торговельні маніпуляції	80%	Відрив фінансового моніторингу від митного контролю та логістичних даних.
Формальні банківські канали	>70%	Експлуатація кореспондентського банкінгу через nested accounts (вкладені рахунки).
Професійні посередники (ВНУП)	~66%	Зловживання адвокатською таємницею та слабкий комплаєнс у нефінансовому секторі.
Віртуальні активи та VASP	25%	Використання міксерів, OTC-брокерів та слабка імплементація Travel Rule.

Не менш критичною є оцінка глобальних ризиків фінансування тероризму (ФТ). Комплексне дослідження, що охопило дані понад 80 юрисдикцій за 10 років, виявило, що 69% країн мають серйозні або структурні недоліки у розслідуванні та судовому переслідуванні злочинів, пов'язаних з ФТ. Цей розрив між технічною наявністю законів та їх практичним застосуванням підсилюється низкою макроекономічних вразливостей: у 30% випадків ключовим фактором ризику визначено контроль терористичних груп над природними ресурсами, ще у 30% — наявність прозорих кордонів, а у 20% — системну корупцію та домінування готівкової тіньової економіки. У відповідь на ці виклики, а також для реалізації дорожньої карти G20 щодо покращення транскордонних платежів, FATF у червні 2025 року ухвалила епохальні зміни до Рекомендації 16, що регулює платіжну прозорість. Нові вимоги стандартизують дані, які повинні супроводжувати кожен платіж, враховуючи перехід світової фінансової системи на стандарт повідомлень ISO 20022. Оновлений стандарт не лише усуває інформаційні розриви під час швидких електронних переказів, але й зобов'язує фінансові установи впроваджувати технології

попередньої верифікації банківських реквізитів отримувача, що має стати потужним інструментом протидії кібершахрайству та соціальній інженерії.

Стратегічний баланс між безпекою та інклюзією відображено в оновленому Керівництві FATF щодо фінансової інклюзії та відповідних змінах до Рекомендації 1 (Ризик-орієнтований підхід), фіналізованих у червні 2025 року. FATF офіційно визнає, що надмірно консервативний підхід, який призводить до масового закриття рахунків або відмови в обслуговуванні цілим категоріям клієнтів (мігрантам, малозабезпеченим верствам, НПО), парадоксальним чином підвищує загальнонаціональні ризики відмивання коштів. Виштовхування суб'єктів у нерегульований готівковий простір позбавляє ПФР видимості фінансових потоків. Тому нова доктрина FATF категорично вимагає від регуляторів заохочувати застосування спрощених заходів належної перевірки (SDD) для продуктів та клієнтів із підтвердженим низьким рівнем ризику, створюючи безпечну гавань для фінансових установ, які сприяють інклюзії, та звільняючи їх від необґрунтованих наглядових санкцій. Водночас ситуація у сфері віртуальних активів залишається зоною найвищої регуляторної напруги: 75% оцінених юрисдикцій не виконують повною мірою вимоги Рекомендації 15, що свідчить про значне відставання крипто-комплаєнсу від стандартів традиційного фінансового сектору та створює глобальні лазівки для ухилення від санкцій та відмивання коштів.

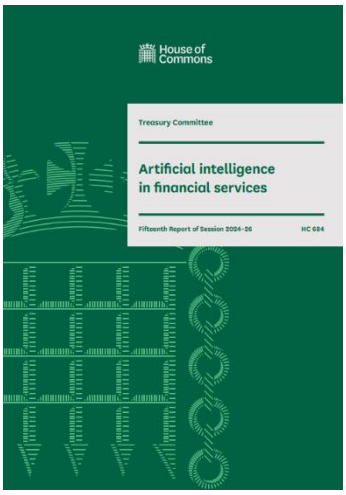
Висновки:

- **Банки та платіжні установи зобов'язані провести масштабний аудит своїх систем обробки платежів на відповідність стандарту ISO 20022**, забезпечивши здатність передавати розширені метадані про ініціатора та бенефіціара без втрат у транскордонних кореспондентських ланцюгах.
- З огляду на те, що 80% схем фінансування розповсюдження ЗМЗ спираються на маніпуляції з торговельними операціями, **комплаєнс-підрозділам банків необхідно інтегрувати модулі моніторингу TBML**, здійснюючи скринінг не лише фінансових реквізитів, але й митних кодів товарів, логістичних маршрутів та контрагентів у ланцюгах постачання.
- **Національним регуляторам необхідно розробити та запровадити чіткі інструкції щодо застосування SDD**, які б гарантували фінансовим установам захист від наглядових санкцій у разі прийняття на обслуговування низькоризикових категорій клієнтів, тим самим перешкоджаючи шкідливій практиці "де-рискінгу".
- Враховуючи, що 75% юрисдикцій не відповідають вимогам щодо регулювання віртуальних активів, **СПФМ повинні імплементувати жорсткі політики блокування транзакцій або застосування EDD для будь-яких взаємодій з постачальниками криптопослуг (VASP), які зареєстровані в країнах зі слабким рівнем імплементації «Travel Rule».**

Штучний інтелект у фінансових послугах [6]

Звіт Казначейського комітету Палати громад Парламенту Великої Британії являє собою глибоке дослідження впливу штучного інтелекту (AI) на екосистему фінансових послуг, розглядаючи його крізь призму як операційних можливостей, так і екзистенційних загроз для фінансової стабільності та захисту споживачів. Документ фіксує тектонічний зсув у технологічній інфраструктурі ринку: станом на 2025 рік понад 75% фінансових установ Великої Британії інтегрували рішення на базі AI у свою діяльність, причому авангардом цього процесу виступають страхові корпорації та транснаціональні банківські конгломерати. Методологія комітету, що

[6] https://committees.parliament.uk/publications/51128/documents/283671/default/



спирається на десятки експертних суджень та аналіз регуляторних звітів, розкриває дуальну природу алгоритмічних інновацій у сфері ПВК/ФТ. З одного боку, предикативний AI радикально оптимізує рутинні комплаєнс-процеси — наприклад, використання алгоритмів машинного навчання для аналізу документації при онбордингу дозволило окремим банкам скоротити час на процедури KYC на 90%, а також суттєво підвищити точність виявлення аномальних патернів, зменшуючи частку хибнопозитивних спрацьовувань. З іншого боку, генеративний AI діє як потужний мультиплікатор загроз, полегшуючи доступ до інструментів фінансової злочинності. Зокрема, використання діпфейку для підробки аудіо та відео підтвердження особистості дозволяє зловмисникам обходити системи біометричної верифікації клієнтів та масштабувати складні схеми соціальної інженерії до рівня епідемії.Найбільш тривожний аналітичний блок звіту присвячений системним, макроекономічним ризикам для фінансової стабільності, які генеруються неконтрольованим використанням AI. Комітет ідентифікує феномен «стадної поведінки» як критичну вразливість сучасних ринків. Оскільки все більше фінансових інституцій покладаються на ідентичні або схожі масиви даних та алгоритмічні моделі для ухвалення торговельних і кредитних рішень, виникає ризик синхронної автоматизованої реакції на ринкові шоки. У стресових ситуаціях такі алгоритми можуть одночасно почати скидати активи, провокуючи каскадні обвали ліквідності, які розвиватимуться зі швидкістю, що перевищує здатність регуляторів втрутитися і зупинити паніку. Крім того, звіт розкриває загрозливі масштаби операційної концентрації та залежності британського фінансового сектора від вузького олігополістичного пулу технологічних гігантів. Згідно з даними Банку Англії, лише три провідні американські компанії забезпечують близько 75% хмарної інфраструктури, 45% розгортання базових моделей AI та 30% послуг обробки даних для фінансового сектору. Ця надконцентрація означає, що успішна кібератака, технічний збій або алгоритмічна галюцинація на рівні одного провайдера неминуче трансформується у системну кризу всієї банківської мережі країни.

Аспект впливу AI	Операційні переваги для ПВК/ФТ	Системні загрози та ризики (ПВК/ФТ та Стабільність)
Аналіз даних (KYC/CDD)	Зниження часу на обробку документів до 90%. Автоматизований збір даних з відкритих джерел (OSINT).	Вразливість до Deepfakes під час дистанційного онбордингу. Ризик дискримінаційної упередженості в алгоритмах скорингу.
Моніторинг транзакцій	Радикальне зменшення хибнопозитивних результатів. Виявлення неочевидних нелінійних зв'язків.	Ризик "чорного ящика": нездатність пояснити логіку блокування транзакції регулятору.
Архітектура ринку	Зниження витрат на персонал комплаєнс відділів. Пришвидшення швидкості транзакцій.	"Стадна поведінка" алгоритмів. Критична операційна залежність від 3-х провайдерів хмарних послуг (75% ринку).

У відповідь на ці безпрецедентні виклики Комітет жорстко оцінює існуючу регуляторну парадигму. На відміну від Європейського Союзу з його Законом про штучний інтелект (AI Act), Велика Британія не має спеціалізованого законодавства щодо AI у фінансах, покладаючись на технологічно нейтральний підхід, за якого Управління з фінансового нагляду (FCA) та Банк Англії застосовують до алгоритмів існуючі правила корпоративного управління та пруденційного нагляду. Парламентарі вважають таку реактивну позицію недостатньою і формулюють низку безапеляційних рекомендацій. Найважливішою інституційною вимогою є зобов'язання

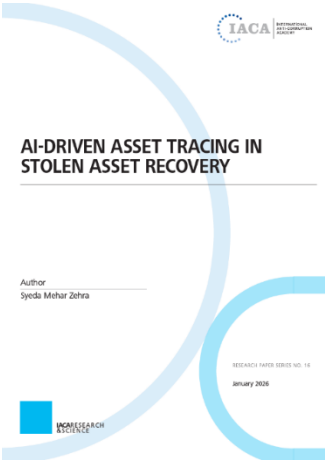
Казначейства Його Величності до кінця 2026 року офіційно визначити провідних провайдерів хмарних послуг та розробників генеративного AI як «Критичних третіх сторін» (Critical Third Parties). Цей статус, ідеологічно споріднений з європейським регламентом DORA, надасть фінансовим наглядовим органам безпрецедентні повноваження: вони зможуть здійснювати прямий аудит технологічних гігантів, перевіряти стійкість їхніх серверів та встановлювати обов'язкові стандарти кібербезпеки незалежно від їхньої географічної юрисдикції. Другою фундаментальною рекомендацією є вимога до Банку Англії та FCA негайно запровадити проведення стрес-тестів для фінансових установ, сфокусованих на використанні AI. Ці симуляції повинні перевірити здатність банків виживати в умовах синхронних алгоритмічних збоїв, атак з використанням отруєних даних (data poisoning) та масованих deepfake-кампаній.

Висновки:

- У відповідь на епідемію deepfake-шахрайства, **фінансовим установам критично необхідно модернізувати протоколи дистанційного онбордингу клієнтів**, інтегрувавши технології безперервного аналізу живої присутності та багатофакторної поведінкової біометрії, що не спирається виключно на візуальне розпізнавання обличчя.
- **Фінансові установи зобов'язані переглянути стратегії управління ризиками аутсорсингу** в очікуванні активації режиму «Критичних третіх сторін», закріпивши в контрактах з хмарними провайдерами безумовне право на проведення незалежного аудиту їхніх алгоритмічних та інфраструктурних рішень.
- **Підрозділам з комплаєнсу необхідно розробити та імплементувати жорсткі політики управління алгоритмічними ризиками**, які гарантуватимуть принцип «пояснюваності» AI: кожне автоматизоване рішення має супроводжуватися логічним обґрунтуванням, зрозумілим для аудитора та клієнта.
- **Регулятори мають розширити традиційні сценарії стрес-тестування банківського сектору, додавши симуляції каскадних відмов зовнішніх AI-моделей**, змушуючи банки резервувати додатковий капітал під операційні ризики, пов'язані з високим рівнем автоматизації.

Звіти окремих інституцій та експертів

Використання штучного інтелекту для відстеження та повернення викрадених активів у міжнародних антикорупційних розслідуваннях [7]



Документ, підготовлений у межах серії досліджень Міжнародної антикорупційної академії (IACA), присвячений аналізу потенціалу застосування штучного інтелекту для виявлення, відстеження та повернення активів, отриманих у результаті корупції та інших фінансових злочинів. У дослідженні підкреслюється, що повернення викрадених активів є одним із найбільш складних і водночас критично важливих компонентів глобальної антикорупційної політики, оскільки незаконні фінансові потоки, сформовані через корупцію, розкрадання державних коштів та відмивання доходів, щорічно позбавляють держави значних ресурсів, необхідних для соціально-економічного розвитку. За оцінками міжнародних організацій, лише незначна частина таких активів фактично повертається державам походження,

[7] https://www.iaca.int/media/attachments/2026/02/02/iacare_final.pdf

оскільки злочинці використовують складні транснаціональні фінансові структури, офшорні юрисдикції, мережі номінальних власників та інші механізми приховування бенефіціарного контролю. У цьому контексті традиційні механізми фінансових розслідувань і міжнародної правової допомоги часто виявляються повільними, фрагментованими та реактивними, що створює значний розрив між швидкістю розвитку фінансових технологій та можливостями державних інституцій ефективно протидіяти незаконним фінансовим потокам.

У дослідженні детально розглядається міжнародна правова архітектура повернення активів, сформована передусім Конвенцією Організації Об'єднаних Націй проти корупції (UNCAC), яка закріпила повернення активів як фундаментальний принцип міжнародного права. Глава V цієї Конвенції встановлює зобов'язання держав співпрацювати у питаннях ідентифікації, відстеження, заморожування, конфіскації та повернення доходів від корупційних злочинів. Конвенція передбачає широкий спектр механізмів співробітництва, включаючи пряме повернення активів, міжнародну конфіскацію, застосування конфіскації без обвинувального вироку, а також механізми взаємної правової допомоги. Паралельно з UNCAC важливу роль відіграє ініціатива Stolen Asset Recovery (StAR), створена Світовим банком та Управлінням ООН з наркотиків і злочинності (UNODC) з метою підтримки держав у процесі повернення незаконно привласнених активів. StAR надає технічну допомогу, розробляє методологічні рекомендації та сприяє зміцненню міжнародного співробітництва, проте навіть за наявності цих механізмів держави стикаються з численними перешкодами, серед яких – обмежений доступ до фінансової інформації, правові розбіжності між юрисдикціями, складність доведення бенефіціарного контролю над активами та низький рівень міжвідомчої координації.

У роботі підкреслюється, що ефективне повернення активів неможливе без інтенсивної міжнародної співпраці та оперативного обміну інформацією між державами. Автор наголошує на важливості принципів взаємності, проактивності, придатності та неформальної комунікації між компетентними органами різних країн. Особлива роль у цьому процесі належить підрозділам фінансової розвідки, які виступають ключовими інституціями у виявленні незаконних фінансових потоків та підтримці фінансових розслідувань. Завдяки аналізу підозрілих транзакцій, банківських даних, реєстрів нерухомості, корпоративних реєстрів та відкритих джерел інформації вони здатні встановлювати зв'язки між фізичними особами, юридичними структурами та активами. Однак навіть ці інституції стикаються з серйозними обмеженнями, зокрема недостатнім доступом до даних про бенефіціарну власність, браком аналітичних ресурсів, обмеженим використанням сучасних цифрових інструментів та нерівномірним рівнем міжнародного співробітництва.

У цьому контексті автор розглядає технологічні інновації, насамперед штучний інтелект, як потенційно трансформаційний інструмент для модернізації системи фінансових розслідувань. Застосування технологій штучного інтелекту дозволяє аналізувати великі обсяги структурованих і неструктурованих даних, виявляти аномальні фінансові операції та встановлювати складні мережеві зв'язки між учасниками незаконних схем. У дослідженні описано три ключові технологічні підходи, які можуть суттєво підвищити ефективність відстеження активів. Перший із них – мережевий аналіз, який дає змогу візуалізувати взаємозв'язки між фізичними особами, компаніями, трастами та фінансовими посередниками, що дозволяє розкривати приховані структури бенефіціарної власності. Другий підхід – виявлення аномалій, заснований на алгоритмах машинного навчання, які здатні визначати нетипові фінансові операції або поведінкові патерни, що можуть свідчити про спроби приховування незаконних активів. Третій підхід – обробка природної мови (NLP), яка дає змогу аналізувати великі масиви неструктурованих текстових даних, таких як судові документи, корпоративні звіти, журналістські розслідування або витоки інформації, наприклад матеріали типу Panama Papers або Pandora Papers. Поєднання цих технологій дозволяє створювати комплексні аналітичні системи, здатні

автоматично інтегрувати дані з різних джерел та формувати цілісну картину незаконних фінансових потоків.

Практичну цінність цих підходів автор демонструє на основі аналізу кількох масштабних міжнародних кейсів повернення активів. Зокрема, розглядається справа так званих «активів Абачі» в Нігерії, коли протягом 1990-х років президент Сани Абача та його оточення вивели з державного бюджету мільярди доларів через складну мережу офшорних компаній та банківських рахунків. Повернення цих коштів тривало понад два десятиліття та вимагало масштабної міжнародної співпраці. Аналіз показує, що використання штучного інтелекту могло б значно прискорити процес ідентифікації пов'язаних компаній і фінансових потоків. Іншим прикладом є скандал із державним інвестиційним фондом 1MDB у Малайзії, де приблизно 4,5 млрд доларів були незаконно привласнені через складні міжнародні фінансові операції. У цьому випадку застосування алгоритмів машинного навчання могло б дозволити значно раніше виявити підозрілі фінансові потоки та взаємозв'язки між офшорними структурами. Третій кейс стосується повернення активів між Узбекистаном і Швейцарією, пов'язаних із корупційними схемами у телекомунікаційному секторі. Аналіз показує, що використання AI-інструментів могло б значно полегшити обробку великих обсягів банківських даних, контрактів і судових документів, а також допомогти встановити зв'язки між компаніями-посередниками та кінцевими бенефіціарами.

На основі проведеного аналізу автор пропонує концептуальну ризик-орієнтовану модель використання штучного інтелекту у процесі повернення активів. Ця модель передбачає інтеграцію технологічних інструментів у три основні етапи процесу фінансових розслідувань. Перший етап полягає у виявленні активів шляхом автоматизованого аналізу даних із різних джерел, включаючи реєстри бенефіціарної власності, санкційні списки, корпоративні бази даних та витоки інформації. Другий етап передбачає пріоритизацію справ на основі оцінки ризиків, зокрема вартості активів, ймовірності їх повернення, рівня співпраці юрисдикцій та суспільної значущості справи. Третій етап передбачає створення цифрових платформ для міжнародної координації розслідувань та обміну інформацією між державними органами, міжнародними організаціями та фінансовими установами. Така модель дозволяє трансформувати процес повернення активів із реактивного підходу, що базується на окремих розслідуваннях, у

Висновки:

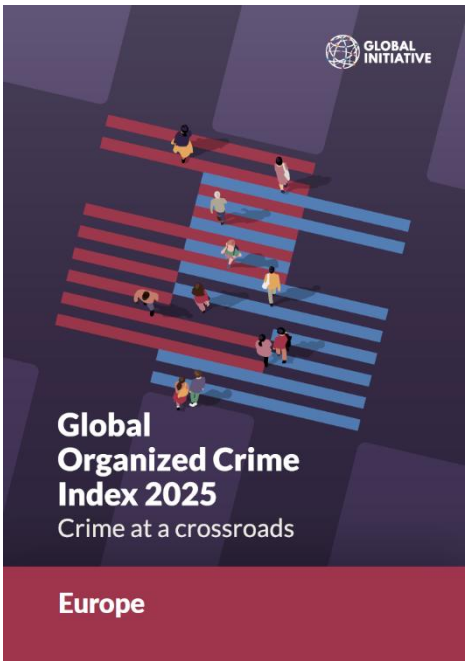
- **Штучний інтелект може радикально скоротити час фінансових розслідувань.** AI-алгоритми здатні автоматично аналізувати великі масиви фінансових і корпоративних даних, що дозволяє значно швидше виявляти схеми приховування активів, ніж традиційні методи ручного аналізу.
- **Інтеграція реєстрів бенефіціарної власності з AI-аналітикою є критичною умовою ефективного повернення активів.** Поєднання даних про бенефіціарів, корпоративних реєстрів, банківських транзакцій та відкритих джерел дозволяє виявляти складні корпоративні структури, які використовуються для приховування незаконних активів.
- **Ризик-орієнтована модель пріоритизації справ може значно підвищити результативність міжнародних розслідувань.** Використання AI для оцінки вартості активів, рівня співпраці юрисдикцій та ймовірності конфіскації дозволяє спрямовувати ресурси на справи з найбільшим потенціалом повернення активів.
- **Ефективне використання AI у сфері повернення активів потребує нової глобальної інституційної інфраструктури.** Необхідно створити міжнародні платформи співпраці (зокрема міжнародну AI-лабораторію під егідою UNODC та Світового банку), які забезпечать стандартизацію технологій, навчання фахівців та рівний доступ держав до аналітичних інструментів.

проактивну систему фінансової розвідки, орієнтовану на аналіз даних і раннє виявлення незаконних активів.

Окремий розділ дослідження присвячений правовим та етичним викликам використання штучного інтелекту у фінансових розслідуваннях. Автор наголошує, що використання AI пов'язане з ризиками порушення конфіденційності даних, алгоритмічної упередженості, недостатньої прозорості алгоритмів та потенційного порушення прав людини. Для мінімізації цих ризиків необхідно забезпечити відповідність систем штучного інтелекту міжнародним стандартам захисту даних, таким як GDPR, а також впроваджувати принципи прозорості, пояснюваності та людського контролю над автоматизованими рішеннями. Особливу увагу приділено концепції Explainable AI, яка передбачає можливість пояснення логіки прийняття рішень алгоритмами, що є критично важливим для використання результатів AI-аналізу у судових процесах.

У завершальній частині дослідження сформульовано низку політичних рекомендацій для урядів та міжнародних організацій. Серед них – інтеграція штучного інтелекту в механізми UNCAC і StAR, створення міжнародної лабораторії штучного інтелекту для повернення активів під егідою UNODC та Світового банку, інтеграція реєстрів бенефіціарної власності з аналітичними AI-системами, а також розробка стабільних фінансових механізмів для підтримки впровадження таких технологій у країнах, що розвиваються. Загалом дослідження робить висновок, що штучний інтелект має потенціал суттєво підвищити ефективність глобальної системи повернення активів, зменшити витрати на фінансові розслідування, прискорити міжнародну співпрацю та посилити прозорість використання повернених коштів, однак його впровадження повинно супроводжуватися належними правовими та етичними гарантіями.

Організована злочинність у Європі 2025: між високою інституційною стійкістю та адаптивною кримінальною екосистемою [8]



Документ, підготовлений Global Initiative Against Transnational Organized Crime, формує комплексну аналітичну картину стану організованої злочинності та інституційної спроможності протидії їй у 44 країнах Європи станом на 2025 рік. Індекс побудований на двох взаємопов'язаних компонентах — рівні кримінальності (який охоплює кримінальні ринки та злочинців) і рівні стійкості, що відображає здатність держав запобігати, виявляти та нейтралізовувати загрози. Середній показник кримінальності Європи становить 4,74, тоді як показник стійкості — 6,28, що є найвищим серед усіх регіонів світу. Водночас документ наголошує, що формально високий рівень стійкості не супроводжується сталим зниженням кримінальної активності, а сама злочинність демонструє здатність до адаптації та трансформації.

У вступній частині особливий акцент зроблено на впливі повномасштабної війни проти України на безпекову архітектуру Європи. Конфлікт розглядається не лише як геополітичний фактор, а як середовище, в якому злочинці адаптують свої операційні моделі, диверсифікують доходи та інтегруються в нові економічні процеси. Потенційне припинення бойових дій або період відбудови також

[8] https://static.rusi.org/strengthening-financial-investigation-wildlife-crime-central%20africa_0.pdf

ідентифікуються як етапи підвищеного ризику інфільтрації організованих мереж у державні програми, логістичні ланцюги та фінансові потоки.

Структурно Європа залишається другим найменш криміналізованим континентом після Океанії, однак внутрішньорегіональні диспропорції є суттєвими. Частина країн поєднує високий рівень стійкості з відносно низькою кримінальністю, проте існують юрисдикції, де високі показники кримінальності співіснують із формально розвиненою інституційною системою. Це свідчить про те, що рівень економічного розвитку або формальна демократичність не гарантують низького рівня організованої злочинності.

Найбільш значущим кримінальним ринком у Європі залишаються фінансові злочини. Йдеться про складні шахрайські схеми, інвестиційні афери, компрометацію ділової електронної пошти, податкові злочини, розкрадання та інші форми економічних зловживань. Ці злочини характеризуються високим рівнем цифровізації, транснаціональності та інтеграції у легальні фінансові системи. У Західній Європі вони часто пов'язані з використанням розвинених фінансових інструментів та відкритих ринків капіталу, тоді як у Центральній та Східній Європі значну роль відіграють фактори корупції та політичної вразливості. Фінансові злочини виступають не ізольованим сегментом, а інфраструктурною основою для інших кримінальних ринків, забезпечуючи легалізацію доходів і їх подальшу реінвестицію.

Висновки:

- **Попри найвищий у світі рівень інституційної стійкості, Європа не демонструє системного зниження кримінальності, що свідчить про розрив між нормативною відповідністю та реальною ефективністю протидії.** Посилення законодавства та міжнародної співпраці потребує доповнення проактивними механізмами управління ризиками у фінансовому та цифровому середовищі.
- **Фінансові та кіберзалежні злочини стали структурним ядром європейської організованої злочинності, інтегрованим у легальну економіку.** Їх масштаб і швидкість вимагають глибшої інтеграції фінансової розвідки, кібераналітики, контролю криптоінфраструктури та ризик-орієнтованого нагляду за цифровими платіжними системами.
- **Організована злочинність у Європі трансформується у мережеву, мультинаціональну та гнучку модель, де іноземні учасники відіграють дедалі більшу роль.** Це потребує розширення спільних транскордонних розслідувань, уніфікації процедур конфіскації активів і системного обміну фінансовою інформацією між юрисдикціями.
- **Найбільш уразливими залишаються фінансові механізми, логістичні хаби та сфери з високою концентрацією економічних інтересів, тоді як слабкість антивідмивальних інструментів і прозорості врядування створює довгострокові ризики інфільтрації державних та приватних структур.** Без посилення підзвітності, бенефіціарної прозорості та реальної імплементації ризик-орієнтованого підходу стратегічне стримування організованої злочинності залишатиметься обмеженим.

Другим за значущістю напрямом є кіберзалежна злочинність, де Європа виступає одним із глобальних осередків активності. Сюди входять атаки із застосуванням програм-вимагачів, розповсюдження шкідливого програмного забезпечення, криптовалютне шахрайство та інші форми кіберексплуатації. Особливої уваги заслуговує тенденція до розмивання меж між класичною кіберзлочинністю та діяльністю учасників, пов'язаних із державними або геополітичними інтересами. У звіті підкреслюється, що ці злочини часто не залежать від рівня формальної стійкості держав і здатні

обходити традиційні механізми контролю, що ставить під сумнів ефективність наявних моделей регулювання.

Наркотичні ринки залишаються ключовим елементом кримінальної економіки Європи. Найбільш динамічне зростання зафіксовано на ринках кокаїну та синтетичних наркотиків. Європа функціонує одночасно як великий споживчий ринок, транзитний хаб і центр переробки. Після посилення контролю в основних портах, таких як Антверпен і Роттердам, спостерігається переорієнтація трафіку на другорядні порти, що демонструє високу адаптивність мереж. Значна частина кокаїну надходить із Південної Америки через Західну Африку та Карибський регіон. Паралельно Європа стала важливим центром виробництва синтетичних наркотиків, зокрема в Бельгії, Нідерландах і Польщі. Особливу тривогу викликає зростання ролі синтетичних опіоїдів, які формують нові ризики для систем охорони здоров'я та безпеки.

Ринки торгівлі людьми та незаконного переправлення мігрантів залишаються стабільно поширеними, особливо вздовж Західнобалканського маршруту. Вони тісно пов'язані з борговою експлуатацією, примусовою працею та сексуальною експлуатацією, що вказує на комплексність цих явищ. Водночас екологічні злочини та окремі товарні ринки мають менший вплив порівняно з іншими регіонами світу.

У частині аналізу злочинців зафіксовано поступове зростання їхньої присутності з 2021 року. Найбільш динамічно розвивається категорія іноземних учасників, які формують мультинаціональні мережі з гнучкою структурою та цифровими моделями координації. Традиційні мафіозні структури зберігають вплив у певних країнах, зокрема в Італії та на Балканах, однак дедалі більшу роль відіграють децентралізовані кримінальні мережі. Приватний сектор виступає важливим посередником у легалізації доходів, тоді як державні або квазідержавні учасники, хоча й менш поширені, залишаються фактором ризику через можливу корупційну співпрацю.

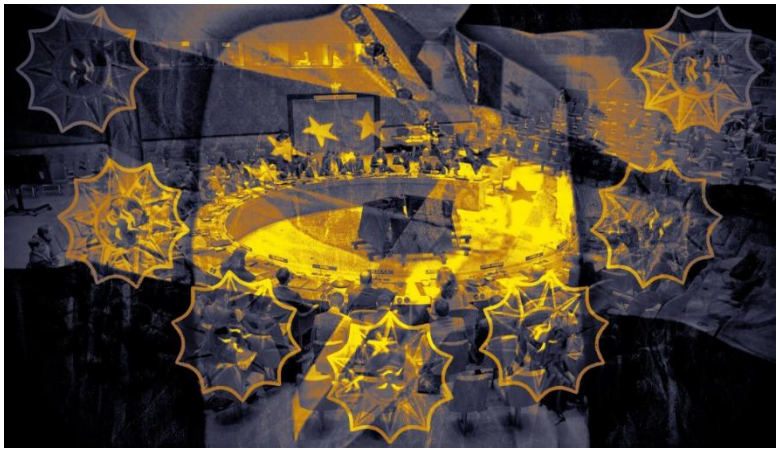
Розділ, присвячений стійкості, демонструє, що Європа лідирує за показниками міжнародної співпраці, національного законодавства та територіальної цілісності . Проте окремі індикатори — зокрема антилегалізаційні механізми, економічна регуляторна спроможність та прозорість уряду — залишаються відносно слабшими. Відзначається також зменшення простору для громадянського суспільства та журналістів, що потенційно підриває механізми громадського контролю. Таким чином, попри формальне лідерство за рівнем стійкості, континент стикається з необхідністю постійного оновлення стратегій у відповідь на цифровізацію, геополітичні виклики та трансформацію кримінальних моделей.

Загалом документ формує цілісне бачення організованої злочинності в Європі як складної, мережевої та глибоко інтегрованої у легальну економіку системи, що еволюціонує швидше, ніж традиційні інституційні механізми реагування. Він підкреслює необхідність переходу від реактивної моделі протидії до стратегічного управління ризиками, яке охоплює фінансову інфраструктуру, цифрове середовище, транскордонну координацію та забезпечення реальної, а не декларативної прозорості.

Чому Венесуела залишається наркодержавою навіть без Мадуро? [9]

Арешт Ніколаса Мадуро 3 січня 2026 року став безпрецедентним актом міжнародного втручання, що сколихнув дипломатичні столиці та кримінальний світ. Для пересічних венесуельців це була довгоочікувана подія, але для наркобізнесу — втрата, здавалося б, невід'ємного елемента системи.

[9] https://insightcrime.org/investigations/cocaine-venezuela-cartel-suns-post-maduro/



Однак, всупереч сподіванням, падіння «короля» не призвело до краху імперії. Як слушно зауважив аналітик Філ Гансон, який прожив у Венесуелі понад 25 років, наркотрафік з Венесуели існував задовго до Мадуро і, найімовірніше, переживе його. Питання лише в тому, чи продовжить кокаїновий бізнес регулюватися чавістським режимом, чи його ослаблення призведе до фрагментації та хаосу, або ж, як це вже неодноразово було в історії, просто змінить форму. Відповідь на це питання криється в глибокій трансформації венесуельської держави, яка відбулася за чверть століття правління так званої «боліваріанської революції». Сьогодні Венесуела є не просто транзитною країною на шляху колумбійського кокаїну, а повноцінним і самодостатнім гравцем на світовому наркоринку: вона виробляє власний кокаїн, контролює логістику, має розгалужену інфраструктуру та глибоко інтегрована у міжнародні мережі збуту, особливо ті, що ведуть до Європи. І хоча Мадуро, який постав перед судом у Нью-Йорку, був головним архітектором і менеджером цієї системи в її нинішньому вигляді, її фундамент — «Картель Сонця» (Cartel de los Soles) та інституціоналізована на всіх рівнях корупція — залишилися не просто недоторканими, а й функціонують у звичному режимі.

Нова президентка Дельсі Родрігес, призначена конституційно і, фактично, благословлена Вашингтоном, опинилася на надзвичайно хиткому політичному канаті, де на кону стоять колосальні кримінальні прибутки та саме існування режиму. З одного боку, вона мусить всіляко задобрити Сполучені Штати, щоб запобігти подальшому військовому втручанню, яке загрожує самому існуванню чавізму як політичної сили. З іншого боку — вона має зберегти лояльність силовиків та радикальних елементів, вихованих на агресивній антиімперіалістичній риториці, для яких будь-які поступки США є зрадою ідеалів революції.

Ключ до цього крихкого балансу — кримінальні доходи, доступ до яких режим перетворив на основний механізм державного управління та утримання влади. Родрігес, хоч і не належить до вузького кола найбільш наближених до Чавеса військових, сама неодноразово згадувалася в контексті корупційних схем та навіть привертала увагу Управління з боротьби з наркотиками (DEA). Тому її завдання полягає не в тому, щоб викорінити корупцію, а в тому, щоб зробити її менш помітною, менш скандальною, щоб не дати Вашингтону приводу для нового вторгнення, водночас забезпечуючи безперебійний потік «кримінальної ренти» до кишень генералітету та вірних політиків, насамперед таких як Діосдадо Кабельйо.

Історія «Картелю Сонця» сягає корінням у 1990-ті роки, задовго до приходу Мадуро до влади, ще за президентства Уго Чавеса. Назва походить від золотих зірок на еполетах генералів Національної гвардії. Спочатку це були не пов'язані між собою осередки військових, які за певну плату просто заплющували очі на транзит колумбійського кокаїну через територію країни. Переломним моментом стала невдала спроба державного перевороту проти Чавеса у 2002 році. Після цього, відчувши загрозу з боку США та Колумбії, які визнали тимчасовий уряд, Чавес почав цілеспрямоване зближення зі своїми ідеологічними союзниками — колумбійськими лівими партизанами. Це був стратегічний альянс: підтримка «боліваріанської революції» в обмін на доступ до величезних прибутків від наркоторгівлі.

Чавес делегував керування цими зв'язками найбільш довіреним військовим, зокрема Уго «Ель Полло» Карвахалю, голові військової розвідки, та генералу Кліверу Алькалі. Обидва згодом були засуджені в США за наркотрафік, а їхні свідчення стали ключовими для розуміння глибини цього

симбіозу. Але головним виконавцем і найвпливовішою фігурою став Діосдадо Кабельйо. Кабельйо сьогодні втілює гібридну природу сучасної венесуельської влади: він одночасно військовий, політик, міністр, голова телекомунікаційної комісії, екс-губернатор і, за даними американської прокуратури, активний кримінальний оператор. За Чавеса склалася негласна суспільна угода: військова та політична еліта отримує безкарний доступ до кримінальної ренти в обмін на абсолютну лояльність режиму та збереження таємниці.

Коли Ніколас Мадуро прийшов до влади після смерті Чавеса у 2013 році, він успадкував не лише президентське крісло, але й цю розгалужену корупційну систему. Проте країна, яку він отримав, кардинально відрізнялася від тієї, що була за Чавеса. Нафтовий бум закінчився, ціни на нафту впали, економіка стрімко скочувалася в прірву гіперінфляції, а міжнародні санкції дедалі більше ізолювали Каракас. На відміну від харизматичного Чавеса, Мадуро не мав міцних особистих зв'язків з армією та елітами. Зіткнувшись із економічним колапсом та загрозою внутрішніх заколотів, він не міг більше купувати лояльність генералів прямими виплатами з державної скарбниці, яка порожніла. Тому він зробив наступний логічний крок: перетворив неформальну практику епохи Чавеса на системну основу державного управління.

У цій системі формальні інститути влади та злочинні структури не просто співіснують, а утворюють симбіоз, де вони доповнюють одна одну. Збройні групи отримують контроль над певними територіями та кримінальними ринками, забезпечуючи там «порядок», необхідний для бізнесу. Натомість високопосадовці, які володіють важелями державної влади, гарантують цим групам недоторканність та доступ до ресурсів.

Ця система найбільш яскраво та небезпечно проявилася в армії, яка за Мадуро перетворилася з інституту захисту кордонів на силу політичних репресій та головного економічного гравця на чорному ринку. Сьогодні армія більше не просто закриває очі на злочинність — вона стала її безпосереднім організатором, бенефіціаром та регулятором.

З 2016 року, зі створенням Оріноцького гірничодобувного поясу (Arco Minero del Orinoco) та Військової компанії гірничодобувної, нафтової та газової промисловості (CAMIMPEG), армія отримала прямий контроль над усім ланцюжком незаконного видобутку золота. За оцінками організації FACT, до 91% золота, що експортується з Венесуели, має нелегальне походження. Це золото на мільярди доларів щорічно.

У південних штатах Болівар та Амасонас армія тісно співпрацює з колумбійськими партизанами з ELN. Як розповів один із венесуельських опозиційних діячів, «партизани та армія працюють разом.

Така ж схема працює на сухопутних та морських кордонах. Після занепаду контрабанди пального через зупинку нафтопереробних заводів, військові швидко диверсифікували свій бізнес, переключившись на контрабанду продуктів харчування, ліків, худоби та, що особливо цинічно, на стягування плати з мігрантів, які тікають від економічного краху.

Сполучені Штати роками намагалися концептуалізувати цю складну систему, щоб боротися з нею юридично та політично. В обвинувальному акті 2020 року, представленому ще за першої адміністрації Трампа, «Картель Сонця» змальовувався як класична вертикально інтегрована терористична організація на чолі з Мадуро. У 2025 році адміністрація Трампа пішла ще далі, визнавши картель іноземною терористичною організацією (FTO), що фактично прирівняло увесь уряд Венесуели до терористів і дозволило висувати звинувачення у «матеріальній підтримці тероризму» будь-кому, хто мав справу з режимом. Це риторичне та юридичне нагнітання створило підґрунтя для силового захоплення Мадуро.

Однак новий обвинувальний акт 2026 року, оприлюднений після арешту, пропонує зовсім інше, набагато глибше визначення. Прокурори тепер описують «Картель Сонця» не як організацію з чіткою ієрархією, а як «культуру корупції, в якій могутні венесуельські еліти збагачуються за

рахунок наркоторгівлі та захисту своїх партнерів-наркоторговців». Це кардинальна зміна парадигми та де-факто визнання того, що Сполучені Штати мають справу не з традиційним картелем, який можна знешкодити, усунувши лідера, а з глибоко вкоріненою, системною патологією державного управління. Це визначення майже дослівно збігається з тим, що аналітики InSight Crime називають «гібридною державою».

Саме ця системність пояснює, чому падіння Мадуро має такий обмежений вплив на наркотрафік. Його наступниця Дельсі Родрігес, хоч і не є військовою і не належить до найвужчого ядра «преторіанської гвардії», також фігурує в численних звітах як особа, безпосередньо причетна до корупційних схем, зокрема до розкрадання державних контрактів. Міністр оборони Володимир Падріно Лопес, який перетворив армію на головну опору режиму, та міністр внутрішніх справ Діосдадо Кабельйо, на голови яких США призначили винагороду в 15 та 25 мільйонів доларів відповідно, не просто залишилися на своїх посадах — вони, за іронією долі, стали головними співрозмовниками Вашингтона.

Ситуація на місцях також зазнала тактичних змін, але аж ніяк не стратегічного розгрому трафіку. Військова присутність США в Карибському басейні та ракетні удари по швидкісних катерах, які підозрювалися у перевезенні наркотиків, змусили контрабандистів тимчасово адаптуватися. Північний маршрут через Кариби, за свідченнями джерел у прибережних штатах, практично закрито. Військове керівництво, побоюючись арешту високопосадовців, призупинило великі морські відправлення. Однак це не призвело до скорочення обсягів торгівлі, а лише перенаправило потоки.

Сьогодні кокаїн, значна частина якого тепер призначена для Європи (ринок якої вже перевершив американський за обсягами), йде альтернативним, південним шляхом — через важкодоступні джунглі штатів Амасонас і Болівар до узбережжя Атлантики, або далі до Гаяни та Суринаму. Саме там, за даними джерел, активізувалося будівництво нарко-субмарин. Ці тихохідні, але малопомітні апарати здатні брати на борт до дев'яти тонн кокаїну та доставляти його безпосередньо до берегів Європи, уникаючи контролю в Карибському морі.

Таким чином, усунення Ніколаса Мадуро, архітектора гібридної кримінальної держави, мало що змінило в глибинній динаміці наркотрафіку у Венесуелі. Дельсі Родрігес, ймовірно, намагатиметься уникати публічних скандалів, які могли б спровокувати нове військове втручання США, але вона об'єктивно не може і, найімовірніше, не хоче перекривати кримінальний потік, який є фінансовим фундаментом її влади та запорукою лояльності силовиків.

Вашингтон, зі свого боку, зосереджений на нагальних питаннях — відновленні видобутку нафти, стабілізації економіки та стримуванні

Висновки:

- **Інституціоналізація корупції.** У Венесуелі сформувалася не просто корумпована влада, а «гібридна кримінальна держава», де армія та чиновники системно отримують доступ до наркотрафіку, незаконного видобутку золота та контрабанди як плату за лояльність режиму.
- **Живучість системи.** Арешт лідера (Мадуро) не зруйнував наркокартель. Ключові фігури (Кабельйо, Падріно) залишилися при владі, і бізнес продовжує функціонувати.
- **Боротьба з наркотрафіком відходить на другий план перед геополітичними інтересами.** США, попри офіційну риторику та багатомільйонні нагороди за голови венесуельських міністрів, готові співпрацювати з тими ж самими людьми заради стабільності, нафти та врегулювання міграційної кризи.
- **Адаптивність маршрутів.** Фізичне блокування одного каналу трафіку не зупиняє потік наркотиків, а лише змінює його географію. Бізнес миттєво переорієнтовується на інші, менш захищені маршрути.

міграційних потоків — і, схоже, готовий тимчасово заплющити очі на кримінальну сутність режиму в обмін на передбачуваність і співпрацю. Допоки чавістська система залишається при владі, кокаїновий бізнес у Венесуелі не просто виживе — він процвітатиме, гнучко адаптуючись до нових політичних реалій. Наркодержава, побудована на інституціоналізованій корупції та гібридному управлінні, виявилася набагато міцнішою та живучою за її творця.

Крипто-привиди: Як стокова модель та кіт із дзвіночком викрили мільярдну схему Ірану [10]

У сучасному світі, де глобальні фінансові потоки контролюються дедалі жорсткіше, а міжнародні санкції стають чи не основною зброєю стримування авторитарних режимів, найнебезпечніші гравці вчаться грати за новими правилами. Вони опановують цифровий простір, реєструють фірми в престижних юрисдикціях із ліберальним корпоративним законодавством та створюють віртуальні особистості, які неможливо відрізнити від реальних.

Оприлюднене розслідування OCCRP пропонує захопливий та водночас моторошний погляд на те, як поєднання креативного підходу до створення фіктивних керівників та випадкове фото домашнього улюбленця дозволили розплутати одну з найскладніших фінансових мереж сучасності, що живить Корпус вартових ісламської революції — організацію, відповідальну за криваве придушення протестів та дестабілізацію Близького Сходу.

В епіцентрі цієї історії знаходиться загадкова постать на ім'я Елізабет Ньюман. Згідно з офіційним британським реєстром компаній Companies House, вона є директоркою та "особою зі значним контролем" над двома криптовалютними біржами — Zedcex та Zedxion. Ці платформи, зареєстровані у Сполученому Королівстві, заявляють про щоденний обіг цифрових активів на суму, що сягає понад мільярд доларів. Офіційні документи та корпоративна звітність малюють портрет впливової бізнес-леді домініканського походження, чия діяльність охоплює три континенти. Її поштові адреси варіюються від розкішної нерухомості на узбережжі Карибського моря до престижного офісу в лондонському Ковент-Гардені та футуристичного хмарочоса в Дубаї. На папері Елізабет Ньюман — зразкова міжнародна підприємиця, втілення глобалізованого капіталізму. Проблема лише в тому, що Елізабет Ньюман не існує. Вона — корпоративна фікція, привид, створений алгоритмами та бюрократичною байдужістю.

Журналісти OCCRP, провівши багатомісячне розслідування, виявили, що обличчя, яке використовувалося в офіційних маркетингових матеріалах бірж для презентації "виконавчої директорки", є не чим іншим, як стоковим відеороликом, придбаним на платформі Shutterstock. Відео мало красномовну назву "Pretty black woman talking to camera" — "Вродлива чорношкіра жінка розмовляє з камерою". Жінка на відео, ймовірно, навіть не підозрює, що вже кілька років "керує" багатомільярдними фінансовими потоками. Інші нібито ключові співробітники компанії, представлені в тому ж відео як фінансовий адміністратор "Сміт" та керівник команди "Мухаммад", також виявилися стоковими моделями, чиї обличчя можна придбати за кілька доларів. Це відкриття перетворює Елізабет Ньюман на ідеальний символ сучасної тіньової

[10] https://www.occrp.org/en/investigation/the-cat-and-the-stock-footage-ceo-how-a-digital-trail-helped-unmask-an-iranian-money-machine

фінансової системи: юридичну фікцію, створену виключно для того, щоб надати легітимного вигляду грошовим потокам, які, за даними американського Мінфіну, сягають десятків мільярдів доларів і живлять одну з найрепресивніших силових структур світу.

Ці потоки, як стверджується в офіційних документах Управління з контролю за іноземними активами Міністерства фінансів США, ведуть до Бабака Занджані — іранського фінансиста з кримінальним минулим, яке могло б стати сюжетом для голлівудського трилера. У 2016 році Занджані був засуджений в Ірані до страти через розкрадання державних нафтових коштів на десятки мільярдів доларів. Здавалося б, його кар'єра завершена, а ім'я назавжди зникне з фінансових зведень. Однак, замість того, щоб зникнути з поля зору, він не лише отримав помилування у 2024 році, але й, за даними американської розвідки, був достроково звільнений з в'язниці ще у 2019 році з єдиною метою — відмивати гроші для того самого режиму, який його ув'язнив.

Його ключовий клієнт і бенефіціар — Корпус вартових ісламської революції (IRGC), військово-політичне угруповання, яке є не лише елітним бойовим підрозділом, але й величезним бізнес-конгломератом, що контролює значні сектори іранської економіки. Саме IRGC відігравав ключову роль у кривавому придушенні загальнонаціональних протестів, внаслідок яких, за даними Amnesty International та інших правозахисних організацій, загинули тисячі мирних демонстрантів.

Біржі Zedcex та Zedxion, зареєстровані у Великій Британії, стали ідеальним інструментом для обходу міжнародних санкцій, накладених на Іран та IRGC. Вибір юрисдикції не був випадковим. Велика Британія, попри свою репутацію фінансового центру з високими стандартами, донедавна мала надзвичайно ліберальне корпоративне законодавство. Реєстр компаній працював за принципом "скриньки чесності" — він брав інформацію на віру, не перевіряючи її достовірність і не вимагаючи підтвердження особи директорів. Формально Zedcex та Zedxion звітували до реєстру як "dormant" — неактивні компанії, що не ведуть жодної діяльності та не мають оборотів. Це дозволяло їм уникати сплати податків і не привертати уваги фінансових регуляторів. Однак насправді, за даними аналітичної компанії TRM Labs, яка спеціалізується на відстеженні криптовалютних транзакцій, через ці платформи пройшло приблизно 1 мільярд доларів, прямо або опосередковано пов'язаних з IRGC. Це дозволило мережі Занджані використовувати престижний британський корпоративний фасад для діяльності, яка, за твердженням американського Мінфіну, включала не лише обслуговування потреб IRGC в середині країни, але й фінансування міжнародних терористичних організацій.

Йдеться про єменських хуситів — угруповання, визнане США як "Спеціально визначена глобальна терористична організація". TRM Labs виявила перекази на суму понад 10 мільйонів доларів через ці біржі на адресу Саїда Ахмада Мухаммада аль-Джамаля, якого американське казначейство описує як високопоставленого фінансового чиновника хуситів, що діє за підтримки IRGC. Хусити, які контролюють значну частину Ємену, включаючи столицю Сану, в останні роки здійснюють систематичні атаки на комерційні судна в Червоному морі, використовуючи ракети, безпілотники та морські міни, що загрожує глобальній свободі судноплавства та світовій торгівлі. Таким чином, гроші, які номінально проходили через "сплячі" британські компанії з вигаданими директорами, фактично фінансували військові дії, що дестабілізують цілий регіон і ставлять під загрозу міжнародні торговельні шляхи.

Зв'язок Занджані з цими біржами, попри всі зусилля приховати його за фасадом Елізабет Ньюман, виявився напрочуд прозорим, якщо знати, де шукати і як поєднувати, здавалося б, не пов'язані між собою цифрові докази. У метаданих технічного документа біржі Zedxion, який було оновлено у вересні 2023 року, автором правок був вказаний сам Бабак Занджані. Це означає, що людина, яка офіційно все ще перебувала під загрозою смертного вироку (хоча, ймовірно, вже була на свободі), особисто редагувала стратегічний документ компанії. Крім того, у жовтні

2024 року він опублікував на YouTube відео, де сидить в офісному кріслі перед великим екраном, на якому відображається інтерфейс торгової платформи Zedcex. Скріншот із цього відео з'явився на його сторінці у Facebook. Здавалося б, він навіть не надто переймався конспірацією, демонструючи свою причетність до цих активів. Однак найцікавішим і найбільш промовистим у цьому розслідуванні став не прямий цифровий слід, а непрямий, залишений людьми з його найближчого оточення.

Цією людиною виявилася Солмаз Бані, колишня модель, яка також використовує імена Ніюша та Сара Бані. Вона є романтичною партнеркою Занджані, про що свідчать численні фотографії та зворушливі пости в соціальних мережах. В її акаунтах у соціальних мережах збереглися численні докази її тісного зв'язку з бізнес-імперією Zanjani. У своєму профілі в Instagram вона називала себе "президенткою BZ Group" — холдингу компаній, що носять ініціали Занджані (Babak Zanjani), зареєстрованих переважно в Дубаї. Вона була контактною особою для вебсайту BZ Group, володіла часткою в одній з її дочірніх компаній — BZ Motorcycles, а на одному з електронних листів, що стосувався розсилки новин криптобіржі Zedxion, спливло її ім'я в автозаповненні поруч з ім'ям "Babak". Навіть клієнтський відгук для компанії BZ Broker Limited, яку, згідно з британським реєстром, формально очолювала примарна Елізабет Ньюман, був написаний саме Солмаз Бані. Таким чином, вона виступала операційною менеджеркою, контактною особою та публічним обличчям імперії, тоді як офіційним директором значилася жінка зі стокового фото.

Висновки:

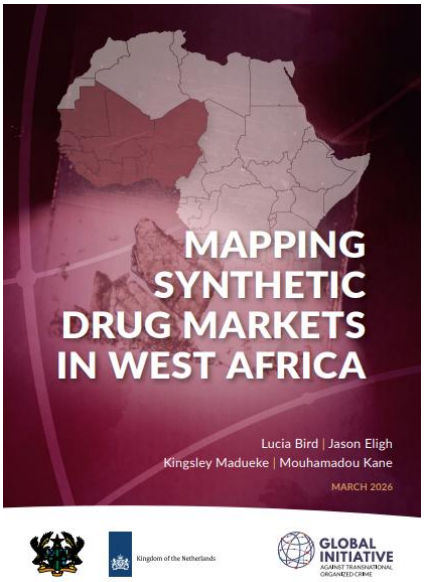
- **Злочинні мережі масово використовують стокові фотографії та вигадані особи.** Це дозволяє їм реєструвати компанії в престижних юрисдикціях і надавати вигляд легітимності нелегальним фінансовим потокам.
- **Використання статусу "dormant company" (неактивна компанія)** є ефективним інструментом для приховування масштабної фінансової діяльності. Компанії можуть роками звітувати про відсутність оборотів, тоді як насправді через них проходять мільярди доларів.
- **Криптовалюта як інструмент обходу санкцій:** Розслідування підтверджує, що криптовалютні біржі, навіть зареєстровані у країнах з розвиненою економікою, можуть стати ключовим інструментом для обходу міжнародних санкцій.
- **Необережне ведення соціальних мереж фігурантами створює цифровий слід,** який часто є надійнішим за будь-які фінансові документи. Поєднання цього сліду з даними з офіційних каналів компаній дозволяє журналістам-розслідувачам встановлювати зв'язки, які злочинці намагаються приховати.

Але справжньою "зіркою", яка поставила фінальну крапку в цьому детективі, став домашній улюбленець пари. У травні 2024 року офіційний Telegram-канал криптобіржі Zedxion опублікував фото майже повністю білого кота з характерними сіро-коричневими плямами на мордочці та яскравим фіолетовим дзвіночком на нашийнику. За кілька місяців до цього, у лютому 2025 року, на Facebook-сторінці "Niu Niu" — одного з альтер-его Солмаз Бані, яке вона використовувала для спілкування з друзями, — з'явилося фото кота з ідентичними мітками та таким самим фіолетовим дзвіночком. Збіг забарвлення та аксесуара вже був надто промовистим, але справжнім доказом став інтер'єр: кіт сидів під столом зі стільцями, що мали дуже специфічну, впізнавану форму ніжок. Ті самі стілець і стіл з'явилися на іншому фото, опублікованому на фан-сторінці Занджані в Instagram. На цьому фото іранець уже грав із собакою в тій самій кімнаті, з тими самими меблями. Таким чином, випадкове фото домашнього улюбленця, опубліковане на офіційному каналі криптобіржі, стало відсутньою ланкою, що фізично поєднала абстрактну корпоративну структуру, зареєстровану в Лондоні, з реальним побутом її справжніх бенефіціарів. Кіт з фіолетовим дзвіночком виявився найнадійнішим доказом існування мережі.

Ця історія є яскравим прикладом того, як глобальна фінансова система досі залишається вразливою до системних зловживань. Хоча Велика Британія ухвалила Акт про економічні злочини та корпоративну прозорість 2023 року, який зрештою вимагатиме верифікації осіб директорів компаній, це вже не матиме жодного значення. Злочинці вміло скористалися "перехідним періодом", наданим законом, який дозволяє існуючим компаніям протягом року не виконувати нові вимоги. За час, поки законодавці та регулятори розгойдувалися, через їхні біржі, встигли пройти мільярди доларів. Ці гроші вже виконали свою роль: вони допомогли режиму втримати владу, фінансували придушення протестів і підтримали військові дії хуситів.

Розслідування OCCRP демонструє не лише винахідливість та цинізм зловмисників, які перетворили створення фіктивних осіб на справжнє мистецтво, але й те, що в епоху цифрових технологій приховати правду стає дедалі важче. Це історія про те, як глобалізований світ, побудований на довірі до паперів та репутації юрисдикцій, може бути використаний проти самого себе, і як часом найскладніші злочини розкриваються завдяки найпростішим людським доказам.

Синтетична загроза: Як нові наркотики змінюють безпековий та соціальний ландшафт Західної Африки [11]



Західна Африка, регіон, що історично потерпав від політичної нестабільності, бідності та транзиту кокаїну, сьогодні стоїть на порозі безпрецедентної катастрофи, природа якої криється не в традиційній збройній боротьбі за ресурси, а в тихому, але стрімкому поширенні синтетичних наркотиків. Це явище, детально задокументоване в дослідженні GI-TOC є не просто черговою проблемою громадського здоров'я, а фундаментальним зрушенням, яке змінює саму тканину суспільства, економіки та безпеки в усьому регіоні.

Ключова відмінність цієї нової хвилі від попередніх етапів наркоторгівлі полягає в самій природі ринку. Раніше споживання в регіоні формувалося переважно як "побічний ефект" транзиту кокаїну та героїну до Європи — частина вантажу осідала на місцевих ринках, створюючи обмежений попит. Сьогодні ж драйверами виступають зовсім інші чинники.

Сучасний ринок синтетики — це децентралізована, фрагментована екосистема з надзвичайно низьким порогом входу. Для виробництва чи імпорту синтетичних наркотиків більше не потрібні багаторічні зв'язки, величезні плантації чи складні трансконтинентальні логістичні ланцюги, які контролюються ієрархічними злочинними синдикатами. Сьогодні достатньо мати доступ до інтернету, невеликий стартовий капітал і знати хімічну формулу. Психотропні речовини та їхні прекурсори можна замовити на відкритих онлайн-майданчиках або в даркнеті, доставити поштою чи кур'єрською службою, а вже на місці, в орендованій кімнаті чи навіть у пересувній лабораторії в автомобілі, перетворити на готовий продукт. Це докорінно змінює правила гри, демократизуючи злочинний бізнес і залучаючи до нього нову хвилю підприємців, для яких торгівля наркотиками стає "містком" для швидкого накопичення капіталу.

Географія цього явища вже давно вийшла за межі окремих країн. Дослідження GI-TOC фіксує, що між 2023 та 2025 роками ринок синтетичних наркотиків став найбільш швидкозростаючим

[11] https://globalinitiative.net/wp-content/uploads/2026/03/Lucia-Bird-et-al-Mapping-synthetic-drug-markets-in-West-Africa-GI-TOC-March-2026.pdf

кримінальним ринком у Західній Африці, причому його вплив посилився у шести країнах регіону. Це не просто ізольовані спалахи, а взаємопов'язана мережа, де Нігерія виступає епіцентром виробництва метамфетаміну, Сьєрра-Леоне — ключовим вузлом синтезу кушу, а Гамбія — регіональним хабом для реекспорту екстазі. Ланцюги постачання простягаються далеко за межі Африки: Китай та Індія є основними джерелами синтетичних канабіноїдів, нітазенів та прекурсорів для метамфетаміну; Нідерланди та Велика Британія фігурують як ключові експортери екстазі та компонентів для кушу; Пакистан стає альтернативним джерелом трамадолу після посилення контролю в Індії. Ця глобалізація постачання робить боротьбу з ринком неймовірно складною, адже перекриття одного каналу миттєво компенсується за рахунок іншого.

Спектр речовин, що заполонили регіон, вражає своєю різноманітністю та рівнем небезпеки. Історично домінуючий трамадол, який перетворив Західну Африку на світового лідера за обсягами вилучень, поступово поступається місцем ще небезпечнішим похідним. Тапентадол, який часто змішують з карізопродолом, став звичнішим явищем на ринках багатьох країн, ніж сам трамадол. Але найбільше занепокоєння викликає поява нітазенів — синтетичних опіоїдів, потужність яких у десятки разів перевищує потужність фентанілу. Виявлені у зразках кушу в Сьєрра-Леоне, вони перетворили цю суміш на смертоносний коктейль. Саме з їхньою появою у 2022 році пов'язують різке зростання кількості летальних випадків на вулицях Фрітауна та інших міст. Ситуація ускладнюється тим, що нітазени та синтетичні канабіноїди (найпоширеніший з яких — MDMB-4en-PINACA) часто потрапляють до організму споживачів несвідомо, у сумішах з іншими наркотиками, що робить передозування практично непередбачуваним.

Стрімке зростання ринку неможливе без появи нових гравців. Дослідження окреслює складну, багаторівневу структуру злочинних суб’єктів, яка простягається від фінансистів-власників, що ховаються за легальним бізнесом і купують політичний захист, до "кухарів" — хіміків-самоучок або дипломованих фахівців, чиї знання є ключовим активом у виробництві метамфетаміну чи кушу. Важливу роль відіграють представники діаспори в Європі та Азії, які виступають сполучною ланкою з постачальниками. На нижчих рівнях — численні дрібні дилери та власники точок для споживання (так звані "cartels" у Сьєрра-Леоне або "fumoirs" у Кот-д'Івуарі), які часто є колишніми учасниками банд, що перекваліфікувалися з вуличного насильства на більш прибуткову та менш ризиковану торгівлю наркотиками. У Нігерії, наприклад, вуличні банди на кшталт "Yandaba" в Кано чи "area boys" в Ібадані глибоко інтегровані в дистрибуцію трамадолу, контролюючи цілі райони та транспортні вузли.

Паралельно з еволюцією ринку відбувається еволюція методів його захисту. На відміну від ринку кокаїну, який часто потребує політичного покровительства, захист синтетики є більш фрагментованим і локалізованим. Він зосереджений у ключових точках: портах і аеропортах, де корумповані чиновники за винагороду заплющують очі на контейнери з прекурсорами; у місцях розташування лабораторій, де зв'язки з поліцією є запорукою безпеки; і, звичайно, на рівні роздрібної торгівлі, де дрібні оборудки з дільничними гарантують безперешкодну роботу точок продажу. Цей децентралізований захист робить систему надзвичайно гнучкою та стійкою до ударів по окремих ланках.

Одним із найтривожніших висновків звіту є визнання критичного розриву між швидкістю еволюції ринку та спроможністю регіону адекватно на нього відповісти. Більшість країн Західної Африки не мають необхідного обладнання та технічних навичок для проведення хімічного аналізу нових психоактивних речовин. Лабораторії часто працюють не на повну потужність, а їхні методики налаштовані на пошук відомих речовин, таких як трамадол, але не здатні ідентифікувати нові сполуки, як-от різноманітні нітазени. Це створює своєрідну сліпоту: офіційна статистика не відображає реальної картини, а органи охорони здоров'я не знають, з чим саме їм доводиться мати справу. Яскравим прикладом є ситуація з кушем — лише після тестування 2024 року стало відомо про наявність у ньому опіоїдів, що дозволило почати використовувати

налоксон для порятунку життів при передозуванні. До цього моменту всі зусилля були по суті марними, оскільки базувалися на хибних припущеннях.

Наслідки цього розриву є жахливими. Молодь, яка становить основну масу споживачів, втрачає здоров'я, соціальні зв'язки та перспективи на майбутнє. Відповідь правоохоронних органів, зосереджена на арештах дрібних дилерів і споживачів, не тільки неефективна, але й контр-продуктивна. Вона лише посилює стигматизацію, переповнює в'язниці найбільш уразливими верствами населення і ніяк не впливає на верхівку злочинної піраміди. Більше того, як показує досвід боротьби з трамадолом, посилення тиску на один ринок часто призводить до неочікуваних наслідків: зростання цін на нього та появи ще небезпечніших замінників, що лише поглиблює кризу.

Висновки:

- **Фрагментація криміналітету через низький поріг входу:** На відміну від традиційних наркотиків, синтетичні ринки не вимагають складних міжнародних зв'язків чи значних капіталовкладень. Прекурсори можна замовити онлайн через поштові служби, що дозволяє численним новим дрібним гравцям швидко входити в бізнес.
- **Вибухове зростання ринку синтетичних опіоїдів:** Синтетичні опіоїди, зокрема нітазени і похідні трамадолу, стали головною загрозою для здоров'я населення. Вони спричиняють різке зростання смертності від передозувань, особливо серед молоді.
- **Критичне відставання реакції:** Здатність регіону реагувати на загрозу стрімко відстає від її еволюції. Більшість країн не мають лабораторій для ідентифікації нових речовин, що унеможливлює ефективну політику у сфері безпеки.
- **Глобальний характер ланцюгів постачання:** Ринок синтетики в Західній Африці є невід'ємною частиною глобальної торгівлі. Ключовими експортерами прекурсорів та готових речовин виступають Китай та Індія.

Таким чином, Західна Африка опинилася в пастці, де традиційні, засновані на репресіях підходи не працюють проти гнучкого, технологічно підкованого ворога. Звіт GI-TOC чітко показує, що єдиний шлях вперед лежить через кардинальну зміну парадигми. Відповідь має бути комплексною, регіонально скоординованою та, найголовніше, заснованою на доказах. Це означає нагальні інвестиції в хімічну сферу та створення систем раннього попередження, щоб знати, з чим саме боротися. Це означає гармонізацію законодавства, яке має дозволяти швидке блокування цілих родин нових речовин, а не лише їхніх окремих хімічних формул. Це означає налагодження дієвої міжнародної співпраці для посилення контролю за експортом прекурсорів з Азії та Європи.

Але найважливіше — це визнання того, що наркозалежність є проблемою здоров'я, а не кримінальною провиною. Розширення доступу до лікування, включаючи замісну терапію, вільний доступ до налоксону та впровадження альтернативних покаранню програм для споживачів — це не прояв слабкості, а єдиний дієвий спосіб зменшити руйнівні наслідки та врятувати ціле покоління від тіньової хімії, яка вже зараз переписує долю регіону. Час для повільних, фрагментованих і недалекоглядних рішень минув.

Реагування на фінансування російських диверсій: інституційні прогалини та роль фінансового сектору [12]

Аналітичний звіт Королівського об'єднаного інституту оборонних досліджень (RUSI), підготовлений дослідниками Кінгою Редловською, Мартою Попик та Томом Кітінгом, становить глибоке розслідування еволюції гібридної війни російської федерації в Європі, з фокусом на інфраструктуру фінансового забезпечення диверсійної діяльності. Дослідження фіксує концептуальну зміну доктрини російських спецслужб (насамперед ГРУ): відмову від складних, багаторічних операцій кадрових розвідників на користь так званої «гіг-економіки» диверсій. Ця модель спирається на масове дистанційне вербування через зашифровані месенджери (зокрема Telegram) звичайних громадян, маргіналізованих осіб та підлітків для виконання одноразових завдань. Спектр цих завдань варіюється від підготовчих і символічних (фотографування військових баз, малювання антиукраїнських графіті) до безпосередніх кінетичних атак (підпали складів з гуманітарною допомогою, закладання посилок-бомб у логістичні мережі). Використання «одноразових агентів» — часто громадян України або Білорусі — є свідомою стратегією агресора, що має подвійну мету: по-перше, забезпечення правдоподібного заперечення причетності російської держави, а по-друге, розпалювання антимігрантських та антиукраїнських настроїв у європейських суспільствах з метою ерозії політичної підтримки Києва. З огляду на те, що такі операції є надзвичайно дешевими, фінансовий мотив стає головним рушієм вербування, перетворюючи фінансову систему на ключове поле бою.

Механіка фінансування цієї «гіг-економіки» характеризується високою адаптивністю та навмисною експлуатацією прогалин у глобальній системі ПВК/ФТ. Головним інструментом забезпечення швидкості та анонімності транзакцій стала криптовалюта, проте її використання відрізняється від традиційних схем відмивання коштів. Аналіз блокчейну показує, що російські куратори не використовують складних методів обфускації, таких як крипто-міксери або privacy coins, віддаючи перевагу швидкості та простоті базових активів (Bitcoin, USDT). Анонімність досягається через специфічну інфраструктуру маршрутизації. У показовому кейсі канадського підлітка Лейкена Павана, який отримав 600 доларів у біткоїнах за розвідку в Польщі, криміналістичний аналіз виявив, що кошти надійшли безпосередньо з майнінгового пулу. Оскільки пули акумулюють винагороди тисяч незалежних майнерів, вони структурно розривають ланцюг походження коштів, унеможливлюючи ідентифікацію початкового відправника. Іншим критичним елементом є мережа позабіржових (OTC) криптоброкерів. В одному з кейсів троє диверсантів у Європі отримали по 1000 USDT з єдиного гаманця нерегульованого брокера, що фізично перебував в Україні. Цей факт підсвічує найвразливішу ланку злочинної схеми — етап конвертації криптоактивів у фіатну готівку (cash-out) через мережі криптоматів та неформальних обмінників. Окрім цифрових активів, куратори застосовують оплату готівкою через фізичних кур'єрів, розрахунки через посередників, а також фізичну оплату (наприклад, передача автомобіля замість обіцяних 10 000 євро за підпал IKEA в Литві), що доводить багатовекторність фінансової логістики терору.

[12] https://www.rusi.org/explore-our-research/publications/insights-papers/responding-russian-sabotage-financing

Канал фінансування	Характеристика використання у диверсійних схемах	Вразливість для виявлення
Майнінгові пули	Виплата безпосередньо з пулу для розриву зв'язку з ініціатором.	Вкрай низька. Блокчейн-аналітика впирається у легітимний агрегатор транзакцій.
Стейблкоїни та OTC-брокери	Масові виплати виконавцям з єдиного брокерського гаманця (по ~1000$).	Висока. Регулярні перекази з одного джерела різним непов'язаним особам є чітким патерном.
Криптомати та термінали Cash-out	Перетворення цифрових активів у готівку в країні проведення диверсії.	Середня. Вимагає жорсткого відеоспостереження та KYC для транзакцій малого обсягу.
Фізична оплата	Передача майна (автомобілів) замість готівки.	Низька. Потребує інтеграції реєстрів рухомого майна з базами даних кримінальної поліції.

Головний концептуальний висновок звіту RUSI полягає в констатації паралічу європейської правоохоронної архітектури через відсутність адекватної правової бази для протидії гібридним загрозам. На рівні законодавства ЄС та більшості країн НАТО не існує єдиного, функціонального визначення поняття «саботаж» (диверсія), яке б охоплювало не лише акт фізичного знищення, а й логістичну, фінансову та розвідувальну підготовку. Як наслідок, правоохоронні органи змушені кваліфікувати дії «одноразових агентів» за загальними статтями кримінального кодексу — як дрібне хуліганство, вандалізм або ізольований підпал. Такий підхід ігнорує стратегічний умисел (нанесення шкоди нацбезпеці) і призводить до винесення вкрай м'яких вироків, які абсолютно не виконують функції стримування для потенційних найманців з гіг-економіки. Найбільш руйнівним наслідком цього юридичного вакууму є неможливість повноцінного застосування інструментарію протидії фінансуванню тероризму. Оскільки дії не кваліфікуються як тероризм, фінансові розвідки та банки не мають правових підстав для превентивного заморожування активів підозрюваних, обміну розвідувальними даними у реальному часі та застосування секторальних санкцій до мереж

Висновки:

- **Урядам країн ЄС та їхнім союзникам необхідно терміново імплементувати в національне кримінальне законодавство комплексне визначення «диверсії» (саботажу), прямо включивши до нього фінансове сприяння та вербування**, що дозволить легітимно застосовувати до цих злочинів увесь спектр інструментів боротьби з фінансуванням тероризму (заморожування рахунків, конфіскація).
- **Національним ПФР у координації з криптоаналітичними компаніями потрібно розробити та розіслати банкам і VASP оновлені списки індикаторів ризику (типології)**, що фокусуються на мікропереказах у криптовалюті (до 2000 доларів), які надходять від неідентифікованих OTC-брокерів до фізичних осіб у транзитних країнах.
- **Наглядовим органам необхідно різко посилити контроль за операціями «cash-out» (криптомати, P2P-платформи), вимагаючи обов'язкової KYC навіть для транзакцій на мінімальні суми**, оскільки саме переведення криптовалюти в готівку є найбільш вразливим місцем у фінансовій логістиці «одноразових агентів».
- Для ефективної протидії мережам фінансування саботажу **потрібно створити транскордонні міжвідомчі аналітичні групи, які б в режимі реального часу об'єднували дані контррозвідки, ПФР та відділів комплаєнсу великих фінансових установ** (за моделлю державно-приватного партнерства EFIPPP).

брокерів, які обслуговують ці платежі. Автори наполягають, що без визнання фінансового та логістичного сприяння гібридним атакам злочином проти національної безпеки, європейський фінансовий сектор залишатиметься нездатним зупинити мікроплатежі, які живлять російську військову машину.

Інші новини

Тіньова столиця: Як CJNG контролює Гвадалахару [13]

Коли 22 лютого 2026 року над Гвадалахарою здійнявся дим палаючих автомобілів та вантажівок, а кулеметні черги розірвали звичний гул п'ятимільйонного мегаполісу, світ став свідком не просто чергового спалаху нарковійни. Це була демонстрація влади, оголення механізмів, які роками вибудовував Картель Нового Покоління Халіско (CJNG). Координовані атаки стали прямою відповіддю на ліквідацію беззмінного лідера угруповання, Немесіо Осегери Сервантеса, відомого як Ель Менчо.

Президентка Мексики Клаудія Шейнбаум та губернатор Халіско Пабло Лемус поспішили заспокоїти націю та інвесторів, запевняючи, що ситуацію взято під контроль, а насильство було "надзвичайною подією", яка не відображає щоденної реальності. Але для тих, хто знайомий з подвійним життям Гвадалахари, ці події не стали несподіванкою. Вони були лише видимим, кривавим проявом глибоко вкоріненої, хронічної хвороби, яка руйнувала місто зсередини щонайменше з 1980-х років.

Гвадалахара, яку пишно називають "мексиканською Кремнієвою долиною" за її технологічний та економічний бум останніх трьох десятиліть, завжди вела подвійне життя. Вона є не лише політичним, фінансовим та культурним серцем західної Мексики, але й головним операційним штабом, тилом та домівкою для еліти одного з найнебезпечніших злочинних синдикатів світу.

З моменту свого виникнення у 2010 році з уламків картелів Сіналоа та Міленіо, CJNG обрав для себе унікальну, хоча й жорстоку, стратегію виживання та експансії. У той час як в інших частинах країни картель вів відкриті війни, кидаючи виклик уряду та конкурентам, у власній столиці він зробив ставку на "невидимий" контроль. Цей підхід виявився набагато ефективнішим за щоденні перестрілки. Він базується на глибокому, майже паразитичному, проникненні в соціальну, економічну та політичну тканину міста. Гвадалахара пропонує картелю ідеальні умови для існування. Динамічна формальна економіка, з її ресторанами, торговими центрами, житловими комплексами та автозаправними станціями, створює бездонну кишеню для відмивання мільярдних прибутків від наркоторгівлі, викрадення пального, вимагання та інших злочинних ринків.

Стратегічне розташування міста також відіграє ключову роль. Гвадалахара є вузловим транспортним центром, звідки мережа автомагістралей розходиться на північ до кордону зі США, на захід до тихоокеанських портів, і вглиб країни. Це робить її ідеальним логістичним хабом для транспортування наркотиків, зброї та готівки.

[13] https://insightcrime.org/news/how-cjng-control-works-guadalajara-with-without-el-mencho/

Але справжня влада CJNG у Гвадалахарі полягає в управлінні кримінальним світом. Через розгалужену систему місцевих осередків, відомих як "plazas", картель поділив місто на сфери впливу, встановивши чіткі, хоч і неписані, правила для всіх без винятку, хто займається незаконним бізнесом на його території. Від дрібних вуличних банд, які контролюють продаж наркотиків у конкретному кварталі, до незалежних груп вимагачів чи перекупників краденого — всі вони змушені визнавати владу картелю. Як зазначають місцеві експерти та кримінологи, іншого кримінального "бренду" в місті практично не існує. Усі групи, які формально не належать до CJNG, зобов'язані укласти з ним угоду, платити податок і неухильно дотримуватися встановлених норм.

Ця тіньова влада регулює буквально все. Картель може встановлювати роздрібні ціни на наркотики в різних районах, визначати, кому і де дозволено торгувати, а де торгівля взагалі заборонена. Він вирішує, які райони є "закритими" для вимагання, захищаючи місцевий бізнес в обмін на лояльність, або ж, навпаки, встановлює ставки данини для інших. У разі виникнення суперечок між дрібними кримінальними гравцями, картель виступає в ролі верховного арбітра.

Ключовим елементом цієї стратегії є тотальна корупція державних інститутів. Замість того, щоб щодня воювати з поліцією, CJNG надає перевагу її підкупу. Замість того, щоб уникати судів, він намагається поставити там своїх людей. Це дозволяє картелю діяти з тіні, використовуючи точкове насильство, погрози та вибіркові вбивства як інструменти контролю, а не як метод ведення бойових дій. Це створює тривожну нормалізацію злочинності, де зникнення людини стає буденністю, а страх — постійним тлом повсякдення.

Найжахливішим, найцинічнішим проявом цього "невидимого" контролю стала епідемія зникнень. Приблизно з 2013 року кількість зниклих безвісти тут зростає в геометричній прогресії, давно випереджаючи офіційні показники вбивств. Правда про те, що відбувається зі зниклими, час від часу спливає назовні завдяки мужності пошукових загонів. Саме такі люди знаходять докази жахливих злочинів.

Втім, цей "невидимий" контроль, цей фасад відносного спокою, завжди залишається лише ілюзією. У 2011, 2012 та 2015 роках картель уже паралізовував місто у відповідь на арешти чи втрати. Але те, що сталося 22 лютого 2026 року, перевершило попередні спалахи за масштабом та зухвалістю. Координовані атаки, що поширилися на 20 штатів, але зосередилися саме в Гвадалахарі, де загинуло щонайменше 10 нацгвардійців, були не просто актом помсти. Це була складна, прорахована військова операція, покликана продемонструвати, що структура залишається боєздатною, керованою та вкрай небезпечною навіть після втрати лідера.

Насильство не обмежилося лише сутичками з силовиками. Воно мало на меті посіяти паніку серед цивільного населення. Телефони містян вибухнули повідомленнями та відео, що поширювали страх. Це була інформаційно-психологічна операція, покликана змусити людей залишатися вдома, посилити тиск на владу та довести, що картель все ще контролює вулиці. І хоча офіційні особи швидко заявили про відновлення порядку, мешканці міста, з якими спілкувалися журналісти, описували зовсім іншу реальність.

Смерть Ель Менчо, безсумнівно, створила вакуум влади на самій верхівці ієрархії CJNG. Це спровокує жорстоку внутрішню боротьбу за контроль над фінансовими потоками та маршрутами, і ця боротьба, найімовірніше, виллється в нову хвилю насильства, цього разу вже між різними фракціями всередині картелю.

Але для пересічних мешканців Гвадалахари кардинальних змін може й не настати. Доки держава не запропонує реальної альтернативи цій тіньовій владі — не лише силової, але й соціальної, економічної та інституційної — Гвадалахара приречена жити в стані крихкого затишшя. Вона залишиться містом, де блиск високих технологій поруч з чорними ринками, де студенти на шкільних заняттях обговорюють, хто насправді контролює їхні райони. І це крихке

затишшя будь-якої миті може бути знову розірване черговою хвилею насильства, яка нагадає всім, хто є справжнім господарем у цій тіньовій столиці Мексики.

Для загального розвитку

Крізь блокчейн у реальність: Як криптовалютні потоки розкривають анатомію сучасної нелегальної економіки [14]

У той час як світ обговорює волатильність цифрових активів та їхню роль у легітимних фінансах, існує тіньова сторона криптоекономіки, яка стає дедалі більш структурованою, професійною та, що найважливіше, вразливою до глибинного аналізу.

Щорічний звіт Chainalysis про криптозлочинність за 2026 рік демонструє низку парадоксальних явищ: хоча загальні обсяги транзакцій, пов'язаних із даркнет-ринками, можуть демонструвати певне скорочення або стагнацію в окремих сегментах, глибинні структурні зміни вказують на безпрецедентну еволюцію нелегального бізнесу в бік стійкості, глобалізації та, що найважливіше, дедалі тіснішого зв'язку з реальними людськими трагедіями.

Одним із найбільш промовистих та водночас обнадійливих прикладів такої аналітичної спроможності став ретельний аналіз ринку фентанілу. Після трагічного піку смертності від передозувань у Сполучених Штатах, який сягав майже 80 000 смертей на рік, нарешті намітилося суттєве та стійке зниження. Перед дослідниками та політиками постало питання: що саме спрацювало? Виявилося, що ключовим фактором стало не просто посилення контролю на кордонах, яке часто є лише боротьбою з наслідками, а стратегічне порушення ланцюгів постачання на самому початку — на етапі закупівлі хімічних прекурсорів, необхідних для синтезу смертоносного наркотику. І саме дані блокчейну надали майже детективні докази цієї тези, перетворивши абстрактні припущення на математично підтверджену реальність.

Починаючи з середини 2023 року, обсяги криптовалютних платежів, які спрямовувалися на адреси китайських брокерів, що спеціалізувалися на торгівлі хімічними прекурсорами для синтезу фентанілу, різко пішли вниз. Це падіння не було випадковим коливанням ринку, воно стало прямим і майже негайним наслідком серії дипломатичних та правоохоронних заходів: запровадження санкцій, кримінальних переслідувань конкретних мереж та історичних двосторонніх домовленостей між США та Китаєм щодо співпраці у боротьбі з наркотиками.

Китайські брокери почали масово публікувати оголошення про відмову від роботи з клієнтами з Північної Америки, скаржачись у приватних повідомленнях на майже стовідсоткове затримання вантажів на тлі загострення торговельної війни та посилення митного контролю. Вони більше не хотіли ризикувати вантажами, дев'ять із десяти яких потрапляли в руки влади. Відповідно, гроші перестали надходити.

Ключовий висновок, який робить Chainalysis разом із авторами наукової статті в журналі Science, полягає в тому, що падіння криптовалютних потоків до постачальників прекурсорів випередило зниження рівня смертності від передозувань приблизно на три-шість місяців. Це той самий лаг, який необхідний, щоб ланцюг постачання повністю вичерпався, наявні запаси розчинилися, а

[14] https://www.chainalysis.com/blog/crypto-drug-sales-darknet-markets-2026/?mkt_tok=NTAzLUZBUC0wNzQAAAGgOrrKi71E5kigrOZ1-VPr5U-bM8nUaOKloXnOqwEIzd6V6RJVfvaG09ryB35TV970M3NfWkCbj4MIEHKHvyXIzYHZCLMFwd434tgWURokbW4t

синтезований наркотик перестав надходити до кінцевих споживачів на вулицях американських міст.

Однак проблема наркоторгівлі, звісно ж, не обмежується лише опіоїдами, і блокчейн-аналітика дозволяє вивчати й інші види речовин із не менш вражаючою точністю. Канадське дослідження, інтегроване у звіт, виявило ще одну важливу закономірність, яка розділяє природу споживання стимуляторів та його вплив на громадське здоров'я. Аналізуючи кореляцію між криптовалютними транзакціями на даркнет-ринках та реальними показниками системи охорони здоров'я, такими як кількість візитів до відділень невідкладної допомоги, госпіталізацій та смертей, дослідники натрапили на статистичний феномен. Виявилося, що існує кардинальна різниця між впливом малих та великих транзакцій. Дрібні платежі на даркнет-ринки, умовно кажучи, на суму менше п'ятисот доларів, які, ймовірно, здійснюються кінцевими споживачами для особистого вживання, не демонструють жодного статистично значущого зв'язку з кількістю викликів швидкої або летальних випадків. Трендова лінія залишається практично плоскою, що може свідчити про те, що помірне або контрольоване вживання рідше призводить до гострих станів, які потребують госпіталізації. На противагу цьому, великі транзакції на суму понад п'ятсот доларів мають пряму, чітко виражену кореляцію з погіршенням громадського здоров'я: будь-яке зростання обсягів таких платежів невдовзі призводить до статистично значущого сплеску госпіталізацій, пов'язаних із вживанням стимуляторів. Механізм цього явища простий і водночас жорстокий у своїй економічній логіці: великі суми означають або важке, хронічне особисте споживання з високим ризиком передозування, або, що значно частіше, подальший перепродаж і розповсюдження серед ширшого кола споживачів.

Гроші рухаються в блокчейні задовго до того, як дилер фізично розповсюдить товар по мікрорайонах, і задовго до того, як кінцевий споживач опиниться в реанімації з зупинкою серця. Це ще раз підтверджує фундаментальну тезу звіту: аналіз криптовалютних потоків — це не просто інструмент фінансового моніторингу, а операційне джерело даних для системи охорони здоров'я, яке дозволяє передбачати навантаження на лікарні та розподіляти ресурси рятувальних служб із безпрецедентною точністю.

Даркнет-ринки сьогодні більше не є ізольованими віртуальними вітринами для роздрібної торгівлі, якими вони були на зорі свого існування. Еволюціонувавши, вони сформували складну, високоорганізовану та глобалізовану мережу оптового постачання, де одні майданчики виступають постачальниками для інших, створюючи багаторівневу дистриб'юторську систему, яка нагадує легальних логістичних гігантів.

Закриття Abacus Market у липні 2025 року, який на той момент був найбільшим біткоїн-ринком для західних покупців, не знищило бізнес, а лише тимчасово перенаправило фінансові та товарні потоки. Його місце із вражаючою швидкістю посів TorZon, який не лише став новим центром тяжіння для роздрібних клієнтів, але й увійшов до елітної когорти ключових гравців у системі міжринкових транзакцій. Аналітики фіксують, що TorZon за обсягами внутрішньомережевого постачання поставив себе в один ряд із такими визнаними гігантами, як російськомовні платформи Mega, Kraken, OMG!OMG! та Blackspruit. Це свідчить про неймовірно високий рівень адаптивності та стійкості тіньової економіки: коли один вузол складної мережі знищується правоохоронцями, бізнес майже без затримки мігрує, а капітал миттєво перетікає до наступного, часто більш захищеного, гравця.

Аналітики Chainalysis фіксують, що після будь-якого серйозного хакерського злому, викриття або добровільного закриття майданчика негайно виникає характерний сплеск внутрішньомережевих переказів — дилери та адміністратори ринків у паніці, але організовано шукають нові притулки для своїх запасів і фінансових резервів, переміщуючи мільйони доларів між платформами, щоб відновити ланцюжки постачання та зберегти капітал від арештів. Цей

феномен став маркером зрілості злочинного світу, який навчився керувати ризиками так само професійно, як і корпорації.

Паралельно з ринком наркотичних речовин кардинально трансформується і сегмент так званих фрод-шопів — спеціалізованих інтернет-магазинів, що торгують викраденими даними кредитних карток, персональними даними та інструментами для шахрайства. Тут спостерігається драматичне падіння річних обсягів транзакцій — з 205 до 87 з половиною мільйонів доларів. На перший погляд, це може виглядати як беззаперечна перемога правоохоронних органів над кіберзлочинністю. Однак більш глибокий аналіз свідчить, що це не стільки тотальна перемога, скільки зміна обличчя та бізнес-моделі самого шахрайства.

Успішні міжнародні операції проти ключових платіжних процесорів на кшталт Universal Anonymous Payment System (UAPS) та сервісів відмивання грошей Cryptex завдали нищівного удару по традиційній, орієнтованій на російськомовну аудиторію веб-інфраструктурі. Цей колись потужний сектор розпався на безліч дрібних, розрізнених гравців, які тепер змушені працювати з роздрібними клієнтами, здійснюючи невеликі за обсягом транзакції, що свідчить про фрагментацію ринку та втрату довіри.

Водночас на кримінальну арену вийшли нові, набагато потужніші та організованіші гравці — китайськомовні мережі, що базуються на платформі Telegram. Вони функціонують за зовсім іншою, оптовою моделлю, яка більше нагадує B-2-B, продаючи бази даних скомпрометованих карток величезними партіями безпосередньо перекупникам, а не кінцевим шахраям-аматорам. Середній розмір однієї транзакції в цих мережах є значно вищим, ніж у російськомовних конкурентів, що підтверджує їхню спеціалізацію на великому гурті. При цьому, самі Telegram-канали, попри те, що основне спілкування ведеться китайською мовою, часто пропонують автоматизований переклад інтерфейсу та підтримку англійською, орієнтуючись на глобального покупця з будь-якого куточка світу. Цей структурний зсув яскраво демонструє, що злочинний світ здатний швидко консолідуватися на нових, стійких до тиску соціальних платформах, уникаючи вразливих веб-сайтів та переходять до більш прибуткової гуртової торгівлі.

У підсумку, звіт Chainalysis підкреслює фундаментальну зміну парадигми у розумінні природи криптозлочинності. Цінність технології блокчейн для боротьби з нелегальною діяльністю більше не вимірюється виключно обсягами вилучених коштів або кількістю закритих сайтів, як це було ще кілька років тому. Головним активом стає видимість, прозорість.

Сама природа розподіленого реєстру, який зберігає незмінний запис кожної транзакції, дозволяє побачити в реальному часі, як саме функціонує тіньова економіка. Це дає змогу суспільству та державі перейти від реактивної моделі, за якої ми лише констатуємо зростання смертності або публікуємо статистику вилучених наркотиків через півроку після подій, до проактивної, заснованої на аналізі намірів, фінансових потоків та предиктивному моделюванні.

У світі, де економічна активність дедалі більше переміщується на блокчейн, цей інструмент стає незамінним не лише для поліції та спецслужб, але й для політиків, які формують стратегію боротьби з наркотрафіком, для регуляторів фінансових ринків. Здатність бачити загрозу до того, як вона стане невідворотною, — ось головний стратегічний урок звіту.

Ваша думка важлива!

1. Які саме нормативні та практичні механізми можуть бути запроваджені в Україні для реалізації принципу мінімізації персональних даних у процедурах ідентифікації та перевірки клієнтів (KYC/CDD), не знижуючи при цьому ефективності виявлення складних схем відмивання коштів і фінансування тероризму?
2. Яким чином використання штучного інтелекту у сферах фінансового моніторингу, комплаєнсу та ПВК/ФТ в Україні може підвищити ефективність виявлення складних транснаціональних схем відмивання коштів і фінансування тероризму, не створюючи при цьому нових ризиків дискримінації та непрозорості рішень?
3. Наскільки можливо створити жорсткішу систему верифікації кінцевих бенефіціарів? Яким чином можна запобігти появі "віртуальних" осіб у реєстрах компаній?
4. З огляду на високий рівень цифровізації державних послуг та, водночас, складну безпекову ситуацію, наскільки вразливими є українські банки та платіжні системи до атак з використанням шкідливого ПЗ?
5. Враховуючи, що ключовим каналом постачання синтетичних прекурсорів є міжнародні поштові відправлення, наскільки ефективною є система скринінгу в поштових операторів та на митниці для виявлення невеликих партій хімічних речовин, замовлених онлайн? Чи готова Україна до такої форми контрабанди?
6. Якими можуть бути ефективні підходи держав до регулювання P2P-транзакцій зі стейблкоїнами, які здійснюються без участі регульованих посередників, і як при цьому можна поєднати цілі протидії відмиванню коштів із підтримкою розвитку цифрових фінансових інновацій?

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-2026-10

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].