Методологічний бюлетень

Серійний номер: МінФін-AML-2026-09

Лютий 2026

“Знати недостатньо – потрібно діяти”

Йоганн Ґете

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

Корпоративна відповідальність у цифрову епоху: підхід OECD до управління штучним інтелектом [1]

Документ OECD є комплексним методологічним керівництвом, спрямованим на інтеграцію принципів відповідального ведення бізнесу та управління ризиками у всі етапи розробки, впровадження та використання систем штучного інтелекту. Його основною метою є формування цілісної моделі корпоративної та регуляторної відповідальності, у межах якої штучний інтелект розглядається не лише як технологічний продукт, а як соціально, економічно та правово значуща інфраструктура, здатна створювати як позитивні ефекти, так і системні ризики для прав людини, ринкової стабільності, конкуренції та суспільної довіри. Документ позиціонує належну перевірку у сфері AI як інструмент забезпечення сталого розвитку, інноваційної конкурентоспроможності та довгострокової легітимності бізнесу

[1] https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/02/oecd-due-diligence-guidance-for-responsible-ai_7831bb49/41671712-en.pdf

в умовах посилення регуляторного тиску та фрагментації міжнародних підходів.

В основі керівництва лежить адаптація загальної моделі процедури належної перевірки у сфері відповідального ведення бізнесу до специфіки життєвого циклу AI-систем. OECD виходить із того, що ризики, пов'язані зі штучним інтелектом, не обмежуються етапом експлуатації, а формуються ще на стадіях збору та обробки даних, проєктування архітектури, навчання моделей, інтеграції в бізнес-процеси та масштабування. У зв'язку з цим документ вибудовує логіку безперервного управління ризиками, що охоплює формування внутрішніх політик, інституціоналізацію відповідальності, ідентифікацію та пріоритизацію негативних впливів, запровадження механізмів їх запобігання та пом'якшення, системний моніторинг ефективності заходів, комунікацію зі стейкхолдерами та забезпечення відшкодування шкоди у разі її заподіяння.

Суттєвою особливістю документа є відхід від вузького технократичного розуміння управління AI. Автори наголошують, що ефективна належна перевірка неможлива без інтеграції технологічних, правових, організаційних і соціальних компонентів у єдину систему управління. Управління ризиками штучного інтелекту має бути вбудоване у загальні механізми стратегічного планування, управління комплаєнсом, внутрішнього аудиту та корпоративної культури. У цьому контексті документ підкреслює необхідність залучення вищого керівництва до формування цілей, визначення рівня прийнятного ризику та контролю реалізації політик у сфері AI.

Окремий акцент зроблено на принципі розподіленої відповідальності у ланцюгу створення вартості. OECD послідовно демонструє, що жоден учасник AI-екосистеми не може бути звільнений від обов'язків належної перевірки лише на тій підставі, що він не є безпосереднім розробником технології. Постачальники даних, хмарної інфраструктури, програмних компонентів, фінансування, інтеграційних рішень та користувачі несуть власну частку відповідальності залежно від рівня впливу на функціонування системи. Такий підхід спрямований на запобігання фрагментації відповідальності та формуванню «сірих зон», у яких ризики залишаються без належного управління.

Документ приділяє значну увагу методології ідентифікації та оцінки ризиків. Підкреслюється, що аналіз має охоплювати не лише прямі технічні збої або помилки алгоритмів, а й ширший спектр потенційних негативних наслідків, включно з дискримінацією, порушенням приватності, обмеженням доступу до послуг, посиленням соціальної нерівності, маніпулятивним впливом, ризиками зловживання технологіями подвійного призначення та використанням AI в умовах слабких інституцій. При цьому ризик-орієнтований підхід розглядається як динамічний процес, що має регулярно переглядатися з урахуванням змін у технологіях, бізнес-моделях і регуляторному середовищі.

Важливим блоком керівництва є питання управління даними та алгоритмічною прозорістю. OECD наголошує, що якість, походження та умови збору даних безпосередньо визначають рівень ризику майбутніх AI-систем. У документі обґрунтовується необхідність впровадження процедур відповідального джерелування, верифікації, документування та аудиту датасетів, а також забезпечення можливості відстеження рішень моделей. Прозорість, пояснюваність і простежуваність розглядаються не як факультативні елементи, а як інструменти запобігання системним помилкам і підвищення підзвітності перед регуляторами та суспільством.

Суттєве місце у звіті займає тема взаємодії із зацікавленими сторонами. Документ формує концепцію змістовної взаємодії із заінтересованими сторонами як постійного двостороннього процесу, що має супроводжувати всі етапи життєвого циклу AI. Йдеться не лише про формальні консультації, а про реальне залучення працівників, споживачів, уразливих груп, профспілок, громадських організацій і професійних спільнот до обговорення ризиків, пріоритетів і варіантів реагування. Такий підхід покликаний підвищити якість управлінських рішень, запобігти репутаційним кризам і сформувати довіру до технологій.

Окремий розділ присвячено співвідношенню належної перевірки з вимогами конкуренційного права, комерційної таємниці та захисту інтелектуальної власності. OECD визнає легітимність цих інтересів, проте наголошує, що вони не можуть використовуватися як підстава для уникнення прозорості та відповідальності. Підприємствам рекомендується інтегрувати процедури належної перевірки у сфері штучного інтелекту у загальні програми комплаєнсу та антимонопольного контролю, забезпечуючи баланс між співпрацею, інноваціями та дотриманням правових обмежень.

Важливим елементом документа є аналіз можливостей використання самого штучного інтелекту для підтримки процесів належної перевірки. Розглядаються приклади застосування AI для аналізу ланцюгів постачання, моніторингу інформаційного простору, виявлення ранніх сигналів ризику та перевірки походження продуктів. Водночас підкреслюється, що такі інструменти не можуть замінити людського судження і потребують власних механізмів контролю та валідації.

Завершальна частина керівництва присвячена питанням процедур відновлення та компенсації та відповідальності за наслідки. OECD наполягає на тому, що належна перевірка не завершується на етапі запобігання ризикам, а має включати ефективні механізми реагування на інциденти, внутрішні розслідування, доступні канали подання скарг і співпрацю з постраждалими сторонами. Відшкодування шкоди та відновлення порушених прав розглядаються як ключовий критерій реальної, а не формальної відповідальності бізнесу.

У підсумку документ формує цілісну концепцію управління штучним інтелектом як міждисциплінарного процесу, що поєднує технологічну експертизу, правове регулювання, соціальну відповідальність і корпоративну етику. OECD демонструє, що відповідальний AI є не окремою галуззю комплаєнсу, а складовою сучасної моделі стійкого бізнесу, у межах якої інновації, захист прав людини, фінансова стабільність і регуляторна відповідність мають розглядатися як взаємопов’язані елементи єдиної системи управління ризиками.

Висновки:

- **Керівництво OECD формує уніфіковану модель належної перевірки у сфері штучного інтелекту,** інтегровану в загальну систему відповідального корпоративного управління, у межах якої управління AI-ризиками стає постійною функцією управління, комплаєнсу та внутрішнього контролю.
- **Відповідальність за негативні впливи AI системно розподіляється між усіма учасниками ланцюга створення вартості —** від постачальників даних та інфраструктури до кінцевих користувачів, що унеможливлює перекладання ризиків і формує модель спільної, але диференційованої відповідальності.
- **Ризик-орієнтований підхід визначається базовим принципом управління AI:** належна перевірка фокусується на високоризикових сферах застосування та розглядається як безперервний процес поступового вдосконалення, а не як формальна процедура відповідності.
- **Системна взаємодія із зацікавленими сторонами, забезпечення прозорості, простежуваності та наявність механізмів ремедіації** визнаються необхідною умовою легітимного використання AI та довгострокової регуляторної і репутаційної стійкості підприємств.

Штучний інтелект на ринках капіталу ЄС: між операційною ефективністю, регуляторними викликами та новими системними ризиками [2]

Звіт Європейського органу з цінних паперів та ринків (ESMA) присвячений комплексному аналізу рівня впровадження штучного інтелекту (AI) у секторі ринків капіталу Європейського Союзу та його впливу на операційну модель, ризик-профіль і конкурентоспроможність фінансових установ. Дослідження ґрунтується на результатах масштабного опитування, проведеного влітку 2025 року серед 728 фінансових установ із 19 держав-членів ЄС, які представляють інвестиційні компанії, керуючих активами, банки, фінансові ринкові інфраструктури та кредитні рейтингові агентства. Звіт має на меті подолати фрагментарність наявних даних про використання штучного інтелекту у фінансовому секторі та сформувати системне уявлення для регуляторів і наглядових органів.

Автори виходять із того, що сучасний етап розвитку великих мовних моделей і генеративного штучного інтелекту істотно прискорив цифрову трансформацію фінансових ринків, водночас створивши нові виклики для нагляду та управління ризиками. Незважаючи на тривалу історію використання алгоритмічних та аналітичних моделей у фінансах, саме поява генеративних технологій після 2023 року стала каталізатором масового інтересу до AI як стратегічного інструменту підвищення ефективності. При цьому ESMA підкреслює, що інституційні можливості регуляторів щодо моніторингу цих процесів залишаються обмеженими, а наглядові підходи перебувають на стадії формування.

Аналіз рівня впровадження демонструє, що використання штучного інтелекту у секторі цінних паперів залишається частковим і нерівномірним. Майже половина опитаних компаній не має жодних активних або запланованих застосувань AI, що свідчить про обережність ринку та структурні бар'єри для цифровізації. Водночас великі фінансові групи майже повністю інтегрували AI у свою діяльність або перебувають на завершальних етапах його впровадження. Таким чином, формується технологічний розрив між великими та малими учасниками ринку, який може посилювати концентрацію та знижувати конкурентну динаміку.

Інвестиційна поведінка компаній підтверджує цю асиметрію. Лише менше половини респондентів здійснювали інвестиції у AI у 2024 році, причому основний обсяг вкладень припадає на великі корпорації. Разом із тим більшість учасників ринку декларують наміри нарощувати інвестиції у 2025–2027 роках, що свідчить про формування довгострокового тренду. Ключовою мотивацією для таких вкладень є прагнення до оптимізації витрат і підвищення операційної ефективності, а не безпосереднє зростання доходів. Очікування щодо впливу AI на прибутковість залишаються стриманими, особливо серед малих і мікропідприємств.

Дослідження сфер застосування показує, що на поточному етапі штучний інтелект переважно використовується у допоміжних і внутрішніх функціях. Найпоширенішими є інструменти для підготовки, узагальнення та аналізу текстів, внутрішні цифрові асистенти, автоматизація програмування, переклад і обробка даних. Застосування AI у ключових інвестиційних і торговельних процесах залишається обмеженим і здебільшого перебуває у стадії пілотних

[2] https://www.esma.europa.eu/sites/default/files/2026-02/ESMA50-481369926-30599_TRV_Risk_Analysis_AI_adoption_and_trends_in_securities_markets.pdf

проєктів. Переважна більшість рішень функціонує за моделлю «людина в контурі», коли остаточні рішення ухвалюються співробітниками, а автономність алгоритмів є низькою.

У технологічному вимірі звіт фіксує домінування генеративного штучного інтелекту, який становить основну частку всіх зафіксованих випадків використання. Поряд із ним застосовуються інструменти обробки природної мови та класичного машинного навчання, тоді як агентні системи з елементами планування і взаємодії з зовнішніми інструментами лише починають проникати у фінансовий сектор. Навіть у цих випадках компанії прагнуть обмежувати рівень автоматизації, щоб зберігати контроль над ризиками.

Серед основних переваг використання AI респонденти насамперед відзначають можливість ефективної роботи з великими масивами даних, оптимізацію внутрішніх процесів, скорочення операційних витрат і підвищення якості аналітики. Значна частина компаній також визнає позитивний вплив технологій на функції комплаєнсу, управління ризиками та внутрішнього контролю. Разом із тим створення принципово нових бізнес-моделей або джерел доходів поки що не є домінуючим результатом цифровізації, що свідчить про еволюційний, а не революційний характер трансформації.

Оцінка ризиків демонструє високий рівень обізнаності учасників ринку щодо потенційних загроз, пов'язаних із використанням штучного інтелекту. Найбільш значущими вважаються ризики, пов'язані з якістю даних, їх захистом і управлінням, а також із галюцинаціями моделей і кібербезпекою. Важливим чинником вразливості є залежність від третіх постачальників технологічних рішень, що посилює операційні ризики та може мати системний ефект у разі масштабних збоїв. Додатковим викликом є дотримання регуляторних вимог, зокрема положень Регламенту ЄС про штучний інтелект, які істотно впливають на організацію процесів управління моделями.

Висновки:

- **Фінансовим установам доцільно формалізувати систему управління AI:** створити внутрішні комітети, політики валідації моделей, процедури контролю автономності та відповідальності. Без цього масштабування технологій призведе до зростання операційних і регуляторних ризиків.
- **Для зменшення залежності від зовнішніх провайдерів компаніям варто інвестувати у власні дата-платформи, аналітичні команди та навчання персоналу.** Внутрішні дані й експертиза є ключовим фактором стійкої цифровізації.
- **Висока концентрація хмарних і модельних постачальників вимагає впровадження стратегій використання кількох хмарних провайдерів, планів виходу та регулярного тестування стійкості відповідно до DORA.** Це має стати стандартною практикою управління операційним ризиком.
- **З огляду на поширення використання AI у сферах ПВК/ФТ, комплаєнсу та аналітики, регулятори й установи мають інтегрувати AI у ризик-орієнтовані моделі контролю,** забезпечивши прозорість, пояснюваність і аудитованість алгоритмів.

Організаційний аналіз свідчить про значний дефіцит компетенцій у сфері штучного інтелекту на всіх рівнях управління. Лише незначна частина керівників і операційного персоналу володіє глибоким розумінням відповідних технологій. Це зумовлює залежність від зовнішніх консультантів і постачальників, а також підвищує ризики помилок у впровадженні. Водночас більшість компаній уже розпочали або планують програми навчання персоналу, що розглядається як ключова умова сталого розвитку цифрових компетенцій.

У сфері інфраструктури дослідження фіксує домінування хмарних рішень, причому значна частина компаній користується послугами одного постачальника. Ринок послуг із розробки моделей, обчислювальних ресурсів і

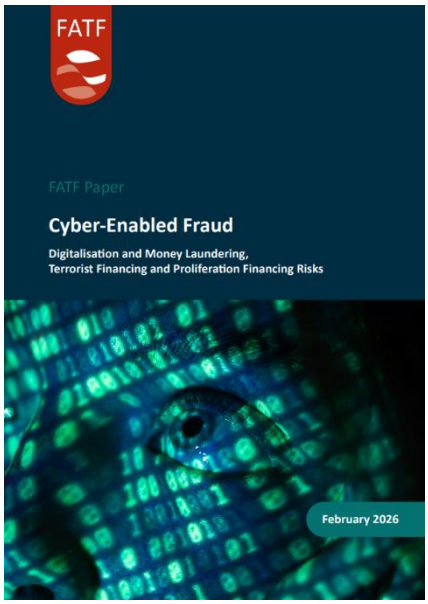
обробки даних характеризується високою концентрацією, а основні провайдери перебувають за межами Європейського Союзу. Це формує стратегічну залежність фінансового сектору від позаєвропейських технологічних корпорацій. Хоча багато компаній декларують використання кількох постачальників, реальна диверсифікація часто залишається обмеженою.

Щодо розробки моделей і використання даних, звіт демонструє поєднання зовнішніх і внутрішніх підходів. Частина компаній використовує готові комерційні рішення, інші здійснюють адаптацію моделей під власні потреби або розробляють їх самостійно. Великі установи частіше використовують внутрішні масиви даних для навчання та донавчання моделей, що підвищує точність і релевантність результатів, тоді як малі компанії більшою мірою залежать від відкритих і комерційних джерел.

Окрему увагу автори приділяють практиці використання публічних генеративних інструментів співробітниками. Переважна більшість компаній дозволяє доступ до таких сервісів, причому значна частина — без формалізованих обмежень і внутрішніх правил. Відсутність чітких політик у цій сфері створює додаткові ризики витоку інформації, порушення конфіденційності та недотримання регуляторних вимог.

У підсумку ESMA доходить висновку, що штучний інтелект у секторі ринків капіталу ЄС перебуває на стадії контрольованого розвитку, коли основний акцент робиться на підвищенні ефективності та збереженні стабільності. Технологія ще не стала повноцінним джерелом стратегічної переваги для більшості учасників ринку, однак її значення поступово зростає. Водночас концентрація інфраструктури, залежність від зовнішніх постачальників, дефіцит компетенцій і регуляторна складність формують системні виклики для фінансової стабільності. У цих умовах ESMA розглядає подальший моніторинг розвитку AI як необхідний елемент наглядової діяльності та ключовий інструмент забезпечення стійкості європейських фінансових ринків.

Фінансові потоки шахрайства в цифрову епоху: міжнародний досвід FATF [3]



У документі FATF здійснено комплексний аналіз феномену кіберзумовленого шахрайства як одного з наймасовіших та найдинамічніших джерел незаконних доходів у сучасній цифровій економіці та як одного з ключових чинників ризику для систем протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Документ підготовлено в межах довгострокової стратегії FATF щодо оцінки наслідків цифровізації для глобальної системи фінансової безпеки та спрямовано на формування спільного розуміння нових типологій шахрайства серед національних органів влади, фінансових установ, постачальників послуг з віртуальними активами та визначених нефінансових установ і професій.

У вступній частині наголошується, що стрімке впровадження цифрових фінансових технологій, дистанційних сервісів і миттєвих платіжних інструментів, особливо після пандемії COVID-19, радикально змінило середовище здійснення фінансових операцій. Поряд із підвищенням ефективності та доступності фінансових послуг ці процеси створили сприятливі умови для масштабування шахрайських схем, які базуються на соціальній інженерії, маніпуляціях із персональними

[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Cyber-Enabled-Fraud%E2%80%93Digitalisation-and-ML-TF-PF-Risks.pdf.coredownload.inline.pdf

даними, використанні підроблених цифрових платформ та психологічному впливі на жертв. FATF підкреслює, що сучасне кіберзумовлене шахрайство характеризується високим рівнем професіоналізації, транснаціональності та технологічної складності.

У першому розділі звіту наведено узагальнену картину масштабів проблеми на основі даних держав-членів FATF, фінансових розвідок та правоохоронних органів. Більшість проаналізованих юрисдикцій визначають шахрайство як один із ключових ризиків відмивання коштів, а в окремих країнах воно становить найбільшу частку у структурі загальної злочинності. Автори звертають увагу на те, що реальні обсяги збитків значно перевищують офіційну статистику, оскільки значна частина жертв не повідомляє про інциденти. Таким чином, кіберзумовлене шахрайство розглядається не як другорядна форма злочинності, а як системна загроза економічній безпеці та довірі до фінансових інститутів.

Окремий аналітичний блок присвячено чинникам, що сприяють поширенню шахрайства. До них віднесено використання штучного інтелекту, діпфейків, автоматизованих фішингових кампаній, фейкових інвестиційних платформ, соціальних мереж і месенджерів як основних каналів комунікації з потенційними жертвами. Документ демонструє, що ці технології дозволяють злочинцям здійснювати масові атаки з мінімальними витратами, адаптувати сценарії під різні аудиторії та швидко змінювати тактику у відповідь на дії правоохоронних органів.

Значну увагу приділено ролі фінансової інфраструктури у сприянні шахрайським схемам. Миттєві платежі, транскордонні перекази, електронні гаманці та віртуальні активи створюють можливість для швидкого переміщення коштів до моменту їх виявлення. FATF підкреслює, що злочинці активно використовують багаторівневі платіжні ланцюги, фінтех-посередників і криптовалютні сервіси для ускладнення фінансового трасування та уникнення повернення активів.

У документі також описано тенденцію до формування спеціалізованих «скам-центрів», які функціонують як організовані кримінальні підприємства. Такі структури часто поєднують шахрайство з торгівлею людьми, примусовою працею, незаконною міграцією та професійними послугами з відмивання коштів. У результаті кіберзумовлене шахрайство інтегрується у ширші транснаціональні кримінальні екосистеми, що значно ускладнює їх викриття та ліквідацію.

Другий розділ звіту присвячено аналізу того, яким чином стандарти FATF можуть використовуватися для протидії кіберзумовленому шахрайству. Автори наголошують, що ефективна боротьба можлива лише за умови комплексного застосування інструментів ПВК/ФТ/ФР, а не через ізольовані антикримінальні заходи. Особливий акцент робиться на підвищенні прозорості платіжних операцій, зокрема шляхом впровадження механізмів підтвердження отримувача, посилення вимог до ідентифікації клієнтів і контролю операцій у децентралізованих середовищах.

Важливе місце у звіті займає тема повернення активів. FATF відзначає необхідність створення механізмів швидкого призупинення платежів, замороження коштів, застосування конфіскації без обвинувального вироку та розвитку неформального міжнародного співробітництва. Ці інструменти розглядаються як ключові для зниження економічної привабливості шахрайства.

Окремо аналізується регулювання ринку віртуальних активів. FATF підтверджує стратегічне значення стандартів щодо постачальників послуг з віртуальними активами, включно з вимогами щодо ідентифікації клієнтів, відстеження транзакцій та обміну інформацією. Недостатня імплементація цих стандартів у низці юрисдикцій створює «регуляторні прогалини», які активно використовуються злочинними мережами.

Значна увага приділяється прозорості бенефіціарної власності. Автори підкреслюють, що шахрайські мережі системно використовують компанії-оболонки та номінальні структури для

маскування доходів, тому ефективні реєстри кінцевих бенефіціарних власників є критично важливими для фінансових розслідувань.

У документі також розглядається роль міжсекторального партнерства та координації. FATF підкреслює, що без постійної взаємодії між фінансовими розвідками, правоохоронними органами, банками, фінтех-компаніями та цифровими платформами протидія шахрайству буде фрагментованою та малоефективною. Як перспективну модель наводяться національні координаційні центри з протидії шахрайству.

Останній тематичний блок присвячено використанню сучасних аналітичних технологій. FATF визнає, що традиційні ручні методи аналізу не відповідають масштабам проблеми, тому рекомендується широке впровадження машинного навчання, поведінкової аналітики, систем ризик-скорингу та моніторингу транзакцій у реальному часі.

У підсумковій частині документа наголошується, що кіберзумовлене шахрайство стало глобальною загрозою, яка системно підриває довіру до фінансових систем. FATF підтверджує намір зосередити значну частину своєї діяльності на цій тематиці у найближчі роки та закликає держави до посилення імплементації міжнародних стандартів і розвитку міжнародної співпраці.

Висновки:

- **Шахрайство, вчинене у цифровому середовищі трансформувалося у системне джерело незаконних доходів,** тісно інтегроване з механізмами відмивання коштів, що потребує його повноцінної інтеграції у національні та секторальні оцінки ризиків.
- **Висока швидкість переміщення коштів у цифровому середовищі** робить критично важливими механізми негайного блокування платежів і міжнародної координації для повернення активів.
- **Недостатня імплементація стандартів щодо VASP та прозорості бенефіціарної власності** створює ключові вразливості, які активно використовуються шахрайськими мережами.
- **Без системного впровадження аналітичних технологій та міжсекторальної співпраці** держави не здатні ефективно протидіяти масштабам сучасного шахрайства, вчиненого у цифровому середовищі.

Звіти окремих інституцій та експертів

Анатомія терору: Як європейські технології живлять російську дронову війну [4]

Крижана темрява, яка щовечора огортає домівки українців, є не просто наслідком воєнних дій, а результатом складного технологічного ланцюжка, що простягається від конструкторських бюро в росії до фабрик з виробництва мікросхем у Європі та Китаї, і далі — до тіньових посередників, які забезпечують безперебійне постачання. Це історія про те, як глобальна економіка, попри санкції та моральні застереження, продовжує живити військову машину кремля, роблячи співучасником страждань мільйонів українців фактично

[4] https://www.occrp.org/en/investigation/made-in-the-eu-dropped-on-kyiv-how-european-parts-are-enabling-russias-winter-drone-war

кожного, хто користується звичайною побутовою електронікою, адже саме такі, здавалося б, невинні компоненти лежать в основі російського дрона-камікадзе «Герань-2».

Цей безпілотник, який в Україні називають просто «Шахед» (на згадку про його іранське походження), став головним інструментом терору проти цивільної інфраструктури. Минулого року, за даними Повітряних сил України, було лише дев'ять днів, коли країна не потерпала від його атак. Загалом у 2025 році росія застосувала 34 000 таких дронів — це більше половини від усіх безпілотних ударів. Вони не просто влучають у ціль: їхня тактика полягає у створенні роїв, які виснажують українську протиповітряну оборону, розчищаючи шлях для більш досконалих і руйнівних крилатих ракет. Вони летять низько, повільно, їх важко виявити, але легко виробляти у величезних кількостях на заводі в російському Татарстані. Іван Киричевський, експерт київського центру Defense Express називає «Герань-2» найкращим дроном у своєму класі у світі. Його вартість — від 20 до 50 тисяч доларів — робить його «крилатою ракетою для бідних», доступною зброєю масового ураження, здатною долати 2500 кілометрів.

Однак навіть «зброя для бідних» потребує високотехнологічних компонентів, яких росія не виробляє. І саме тут починається історія, яку журналісти OCCRP, De Tijd, The Kyiv Independent та інших видань розкрили у своєму гучному розслідуванні. Дослідження збитих дронів, проведені Головним управлінням розвідки України, показують разючу картину: «Герань-2» — це збірний продукт глобалізованого світу. З сотень компонентів лише кілька десятків мають російське маркування. Решта — продукція компаній зі США, Китаю та, що найважливіше, з Європи. Понад сто деталей, вироблених приблизно двадцятьма європейськими фірмами, були знайдені в уламках цих безпілотників. Це мікросхеми, транзистори, діоди, антени, навігаційні приймачі та паливні насоси. Вони є нервовою системою, мозком і м'язами дрона, який щодня несе смерть і руйнування.

Європейський Союз, усвідомлюючи загрозу, ще у 2022 році запровадив заборону на експорт до росії товарів подвійного призначення. Санкції посилювалися, додавалися нові обмеження, а у 2024 році від європейських виробників почали вимагати включати в контракти з іноземними клієнтами пункт про заборону реекспорту до росії. Девід О'Салліван, спеціальний посланник ЄС із питань санкцій, у коментарі для журналістів запевнив, що боротьба з обходом санкцій є ключовим пріоритетом, і він особисто веде діалог із третіми країнами, щоб запобігти використанню їхньої юрисдикції для продажу чутливих товарів до росії. Здавалося б, механізм працює.

Однак реальність виявляється набагато складнішою, ніж будь-які дипломатичні запевнення. Журналісти отримали доступ до даних платформи Import Genius, яка фіксує світові торговельні потоки. Цифри вражають: у період із січня 2024 року по березень 2025 року було здійснено 672 поставки санкційних компонентів, вироблених цими європейськими компаніями, до росії. Відправниками виступили 178 фірм, і левова частка з них зареєстрована в Китаї та Гонконгу. Це означає, що європейські технології подорожують складною логістичною стежкою: спочатку їх законно продають, скажімо, до Гонконгу, а звідти, через підставні компанії та «брокерів», вони вже нелегально потрапляють до російських оборонних заводів. Цей механізм став настільки відпрацьованим і масштабним, що його важко назвати інакше як індустрією обходу санкцій.

Однією з найбільш показових є історія швейцарської компанії u-blox, відомого виробника навігаційних систем і мікросхем. Її GNSS-приймачі, які дозволяють дрону орієнтуватися в просторі з високою точністю, були виявлені в збитому під Києвом безпілотнику. У відповідь на запит журналістів компанія надала кілька стандартних пояснень, які стали вже класичним набором виправдань у подібних випадках. Компоненти могли бути придбані ще до введення санкцій. Їх могли продати клієнти «брокерам» у країнах, які не приєдналися до санкцій. Їх могли ввезти контрабандою. Або ж їх демонтували з якогось іншого готового виробу, наприклад, зі старого автомобіля чи промислового обладнання, і вбудували в дрон. Кожне з цих пояснень

окремо звучить правдоподібно, але разом вони створюють картину безпорадності перед масштабами проблеми.

Інший гігант — нідерландська компанія Nexperia, один із провідних світових виробників напівпровідників. Її продукція фігурує майже у 300 поставках, зафіксованих у базі даних. Речник компанії Ганнес ван Ремдонк у листі до редакції висловив «розчарування» тим, що, попри всі зусилля, продукція опиняється там, де не повинна. Він апелював до фізичної неможливості контролю: чипи Nexperia надзвичайно малі, їх виробляють мільйонами, і вони використовуються в усьому — від пральних машин і холодильників до автомобілів. Технічно неможливо додати до кожного з них функцію відстеження або ідентифікації. Ланцюги постачання напівпровідників настільки складні й заплутані, що виробник фізично не може простежити, де опиниться кожен конкретний чіп. Він запевнив, що компанія співпрацює з владою та неурядовими організаціями, щоб допомогти зупинити такі випадки.

І саме в цьому полягає головна дилема санкційної політики. Алекс Прецанті, спеціаліст із санкцій та співзасновник проєкту State Capture Accountability Project, порівнює це з грою в «крота». Санкційні органи можуть скільки завгодно переслідувати корпоративні структури, але посередники щодня можуть відкривати десятки нових компаній, які існуватимуть лише на папері, достатньо довго, щоб провернути одну оборудку. Він зазначає, що вимога ЄС про включення «антиросійського застереження» в контракти має дуже обмежений ефект, оскільки його легко обійти через ланцюжок перепродажів. Єдиний радикальний спосіб — посилити тиск на Китай, але це, за словами Прецанті, було б рівнозначно оголошенню торговельної війни, на що Брюссель навряд чи піде. Тому гра в «кота і мишу» триває, і поки політики в Брюсселі обговорюють 20-й пакет санкцій, російські дрони продовжують падати на житлові квартали.

Трагедія, яка сталася в ніч на 11 лютого 2026 року в Харківській області, є кривавим підтвердженням цієї безпорадності. «Герань-2» влучила в житловий будинок, забравши життя чоловіка та трьох його малолітніх дітей. Його вагітна дружина дивом вижила, отримавши поранення. За даними ООН, лише у 2025 році від російських ударів далекобійною зброєю загинули 682 цивільні особи. За кожним із цих випадків стоять не лише російські військові злочинці, а й тіньові торговці, китайські посередники та, опосередковано, європейські корпорації, які, попри всі застереження, не змогли або не захотіли створити систему контролю, здатну запобігти використанню їхньої продукції як зброї.

Владислав Власюк, радник президента України з питань санкційної політики, тримаючи в руках уламок фюзеляжу збитого «Шахеда», говорить про те, що ланцюжки постачань стають дедалі складнішими. З'являються багаторівневі схеми, нові країни-посередники, а оплата дедалі частіше здійснюється через криптовалюти, що робить фінансове відстеження майже неможливим. Він наголошує: аргументи виробників про те, що

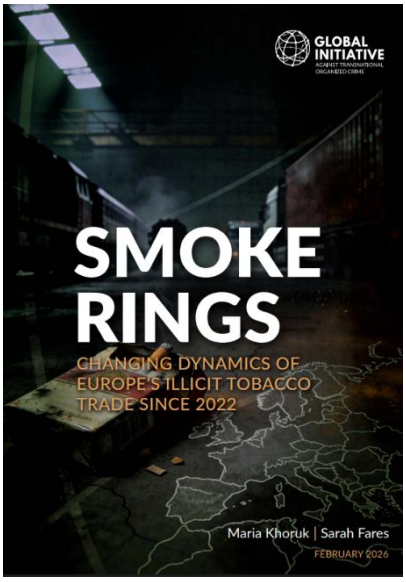
Висновки:

- **Нездатність санкцій:** Попри чотири роки посилення санкцій ЄС, російський ВПК продовжує у промислових масштабах отримувати європейські компоненти для виробництва дронів.
- **Китай як головний канал постачання:** Основним механізмом обходу санкцій є реекспорт через компанії-посередники в Китаї та Гонконгу.
- **Безпорадність виробників:** Європейські компанії визнають факт потрапляння їхньої продукції до російських дронів, але виправдовуються складністю глобальних ланцюгів постачання та неможливістю відстежити долю кожного мікрочипу.
- **Гуманітарна катастрофа як результат:** Відсутність дієвого контролю за технологіями має прямі людські наслідки. Понад мільйон українців залишаються без світла та тепла взимку, а цивільне населення гине під час щоденних атак дронами.

вони продають мільйони маленьких дешевих деталей і не можуть контролювати їхній кінцевий шлях, більше не працюють. Минуло майже чотири роки повномасштабної війни, і ця відповідь, за його словами, «більше не є прийнятною». Виробники та їхні великі дистриб'ютори повинні робити більше, шукати інноваційні способи відстеження, тиснути на своїх партнерів і вимагати прозорості.

А тим часом українці продовжують боротися, змушені виживати, розуміючи, що наступна атака — лише питання часу.

Як війна та санкції змінили нелегальний тютюновий ринок Європи [5]



У той час як офіційна статистика фіксує невпинне зниження рівня куріння в Європі, підживлюючи оптимізм громадських організацій та урядів, під поверхнею цих позитивних тенденцій формується тривожний контр-наратив. Споживання нелегального тютюну на континенті не просто зберігається, а демонструє стійке зростання, перетворюючись на складну, багатовимірну проблему, що сягає корінням у глибинні геополітичні зрушення, економічну нерівність та технологічну еволюцію кримінальних ринків.

Новаторське дослідження GI-TOC пропонує безпрецедентний за глибиною аналіз цього феномену. Ця індустрія, яка часто сприймається як другорядна порівняно з наркотрафіком чи торгівлею людьми, насправді є надзвичайно прибутковою, тісно переплетеною з легальною економікою та здатною фінансувати не лише організовану злочинність, а й цілі авторитарні режими.

Протягом десятиліть архітектура нелегального тютюнового ринку Європи виглядала відносно стабільною та прогнозованою. В її основі лежав простий, але потужний стимул – різниця в ціні, зумовлена непропорційним податковим навантаженням у різних юрисдикціях. Західноєвропейські країни з високими акцизами, такі як Велика Британія (де пачка цигарок коштує близько 17 євро), Франція (близько 10 євро) та Німеччина, виступали прибутковими ринками збуту. Натомість Східна Європа, зокрема Білорусь, Молдова та Україна, де ціна на ту ж саму пачку могла бути втричі-вп'ятеро нижчою (близько 3 євро в Україні), стали природними центрами виробництва та транзиту.

Ці пострадянські держави успадкували від СРСР потужну тютюнову промисловість з величезними фабриками, здатними виробляти мільярди цигарок на рік. В умовах слабкості державних інституцій, поширеної корупції та економічної депресії 1990-х, цей промисловий потенціал швидко знайшов своє застосування в тіньовій економіці. Контрабанда, від масштабних поставок у залізничних вагонах до дрібної діяльності через кордон, стала для багатьох чи не єдиним засобом до існування, що сформувало високий рівень суспільної толерантності до цього явища. Розширення ЄС на схід у 2000-х роках, яке ліквідувало внутрішні кордони за Шенгенською угодою, випадково створило ідеальні умови для контрабандистів, відкривши їм вільний шлях до багатих споживачів Заходу.

Особливе місце в цій системі посідала Білорусь, де нелегальна торгівля тютюном набула ознак системного, державного підприємства. Гродненська тютюнова фабрика "Неман", розташована всього за 20 кілометрів від польського кордону, є яскравим прикладом такого симбіозу. Її

[5] https://globalinitiative.net/wp-content/uploads/2026/02/Maria-Khoruk-and-Sarah-Fares-Smoke-Rings-Changing-dynamics-of-Europes-illicit-tobacco-trade-since-2022-GI-T.pdf

виробничі потужності були настільки надлишковими, що для "внутрішнього споживання" кожному білорусу довелося б викурювати по пів пачки цигарок щодня, що є статистично неможливим. Очевидно, що значна частина продукції – за деякими оцінками, близько третини, або 6,5 мільярда цигарок щороку – призначалася для нелегального експорту до ЄС та Великої Британії. Цей бізнес, тісно переплетений з оточенням Олександра Лукашенка, не був стихійним. Згідно з даними розслідувань та санкційними списками ЄС, він отримував організаційну та інфраструктурну підтримку на найвищому рівні. Приватні компанії, наближені до режиму, отримували вигідні концесії на будівництво логістичних центрів на ключових прикордонних переходах, а також діяли в особливих економічних зонах, як-от "Бреміно-Орша", що дозволяло їм оптимізувати логістику контрабандних потоків. Більше того, як зазначається в документі, та сама інфраструктура, що використовувалася для переправлення цигарок, під час штучно створеної міграційної кризи на кордонах ЄС у 2021 році слугувала для розміщення нелегальних мігрантів, яких потім переправляли через кордон. Це демонструє, як тіньова економіка стає інструментом гібридної війни.

Однак починаючи з 2020 року цей злагоджений механізм почав давати збої. Пандемія COVID-19 першою оголила вразливість довгих ланцюгів поставок. Але справжнім тектонічним зрушенням стало повномасштабне вторгнення росії в Україну у 2022 році. Ця подія стала каталізатором, який не просто ускладнив, а докорінно зламав стару парадигму. Запроваджені Євросоюзом, США, Великою Британією та іншими країнами безпрецедентні санкції проти Білорусі та росії були націлені, зокрема, й на тютюнову індустрію. Під обмеження потрапили не лише "Неман", а й інші виробники та ключові бізнесмени.

Закриття переважної більшості офіційних прикордонних переходів між Білоруссю та ЄС (з 18 залишилося відкритими лише 4) у поєднанні з посиленим контролем залізничних вантажів створило "залізну завісу" на східному кордоні. Хоча санкції не змогли повністю перекрити кисень контрабанді (про що свідчать рекордні вилучення в Литві у 2022 році та 12-кратне зростання вартості вилучених білоруських цигарок у Польщі у 2023-му), вони змусили злочинні угруповання до радикальної інновації. Старі методи, як-от масштабне переправлення товару в потягах з добривами чи лісоматеріалами, стали надто ризикованими.

Відповіддю став перехід до тактики "малих форм". Звіт GI-TOC детально описує новітні методи, які дедалі частіше фіксуються прикордонниками. Це метеорологічні аеростати, оснащені GPS-трекерами, які здатні переносити до 2 тисяч пачок цигарок на відстань до 700 кілометрів. Це саморобні дрони, що перелітають кордон. Це навіть замасковані плоти, які сплавляються річками з Білорусі до Латвії, та підземні тунелі. Такі операції вимагають участі добре скоординованих груп по обидва боки кордону. Хоча обсяги однієї такої поставки незрівнянно менші, ніж вантажівка чи потяг, висока частота та складність виявлення роблять цю стратегію життєздатною, особливо в умовах, коли традиційні маршрути заблоковані. Водночас для великих партій злочинці почали використовувати складні, кружні маршрути, відправляючи контейнери з білоруськими цигарками через порти Південно-Східної Азії або ОАЕ, маскуючи їх походження та користуючись меншою увагою до азійського напрямку порівняно з латиноамериканським, який асоціюється з кокаїном.

Найсуттєвішим і, ймовірно, довгостроковим наслідком цих змін стало безпрецедентне зростання так званого "партизанського виробництва" (guerrilla production) безпосередньо в країнах Європейського Союзу. Це явище є класичним прикладом у кримінальній економіці: перенесення виробництва якомога ближче до кінцевого споживача з метою мінімізації ризиків перетину кордонів та скорочення логістичних витрат. До 2023 року, за даними Європейського бюро з питань боротьби з шахрайством (OLAF), до 60% такого товару вироблялося вже всередині ЄС.

Це вже не кустарне виробництво минулого. Сьогодні це високотехнологічні підпільні фабрики, які правоохоронці дедалі частіше виявляють у Бельгії, Нідерландах, Іспанії, Німеччині та Польщі. Вони оснащені професійним промисловим обладнанням, часто придбаним на онлайн-майданчиках типу Alibaba або отриманим із закритих законних тютюнових фабрик у Східній Європі та на Балканах. У лютому 2025 року бельгійська поліція викрила фабрику в Ломмелі, де одночасно працювали чотири виробничі лінії, працювало близько 50 робітників, а збитки для бюджету оцінили у понад 14 мільйонів євро. Саме такі об'єкти, здатні випускати понад мільйон цигарок на день, і формують сьогоднішню пропозицію. Їхня "партизанська" суть полягає в мобільності та швидкій адаптації: вони не працюють довго на одному місці, орендуючи склади чи фермерські будівлі на короткий термін, і можуть згорнутися та переїхати за лічені дні після сигналу про небезпеку.

Організація такого виробництва є водночас високопрофесійною та глибоко експлуататорською, що створює складну соціальну дилему. Ключову роль у ньому відіграє мобільність робочої сили з традиційних тютюнових регіонів. На фабриках, які ліквідовує поліція, найчастіше працюють громадяни України, Молдови, Румунії, Болгарії. Це люди, які часто мають досвід роботи на легальних тютюнових підприємствах у своїх країнах і володіють необхідними технічними навичками для обслуговування складних машин. З одного боку, вони приваблені надзвичайно високою зарплатою, яка може сягати від 2 до 10 тисяч євро на місяць. З іншого боку, умови їхньої праці нагадують рабські. Звіт детально описує систему тотального контролю: 12-годинний робочий день, проживання прямо на території фабрики в приміщеннях із зачиненими вікнами, вилучення паспортів і мобільних телефонів, заборона на вихід назовні. У закритих приміщеннях люди можуть проводити тижнями, не бачачи сонячного світла. В одній з викритих іспанських фабрик у житлових кімнатах знайшли таблетки вітаміну D, які видавали робітникам, щоб компенсувати цю депривацію. Попри ці ознаки, правоохоронці часто розглядають цих людей не як жертв торгівлі людьми, а як свідомих співучасників, оскільки вони добровільно погодилися на таку роботу та отримують високу винагороду. Ця "сіра зона" між експлуатацією та добровільною згодою, між жертвою та злочинцем, є однією з найскладніших етичних і правових проблем, яку порушує дослідження.

Паралельно зі зміною географії виробництва та методів транспортування відбувається не менш важлива цифрова трансформація каналів збуту. Традиційна вулична торгівля, яка в багатьох мегаполісах Європи десятиліттями контролювалася етнічними угрупованнями (зокрема, в'єтнамськими в Берліні чи афганськими та пакистанськими в Парижі), дедалі більше доповнюється, а подекуди й витісняється онлайн-продажами. Цифрові платформи стали ідеальним середовищем для цього бізнесу через відносно м'яке покарання порівняно з наркотиками. Нелегальний тютюн вільно продається на маркетплейсах, у соціальних мережах, але найбільшого поширення набули закриті чи відкриті канали в зашифрованих месенджерах, перш за все в Telegram. Там створено цілі спільноти з тисячами підписників, де публікуються прайс-листи, фотографії продукції та умови доставки.

Важливою інновацією, яка кардинально ускладнює роботу правоохоронців, став перехід до "безконтактної" торгівлі з використанням служб поштової доставки дрібних вантажів. Стратегія "мало, але часто" дозволяє обходити вибірковий митний контроль, який фізично не в змозі перевірити колосальний потік дрібних посилок, особливо з країн, де поріг безмитного ввезення є високим. Це відкриває шлях на ринок не лише для організованих груп, а й для дрібних, опортуністичних продавців. Окрему тривогу викликає зростання популярності нелегальних електронних сигарет та вейпів, які в деяких країнах (як-от Німеччина) можуть становити до 80% ринку. Вони часто містять небезпечні домішки, включно з синтетичними канабіноїдами, і, завдяки агресивному онлайн-маркетингу, легко досягають молодіжної аудиторії, створюючи нові ризики для громадського здоров'я.

Таким чином, європейський нелегальний тютюновий ринок вступив у фазу зрілої, поліцентричної складності. Він більше не є простою лінійною системою "Схід виробляє – Захід споживає". Стара модель співіснує з новою, створюючи гібридну реальність. Традиційні гравці, як-от Білорусь, не зникли, але вони змушені адаптуватися, переорієнтовуючись на сусідні ринки (Польщу, країни Балтії) та використовуючи дрібніші, більш ризиковані методи доставки. Водночас нові виробничі хаби в самому ЄС, що спираються на технічну кваліфікацію та експлуатовану працю мігрантів зі Сходу, стали основними постачальниками для найприбутковіших ринків Західної Європи. Ця нова екосистема підтримується "сірими" посередниками: власниками складів, логістичними компаніями, постачальниками сировини, онлайн-платформами. Усі вони, часто не усвідомлюючи цього або свідомо заплющуючи очі, стають частиною злочинної економіки, яка не лише позбавляє державні бюджети мільярдів євро податкових надходжень (лише Франція втрачає близько 7,3 мільярда євро щороку), але й фінансує авторитарні режими, підживлює організовану злочинність і будується на прихованих формах примусу та експлуатації людей.

Висновки:

- **Війна в Україні та санкції проти Білорусі зруйнували традиційну модель** домінування східноєвропейських постачальників. Це спричинило стрімке зростання підпільного виробництва в самому ЄС.
- **Успіх нової моделі тримається на мобільності дешевої робочої сили** зі Східної Європи. Працівники підпільних фабрик часто перебувають в умовах, близьких до рабських.
- **Ринок збуту радикально змінився** завдяки переходу від вуличної торгівлі до онлайн-платформ, зокрема Telegram. Метод дрібних поштових відправлень дозволяє контрабандистам ефективно обходити митний контроль.
- **Білорусь є яскравим прикладом використання тютюнової контрабанди як інструменту державної політики.** Інфраструктура, створена для виробництва та переправлення цигарок, була інтегрована в гібридні операції режиму, що демонструє прямий зв'язок між тіньовою економікою та загрозами національній безпеці.

Дослідження GI-TOC завершується чітким меседжем: перед обличчям цієї нової, фрагментованої та технологічно оснащеної реальності, відповідь держави не може бути лінійною. Вона вимагає комплексного підходу, який поєднує посилення контролю за постачанням обладнання та сировини, притягнення до відповідальності цифрових платформ, гармонізацію податкової політики в ЄС, глибоке розуміння соціально-економічних причин залучення людей у цей бізнес та, найголовніше, усвідомлення того, що за кожним тіньовим центром стоять не лише втрачені податки, але й складні, часто фундаментальні виклики для європейської безпеки.

Тіньова війна: Чому зростання санкцій США не гарантує поразки наркокартелів [6]

Війна з наркотрафіком, яку Сполучені Штати ведуть уже півстоліття, вступила в нову фазу. На зміну гучним спецопераціям із захоплення лідерів картелів прийшла тиха, але не менш масштабна фінансова битва. Останніми роками, особливо з початком другого президентського терміну Дональда Трампа, Вашингтон взяв курс на тотальне санкційне ураження наркокартелів Латинської Америки.

Аналіз діяльності Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) свідчить про безпрецедентне розширення санкційних списків: 2025 рік став рекордним

[6] https://insightcrime.org/news/us-sanctions-latin-america-have-increased-but-can-they-enforced/

за кількістю нових призначень, спрямованих проти організованої злочинності в регіоні, навіть на тлі загального скорочення глобальних санкцій. Однак за цими вражаючими цифрами криється глибока системна проблема, яка ставить під сумнів ефективність усієї стратегії: спроможність примусового виконання санкцій катастрофічно відстає від політичних амбіцій, перетворюючи санкції на потужний інструмент символічної політики, але доволі слабку зброю реального впливу на транснаціональні злочинні синдикати.

Еволюція американського підходу до боротьби з наркотрафіком є показовою історією адаптації до мінливої природи злочинності. Упродовж десятиліть стратегія Вашингтона базувалася на простій логіці: захопиш лідера — знешкодиш організацію. Тисячі доларів витрачалися на розвідку, стеження та операції із затримання таких постатей, як Пабло Ескобар або Хавієр "Ель Чапо" Гусман. Результат виявився парадоксальним: замість колапсу, злочинні імперії демонстрували дивовижну живучість, фрагментуючись на менші, агресивніші угруповання, які ставали ще важчими для контролю, а потоки наркотиків не лише не скорочувалися, а й зростали. Цей гіркий досвід змусив американських стратегів, зокрема в Управлінні з боротьби з наркотиками, переосмислити саму природу картелів. Їх почали розглядати не як ієрархічні структури з чіткою вертикаллю влади, а як адаптивні фінансово-логістичні мережі, гнучкі та стійкі до втрати навіть ключових лідерів. Завдання змінилося: тепер потрібно було не просто "обезголовити" дракона, а перекрити кисень його фінансовій системі, порушити зв'язки, які дозволяють йому функціонувати.

Ключовим ідеологічним поворотом, який уможливив масштабування санкційного тиску, стало зближення понять наркотрафіку та тероризму в риториці та політичних інструментах американської адміністрації. Прирівнявши діяльність наркокартелів до терористичних загроз, Білий дім відкрив собі доступ до набагато ширшого арсеналу засобів, передбачених законодавством про боротьбу з тероризмом. Це дозволило Міністерству фінансів активніше застосовувати механізм призначення "спеціально визначених глобальних терористів" не лише до безпосередніх торговців наркотиками, але й до цілої периферійної інфраструктури: відмивачів грошей, постачальників хімічних прекурсорів, власників підставних компаній та корумпованих чиновників. Паралельно OFAC значно активізувало використання позначки "транснаціональна злочинна організація", яка у 2025 році з'являлася у санкційних списках набагато частіше, ніж у попередні роки. Це розширення правових підстав для санкцій зробило мішенню не лише лідерів, а й будь-кого, хто так чи інакше дотичний до злочинної діяльності.

Географія санкційних ударів у 2025 році вражає своєю широтою та демонструє глобальний характер наркотрафіку. Беззаперечним лідером за кількістю нових об'єктів санкцій залишаються мексиканські картелі, які традиційно вважаються головною загрозою для США. OFAC провело справжню "зачистку" серед фірм, пов'язаних із картелем "Сіналоа". Під удар потрапили не лише очевидні підозрювані, але й цілі сектори легальної економіки, які використовувалися для відмивання нарко-доларів: компанії у сфері туризму, спа-салони, агентства нерухомості. Особливу увагу було приділено мережам, що контролюються "Чапітос" — синами легендарного Ель Чапо, які, за даними американської розвідки, вибудували складну систему легалізації доходів через, здавалося б, цілком респектабельний бізнес. Одночасно санкції посипалися на постачальників пального та автозаправні станції, афілійовані з картелем "Халіско " та картелем "Санта-Роса-де-Ліма", що вказує на прагнення перекрити не лише фінансові, а й матеріально-технічні потоки, необхідні для функціонування злочинних армій.

Венесуела стала другим за масштабом епіцентром активності, де кількість нових санкційних дій у 2025 році зросла майже втричі. Тут інтереси боротьби з наркотрафіком тісно переплелися з геополітичним тиском на режим Ніколаса Мадуро. Призначення військового угруповання "Картель Сонця" глобальною терористичною організацією стало безпрецедентним кроком, який фактично прирівняв частину венесуельського державного апарату до нарко-терористичних структур. Водночас OFAC активізувало переслідування судноплавних компаній та окремих суден, що працюють у венесуельському нафтовому секторі. Їх звинувачують у транспортуванні венесуельської нафти з використанням оманливих методів судноплавства, що дозволяє уникати нафтових санкцій та, згідно з американською риторикою, фінансує "корумпований нарко-терористичний режим". Цей підхід демонструє, як санкції проти наркотрафіку стають універсальним інструментом для досягнення ширших зовнішньополітичних цілей.

Ще одним важливим напрямком санкційного удару стали країни Центральної та Південної Америки, які раніше перебували на периферії уваги OFAC. Коста-Рика, Гаяна та Суринам опинилися під прицілом через свою ключову роль у транзиті кокаїну. Санкції проти портових чиновників, судноплавних фірм та операторів літаків, яких звинувачують у сприянні переправленню кокаїну через Карибський басейн до Європи та США, сигналізують про визнання Вашингтоном того факту, що боротьба з наркотрафіком неможлива без тиску на транзитні держави. Це також є визнанням поразки попередніх стратегій, зосереджених виключно на країнах походження наркотиків. Злочинні мережі просто перенаправили потоки, знайшовши вразливі місця в нових регіонах, і тепер OFAC намагається закрити ці нові "ворота".

Теоретично, перехід до мережевих санкцій мав би посилити позиції OFAC, надавши йому більше важелів впливу. Адже багато підставних компаній зареєстровані в Сполучених Штатах або володіють там активами. Навіть якщо вони не мають безпосередніх зв'язків з американською юрисдикцією, їхня залежність від проведення доларових транзакцій через американські банки робить їх вразливими до дій Міністерства фінансів. Однак на практиці цей потенціал залишається значною мірою нереалізованим.

Статистика свідчить, що правозастосування в основному обмежується блокуванням активів та заборонами на транзакції, які важко відстежити та оцінити. Повідомлення про реальні арешти майна чи суттєві збої в роботі злочинних мереж, які можна було б безпосередньо пов'язати з санкціями, є поодинокими. Суми стягнених цивільних штрафів, хоча й вимірюються сотнями мільйонів доларів, виглядають мізерними на тлі масштабів нарко-індустрії.

Ще більш промовистим є падіння глобальних вилучень коштів за відмивання грошей та порушення санкцій. Падіння з понад 3 мільярдів до 940 мільйонів доларів за рік є тривожним сигналом, який важко пояснити виключно зміною економічної кон'юнктури. Особливо показовим є той факт, що навіть успішне вилучення 12,7 мільйона доларів, пов'язаних із картелем "Сіналоа", стало результатом традиційних арештів та рейдів, проведених правоохоронними органами, а не фінансового блокування, передбаченого санкційним механізмом. Це підкреслює фундаментальну проблему: санкції часто існують у паралельній реальності, поза межами реальних оперативних дій на місцях. Вони створюють правові підстави для дій, але не забезпечують ресурсів для їхнього виконання.

Корінь проблеми криється в інституційній спроможності самого OFAC. Як зазначив колишній чиновник міністерства фінансів Тоні Боррайо, управління хронічно недоукомплектоване кадрами. Його бюджет та штатна чисельність зростають мізерними темпами на тлі лавиноподібного збільшення санкційних завдань. Цей розрив між ресурсами та розширеним мандатом створює ситуацію, коли додавання нових імен до санкційних списків стає значно простішим завданням, ніж реальне відстеження їхніх активів та притягнення до відповідальності. Новий, мережевий підхід лише поглиблює цю проблему, оскільки вимагає

значно глибших і тривaліших розслідувань, аналізу складних фінансових схем та міжнародної координації.

У цих умовах відбувається фактичне перекладання функцій правозастосування на приватний сектор. Американська фінансова спільнота, насамперед банки, стають головними виконавцями санкційної політики. Вони зобов'язані блокувати рахунки та транзакції осіб, що потрапили до санкційних списків, і нести відповідальність за будь-які порушення. Як слушно зауважив Боррайо, цей механізм створює потужний стримувальний ефект, оскільки жодна фінансова установа не ризикне власною ліцензією та репутацією заради сумнівної вигоди від співпраці з картелями. Загроза вторинних санкцій є дієвим інструментом дисципліни фінансового сектору.

Однак ця модель має свої вразливі місця. Для банків заморожування рахунків та повідомлення про підозрілі транзакції є витратною діяльністю, яка не приносить жодного прибутку. Це створює внутрішню напругу між прагненням до ефективності та необхідністю дотримуватися регуляторних вимог, що іноді призводить до прогалин у комплаєнсі. Справа TD Bank, який у 2024 році сплатив понад 3 мільярди доларів штрафу за пропускання "брудних" нарко-грошей через свою систему, є яскравим прикладом того, як навіть найбільші фінансові інституції можуть не впоратися з цим навантаженням. Це свідчить про те, що покладання виключно на приватний сектор у виконанні державної функції боротьби з фінансуванням злочинності має об'єктивні межі.

Адаптивність самих злочинних мереж є ще одним викликом, який часто нівелює зусилля OFAC. Картелі за своєю природою є організаціями, створеними для уникнення уваги правоохоронних органів та санкцій. Вони діють за принципом: щойно OFAC ідентифікує та блокує одну фірму, на її місці з'являються дві нові, часто зареєстровані на підставних осіб в інших юрисдикціях. Історія компанії Sumilab у мексиканському Куліакані, яка постачала хімічні прекурсори для виробництва фентанілу та метамфетаміну для картелю "Сіналоа", є хрестоматійним прикладом цього феномену. Після того, як OFAC наклав санкції на Sumilab у 2023 році за звинуваченнями у постачанні прекурсорів, власники компанії не зупинили діяльність, а провели блискавичну реорганізацію. Вони просто прибрали вивіску Sumilab і створили сім нових компаній, які продовжили ту саму діяльність під новими назвами. Знадобилося два роки та розширення повноважень із залученням механізмів боротьби з тероризмом, щоб OFAC змогло повторно накласти санкції на цю мережу, додавши до списку 12 компаній, пов'язаних із тією ж родиною. При цьому публічної інформації про заблоковані активи, перехоплені вантажі чи порушені ланцюги постачання досі немає.

Додатковим ускладнюючим фактором стає стрімке зростання використання криптовалют злочинними угрупованнями. Перехід на децентралізовані цифрові активи дозволяє картелям ефективно обходити головний інструмент впливу OFAC — блокування активів, яке працює лише тоді, коли злочинці контактують з американською банківською системою через доларові транзакції або рахунки в США. Криптовалютні біржі часто є децентралізованими, а регуляторна база в Сполучених Штатах для цього сектору залишається слабкою та фрагментованою. Як зазначив дослідник Кайл Раттер, це робить криптовалюти логічним вибором для картелів, які прагнуть уникнути фінансового моніторингу. Використання криптовалют ускладнює відстеження фінансових потоків, робить транзакції практично анонімними та дозволяє злочинцям виводити кошти з-під юрисдикції США, фактично нівелюючи санкційний тиск.

Таким чином, перед нами постає картина санкційного парадоксу. З одного боку, Сполучені Штати демонструють безпрецедентну політичну волю, розширюючи визначення тероризму, застосовуючи нові правові інструменти та вражаючи дедалі ширше коло об'єктів. Кількість санкцій зростає в геометричній прогресії, створюючи ілюзію рішучої боротьби.

З іншого боку, реальна спроможність перетворити ці паперові рішення на фактичне блокування активів, порушення логістики та зменшення наркопотоків залишається вкрай обмеженою.

Інституційна неспроможність OFAC, його хронічне недофінансування та нестача кадрів у поєднанні з адаптивністю злочинних мереж та появою нових фінансових технологій створюють розрив, який робить санкції радше потужним інструментом політичної риторики, ніж ефективною зброєю у реальній війні з наркотрафіком.

Допоки цей дисбаланс не буде виправлено шляхом суттєвого збільшення ресурсів OFAC, посилення міжнародної координації арешту активів, запровадження жорсткішого регулювання криптовалютного сектору та розробки механізмів швидшого реагування на реорганізацію злочинних мереж, санкції ризикують залишитися грою. Вашингтон продовжуватиме витрачати величезні ресурси на розширення "чорних списків", а картелі — з легкістю знаходити нові лазівки, мігруючи в непідконтрольні юрисдикції та використовуючи технологічні інновації. Гра триватиме, і в цій грі, попри всю міць американської економіки, злочинні мережі поки що демонструють вищу адаптивність та гнучкість, ставлячи під сумнів саму можливість перемоги виключно фінансовими методами.

Висновки:

- **Стратегічний розрив між призначеннями та правозастосуванням:** попри безпрецедентне зростання кількості санкцій, реальне виконання цих санкцій залишається вкрай обмеженим через хронічне недофінансування та кадровий дефіцит OFAC, що перетворює санкції на потужний інструмент політичної риторики, але слабку зброю реального впливу.
- **Адаптивність злочинних мереж перевершує спроможність регуляторів:** картелі демонструють вражаючу здатність до миттєвої реорганізації, створюючи нові фірми замість заблокованих та використовуючи криптовалюти для уникнення доларових транзакцій.
- **Приватизація правозастосування має об'єктивні межі:** перекладання функцій виконання санкцій на приватний банківський сектор створює небезпечну залежність від корпоративних стимулів.
- **Геополітичне розширення санкцій розмиває їхню ефективність:** використання антитерористичних механізмів для боротьби з наркотрафіком свідчить про перетворення санкцій на універсальний інструмент зовнішньої політики, що ускладнює їхнє цілеспрямоване виконання.

Смерть «Ель Менчо»: Кінець епохи та крипто-спадщина найнебезпечнішого картелю Мексики [7]

У неділю, 22 лютого 2026 року, коли сонце піднімалося над гірськими хребтами мексиканського штату Халіско, ніхто не міг передбачити, що цей день стане переломним у багаторічній війні з наркотрафіком.

У невеликому містечку Тапальпа, загубленому серед соснових лісів, спецпризначенці Збройних сил Мексики, діючи на основі розвідувальних даних, наданих американськими колегами, провели блискавичну операцію, в результаті якої було ліквідовано Немесіо Осегеру Сервантеса,

[7] https://www.bbc.com/news/articles/cy4wywnrdd8o

відомого у всьому світі під грізним прізвиськом "Ель Менчо". Так завершилася ера найбільшого наркобарона сучасності, лідера картелю "Халіско" (CJNG), організації, якій вдалося поєднати середньовічну жорстокість із передовими технологіями XXI століття, створивши гібридну кримінальну імперію, аналогів якій світ ще не бачив.

Ель Менчо, колишній поліцейський, який пройшов шлях від дрібного злочинця до головного ворога американської нації номер один з винагородою у 15 мільйонів доларів за свою голову, побудував імперію не лише на брутальному насильстві та залякуванні населення, але й на холодному, математичному розрахунку, стратегічному мисленні та глибокому розумінні глобальних економічних трендів. І головним інструментом цього розрахунку, тією цеглиною, яка дозволила звести фінансову фортецю, непідвладну традиційним методам боротьби, стали криптовалюти. Він зрозумів те, що довго не хотіли визнавати уряди: майбутнє належить не лише технологіям, але й тим, хто першим зможе поставити їх на службу своїм інтересам.

Картель "Халіско " мовчки і методично будував альтернативну фінансову систему, яка кидала виклик самій основі світового порядку. Як відзначають аналітики провідної компанії з блокчейн-розслідувань TRM Labs та підтверджують матеріали слідчих органів США, CJNG став не просто одним із користувачів криптовалют, а першою мексиканською кримінальною структурою, яка зробила масштабну, системну ставку на цифрові активи як на основний інструмент фінансової логістики та відмивання коштів. І ця ставка спрацювала блискуче. Задовго до подій лютого 2026 року документально підтверджені транзакції картелю через різноманітні криптосервіси обчислювалися вже не десятками, а сотнями мільйонів доларів, створюючи потужний фінансовий потік.

Чому саме криптовалюти стали наріжним каменем фінансової імперії Ель Менчо? Відповідь на це питання криється в архітектурі сучасного глобального наркобізнесу, який давно перестав бути просто вуличною злочинністю і перетворився на багатомільярдну транснаціональну індустрію. Традиційний відмив грошей через банківську систему, з її численними регуляторними вимогами, комплаєнс-процедурами та міжнародними механізмами фінансового контролю, залишає після себе незнищенні сліди, вимагає залучення корумпованих банкірів-посередників, кожен з яких є потенційною точкою витоку інформації, і наражає капітали на постійний ризик блокування, арешту та санкцій.

Криптовалюта ж, з її фундаментальними властивостями псевдонімності, децентралізації та блискавичної швидкості транзакцій, стала для CJNG ідеальним мостом між двома паралельними світами — фізичним світом насильства та віртуальним світом капіталу. Вони одними з перших серед злочинних угруповань усвідомили весь потенціал стейблкоїнів — криптовалют, прив'язаних до курсу долара США, — для миттєвих транскордонних переказів, які дозволяли уникати будь-якого банківського нагляду, валютного контролю та підозрілих поглядів фінансової розвідки. Біткоїн, з його обмеженою емісією та глобальним визнанням, слугував універсальним засобом для розрахунків з постачальниками хімічних прекурсорів з Китаю та інших азійських країн, а також для оплати послуг численних посередників у складних логістичних ланцюжках.

Схеми, які використовували фінансисти картелю, вражали своєю витонченістю та багатошаровістю, нагадуючи складні математичні алгоритми. Готівка, отримана від дрібнооптової та роздрібної торгівлі наркотиками на американських вулицях, накопичувалася, а потім фізично, вантажівками або спеціально обладнаними автомобілями, переправлялася через майже неконтрольовану південну ділянку кордону назад до Мексики.

Там, на безпечних територіях, підконтрольних картелю, вона потрапляла до рук спеціальних брокерів — фінансових посередників, які перетворювали ці гори готівки на "чисті" цифрові активи. Це відбувалося через розгалужену мережу невеликих обмінників, підпільних пунктів та позабіржових (OTC) платформ, де великі суми конвертувалися в криптовалюту без зайвих

запитань. Далі ці цифрові активи вирушали в небезпечну подорож через заплутаний лабіринт електронних гаманців, часто використовуючи децентралізовані крос-чейн біржі та міксери, щоб назавжди замести сліди, розірвавши прямий зв'язок між джерелом коштів та їх кінцевим отримувачем.

У 2023 році правоохоронці США провели резонансне затримання одного з таких брокерів. Під час обшуку в його автомобілі, окрім витонченої електронної техніки, знайшли понад 600 тисяч доларів готівкою, захованих у спеціально обладнаних схованках. Але це була лише крихітна, видима частина величезного айсберга — складної фінансової екосистеми, що поєднувала китайські банки, через які фінансувалися закупівлі прекурсорів, американських дрібних дилерів на вулицях та мексиканських фінансових посередників у єдиний нерозривний ланцюг, який щодня приносив мільйони доларів прибутку.

У звітах американської влади, починаючи з 2022 року, дедалі частіше почали фігурувати дані про підозрілі транзакції, пов'язані з CJNG, на десятки мільйонів доларів, які проходили через найбільші та найвідоміші криптобіржі світу. Слідчі з ФБР та Управління з боротьби з наркотиками (DEA) з тривогою наголошували: картель не просто експериментував з технологією, а глибоко та системно інтегрував її у свою повсякденну фінансову інфраструктуру. Вони використовували як централізовані майданчики, де ще можна було знайти вразливі місця, прогалини в KYC-процедурах або просто корумпованих співробітників, так і впевнено переходили до використання децентралізованих протоколів та анонімних гаманців, коли операція вимагала максимальної конфіденційності. Вони диверсифікували свої ризики і створили таку фінансову мережу, яку було надзвичайно важко зруйнувати одним ударом.

Саме ця унікальна технологічна адаптивність, це вміння швидко вчитися та впроваджувати інновації, дозволила Ель Менчо залишатися невловимим для влади протягом багатьох років, перетворивши його на легенду ще за життя. Його картель випередив своїх головних конкурентів із могутнього картелю Сіналоа не лише у військовій могутності, кількості бойовиків та арсеналі озброєння, але й у фінансовій інженерії, у здатності приховувати та примножувати капітал. Криптовалюти дозволили CJNG скоротити час міжнародних розрахунків з днів, а то й тижнів, до кількох хвилин, зменшити фатальну залежність від вразливих кур'єрів, яких завжди можна було перехопити на кордоні, та диверсифікувати фінансові ризики, виводячи значну частину капіталу з-під прямої юрисдикції будь-якої окремо взятої країни.

Але смерть архітектора цієї крипто-імперії не могла пройти безслідно, не викликавши нищівної реакції. Ліквідація Ель Менчо виявилася не просто спецопераційою місцевого значення, а потужним детонатором, який миттєво підірвав відносний мир і спокій у восьми мексиканських штатах. Картель, раптово втративши свого беззаперечного лідера, не розпався і не зник у підпіллі — він вибухнув неконтрольованою, сліпою агресією, спрямованою на те, щоб помститися і залякати. Замість того, щоб тихо скласти зброю або зачаїтися, бойовики CJNG влаштували справжній терор, масові заворушення та акції відплати.

Вулиці Гвадалахари, другого за величиною міста країни та перлини Халіско, яке готувалося приймати матчі майбутнього чемпіонату світу з футболу, за лічені години перетворилися на справжнє поле бою. Чорні стовпи густого диму здіймалися над сучасними хмарочосами та історичним центром — це палали десятки автомобілів, автобуси, бензоколонки, навіть складські приміщення. Нападники діяли злагоджено, групами, блокуючи цілі райони та відкриваючи вогонь по всьому, що рухалося.

У популярному курортному місті Пуерто-Вальярта, на тихоокеанському узбережжі, тисячі іноземних туристів, які приїхали насолоджуватися сонцем та пляжами, раптово опинилися в пастці. Вони були змушені ховатися в готельних номерах та лобі під завивання сирен, звуки пострілів та істеричні крики на вулицях. Міжнародні авіакомпанії терміново, одна за одною, почали скасовувати всі рейси до Пуерто-Вальярти та Гвадалахари, фактично відрізавши цілі

регіони від зовнішнього світу та кинувши тисячі людей напризволяще. Мексиканська влада, намагаючись хоч якось контролювати ситуацію, офіційно підтвердила загибель щонайменше 25 військовослужбовців Національної гвардії, які першими прийняли на себе удар розлючених нарко-мафіозі. Реальна кількість жертв серед цивільного населення залишалася невідомою і зростала з кожною годиною, обростаючи моторошними чутками.

Для офіційних Мехіко та Вашингтона смерть Ель Менчо — це, безсумнівно, історична, епохальна подія, довгоочікувана перемога, яка варта того, щоб її карбували в підручниках історії. Колишній посол США в Мексиці та впливовий дипломат Крістофер Ландау не скупився на епітети, назвавши ліквідацію наркобарона "величезним досягненням" для всього регіону, від Панами до Канади. Колишній глава міжнародних операцій DEA Майк Віджіл, людина, яка все життя полювала на таких, як Ель Менчо, взагалі охарактеризував цю спецоперацію як "одну з найбільш значущих та результативних в усій історії боротьби з наркотрафіком у Західній півкулі".

Проте, ця гучна перемога може обернутися справжньою пірровою перемогою, якщо подивитися на неї під іншим кутом. Те неймовірне, масштабне та жорстоке насильство, яке спалахнуло по всій країні всього за кілька годин після ліквідації Ель Менчо, є яскравим і незаперечним доказом того, що картель "Халіско" аж ніяк не знищений, не розгромлений і навіть не деморалізований. Він лише втратив свого головного керманича, свого стратега та лідера, але його структура, його бойові загони, його фінансові потоки — все це продовжують існувати та діяти.

Боротьба за владу, за контроль над цими потоками та територіями всередині розколотого CJNG тільки починається, і вона, за оцінками експертів, загрожує вилитися у нову, ще більш криваву хвилю внутрішніх розборок, які можуть перевершити за жорстокістю та цинізмом усе, що було раніше, навіть похмурі часи протистояння з Сіналоа.

Висновки:

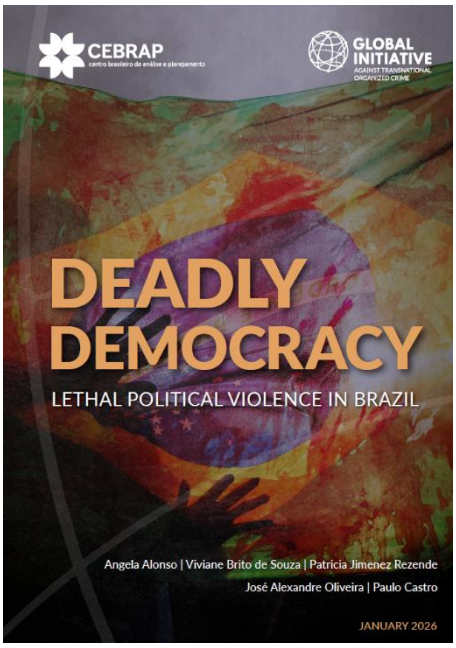
- **Технологічна еволюція наркобізнесу:** Картель CJNG під керівництвом Ель Менчо став першим прикладом масштабної інтеграції криптовалют у фінансову інфраструктуру транснаціональної злочинної організації.
- **Криптовалюти як інструмент глобалізації злочинності:** Цифрові активи дозволили картелю ефективно розраховуватися з міжнародними постачальниками прекурсорів та диверсифікувати ризики, виводячи капітал з-під юрисдикції національних урядів.
- **Тактична перемога зі стратегічними наслідками:** Ліквідація лідера є беззаперечним успіхом для Мексики та США, однак спровокована нею хвиля насильства доводить, що картель як структура не знищений.
- **Зміна природи загроз:** Поєднання традиційного насильства з високими технологіями створює прецедент для інших кримінальних угруповань світу, які тепер мають готову модель для наслідування.

Але найглибший, найважливіший урок смерті Ель Менчо полягає зовсім не в насильстві на вулицях мексиканських міст, яке рано чи пізно вдасться придушити. Він полягає в тій тривожній тіні, яку картель залишив у цифровому просторі, у тій небезпечній спадщині, яка продовжуватиме жити та розвиватися незалежно від того, хто стане наступним лідером угруповання. Картель став не просто злочинним угрупованням, а прототипом, моделлю злочинної організації майбутнього, де злочинці сидять не в печерах з мішками золота, а за моніторами, керуючи багатомільярдними потоками цифрових активів.

Мексика виграла важливу битву, усунувши ворога номер один, але сама війна з нарко-картелями, яка давно перестала бути локальною проблемою однієї країни, вступила в нову, набагато складнішу, технологічнішу та небезпечнішу фазу. І світове співтовариство, всі його

правоохоронні органи та фінансові регулятори, мають усвідомлювати справжні масштаби цієї нової загрози, з якою нам усім доведеться жити і боротися в найближчі десятиліття.

Від конкуренції до ліквідації: еволюція політичних конфліктів у Бразилії [8]



Аналітичний звіт, підготовлений Global Initiative Against Transnational Organized Crime спільно з Centro Brasileiro de Análise e Planejamento, присвячений комплексному дослідженню феномену летального політичного насильства в Бразилії у період 2003–2023 років. Документ виходить із того, що політичні вбивства, замахи та систематичні погрози не є випадковими проявами кримінальної активності, а становлять стійку форму позаінституційного врегулювання політичних конфліктів, яка функціонує паралельно до формальних демократичних процедур. Автори розглядають це явище як одну з ключових загроз якості демократії, верховенству права та довірі до державних інститутів.

У центрі дослідження перебуває створена авторами база даних Brazilian Political Assassination Database, яка охоплює 1 228 випадків летального політичного насильства, зафіксованих у національних медіа протягом двох десятиліть. До вибірки включено як інституційних політичних акторів — кандидатів, обраних посадовців і колишніх чиновників, так і неінституційних учасників політичних процесів — активістів, лідерів соціальних рухів, представників громадських організацій та місцевих спільнот. Методологічно дослідження ґрунтується на адаптованому підході аналізу подій протестної активності, що дозволяє систематизувати інформацію про мотиви, просторовий контекст, методи вчинення злочинів та характеристики жертв.

Автори вводять чітке аналітичне розмежування між поняттями «летальне політичне насильство», «політична летальність» і «політичне вбивство», що дає змогу диференціювати завершені вбивства, замахи та погрози залежно від рівня ескалації конфлікту. Такий підхід дозволяє простежити не лише кінцеві наслідки політичних протистоянь, а й проміжні стадії, на яких держава могла б втрутитися та запобігти подальшій радикалізації.

У географічному вимірі звіт демонструє глибоку територіальну нерівномірність поширення політичного насильства. Найвищі показники зафіксовані у Північному та Центрально-Західному регіонах, де поєднуються слабка інституційна присутність держави, активна експлуатація природних ресурсів, масштабні земельні конфлікти та високий рівень тіньової економічної діяльності. Особливо вразливими є малі муніципалітети, у яких локальні еліти контролюють доступ до бюджетних ресурсів, землі, контрактів і посад, а правоохоронні та судові механізми не здатні ефективно стримувати зловживання владою. У таких умовах фізичне усунення опонентів стає одним із інструментів політичної конкуренції.

Аналіз просторового контексту вчинення злочинів показує, що понад половина вбивств і замахів відбувається у відкритих публічних просторах — на вулицях, дорогах, біля адміністративних будівель або в місцях масового скупчення людей. Це свідчить про низький рівень очікуваної відповідальності та впевненість виконавців у власній безкарності. Водночас значна частина злочинів здійснюється у так званих «оспорюваних просторах», тобто на територіях із невизначеним або конфліктним правовим статусом, зокрема на землях, зайнятих соціальними

[8] https://globalinitiative.net/wp-content/uploads/2026/01/Angela-Alonso-et-al-Deadly-Dynamics-Lethal-political-violence-in-Brazil-GI-TOC-January-2026.pdf

рухами, у зонах індіанських резерватів, екологічних територіях або на фермерських угіддях. Саме в цих середовищах конфлікти між приватними, колективними та кримінальними інтересами найчастіше переходять у насильницьку фазу.

Дослідження методів убивств засвідчує домінування професійно організованого насильства. У переважній більшості випадків використовувалася вогнепальна зброя, а самі злочини мали характер швидких, точно спланованих операцій із залученням найманих виконавців. Типовими є сценарії з використанням автомобілів або мотоциклів, множинними пострілами та негайним зникненням із місця події. Автори пов'язують це з існуванням стабільного ринку контрактних убивств, який функціонує на перетині кримінальних мереж, політичних інтересів і нелегального обігу зброї. Окремо підкреслюється вплив лібералізації збройового законодавства та зростання цивільного володіння вогнепальною зброєю у період правих урядів на загальний рівень летальності.

У соціально-професійному вимірі звіт показує, що основними жертвами є політики місцевого рівня та активісти, які працюють у сферах земельних, екологічних і ресурсних конфліктів. Понад дві третини випадків щодо політиків припадає на муніципальний рівень, де зосереджені ключові важелі розподілу ресурсів і адміністративного впливу. Серед активістів найбільш уразливими є лідери соціальних рухів, громадських і місцевих організацій, проте значна частка жертв припадає і на рядових учасників, що свідчить про використання насильства як інструменту залякування цілих спільнот. Гендерний аналіз підтверджує домінування чоловіків серед жертв, що відображає загальну гендерну структуру політичної сфери, однак окремі випадки вбивств жінок мають додатковий вимір гендерно зумовленого насильства.

Важливу частину дослідження становить аналіз мотивів і типів конфліктів, що призводять до летального насильства. Найбільшу частку становлять конфлікти, пов'язані з інституційною політикою, боротьбою за посади, бюджети та адміністративний контроль, а також земельні спори щодо власності та користування територіями. Меншою, але системно значущою є роль конфліктів навколо економічних можливостей і взаємодії з організованою злочинністю. В усіх цих випадках насильство постає як наслідок неспроможності або небажання сторін використовувати правові та політичні механізми врегулювання спорів.

Темпоральний аналіз демонструє чіткий зв'язок між рівнем летального політичного насильства та виборчими циклами, політичними кризами й змінами влади. Піки насильства припадають на роки імпічменту, спроби перевороту та інтенсивних виборчих

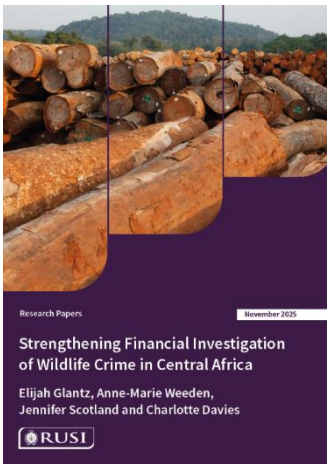
Висновки:

- **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.

кампаній, особливо на місцевому рівні. Автори фіксують значно вищий середній рівень убивств у період правих урядів порівняно з лівими адміністраціями, що пов'язується з радикалізацією політичного дискурсу, ослабленням інституційних стримувань і толерантністю до насильницьких практик.

У підсумку звіт формує цілісну картину летального політичного насильства як структурного елементу сучасної бразильської політичної системи, що відтворюється через поєднання слабкості державних інститутів, економічних інтересів, локальних владних монополій, криміналізації політики та дефіциту ефективного правосуддя. Автори доходять висновку, що без комплексної політики, спрямованої на зміцнення верховенства права, реформу місцевого врядування, контроль за обігом зброї, захист політичних і громадських активістів та посилення антикорупційних і правоохоронних механізмів, тенденція до використання насильства як інструменту політичної боротьби залишатиметься стійкою й надалі підриватиме демократичний розвиток країни.

Екологічна злочинність і фінансова безкарність: інституційні бар'єри регіону Центральної Африки [9]



Аналітичний звіт, підготовлений RUSI, є комплексним міждисциплінарним дослідженням, присвяченим системним причинам неефективності фінансових розслідувань у справах про незаконну торгівлю об'єктами дикої природи (IWT) в країнах Центральної Африки та їхньому впливу на стійкість регіональних механізмів протидії відмиванню коштів і фінансуванню тероризму. Автори виходять із фундаментального положення про те, що екологічна злочинність у сучасному вигляді є не локальним кримінальним явищем, а частиною транснаціональних економічних мереж, інтегрованих у глобальні фінансові та торговельні ланцюги. Відповідно, боротьба з нею лише шляхом кримінального переслідування браконьєрів або дрібних контрабандистів не може забезпечити довгострокового стримувального ефекту без системного фінансового впливу на організаторів і вигодоодержувачів.

Документ розміщує проблематику IWT у ширшому контексті міжнародних стандартів FATF, взаємних оцінок і ризиків потрапляння до переліків юрисдикцій з підвищеним наглядом. Автори демонструють, що формальна відповідність вимогам у сфері ПВК/ФТ, включно з включенням IWT до національних оцінок ризиків, не гарантує ефективності, якщо ці положення не підкріплені операційними механізмами. У цьому сенсі звіт показує розрив між «нормативною вітриною» та реальною спроможністю інституцій діяти, що є характерною проблемою для багатьох держав зі слабкими адміністративними та антикорупційними системами.

Методологічно дослідження спирається на багаторівневу емпіричну базу, що включає стандартизоване опитування ПФР країн Групи з протидії відмиванню коштів у Центральній Африці (GABAC), глибинні інтерв'ю з практиками фінансових розслідувань, аналіз судових рішень, матеріалів кримінальних проваджень, звітів міжнародних організацій і неурядових дослідницьких центрів. Автори наголошують, що тривалий період збору даних дозволив виявити не лише формальні проблеми, а й неформальні практики, професійні установки та

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

внутрішні обмеження, які не фіксуються в офіційній звітності. Це робить документ не просто оглядовим, а глибоко інституційним аналізом функціонування системи.

Значна частина звіту присвячена реконструкції фінансових ланцюгів незаконної торгівлі фауною і флорою, зокрема слоновою кісткою, лускою панголінів, живими тваринами, цінними породами деревини та похідною продукцією. Автори показують, що ці ланцюги мають багаторівневу структуру, яка включає місцевих збирачів, регіональних посередників, логістичних операторів, експортні компанії, фіктивні імпортно-експортні фірми та фінансових агентів у третіх країнах. Фінансові потоки при цьому маскуються через поєднання готівкових розрахунків, мобільних платіжних сервісів, неформальних систем переказів, використання підставних осіб і корпоративних оболонок. У звіті підкреслюється, що така архітектура створює численні точки втручання для фінансової розвідки, однак ці можливості системно ігноруються.

Висновки:

- **Фінансові розслідування у справах щодо незаконної торгівлі дикою природою залишаються епізодичними,** попри формальне визнання IWT як предикатного злочину до відмивання коштів. Відсутність системного залучення фінансових розвідок і низька кількість відповідних STR не дозволяють виявляти кінцевих бенефіціарів та фінансових координаторів злочинних мереж.
- **Домінування практики затримання «на гарячому» призводить до концентрації правоохоронних органів на дрібних виконавцях і вилученнях без подальшого розвитку фінансового компоненту справ.** Такий підхід блокує формування доказової бази для конфіскації активів і притягнення до відповідальності організаторів.
- **Корупція та політичний вплив системно нейтралізують механізми фінансового моніторингу,** знижують готовність банків і слідчих до подання та розвитку повідомлень про підозрілі операції та створюють атмосферу інституційної безкарності для учасників високорівневих схем.
- **Відсутність стандартизованих процедур, спеціалізованої підготовки та сталої міжвідомчої координації не дозволяє інтегрувати фінансові розслідування у повсякденну практику боротьби з IWT.** Без формалізованих стандартних операційні процедури, постійного навчання та транскордонного обміну інформацією регіон не спроможний перейти від ситуативних заходів до системного демонтажу злочинних мереж.

Окрему увагу приділено ролі приватного сектору, зокрема банків, платіжних установ, логістичних компаній і торговельних операторів. Автори відзначають, що фінансові установи в регіоні переважно не розглядають IWT як самостійний високоризиковий сегмент, а відповідні транзакції часто «розчиняються» в загальному масиві торговельних операцій. Відсутність спеціалізованих типологій, галузевих індикаторів ризику та зворотного зв'язку з боку ПФР призводить до низької якості STR і втрати аналітичної цінності повідомлень. Таким чином, система фінансового моніторингу функціонує формально, не виконуючи стратегічної ролі у виявленні організованих екологічних злочинів.

Концепція «пастки затримання під час безпосереднього вчинення злочину» у документі розкривається як прояв глибинних структурних деформацій системи правозастосування. Автори показують, що орієнтація на затримання «на місці злочину» зумовлена не лише законодавчими обмеженнями, а й показниковою логікою роботи правоохоронних органів, дефіцитом аналітичних ресурсів і слабкою координацією з прокуратурою. Такий підхід дозволяє швидко демонструвати формальні результати, але не створює передумов для складних фінансових розслідувань, що потребують часу,

міжвідомчої взаємодії та політичної підтримки.

Корупція в документі аналізується як багатовимірний феномен, що пронизує всі етапи протидії IWT — від видачі дозволів і митного контролю до судового розгляду та виконання вироків. Автори детально описують механізми тиску на слідчих і комплаєнс-офіцерів, практики неформального «врегулювання» справ, залучення політичних покровителів і використання бізнес-структур як прикриття. Особливу увагу приділено проблемі захисту викривачів, відсутність якого фактично блокує внутрішнє виявлення складних схем.

Міжнародний вимір проблеми розглядається крізь призму обмеженої ефективності механізмів взаємної правової допомоги, фінансового обміну та спільних операцій. Автори констатують, що більшість транскордонних фінансових потоків, пов'язаних з IWT, не стають предметом системного аналізу через перевантаженість національних органів, нестачу спеціалізованих кадрів і фрагментацію регіональних ініціатив. У результаті транснаціональні мережі зберігають адаптивність і здатність швидко відновлюватися після локальних втручань.

У завершальній частині звіту автори формують цілісну інтерпретаційну модель, у межах якої слабкість фінансових розслідувань розглядається як симптом глибших інституційних проблем — дефіциту стратегічного управління ризиками, обмеженої автономії правоохоронних органів, нестачі інвестицій у людський капітал і технології, а також недостатньої політичної волі до конфронтації з корупційними мережами. Рекомендації документа спрямовані не на точкові реформи, а на поступову трансформацію всієї екосистеми протидії екологічній злочинності шляхом інституціоналізації фінансових розслідувань, формування спеціалізованих міжвідомчих команд, розвитку державно-приватного партнерства, запровадження антикорупційних гарантій і посилення міжнародної інтеграції.

У підсумку звіт позиціонує фінансові розслідування як ключовий інструмент переходу від реактивної моделі реагування на екологічні злочини до стратегічної моделі управління ризиками, орієнтованої на позбавлення злочинних мереж економічної бази. Він демонструє, що без системного впровадження цього підходу держави Центральної Африки залишатимуться у пастці формальної відповідності стандартам FATF без реального впливу на масштаби незаконної торгівлі та пов'язаних із нею фінансових потоків.

AML Compliance у 2026 році: глобальний огляд [10]

Цей звіт, підготовлений спільно компанією LexisNexis та Міжнародною асоціацією з комплаєнсу (ICA), є одним з найбільш комплексних галузевих видань 2026 року, що охоплює еволюцію регуляторного ландшафту ПВК/ФТ у глобальній перспективі. Документ виконаний у форматі практичного посібника для фахівців із фінансового комплаєнсу та поєднує нормативний огляд із аналітичними спостереженнями щодо правозастосувальної практики та технологічних трендів. Методологічно звіт ґрунтується на синтезі регуляторних документів, законодавства, результатів галузевих опитувань (зокрема, Kroll's Fraud and Financial Crime Survey 2023 та PwC Global Compliance Study 2025) та авторського аналізу авторів-практиків. Структурно документ організований за регіональним принципом: після огляду глобальних трендів та рушіїв регулювання йдуть розділи, присвячені ЄС, Азійсько-Тихоокеанському регіону, Латинській Америці, Близькому Сходу та окремим юрисдикціям — Бразилії, Нідерландам, Сполученому Королівству, Франції, Німеччині, Швейцарії, ОАЕ, Сінгапуру та Гонконгу.

[10] https://www.int-comp.org/insight/e-book-aml-compliance-in-2026-a-global-view/

Аналітично найбільш значущим є розділ про майбутні тренди, що ускладнюють AML-ризики. Звіт констатує безпрецедентний рівень правозастосування: у 2024 році світові регулятори сукупно наклали штрафи у розмірі $19,3 млрд за порушення ПВК/ФТ — абсолютний рекорд. Водночас автори звертають увагу на якісну зміну пріоритетів: більшість керівників, опитаних Kroll, очікують, що регулятори все більше зосереджуватимуться не лише на результатах комплаєнсу (виявлених злочинах), але й на процесі — зокрема, на тому, як організації розгортають та контролюють технологічні рішення. Ця зміна парадигми означає перехід від «outcome-based» до «process-based» регуляторного нагляду, що має глибокі наслідки для операційної документації та внутрішнього аудиту.

Значний аналітичний акцент зроблено на регуляторній трансформації криптоактивів. Звіт системно розкладає хронологію нормативних змін, що охопили 2024–2026 роки: ухвалення MiCA (Regulation EU 2023/1114), що набрав чинності для CASP у грудні 2024 року; DORA (Digital Operational Resilience Act), що почав застосовуватись у січні 2025 року; оновлення FATF Travel Rule у середині 2025 року з вимогою стандартизованих даних про відправника та одержувача; дедлайн транспозиції DAC8 до кінця 2025 року та початок звітування у 2026 році. Ця регуляторна «хвиля» ефективно закриває тривалий правовий вакуум у регулюванні цифрових активів і ставить VASP та CASPs перед необхідністю повноцінної інтеграції в систему AML/CFT-зобов'язань, яка раніше застосовувалась виключно до традиційних фінансових посередників.

Розділ щодо ЄС представляє найбільш деталізований нормативний аналіз. Звіт описує методологію 6AMLD — розширення переліку кримінальних предикатних злочинів до більш ніж 20 категорій (включно з екологічними злочинами та кіберзлочинністю), розширення кримінальної відповідальності до фізичних осіб-представників юридичних осіб, встановлення відповідальності юридичних осіб навіть у випадках, коли злочин став результатом «відсутності нагляду або контролю». Остання норма є правовою інновацією, яка кардинально змінює режим відповідальності: замість вимоги доведення конкретного умислу відповідального менеджера достатньою стає демонстрація системних недоліків контролю. Для фінансових установ це означає, що захист «ми не знали» принципово недостатній — необхідне документоване свідчення того, що належний нагляд справді здійснювався.

Регіональний аналіз виявляє характерну асиметрію між нормативною конвергенцією та правозастосувальною дивергенцією. В ЄС гармонізація прискорюється завдяки пакету AMLR та AMLA, але правозастосування залишається децентралізованим і нерівномірним. В APAC, де понад 40 різних регуляторів здійснюють AML-нагляд, ситуація зворотна: Японія та Китай разом складали близько 80% регіональних витрат на комплаєнс у 2022 році, тоді як менш розвинені юрисдикції стикаються зі структурними дефіцитами ресурсів та інституційної спроможності. PwC's 2025 Global Compliance Study фіксує, що 85% респондентів вважають комплаєнс у APAC таким, що ускладнився. Сінгапурська ініціатива COSMIC (квітень 2024 року) — перша у світі централізована платформа для обміну фінансово-розвідувальною інформацією між установами — є відповіддю на цю проблему, але залишається регіональним прецедентом, а не глобальним стандартом.

Особливу увагу звіт приділяє двом юрисдикційним кейсам, що мають безпосередню релевантність для ПВК/ФТ-спільноти. В Бразилії у 2024 році органи влади наклали штрафів на $75 млн за порушення у сфері криптовалют — найбільший показник у Латинській Америці; Операція «Niflheim» розкрила кримінальну схему відмивання $9,7 млрд через криптоактиви з використанням підставних компаній, ухилення від оподаткування та валютних фронтів. В ОАЕ між липнем та жовтнем 2024 року регулятори призупинили ліцензії 32 золотооброблюючих підприємства після виявлення 256 порушень, пов'язаних з недостатніми практиками ПВК; у серпні 2024 року Центральний банк наклав штраф $1,6 млн на банк за порушення AML/CFT; у червні 2025 року — штраф $54 млн на обмінний пункт за серйозні системні недоліки. Ці

приклади демонструють, що правозастосування в юрисдикціях, які раніше вважалися «м'якими», наближається до стандартів G7.

Заключний розділ звіту «Від комплаєнсу до конкурентної переваги» розвиває інституційно значущу тезу: організації, які сприймають AML/CFT виключно як регуляторне навантаження, втрачають стратегічну перспективу. Автори виокремлюють чотири стратегічні вектори: впровадження AI та агентних систем для детекції аномалій та автоматизації кейс-менеджменту; побудова інтероперабельних платформ для усунення дублювань та інформаційних розривів між системами скринінгу; еволюція KYC у напрямку біометричної верифікації та самосуверенної ідентичності; включення ESG-ризиків у AML-програми як відповідь на нову категорію загроз — «зелене відмивання» (greenwashing). Ця концептуалізація розміщує функцію комплаєнсу не на периферії, а в центрі операційної та стратегічної архітектури сучасної фінансової установи.

Висновки:

- **Рекордний рівень правозастосування у поєднанні з очікуваним переходом регуляторного фокусу на технологічний комплаєнс (моніторинг систем AI, алгоритмічне виявлення підозрілих операцій) означає, що фінансові установи мають переглянути підхід до аудиту власних автоматизованих систем**: регулятор все частіше оцінюватиме не лише наявність технологій, а й їхню ефективність, налаштованість і відповідність.
- **Інституційна архітектура ЄС зазнає фундаментальних змін**: запуск AMLA у липні 2025 року та передача повноважень від EBA у грудні 2025 року означають початок реального централізованого нагляду, який до 2028 року охопить прямий нагляд за найбільш ризиковими суб'єктами.
- Паралельне **підвищення регуляторного тиску в ОАЕ та ширшому регіоні MENA** — після виходу ОАЕ з «сірого списку» FATF у лютому 2024 року та посилення санкційної чутливості у зв'язку з потоками російського капіталу — вимагає від установ з операційною присутністю в регіоні оновлення оцінок ризику і перегляду підходів до посиленої перевірки клієнтів.
- **Стрімке поширення агентського AI в комплаєнс-функціях (з потенціалом підвищення продуктивності на 200–2000% за оцінками McKinsey) несе одночасно операційні переваги та нові регуляторні ризики**: установи, що впроваджують агентські системи, повинні мати чіткі механізми людського нагляду за ключовими рішеннями, документацію логіки алгоритмічних виявлень та готовність обгрунтувати регулятору кожне автоматизоване рішення про відхилення клієнта або формування STR.

Рекомендовані матеріали

Чотири роки під тиском: еволюція санкційного режиму ЄС проти росії від екстреного реагування до стратегічного інструменту [11]

Подкаст RUSI Europe, присвячений четвертій річниці повномасштабного вторгнення росії в Україну, являє собою глибоку аналітичну дискусію між Кінгою Редловською, керівником Центру фінансової безпеки RUSI Europe, та Брісом Де Ш'єтером, керівником підрозділу санкцій Європейської служби зовнішніх зв'язків (EEAS). Розмова конструйована навколо центральної тези: санкційний режим ЄС проти росії здійснив якісний стрибок — від імпровізованого

[11] https://open.spotify.com/episode/5n2dhRulvCi7e11yA8fzAB?si=bHkbZ-YvTQqwDTGQC6a8jw&nd=1&dlsi=3b263e784cd642b8

механізму геополітичної сигналізації до найбільш технічно складного та юридично комплексного обмежувального режиму в історії Союзу. Ця трансформація, що відбулася протягом чотирьох років та охоплює вже 19 санкційних пакетів, заслуговує на детальний аналіз з точки зору архітектурної логіки, інструментального арсеналу та системних обмежень.

Де Ш'єтер описує еволюцію переговорного та імплементаційного процесу у контексті, де технічна складність заходів зростає з кожним пакетом, а швидкість прийняття рішень залишається критичним чинником ефективності. Санкції ЄС функціонують за принципом одностайності: кожен захід потребує консенсусу всіх 27 держав-членів, що створює структурне напруження між бажанням максимальної ефективності та реальністю геополітичних і комерційних розбіжностей між учасниками. Проте, як зазначає представник EEAS, процедурна складність не стала перешкодою для безпрецедентної за масштабом і деталізацією санкційної конструкції.

Ключовим змістовним блоком подкасту є аналіз цільових пріоритетів санкційного тиску. Перший вимір — атака на енергетичні доходи росії: нафтова цінова стеля G7/ЄС, поетапні заборони на імпорт нафти та нафтопродуктів, обмеження на транспортування через застосування санкцій до танкерів «тіньового флоту». Де Ш'єтер підкреслює, що «тіньовий флот» став однією з центральних операційних проблем санкційного правозастосування: мова йде про сотні суден під зручними прапорами, що здійснюють перевезення поза межами страхової інфраструктури G7, намагаючись обійти цінову стелю та ембарго. ЄС та Сполучене Королівство запровадили спеціальний санкційний режим для суден «тіньового флоту», що передбачає заборону заходу в порти, відмову у наданні послуг та можливість конфіскаційних заходів.

Другий вимір — технологічне ембарго через контроль за Common High Priority Items (CHPIs). Список охоплює 50 кодів HS у 4 рівнях пріоритетності, які ідентифіковані на підставі аналізу захоплених на полі бою компонентів. Система CHPIs функціонує як динамічний інструмент: перелік регулярно переглядається на основі даних полю бою та аналітики логістичних ланцюгів. Критичною проблемою, на яку вказують обидва учасники, є транзитні юрисдикції — держави, що не приєдналися до санкцій, але через які йдуть товарні потоки до росії. Механізм «no Russia clause» в контрактах з третіми країнами, запроваджений з 11-го пакету, є спробою ЄС поширити санкційні зобов'язання через договірне право. Його ефективність, однак, обмежена: цей механізм застосовується лише при виявленні фактів переспрямування, але реальний моніторинг залишається в компетенції держав-членів з дуже різними ресурсами та пріоритетами.

Подкаст детально зупиняється на питанні правозастосування та координації з партнерами G7. Де Ш'єтер визнає фундаментальну асиметрію: ЄС має одну з найбільш розроблених нормативних архітектур, але децентралізоване правозастосування, тоді як Офіс з контролю над іноземними активами (OFAC) у США здійснює більш агресивне правозастосування через доступ до доларових транзакцій. Механізм «Snapback» та принцип вторинних санкцій де-факто розширюють юрисдикцію США за межі формальних меж. Для ЄС аналогом є санкції EU FZCO — інструмент автономного режиму, що дозволяє включати до списків осіб та організації за сприяння ухиленню від санкцій, незалежно від їхньої прив'язки до конкретних секторальних

заходів. Це якісний стрибок порівняно з ранніми пакетами: санкції трансформуються з переліку заборонених секторів та осіб на активний механізм переслідування ухилення.

Окрема тематична лінія подкасту — роль третіх країн та геополітична фрагментація глобального санкційного простору. Серед ключових «транзитних вузлів» для продовження постачання санкційних товарів до росії — Туреччина, ОАЕ, Казахстан, Вірменія, деякі держави Центральної Азії та Гонконг. ЄС використовує дипломатичний тиск для роботи з цими юрисдикціями, намагаючись переконати їх у необхідності запровадження власних обмежень або посилення контролю за реекспортом. Де Ш'єтер фіксує певний прогрес у цьому напрямку — зокрема, ОАЕ та Казахстан посилили контроль — але визнає, що системного результату немає. Держави, що не є союзниками, мають власні економічні інтереси у торгівлі з росією, а загроза вторинних санкцій ЄС залишається менш переконливою, ніж американський аналог.

Стратегічний блок розмови торкається питання про те, чи санкції досягають своїх задекларованих цілей. Де Ш'єтер уникає однозначних відповідей, але підкреслює, що цілі санкцій є множинними і не зводяться до простого вимірювання падіння ВВП. Мова йде про підвищення вартості ведення війни, обмеження доступу до критичних технологій, формування тиску на еліти та збереження можливості дипломатичного урегулювання. У цьому контексті санкції розглядаються не як самодостатній механізм, а як один з елементів ширшого інструментарію — поряд із військовою підтримкою, дипломатією та притяганням до відповідальності за міжнародні злочини. Саме таке розуміння дозволяє, на думку учасників, зберігати реалістичні очікування щодо ефективності та продовжувати нарощування тиску попри складнощі правозастосування.

Інші новини

Чому сучасні системи перевірки санкцій є лише вершиною айсберга, і як нам навчитися бачити підводну частину [12]

У світі фінансової безпеки сформувалася небезпечна та дорога ілюзія. Протягом останнього десятиліття ми стали свідками безпрецедентної гонки технологій у сфері комплаєнсу. Фінансові установи витрачають мільйони доларів на вдосконалення систем скринінгу, калібрування алгоритмів пошуку, зменшення відсотка хибно-позитивних спрацьовувань та прискорення обробки транзакцій в режимі реального часу.

Регулятори, своєю чергою, під час перевірок дедалі частіше звертають увагу на технічні налаштування цих систем: чи той відсоток співпадіння обраний, чи оновлюються списки вчасно, чи правильно налаштована логіка транслітерації імен. І це створило хибне коло, де ефективність санкційного комплаєнсу почали ототожнювати виключно з досконалістю програмного забезпечення. Це не просто помилка — це фундаментальне нерозуміння природи сучасних санкційних режимів, яке створює величезні, системні прогалини в глобальній архітектурі безпеки.

Щоб зрозуміти масштаб проблеми, варто усвідомити просту істину: санкції сьогодні — це не просто "чорний список". Сучасний санкційний режим — це складний, багатовимірний організм, що регулює не лише те, з ким ми маємо право вести бізнес, але й що ми можемо продавати,

[12] https://www.amlintelligence.com/2026/02/insight-the-key-flaw-with-modern-sanctions-screening-systems/

куди ми це доставляємо, кому ми надаємо консультаційні послуги, які технології ми передаємо, і навіть яке програмне забезпечення ми маємо право оновлювати на серверах наших клієнтів у певних географічних регіонах. Санкції можуть бути прив'язані до конкретного типу товару подвійного призначення, до цілого сектору економіки держави-агресора, до конкретного проекту, до танкера під прапором певної держави, або навіть до певної глибини морського дна, де прокладається трубопровід. Жодна система скринінгу імен, навіть найдосконаліша, фізично не здатна самостійно виявити порушення, коли мова йде про передачу інженерних креслень електронною поштою, постачання цивільних, на перший погляд, мікросхем, які в підсумку опиняються в системі наведення безпілотника, або про надання юридичних консультацій щодо реструктуризації боргу компанії, що належить особі зі списку SDN.

Перший і найскладніший виклик, який повністю ігнорує парадигма "скринінгу як основи", лежить у царині встановлення бенефіціарної власності та контролю. Ми живемо в епоху безпрецедентної складності корпоративних структур. Трасти, номінальні директори, партнерства, боргові зобов'язання як інструмент контролю — це не винятки, це повсякденна реальність глобального бізнесу. Коли політично значуща особа або особа, що потрапила під санкції, хоче приховати свій контроль над активами, вона ніколи не триматиме 50% акцій на своє ім'я. Вона контролюватиме бізнес через міноритарну частку в 20%, доповнену акціонерною угодою, що надає їй право вето на ключові рішення. Вона використовуватиме складні трастові структури, де вона є бенефіціаром, але формально не володіє акціями. Вона впливатиме через боргове фінансування, де вона є ключовим кредитором, або просто через неформальний клановий чи регіональний вплив, який не фіксується в жодному реєстрі.

І що робить стандартна процедура скринінгу? Вона звіряє список засновників, поданий клієнтом, із санкційним переліком. Не знаходячи збігів, система радісно звітує про "пройдену перевірку", і банк відкриває рахунок або проводить транзакцію. Але чи дійсно ми виконали свою роботу, чи просто відзначили галочку в чек-листі, залишивши реальний контроль з боку підсанкційної особи абсолютно непоміченим? Це риторичне питання, яке має стати наріжним каменем кожної комплаєнс-стратегії.

Другий рівень складності, який розбивається об обмеженість скринінгових систем, — це санкції, прив'язані до товарів, послуг та маршрутів постачання. Уявіть собі легальну, "чисту" компанію з бездоганною репутацією, яка продає промислові насоси. Один і той самий насос, з однаковим кодом, може бути абсолютно законним товаром, якщо його придбає сільськогосподарський кооператив для іригаційної системи. Однак він стає предметом санкційного порушення, якщо той самий кооператив насправді є фіктивною компанією для державного нафтовидобувного підприємства, яке підпадає під секторальні санкції, що забороняють постачання обладнання для глибоководного буріння або видобутку на арктичному шельфі. Система скринінгу бачить лише назву товару (яка може бути свідомо розмитою в інвойсі), суму транзакції та назву компанії-отримувача. Вона не бачить, і не може побачити, кінцевого використання товару. Вона не з'єднає цю поставку з інформацією з митної бази даних про те, що компанія-отримувач ніколи раніше не імпортувала промислове обладнання і займалася виключно торгівлею зерном. Вона не проаналізує, що вантаж прямує не прямим шляхом, а через третю країну, відому як глобальний хаб для реекспорту заборонених технологій до Ірану чи Північної Кореї.

І саме тут ми спостерігаємо найбільшу сліпу пляму сучасної системи протидії відмиванню коштів: фінансові установи чудово відстежують грошові потоки, але майже не аналізують природу товару та логістику його переміщення в комплексі. Банки часто не мають доступу до митних даних в режимі реального часу. Поки ми не навчимося дивитися на транзакцію очима слідчого, який бачить не лише цифри, а й фізичний шлях товару, ми приречені пропускати складні схеми.

Окремої, надзвичайно глибокої уваги заслуговує потенціал, який ми майже не використовуємо — моніторинг транзакцій. Це інструмент, який теоретично міг би стати найпотужнішою зброєю проти прихованих санкційних схем, якби ми перестали сприймати його як додаток до AML, а зробили самостійним напрямком аналітики. Аналіз поведінкових патернів, виявлення аномальних маршрутів руху коштів, раптове зникнення посередників з ланцюжка постачання, різке зростання обсягів торгівлі з юрисдикціями, що перебувають у "сірій зоні" ризику, використання нових банків-кореспондентів у країнах зі слабким комплаєнсом одразу після відкриття рахунку — все це здатне викрити те, що приховано за іменами.

Однак, як свідчить щоденна практика, надзвичайно мало установ впроваджують спеціалізовані правила моніторингу, орієнтовані саме на санкції. Більшість покладається на стандартні AML-тригери, які налаштовані на виявлення відмивання грошей, а не на специфічні ознаки обходу санкцій.

Ще одна критична вада сучасної архітектури комплаєнсу, яку жоден скринінг не виправить, — це глибока структурна фрагментація всередині самих фінансових установ. У переважній більшості банків світу функції розділені настільки жорстко, що ліва рука не просто не знає, що робить права — вони працюють у різних будівлях, з різним керівництвом та різними IT-системами. Команда з торгівельного фінансування перевіряє коносаменти та інвойси, не маючи жодного доступу до даних про підозрілі патерни від AML-відділу, який одночасно аналізує ті самі транзакції. Відділ комплаєнсу може витрачати тижні на ретельне з'ясування складної структури власності клієнта під час онбордингу, але ця безцінна аналітична інформація не передається операційному відділу, який щодня проводить платежі цього клієнта, і не інтегрується в правила моніторингу. Санкційний аналітик бачить збіг за ім'ям у платіжному дорученні, проводить швидку перевірку і знімає тривогу, не підозрюючи, що той самий клієнт фігурує у відкритому розслідуванні відділу боротьби з фінансовими злочинами або що його директор згадується в журналістському розслідуванні як партнер місцевого олігарха. Ефективна протидія сучасним санкційним ризикам вимагає не просто співпраці, а тотальної конвергенції: об'єднання знань про геополітичний контекст, специфіку торгівлі, фінансові потоки, структури власності та репутаційні ризики в єдиному аналітичному просторі, доступному для всіх підрозділів, що працюють з клієнтом.

І нарешті, найскладніший, системний виклик, який виходить далеко за межі компетенції фінансового сектору — це необхідність контролювати нефінансових учасників ринку. Санкції порушуються не в банківських сховищах і не в платіжних терміналах. Вони порушуються в портах, на митних складах, на заводах-виробниках, у вантажівках, що перетинають кордони, і в літаках, що приземляються в третіх країнах. Виробники промислового обладнання, логістичні компанії, брокери, постачальники IT-послуг та інжинірингові фірми часто навіть не підозрюють, що стають частиною складної схеми обходу обмежень. Або, що ще гірше, вони свідомо заплющують очі, перекладаючи всю відповідальність на банк, сподіваючись, що фінансова установа "відсіче" ризик. Але правда полягає в тому, що нефінансові установи здебільшого не регулюються на предмет дотримання санкцій так жорстко, як банки. Вони не зобов'язані мати системи скринінгу, вони не звітують про підозрілі операції, і їх майже ніхто не перевіряє. І саме в цьому регуляторному розриві між фінансовим та реальним секторами економіки виникають найбільші загрози національній та міжнародній безпеці.

Отже, ми опинилися в парадоксальній ситуації: озброївшись найсучаснішим, найдорожчим скринінговим софтом, ми заспокоїли власну пильність, прийнявши інструмент за стратегію, а частину за ціле. Ми витратили мільярди на те, щоб блискавично виявляти збіги зі списками, але майже нічого не витратили на те, щоб навчитися бачити те, що в ці списки не потрапило, але має там бути.

Шлях вперед вимагає кардинальної зміни мислення як від регуляторів, так і від підзвітних установ. Регулятори повинні негайно змістити фокус своїх перевірок з технічного аудиту налаштувань системи на глибоку оцінку ефективності всієї програми комплаєнсу. Замість того, щоб перевіряти, чи є у банку "список SDN" і чи спрацьовує система на 99% збігів, вони мають оцінювати повний цикл: чи аналізує установа структуру контролю за межами прямого володіння акціями? Чи має вона задокументовані та ефективні процедури для перевірки кінцевого використання товарів? Чи інтегровані дані між відділом торгівельного фінансування та відділом AML? Чи використовує банк дані з відкритих джерел та неструктуровану інформацію для поглибленої перевірки клієнтів?

Справжній, надійний захист будується не на сліпій вірі в технології, а на глибокій аналітиці, на міждисциплінарному підході, на постійному, живому обміні інформацією між державами та всередині установ, на визнанні того, що наш противник надзвичайно адаптивний, креативний і завжди буде на крок попереду, якщо ми продовжимо думати категоріями десятирічної давнини. Санкційний комплаєнс — це вже давно не про технічне порівняння рядків у базі даних. Це про розуміння геополітики, про знання тонкощів світової торгівлі, про вміння аналізувати людську поведінку та про здатність з'єднувати, здавалося б, непов'язані факти в єдину картину злочину. Лише тоді ми зможемо побачити не лише верхівку айсберга, яку нам демонструють платіжні доручення, а його приховану, небезпечну підводну частину.

Тіньова крипто-економіка на службі російської воєнної машини: аналіз фінансових ланцюгів ухилення від санкцій [13]

Стаття аналітика RUSI, опублікована у лютому 2026 року, є одним з найбільш методологічно деталізованих публічних досліджень механізмів використання криптовалют у схемах ухилення від санкцій в контексті російської агресії проти України. Дослідження реконструює операційну архітектуру фінансування імпорту Common High Priority Items (CHPIs). На відміну від більшості публічних аналізів, що обмежуються описом загальних схем ухилення, автор розкриває конкретну транзакційну логіку та інституційну екосистему, що забезпечує конвертацію рублів у зовнішні платіжні засоби поза системою SWIFT.

Базовою аналітичною рамкою дослідження є концепт «вбудованої» (embedded) криптоінфраструктури в ланцюгах постачання CHPIs. Автор документує, що криптовалюти, і насамперед стейблкоїни — особливо USDT, — є не альтернативним, а інтегрованим платіжним рівнем усередині багаторівневих схем реекспорту через треті юрисдикції. Типова схема передбачає кілька шарів: на першому — конвертація рублів через OTC-брокерів (позабіржових дилерів) у USDT або інші стейблкоїни; на другому — переміщення коштів через ланцюг гаманців для збільшення відстані від джерела; на третьому — конвертація в цільову валюту юрисдикції-транзитера для фінального платежу постачальнику або посереднику. Стейблкоїни тут виконують функцію «чистої» розрахункової одиниці, що не прив'язана до санкційної юрисдикції, забезпечує швидкий кліринг і дозволяє уникнути банківський комплаєнс.

Центральним об'єктом дослідження є екосистема Garantex-Grinex-A7A5 — послідовність криптоінфраструктурних суб'єктів, що забезпечують операційну безперервність санкційно

[13] https://www.rusi.org/explore-our-research/publications/commentary/shadow-crypto-economy-feeding-russias-war-machine

обмежених транзакцій. Garantex — московська криптобіржа, включена до санкційних списків США та ЄС ще у 2022 році — після включення до SDN-листа не припинила операцій, а трансформувалась: за даними автора, вона функціонувала через перейменовану платформу Grinex та інші наступницькі суб'єкти, що фактично продовжили операційну діяльність під новими ідентифікаторами. Цей кейс демонструє фундаментальну проблему санкційного правозастосування в крипто-просторі: ліквідація юридичної особи не означає ліквідацію бізнес-моделі, яка може бути відтворена в нових корпоративних оболонках.

Найбільш аналітично значущим є опис стейблкоїну A7A5 — відносно маловідомого активу, який, за даними дослідника, обробив транзакцій на загальну суму $93,3 млрд менш ніж за рік операційної активності. Ця цифра є надзвичайно показовою з точки зору масштабу: вона перевищує ВВП більшості середніх держав і свідчить про те, що мова йде не про маргінальний інструмент, а про системно значущий розрахунковий механізм. A7A5 функціонує як «міст» між рублевою зоною та міжнародними ринками, надаючи можливість проводити транзакції, які формально не відображаються в традиційних фінансових даних і тому залишаються поза полем зору стандартних систем моніторингу транзакцій.

Окрему аналітичну цінність становить розділ, присвячений OTC-брокерам як «сліпій зоні» для регуляторів. На відміну від централізованих бірж, що мають ідентифіковані онлайн-інтерфейси та реєстраційні вимоги, OTC-ринок функціонує через неформальні мережі посередників, часто без фіксованих юридичних адрес та з мінімальним KYC. Автор документує, що саме OTC-сегмент є основним каналом конвертації рублів у криптоактиви для подальшого використання у зовнішньоторговельних розрахунках. Ця проблема не є специфічно російською: OTC-торгівля є структурним слабким місцем глобального санкційного правозастосування, оскільки регуляторні вимоги до цього сегменту значно менш розроблені, ніж до централізованих VASP.

Дослідження формулює вісім конкретних рекомендацій для держав та регуляторів. Серед них: посилення тиску на мережі обходу санкцій через проактивну ідентифікацію наступницьких організацій; розширення розвідувальних заходів щодо OTC-брокерів через залучення спеціалізованих блокчейн-аналітичних компаній; розбудова структурованого обміну даними між публічним та приватним секторами для підвищення якості атрибуції; цільовий тиск на «bridging assets» — стейблкоїни та торгові монети, що забезпечують рублево-доларову конвертацію; дипломатичний тиск на юрисдикції, які свідомо не вживають заходів проти підсанкційних платформ; розширення обмежень за межі фінансових посередників на комерційних суб'єктів, що беруть участь у ланцюгах постачання; застосування активних технік атрибуції, включно з аналізом on-chain патернів. Ці рекомендації утворюють комплексну стратегію, що принципово відрізняється від реактивного включення до санкційних списків і вимагає проактивного та технологічно оснащеного підходу.

Бізнес воєнних злочинів та обмежений вплив санкцій [14]

Стаття, опублікована на платформі Just Security, ставить одне з найбільш принципових і водночас методологічно недостатньо розроблених питань у сфері фінансового права та ПВК/ФТ: чому міжнародні злочини — воєнні злочини, злочини проти людяності, геноцид та злочин агресії — досі не стали повноцінними предикатними злочинами в глобальній системі протидії відмиванню коштів? Автори, що спеціалізуються на перетині міжнародного кримінального права та фінансових розслідувань, аргументують, що існуюча нормативна архітектура є достатньою для системних змін — за умови наявності політичної волі та операційного пріоритету.

[14] https://www.justsecurity.org/130431/disrupt-business-war-crimes/

Концептуальна рамка статті будується на аналогії з «промисловими» процесами Нюрнберзького трибуналу, де суб'єктами кримінальної відповідальності були не лише безпосередні виконавці, але й корпоративні структури та особи, що фінансували злочинний режим або отримували від нього прибуток. Автори наводять рішення трибуналу щодо IG Farben, хімічного концерну, що постачав отруйний газ до концентраційних таборів: «Farben крокував разом з Вермахтом і відіграв ключову роль у програмі Німеччини щодо завоювання та захоплення». Ця юридична логіка — кримінальна відповідальність за економічну співучасть — залишається актуальною і сьогодні, однак міжнародний кримінальний суд фактично не переслідував нікого за фінансування або отримання прибутку від міжнародних злочинів.

Стаття документує конкретні «бізнес-моделі» міжнародних злочинів у контексті російської агресії проти України. Масове викрадення українського зерна, яке автори кваліфікують як «складну і координовану логістичну операцію» за участю державних та приватних підприємств, утворює, за їхньою термінологією, «злочинне публічно-приватне партнерство». Програма «відбудови» Маріуполя розглядається як де-факто заміщення населення з корупційними механізмами освоєння бюджетів. Множинні приватні військові компанії, що діяли в Україні — зокрема, «Група Вагнера» до її інтеграції в структури Міноборони — фінансувалися через корпоративні структури, що формально не є суб'єктами міжнародно-правової відповідальності.

Ключовим аналітичним внеском статті є детальний опис операціоналізації методології ПВК/ФТ стосовно міжнародних злочинів. Автори вказують, що система FATF вже містить всі необхідні інструментальні компоненти: вимогу криміналізації відмивання коштів; зобов'язання фінансових установ ідентифікувати та повідомляти про підозрілі транзакції; інтеграцію фінансових розслідувань у переслідування серйозних злочинів; конфіскацію доходів від злочинної діяльності. Відсутнє лише одне — системне включення міжнародних злочинів у перелік «предикатних злочинів», для яких розроблені типологічні карти та «червоні прапорці» відмивання коштів. Автори апелюють до прецеденту: FATF вже розробив аналогічні аналітичні документи для торгівлі людьми, незаконної торгівлі дикою природою та онлайн-сексуальної експлуатації дітей.

Методологічно цінний розділ стосується конкретних прикладів типологічного аналізу стосовно міжнародних злочинів. Автори посилаються на «Amber Alert» Національного агентства з розслідування злочинів Великобританії (NCA) 2020 року щодо Судану — документ, що перерахував 23 конкретних «червоних прапорці» ризику незаконного фінансування, включаючи компанії зі спільною бенефіціарною власністю, що походила із Судану, у секторах добувної промисловості. Цей підхід, за оцінкою авторів, є шаблоном для аналогічних документів щодо росії: юрисдикції реєстрації, строки створення, профілі директорів та акціонерів, патерни та обсяги транзакцій могли б скласти оперативно корисний документ для фахівців з комплаєнсу.

Стаття також аналізує теоретичне питання про те, чи потребує застосування ПВК-режиму до міжнародних злочинів законодавчих змін, чи достатньо операційних. Позиція авторів є чіткою: правова база є достатньою, але вимагає активізації. Міжнародні злочини вже є кримінальними злочинами у більшості юрисдикцій; доходи від них підпадають під загальні норми про відмивання коштів; фінансові установи формально зобов'язані повідомляти про підозрілу діяльність незалежно від категорії предикатного злочину. Однак без спеціалізованих типологічних керівництв банківські комплаєнс-системи, налаштовані на стандартні сигнали

наркотрафіку або шахрайства, не здатні ідентифікувати специфічні ознаки фінансових потоків, пов'язаних із завоюванням, пограбуванням або відбудовою окупованих територій.

Заключна частина статті окреслює конкретний порядок денний для держав і регуляторів: розробка та поширення типологій і «червоних прапорців» для міжнародних злочинів через FATF та регіональні органи; активізація фінансових розслідувань у справах ICC та інших трибуналів; розвиток міжвідомчої координації між органами ПВК/ФТ та прокурорськими структурами, що займаються атроцитетами; розширення практики цивільної конфіскації активів, пов'язаних з воєнними злочинами, на рівні внутрішнього законодавства держав. Автори наполягають, що відповідальність за економічні виміри атроцитетів є не академічним питанням, а практичним інструментом стримування — оскільки раціональні актори, зокрема корпоративні, реагують на фінансові стимули та ризики.

Для загального розвитку

Комплаєнс-театр Binance та ілюзія доброчесності після $4,3 млрд штрафу [15]

Стаття являє собою критичний аналітичний коментар, присвячений одному з найбільш резонансних комплаєнс-скандалів у криптоіндустрії останніх місяців — справі Binance та звинуваченням у систематичному ігноруванні санкційних порушень, пов'язаних з Іраном. Автор, використовуючи метафору театральної вистави, ставить під сумнів автентичність реформ, впроваджених найбільшою у світі криптобіржею після епохального врегулювання з Міністерством юстиції США у листопаді 2023 року, за умовами якого компанія погодилась сплатити рекордний штраф у розмірі $4,3 млрд та прийняти режим зовнішнього моніторингу. Центральним аргументом публікації є теза про те, що демонстративне нарощування штату комплаєнс-підрозділу та публічні заяви про трансформацію корпоративної культури є не стільки свідченням реальних змін, скільки перформативним жестом, розрахованим на задоволення регуляторних очікувань без зміни операційної логіки.

Фактологічну основу статті складають повідомлення видань Fortune, Wall Street Journal та New York Times, за даними яких внутрішні слідчі комплаєнс-підрозділу Binance в період з березня 2024 по серпень 2025 року виявили ознаки проведення через платформу понад $1 млрд у транзакціях, пов'язаних з іранськими суб'єктами. Технічним вектором цих операцій виступав стейблкоїн USDT, що обертається в мережі Tron — інфраструктура, яка традиційно асоціюється з низькими комісіями, швидкою фіналізацією та, відповідно, підвищеними ризиками використання для обходу санкцій. Після того, як фахівці з розслідувань зафіксували результати у внутрішніх звітах та довели їх до відома керівництва компанії, включно з виконавчим директором Річардом Тенгом та директором з комплаєнсу Ноа Перлманом, щонайменше п'ять співробітників підрозділу були звільнені в кінці 2025 року. Принаймні троє з них мали досвід роботи у правоохоронних органах у Європі та Азії; кілька обіймали керівні посади і займалися

[15] https://www.linkedin.com/pulse/lie-ghts-camera-action-binances-compliance-theatre-iran-sanders-xqgyf/?trackingId=%2Fn71aRQ7QdGGteFvguDr7w%3D%3D

глобальними фінансовими розслідуваннями, включно з тим, що пов’язані з ухиленням від санкцій та фінансуванням тероризму.

Автор статті акцентує увагу на принциповій юридичній та регуляторній значущості цих подій у контексті діючого моніторингу. Режим зовнішнього нагляду, встановлений за умовами мирової угоди 2023 року, передбачає не лише фіксацію поточного стану систем комплаєнсу, але й активне виявлення порушень та їхнє усунення. Звільнення співробітників, які здійснювали саме таку функцію, ставить під сумнів ефективність та сумлінність виконання зобов'язань перед Міністерством юстиції. Ключовим юридичним питанням залишається кваліфікація цих дій: чи є звільнення законним управлінським рішенням щодо порушення внутрішньої політики, як стверджує Binance, чи становить воно інституційне придушення whistleblowing-діяльності, що може кваліфікуватися як перешкоджання правосуддю або порушення умов угоди про відстрочення переслідування (DPA/NPA).

Реакція компанії також стала предметом детального аналізу. Binance категорично відкинула звинувачення у санкційних порушеннях, посилаючись на результати внутрішнього розслідування за участю зовнішніх юридичних консультантів, яке не виявило доказів порушення застосовних санкційних законів. Компанія також оприлюднила статистику, за якою питома вага санкційних взаємодій у загальному обсязі торгів знизилася з 0,284% у січні 2024 року до 0,009% у липні 2025 року, що становить скорочення приблизно на 97%. Прямі взаємодії з чотирма основними іранськими криптобіржами скоротилися з $4,19 млн у січні 2024 до $110 тис. у січні 2026 року. Ці цифри Binance представляє як свідчення ефективності своєї комплаєнс-програми — «найкращої в галузі». Автор статті, однак, звертає увагу на те, що самопроголошений статус кращого не позбавляє від відповідальності за виявлені відхилення, а вибіркове цитування статистики не замінює системного аудиту.

Важливий регуляторний контекст додає ініціатива сенатора Річарда Блументаля, який відкрив парламентське розслідування щодо Binance у зв'язку з повідомленнями про перекази на суму $1,7 млрд на рахунки, пов'язані з іранськими організаціями, включно з єменськими хуситами. Запит сенатора стосується не лише самих транзакцій, але й «призупинення та звільнення» тих співробітників, які їх ідентифікували. Паралельно Binance веде власне внутрішнє розслідування, результати якого мають бути направлені до Міністерства юстиції США. Цей факт сам по собі є показовим: якщо компанія не виявила порушень, навіщо звітувати про внутрішнє розслідування регулятору? Публікаційна логіка статті будується на цій суперечності: демонстрація прозорості та одночасне заперечення самого факту проблеми.

Концептуально стаття розвиває дискурс про «комплаєнс-театр» (compliance theatre) — явище, добре відоме в академічній та практичній літературі зі сфери ПВК/ФТ. Під цим терміном розуміється ситуація, коли організація формально відповідає вимогам регулятора — наймає відповідних фахівців, впроваджує технологічні рішення, публікує звіти про прогрес — але при цьому організаційна культура, стимули та управлінські рішення фактично суперечать задекларованим цілям. Ця концепція принципово відрізняється від прямого шахрайства: компанія може щиро вірити у власну доброчесність, одночасно вибудовуючи структури, що системно пригнічують незручні сигнали з нижніх рівнів ієрархії. Саме в цьому й полягає суть підходу, описаного у статті: не злий умисел, а інституційна логіка, що ставить комерційні інтереси вище за зміст комплаєнс-діяльності.

Стаття також торкається ширшого питання про придатність нинішньої моделі ринкового саморегулювання для криптоіндустрії. Після виплати $4,3 млрд і встановлення режиму моніторингу Binance де-факто залишається найбільшою криптобіржею світу та основним вузловим пунктом глобальних потоків цифрових активів. Якщо навіть за таких умов нагляду компанія демонструє поведінку, що описується у публікаціях як придушення внутрішніх розслідувань, це ставить системне питання про достатність наявних правових інструментів.

Потенційне порушення умов DPA може призвести до відновлення кримінального переслідування — але лише якщо регулятор має достатньо доказів і політичну волю для такого кроку. Стаття неявно ставить саме це питання, звертаючись до аудиторії фахівців із комплаєнсу та фінансового права, для яких відповідь на нього має не лише академічний, а й прикладний інтерес.

Ваша думка важлива!

1. Де проходить межа між інноваційною автоматизацією комплаєнсу та створенням нових системних ризиків через неконтрольовану автономність AI-моделей?
2. Як інтегрувати принцип explainability у ПВК/ФТ-процеси без зниження їх ефективності?
3. Які інституційні та кадрові зміни необхідні для того, щоб ПФР, регулятори та наглядові органи України могли ефективно оцінювати ризики штучного інтелекту та здійснювати нагляд за його використанням у фінансовому секторі?
4. 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?
5. Як фінансові установи можуть інтегрувати ризики обходу експортного контролю у свої моделі ризик-орієнтованого підходу?
6. Які індикатори дозволять оцінити реальну ефективність санкцій, а не лише їх кількість?
7. Наскільки ефективним може бути технологічне ембарго в умовах сучасної глобалізованої економіки? Які механізми контролю за обігом мікросхем і критичних компонентів здатні реально обмежити доступ російського ВПК до західних технологій, і де проходить межа між ефективним контролем та неминучими тіньовими поставками?
8. Які правові, організаційні та антикорупційні гарантії необхідно запровадити в Україні для захисту аналітиків, фахівців з комплаєнсу і викривачів, залучених до викриття схем на високому рівні?
9. Враховуючи активний розвиток українського крипто-сектору та його відносно ліберальне регулювання, наскільки вразливою є наша країна для використання її крипто-інфраструктури міжнародними злочинними угрупованнями? Якими є ключові виклики для українських правоохоронних органів у протидії злочинним схемам, що використовують криптоінфраструктуру та обходять традиційні банківські системи?

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-2026-09

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].