Методологічний бюлетень

Серійний номер: МінФін-AML-2026-11

Березень 2026

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

Томас Карлайл

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Антимонопольна політика України у процесі європейської інтеграції [1]

Документ, підготовлений OECD, є комплексним міжнародним експертним оглядом системи конкурентного права та політики України, підготовленим у рамках механізму взаємного огляду Організації економічного співробітництва та розвитку (OECD). Основною метою цього огляду є оцінка ступеня відповідності української системи захисту економічної конкуренції міжнародним стандартам OECD, а також визначення прогресу, досягнутого Україною у реформуванні конкурентного законодавства та практики правозастосування, і окреслення ключових напрямів подальших інституційних та законодавчих змін. Дослідження базується на детальному аналізі нормативної бази, діяльності Антимонопольного комітету України (АМКУ), статистики правозастосування, інтерв’ю з представниками органів

[1] https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/11/oecd-peer-reviews-of-competition-law-and-policy-ukraine-2025_92b30786/218e6881-en.pdf

влади, судової системи, наукової спільноти та бізнесу, а також на порівнянні української практики з міжнародними підходами до регулювання конкуренції.

У звіті значна увага приділяється загальному економічному та інституційному контексту, в якому функціонує система конкурентної політики України. Україна характеризується економікою перехідного типу, що зазнала суттєвих трансформацій після здобуття незалежності та продовжує реформуватися у напрямі гармонізації з правом Європейського Союзу. Водночас економічне середовище країни залишається складним через наслідки повномасштабної війни, структурні дисбаланси в окремих секторах, значну присутність державних підприємств і ризики ринкової концентрації. Сільське господарство, металургія, машинобудування, енергетика та сектор IT відіграють важливу роль у національній економіці, проте функціонування багатьох ринків ускладнюється регуляторними бар'єрами, обмеженим доступом до інвестицій та структурними особливостями економіки. У цьому контексті ефективна конкурентна політика розглядається OECD як один із ключових інструментів підвищення ефективності економіки, стимулювання інновацій та забезпечення добробуту споживачів.

Основою правового регулювання конкуренції в Україні є Закон України «Про захист економічної конкуренції», прийнятий у 2001 році, який сформував фундамент сучасної системи антимонопольного регулювання. Закон встановлює правила щодо заборони антиконкурентних узгоджених дій, запобігання зловживанню монопольним або домінуючим становищем, контролю концентрацій суб'єктів господарювання, а також регулювання антиконкурентних дій органів державної влади. Норми цього закону поширюються на широкий спектр суб'єктів господарювання, включаючи фізичних осіб-підприємців, юридичних осіб, групи компаній, державні підприємства, а також іноземні компанії, діяльність яких може впливати на конкуренцію на території України. Важливою особливістю українського законодавства є також система попереднього погодження концентрацій і певних узгоджених дій, яка передбачає отримання дозволу АМКУ перед реалізацією відповідних економічних операцій.

Центральним органом, відповідальним за реалізацію конкурентної політики та застосування антимонопольного законодавства, є Антимонопольний комітет України. У звіті детально розглядається його інституційна структура, повноваження та механізми діяльності. АМКУ функціонує як незалежний орган державної влади зі спеціальним статусом і має децентралізовану структуру, що включає центральний апарат і територіальні відділення. Керівництво Комітету складається з голови та державних уповноважених, які беруть участь у прийнятті рішень у справах про порушення конкурентного законодавства. Комітет уповноважений проводити розслідування антиконкурентних практик, розглядати справи про зловживання домінуючим становищем, розкривати картельні змови, здійснювати контроль концентрацій, а також проводити адвокацію конкуренції, надаючи рекомендації органам державної влади щодо усунення бар'єрів для конкуренції.

У документі аналізується також система правозастосування у сфері конкуренції, включаючи процесуальні процедури розслідування, інструменти збору доказів та механізми накладення санкцій. OECD відзначає, що Україна досягла певного прогресу у виявленні антиконкурентних змов, зокрема у сфері публічних закупівель, де було виявлено значну кількість випадків змови учасників торгів. Однак ефективність правозастосування залишається обмеженою через недостатні інструменти розслідування, обмежені можливості проведення раптових перевірок і недостатню інтеграцію сучасних економічних методів аналізу ринку. У багатьох випадках аналіз порушень базується переважно на формально-юридичних аргументах, тоді як сучасна міжнародна практика передбачає активне використання економічного аналізу, зокрема оцінку бар'єрів входу на ринок, ринкової влади, ефектів для інновацій та впливу на добробут споживачів.

Окремий розділ звіту присвячений системі контролю за концентраціями суб'єктів господарювання. В Україні діє механізм обов'язкового повідомлення про концентрації, який передбачає необхідність отримання попереднього дозволу Антимонопольного комітету України на здійснення певних угод. OECD визнає, що ця система дозволяє запобігати потенційно шкідливим для конкуренції угодам, однак водночас звертає увагу на необхідність оптимізації порогових значень для повідомлення та спрощення процедур розгляду, щоб зменшити адміністративне навантаження на бізнес і зосередити ресурси антимонопольного органу на найбільш значущих справах.

Звіт також приділяє увагу питанням взаємодії АМКУ з іншими державними органами та галузевими регуляторами. В Україні регулювання багатьох ринків здійснюється спеціалізованими органами, наприклад у сферах енергетики, телекомунікацій або фінансових послуг. Нечіткий розподіл повноважень між цими органами та АМКУ іноді призводить до дублювання функцій або суперечностей у регуляторних рішеннях. OECD підкреслює важливість створення чітких механізмів координації між регуляторами для забезпечення узгодженості державної політики та уникнення конфліктів між регуляторними і конкурентними цілями.

Особлива увага приділяється питанням судового перегляду рішень антимонопольного органу та розвитку приватного правозастосування конкурентного права. Судова система відіграє важливу роль у перевірці законності рішень АМКУ, а також у забезпеченні захисту прав суб'єктів господарювання. OECD зазначає, що розвиток механізмів приватних позовів про відшкодування шкоди, завданої порушенням конкурентного законодавства, може значно посилити загальну ефективність системи захисту конкуренції.

Висновки:

- **Посилення інституційної спроможності АМКУ є критично необхідним.** Необхідно забезпечити стабільне фінансування, професійну незалежність керівництва, збільшення кадрового потенціалу та розширення інструментів розслідування (зокрема, проведення раптових перевірок і доступ до доказів).
- **Конкурентна політика повинна базуватися на економічному аналізі ринку.** Україні необхідно інтегрувати сучасні економічні методи оцінки ринкової влади, бар'єрів входу та інноваційних ефектів у практику АМКУ, що відповідає стандартам OECD та ЄС.
- **Система санкцій і комплаєнсу має бути посилена для створення реального стримувального ефекту.** Розмір штрафів та механізми їх стягнення повинні бути приведені у відповідність до міжнародних стандартів, щоб антиконкурентні практики стали економічно невигідними.
- **Необхідна краща координація між АМКУ та галузевими регуляторами.** Чіткий розподіл повноважень та механізми співпраці між антимонопольним органом і регуляторами енергетики, телекомунікацій та фінансового сектору дозволять уникнути дублювання функцій і підвищити ефективність регулювання.

У підсумку звіт доходить висновку, що за останні роки Україна досягла значного прогресу у гармонізації свого конкурентного законодавства з міжнародними стандартами, зокрема стандартами OECD та правом Європейського Союзу. Було прийнято низку законодавчих змін, спрямованих на посилення повноважень АМКУ, вдосконалення процедур розслідування, розвиток інструментів співпраці з іншими органами влади та підвищення прозорості правозастосування. Водночас система конкурентної політики потребує подальшого розвитку, зокрема шляхом зміцнення інституційної спроможності антимонопольного органу, удосконалення економічного аналізу у правозастосуванні, підвищення ефективності санкцій та поглиблення міжнародного співробітництва у сфері конкурентного права. Реалізація цих

реформ, на думку OECD, сприятиме формуванню більш відкритого, ефективного та інноваційного ринкового середовища, що є важливим чинником довгострокового економічного розвитку України.

Інституційна трансформація фінансового сектору України як передумова післявоєнного економічного зростання [2]

Аналітичний звіт OECD присвячений комплексному дослідженню інституційних та структурних умов розвитку фінансової системи України в контексті війни та майбутньої післявоєнної реконструкції. Документ виходить із того, що повномасштабна агресія росії спричинила значні людські та економічні втрати, однак попри ці виклики фінансова система України продемонструвала відносно високий рівень стійкості. Ця стійкість стала результатом швидкої та скоординованої політики державних органів, зокрема Національного банку України та уряду, а також значної міжнародної фінансової підтримки. Водночас автори звіту наголошують, що збереження макрофінансової стабільності під час війни є лише початковою умовою, тоді як ключовим стратегічним завданням стає створення ефективної, глибокої та інституційно стійкої фінансової системи, здатної мобілізувати ресурси для масштабної реконструкції економіки.

Звіт розглядає фінансову систему України як один із центральних механізмів забезпечення економічного відновлення. Для реалізації післявоєнної реконструкції країна потребуватиме значних обсягів інвестицій, які неможливо забезпечити виключно за рахунок державних фінансів або міжнародної допомоги. Саме тому ключовим завданням визначено розвиток ефективних фінансових ринків, здатних акумулювати внутрішній капітал домогосподарств і підприємств та залучати міжнародних інвесторів. У цьому контексті OECD підкреслює, що фінансові ринки повинні виконувати функцію ефективного розподілу капіталу, спрямовуючи фінансові ресурси до найбільш продуктивних секторів економіки та сприяючи створенню довгострокової економічної вартості. Важливу роль у цьому процесі відіграє також ефективне корпоративне управління, яке формує довіру інвесторів, підвищує прозорість бізнесу та сприяє притоку інвестиційного капіталу.

Документ структурований навколо кількох ключових напрямів реформування фінансової системи. Перший із них стосується розвитку фінансової системи та ринків капіталу. Автори наголошують, що фінансовий сектор України залишається надмірно залежним від банківського кредитування, тоді як ринки капіталу є відносно неглибокими та недостатньо ліквідними. Рівень участі населення у фондовому ринку є надзвичайно низьким: лише невелика частка громадян інвестує у цінні папери або інвестиційні фонди. Це свідчить про низький рівень фінансової інклюзії, обмежений доступ населення до інвестиційних інструментів та недостатній рівень довіри до фінансової системи. Значна частина заощаджень домогосподарств зберігається у вигляді готівки або банківських депозитів, що обмежує можливості мобілізації довгострокового капіталу для економічного розвитку. Для подолання цієї проблеми OECD рекомендує стимулювати розвиток інвестиційних інструментів, підвищувати фінансову грамотність населення та створювати стимули для довгострокових заощаджень.

[2] https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/03/stronger-financial-markets-and-institutions-for-ukraine-s-recovery_99e3d4a5/0c41c8ac-en.pdf

Суттєвою проблемою також є недостатня участь інституційних інвесторів у фінансових ринках. Пенсійні фонди та страхові компанії відіграють незначну роль у формуванні довгострокового інвестиційного капіталу. У більшості розвинених фінансових систем саме такі інституції виступають ключовими інвесторами у корпоративні облігації, акції та інші довгострокові фінансові інструменти. В Україні ж їхня роль залишається обмеженою, що негативно впливає на розвиток ринку капіталу. У звіті підкреслюється необхідність стимулювання розвитку цих інституцій, зокрема через реформування пенсійної системи та створення накопичувальних пенсійних механізмів, які можуть забезпечити стабільний приплив довгострокових інвестицій у національну економіку.

Окрему увагу у звіті приділено проблемі залучення іноземних інвестицій. Автори зазначають, що іноземний капітал відіграє критично важливу роль у фінансуванні відновлення економіки, проте наразі його участь у фінансовому ринку України обмежена. Однією з ключових причин є валютні обмеження, запроваджені під час воєнного стану, а також високий рівень ризиків, пов'язаних із безпековою ситуацією. OECD підкреслює, що після стабілізації макроекономічних та безпекових умов необхідно поступово лібералізувати валютне регулювання та створити умови для активнішої участі іноземних інвесторів у внутрішніх фінансових ринках.

Другий важливий напрям звіту стосується реформування банківського сектору. Незважаючи на війну, банківська система України залишається достатньо капіталізованою та прибутковою, проте її здатність фінансувати реальний сектор економіки залишається обмеженою. Однією з причин цього є значна частка проблемних кредитів, які накопичилися у банківських балансах у попередні роки. OECD рекомендує продовжити роботу зі зменшення обсягу непрацюючих кредитів, зокрема шляхом розвитку вторинного ринку таких активів та створення механізмів їх ефективного управління. Це дозволить вивільнити ресурси банків і спрямувати їх на кредитування бізнесу та домогосподарств.

Важливою структурною характеристикою банківської системи України є високий рівень державної власності. Державні банки контролюють значну частку активів банківського сектору, що у короткостроковій перспективі сприяє стабільності фінансової системи, особливо в умовах війни. Проте у довгостроковій перспективі така структура може обмежувати конкуренцію, знижувати ефективність фінансового посередництва та створювати ризики політичного впливу на кредитні рішення. У звіті пропонується поступово зменшувати роль держави у банківському секторі шляхом приватизації державних банків або часткового розміщення їхніх акцій на фондовому ринку. Такий підхід дозволить залучити приватний капітал, підвищити ефективність банківського сектору та сприяти розвитку ринку капіталу.

Наступний блок звіту присвячений корпоративному управлінню. OECD відзначає, що за останні роки Україна зробила значний прогрес у створенні нормативної бази корпоративного управління, проте ефективність її практичного застосування залишається обмеженою. Однією з проблем є відсутність систематичного моніторингу дотримання стандартів корпоративного управління компаніями, а також недостатня прозорість розкриття інформації. Для підвищення довіри інвесторів необхідно посилити роль регулятора фондового ринку, забезпечити його інституційну незалежність і створити ефективну систему контролю за дотриманням корпоративних стандартів.

Окремий розділ документа аналізує систему управління державним боргом. В умовах війни боргове навантаження на державний бюджет значно зросло, що створює додаткові ризики для макроекономічної стабільності. OECD підкреслює необхідність удосконалення інституційної структури управління державним боргом, зокрема шляхом створення централізованої системи аналізу ризиків, удосконалення управління ліквідністю та розвитку внутрішнього ринку державних облігацій у національній валюті. Розвиток такого ринку дозволить зменшити залежність від зовнішнього фінансування та підвищити стійкість фінансової системи.

Ще одним важливим елементом фінансової системи є захист прав споживачів фінансових послуг. У звіті наголошується, що під час війни фінансові ризики для населення зростають, зокрема через збільшення рівня заборгованості, фінансового шахрайства та недостатній рівень фінансової обізнаності. OECD рекомендує посилити механізми розгляду скарг споживачів, розширити використання альтернативних механізмів вирішення фінансових спорів і забезпечити кращий доступ населення до фінансової інформації. Паралельно необхідно розвивати програми фінансової грамотності, що дозволить громадянам більш усвідомлено приймати фінансові рішення.

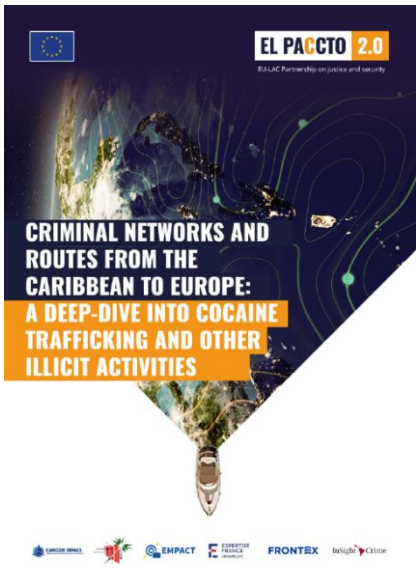
Висновки:

- **Україні необхідно створити глибокий і ліквідний ринок капіталу для фінансування післявоєнної реконструкції.** Необхідно стимулювати участь домогосподарств і інституційних інвесторів, посилити роль пенсійних фондів і страхових компаній та поступово лібералізувати валютні обмеження для залучення іноземних інвесторів.
- **Банківська система повинна перейти від домінування держави до більш конкурентної структури.** Є необхідність у поступовій приватизації державних банків, зменшенні їхньої концентрації активів і скороченні портфеля проблемних кредитів через розвиток вторинного ринку NPL.
- **Система фінансування економіки має бути диверсифікована через розвиток альтернативних фінансових інструментів.** Необхідне розширення використання факторингу, лізингу, кредитних гарантій і іпотечного фінансування для підтримки малого та середнього бізнесу та відновлення житлового сектору.
- **Інституційна якість фінансового регулювання є ключовою умовою залучення інвестицій.** Необхідно посилити незалежність і спроможність регулятора фондового ринку, завершити гармонізацію регуляторної бази з міжнародними стандартами (IOSCO) та покращити корпоративне управління в компаніях.

Важливим стратегічним напрямом є реформування пенсійної системи шляхом запровадження накопичувальних пенсій, забезпечених активами. OECD розглядає таку систему як ключовий інструмент формування довгострокових внутрішніх інвестиційних ресурсів. Накопичувальні пенсійні фонди можуть стати важливими інституційними інвесторами на фінансовому ринку, що сприятиме розвитку ринку капіталу та створенню стабільного джерела фінансування для економічного розвитку. Водночас запровадження такої системи потребує ефективного регуляторного нагляду, прозорої структури управління активами та високого рівня довіри з боку населення.

Загалом звіт формує комплексну дорожню карту реформ, що охоплює короткострокові, середньострокові та довгострокові заходи. Її реалізація має забезпечити трансформацію фінансової системи України у сучасну, ефективну та інтегровану з міжнародними фінансовими ринками систему. У довгостроковій перспективі це повинно сприяти не лише післявоєнному відновленню, а й створенню стійкої економічної моделі розвитку, заснованої на ефективному фінансовому посередництві, прозорому корпоративному управлінні та високому рівні довіри інвесторів до української економіки.

Трансатлантичний наркотрафік: роль Карибського регіону у постачанні кокаїну на європейські ринки [3]



Документ підготовлений у межах програми EL PACCTO 2.0 та присвячений комплексному аналізу ролі Карибського регіону у глобальних ланцюгах незаконного обігу кокаїну, зокрема у контексті постачання наркотиків із Південної Америки на європейські ринки. Дослідження розглядає географічні, організаційні та логістичні фактори, що сприяють перетворенню Карибського басейну на один із ключових транзитних вузлів трансатлантичного наркотрафіку, а також детально описує структуру кримінальних мереж, методи транспортування наркотиків, роль окремих держав регіону та вплив правоохоронних заходів на трансформацію незаконних маршрутів.

У вступній частині дослідження наголошується, що Карибський регіон історично відігравав важливу роль у глобальній торгівлі наркотиками, виступаючи основним транзитним коридором для постачання кокаїну до Сполучених Штатів. Проте зміна структури світового попиту на наркотики, а також активізація європейських ринків призвели до переорієнтації наркотрафіку, внаслідок чого Карибський басейн став важливою відправною точкою для транспортування кокаїну до Європи. Географічне положення регіону, близькість до південноамериканських зон виробництва наркотиків, численні морські маршрути, інтенсивний туристичний та торговельний рух, а також розгалужена портова та авіаційна інфраструктура створюють сприятливі умови для використання легальних транспортних систем у незаконних цілях. Автори документа підкреслюють, що ті самі морські та повітряні маршрути, які забезпечують економічну діяльність регіону, можуть легко використовуватися кримінальними мережами для переміщення наркотиків, що значно ускладнює їх виявлення та припинення.

Дослідження демонструє, що сучасні кримінальні мережі, які організовують транспортування кокаїну через Карибський регіон, мають високий рівень адаптивності та не функціонують у вигляді традиційних ієрархічних наркокартелів. Натомість вони складаються з гнучких, децентралізованих і часто тимчасових альянсів різних учасників, кожен з яких виконує окрему роль у ланцюгу постачання. Південноамериканські організації, передусім з Колумбії та Венесуели, забезпечують виробництво та первинне транспортування наркотиків, тоді як міжнародні брокери координують логістику, фінансування та взаємодію між постачальниками і покупцями. Локальні кримінальні групи, що діють на карибських островах, виконують функції перевалки, транспортування, зберігання та підготовки наркотиків до подальшого транспортування до Європи. У цій системі брокери відіграють ключову роль, оскільки вони забезпечують фінансування операцій, організовують транспортування, координують корупційні зв’язки та забезпечують безпечне проходження вантажів через транзитні території. Значна частина таких брокерів походить із європейських країн або регіону Західних Балкан і виступає посередниками між виробниками наркотиків у Латинській Америці та кримінальними ринками Європи.

У документі детально описуються основні маршрути наркотрафіку, які проходять через Карибський регіон. Автори виділяють два ключові транзитні коридори. Перший передбачає транспортування наркотиків через острови Карибського басейну, де вони переміщуються між різними островами з метою консолідації, зберігання та підготовки до відправлення у напрямку Європи. Велика кількість островів і портів у регіоні дозволяє кримінальним мережам

[3] https://zenodo.org/records/18385156

використовувати складні маршрути, що ускладнює роботу правоохоронних органів. Другий коридор проходить через так званий Південноамериканський Карибський регіон, до якого входять Гаяна, Суринам і Французька Гвіана. Ці території мають прямий вихід до Атлантичного океану та часто використовуються як стартові точки для відправлення великих партій наркотиків безпосередньо до Європи або через Західну Африку. Географічні особливості цих територій, зокрема густі тропічні ліси, розгалужені річкові системи та слабкий контроль кордонів, створюють додаткові можливості для прихованого переміщення наркотиків.

Важливе місце у дослідженні займає аналіз методів транспортування наркотиків. Автори підкреслюють, що Карибський регіон надає кримінальним мережам широкий спектр можливостей для транспортування, що значно підвищує їхню здатність адаптуватися до змін у правоохоронному середовищі. Найбільш поширеним способом залишається використання контейнерних перевезень у комерційних портах, де наркотики приховуються серед легальних вантажів або додаються до контейнерів уже після проходження митного контролю. Водночас активно використовуються швидкісні човни, що здійснюють короткі морські переходи між узбережжям Південної Америки та карибськими островами, риболовецькі судна, яхти, приватні літаки, а також кур'єри, які перевозять невеликі партії наркотиків на комерційних авіарейсах. Останніми роками також спостерігається збільшення використання напівзанурюваних суден і так званих нарко-субмарин, які здатні перевозити великі обсяги наркотиків через Атлантичний океан безпосередньо до Європи.

Документ детально аналізує роль окремих країн у транзиті наркотиків. Домініканська Республіка визначається як один із найважливіших регіональних центрів наркотрафіку до Європи. Її стратегічне розташування, розвинена портова інфраструктура та прямі морські маршрути до великих європейських портів роблять її ключовим вузлом у трансатлантичному наркотрафіку. Через порти країни щорічно проходять мільйони контейнерів, що створює можливість приховувати наркотики серед легальних вантажів. Крім того, країна має прямі авіаційні маршрути до Європи, що дозволяє використовувати кур'єрів для транспортування невеликих партій наркотиків.

Тринідад і Тобаго розглядається як важливий пункт прийому наркотиків, що надходять із Венесуели. Через географічну близькість до венесуельського узбережжя ця держава стала частиною регіональної кримінальної екосистеми, де місцеві банди забезпечують зберігання, перевалку та подальше транспортування наркотиків. Хоча більшість партій не спрямовується безпосередньо до Європи, країна відіграє важливу роль у підготовці наркотиків до подальшого транспортування через інші транзитні точки Карибського басейну або Західної Африки.

Венесуела, у свою чергу, виступає ключовим транзитним центром між зонами виробництва кокаїну в Колумбії та карибськими маршрутами. Наявність великої кількості нелегальних злітно-посадкових смуг, слабкий контроль державних інституцій та високий рівень корупції сприяють функціонуванню наркотрафіку. У дослідженні описується роль так званого «Cartel de los Soles», до якого, за даними аналітиків, можуть бути причетні представники військових і державних структур, що забезпечують сприятливі умови для транспортування наркотиків через державну інфраструктуру.

Документ також розглядає вплив правоохоронних операцій на зміну маршрутів наркотрафіку. Зокрема, посилення військової присутності США у Карибському морі у 2025–2026 роках призвело до тимчасового зменшення використання швидкісних човнів для транспортування наркотиків. Водночас кримінальні мережі швидко адаптувалися до нових умов, використовуючи альтернативні маршрути через Амазонію, Гаяну та Суринам, а також збільшуючи використання авіаційних маршрутів і менш помітних морських суден. Це свідчить про високу гнучкість кримінальних мереж і їхню здатність швидко змінювати логістичні схеми у відповідь на правоохоронний тиск.

Окрему увагу автори приділяють взаємозв'язку наркотрафіку з іншими видами організованої злочинності. У багатьох випадках ті самі кримінальні мережі залучені до незаконної міграції, торгівлі людьми, незаконного обігу зброї та відмивання коштів. Економічні фактори, зокрема бідність і відсутність альтернативних джерел доходу у прибережних громадах, сприяють залученню місцевого населення до наркотрафіку. Кримінальні мережі активно використовують ці соціально-економічні умови, пропонуючи фінансові стимули для участі у перевезенні та зберіганні наркотиків.

Загалом дослідження демонструє, що трансатлантичний наркотрафік через Карибський регіон є складною та динамічною системою, у якій беруть участь численні суб'єкти різного рівня — від локальних кримінальних груп до транснаціональних брокерів і корумпованих державних структур. Висока диверсифікація маршрутів і методів транспортування, а також здатність кримінальних мереж швидко адаптуватися до змін у правоохоронному середовищі роблять боротьбу з цим явищем надзвичайно складною. Автори документа підкреслюють, що ефективна протидія наркотрафіку потребує поглибленої міжнародної співпраці, обміну розвідувальною інформацією та комплексного підходу, який поєднує правоохоронні заходи з антикорупційними та соціально-економічними політиками.

Висновки:

- **Ключовим вузлом боротьби з наркотрафіком є міжнародні брокери та логістичні координатори.** Фокус правоохоронних операцій має зміщуватися від вилучення наркотиків до ідентифікації та нейтралізації брокерів, які координують фінансування, логістику та корупційні зв'язки у трансатлантичному наркотрафіку.
- **Контейнерні порти залишаються найбільш критичною точкою ризику.** Необхідно посилювати контроль у контейнерних терміналах (зони завантаження, контейнерні майданчики, системи доступу персоналу) та впроваджувати антикорупційні механізми для портових працівників.
- **Посилення силових операцій без системної міжнародної координації лише змінює маршрути, але не зменшує обсяг наркотрафіку.** Ефективна протидія можлива лише через інтегровану співпрацю між країнами Карибського регіону, ЄС та транзитними державами, включаючи обмін розвідувальною інформацією.
- **Соціально-економічні фактори є критичним драйвером наркотрафіку.** Без розвитку альтернативних джерел доходу для прибережних громад і зменшення корупції у державних структурах кримінальні мережі продовжуватимуть знаходити нових учасників у ланцюгах перевезення наркотиків.

Стратегія протидії шахрайству Сполученого Королівства на 2026–2029 роки: системний підхід до найбільшої за обсягом злочинності [4]

Документ, опублікований Міністерством внутрішніх справ Сполученого Королівства, є державним стратегічним документом вищого рівня, що визначає урядову позицію щодо протидії шахрайству на чотирирічний горизонт. Стратегія є прямою відповіддю на визнання шахрайства найбільш поширеним видом злочинності в Англії та Уельсі: за даними Crime Survey of England and Wales (CSEW) за рік, що закінчився у вересні 2025 року, було зафіксовано понад 4 мільйони злочинів, що становить 45 відсотків від загальної кількості всіх злочинів. Кожен чотирнадцятий дорослий житель країни став жертвою шахрайства. Економічні та соціальні

[4] https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategy-web.pdf

витрати, пов'язані з цим явищем, досягли щонайменше 14,4 мільярда фунтів стерлінгів у 2023–2024 роках, що свідчить про системну загрозу не лише для окремих осіб, але й для макроекономічної стабільності країни.

Стратегія структурована навколо трьох рівноправних стовпів: DISRUPT (Зруйнувати), SAFEGUARD (Захистити) та RESPOND (Реагувати). Такий підхід відображає принципову позицію регулятора про те, що жодна ізольована міра, будь то кримінальне переслідування, технічна блокування чи просвітницька кампанія, не здатна самостійно вирішити проблему, масштаб якої визначається поєднанням технологічної еволюції, глобалізації організованої злочинності та вразливостей цифрової інфраструктури. Уряд зобов'язується інвестувати понад 250 мільйонів фунтів стерлінгів у реалізацію стратегії протягом 2026–2029 років, що, у поєднанні зі структурними реформами правоохоронної архітектури, свідчить про безпрецедентний рівень державного зобов'язання у цій сфері.

Центральним елементом першого стовпу є створення Онлайн-центру злочинності (Online Crime Centre, OCC) з бюджетом 31 мільйон фунтів стерлінгів, запуск якого заплановано на квітень 2026 року. OCC матиме унікальну інституційну конфігурацію: він об'єднає Міністерство внутрішніх справ, Національне агентство з боротьби зі злочинністю (NCA), Поліцію Лондонського Сіті, розвідувальну спільноту (включаючи GCHQ, Національний центр кібербезпеки та Національні кіберсили), а також представників фінансового, телекомунікаційного, технологічного та кіберіндустріального секторів. Ключовою операційною функцією OCC є агрегування та аналіз великих масивів різнорідних даних від публічних і приватних партнерів в єдиному просторі в режимі реального часу. Це вирішує критичну проблему фрагментованого інформаційного ландшафту, за якого кожен партнер має унікальні дані, але відсутня єдина, спільна та актуальна картина загрози шахрайства. Як наслідок — втрачається час на координацію, а злочинці отримують перевагу першого ходу. Передбачається, що OCC, отримуючи сигнали від нового сервісу Report Fraud та від можливостей "Share and Defend" Національного центру кібербезпеки, зможе ініціювати оперативні втручання — блокування дзвінків, заморожування рахунків, видалення шахрайських веб-сайтів та обмеження акаунтів у соціальних мережах — значно швидше, ніж за існуючих механізмів.

Стратегія приділяє надзвичайно важливу увагу технологічному виміру загрози. Зокрема, систематично аналізуються ризики використання злочинцями генеративного штучного інтелекту (GenAI) — діпфейків, великих мовних моделей та клонування голосу — для підвищення переконливості, масштабу та цільового характеру атак. Фішинг визначається як найпоширеніший метод кібератак, що використовується організованими злочинними угрупованнями (OCGs) проти фізичних осіб та бізнесу, причому злочинці активно застосовують GenAI-інструменти для формування переконливих повідомлень, вбудовування шахрайських QR-кодів у публічних місцях і збору персональних та фінансових даних. Цей аналіз спирається на конкретні дані: Дослідження кібербезпекових інцидентів (Cyber Security Breaches Survey 2025) оцінило 72 000 шахрайських подій щодо британського бізнесу за 12 місяців, а вартість збитків коливалася від менш ніж 100 фунтів до понад 100 000 фунтів стерлінгів за інцидент.

Окрему аналітичну цінність становить блок, присвячений типологіям шахрайства з найвищим рівнем шкоди. NCA визначила кур'єрне шахрайство, інвестиційне шахрайство, шахрайство з переадресацією платежів та романтичне шахрайство основними типами, що спричиняють найбільшу шкоду у Сполученому Королівстві у 2025 році. Авторизовані push-платіжні (APP) шахрайства, де жертви добровільно переказують кошти через обман, демонструють тривожну

статистику: 53 відсотки зафіксованих випадків у 2023 році включали соціальні мережі, платформи обміну повідомленнями та дзвінків; 13 відсотків — аукціонні та торговельні платформи; 12 відсотків — телекомунікаційні платформи. Ці дані недвозначно вказують на необхідність посилення відповідальності операторів цифрових платформ за зловживання своєю інфраструктурою з боку злочинців.

Транснаціональний вимір стратегії не менш важливий. Більше двох третин справ мають міжнародний елемент, що робить шахрайство глобальною проблемою зі значною транскордонною активністю. Уряд підтверджує зобов'язання щодо проведення Глобального саміту з питань шахрайства у Відні у березні 2026 року разом з UNODC та INTERPOL, а також укладання двосторонніх Меморандумів про взаєморозуміння з державами, які є пріоритетними з точки зору походження загрози. В рамках підготовки до саміту Сполучене Королівство профінансувало перший Глобальний звіт INTERPOL щодо фінансового шахрайства та інструментарій ООН з питань шахрайства. В якості конкретних прикладів транскордонної взаємодії наводяться: операція NCA у Нігерії (січень 2026 року) за підтримки даних Meta, яка призвела до ліквідації шахрайського центру; операція у штаті Уттар-Прадеш в Індії (липень 2025 року), спільна розробка CBI, NCA, FBI та Microsoft, що дозволила ліквідувати кол-центр, жертвами якого стали понад 100 британців із сукупними втратами понад 390 000 фунтів стерлінгів; а також санкції у жовтні 2025 року проти мережі Prince Group в Камбоджі, що використовувала примусову працю для проведення онлайн-шахрайства, включаючи заморозку лондонської нерухомості на загальну суму понад 125 мільйонів фунтів стерлінгів.

Стовп SAFEGUARD зосереджений на зміцненні стійкості суспільства та бізнесу. Ключові заходи включають: розширення кампанії "Stop! Think Fraud" на ширший спектр типів шахрайства; підвищення ефективності правоохоронної відповіді через розширення аналітично обґрунтованої проактивної поліцейської діяльності та забезпечення цільової підтримки вразливих осіб; а також підтримку спеціалізованих центрів кіберстійкості для надання рекомендацій бізнесу щодо підвищення стійкості до шахрайства. Документ констатує, що шахрайство непропорційно зростає серед молодих людей порівняно зі старшими категоріями

Висновки:

- **Запуск Онлайн-центру злочинності (OCC) у квітні 2026 року з бюджетом 31 млн фунтів стерлінгів кардинально змінює операційну модель протидії шахрайству:** злиття правоохоронних, розвідувальних та приватних даних в єдиному аналітичному вузлі дозволяє переходу від реактивного розслідування до проактивного блокування загроз у реальному часі. Фінансовим установам необхідно забезпечити технічну готовність до участі в схемах обміну даними OCC.
- **Визнання на стратегічному рівні GenAI як системного інструменту шахраїв** (діпфейки, клонування голосу, великі мовні моделі) **означає, що традиційні моделі виявлення шахрайства**, засновані на поведінкових патернах та статичних правилах, **стають недостатніми**. Підрозділи фінансового моніторингу мають інтегрувати AI-detection у свої процеси ідентифікації.
- **Транскордонний вимір (понад 2/3 справ мають міжнародний елемент) та визнання шахрайства основним предикатним злочином для ВК вимагають від комплаєнс-підрозділів переосмислення підходів до оцінки ризиків** юрисдикцій і моніторингу схем із залученням телекомунікаційної інфраструктури, платформ соціальних мереж та криптовалют.
- Введення Хартії жертв шахрайства (Q2 2027) та реструктуризація правоохоронних повноважень на користь NPS/NCA означає зміцнення вимог до операційної співпраці фінансових установ з правоохоронцями, зокрема щодо заморожування активів, відновлення вкраденого та повідомлення про підозрілі операції.

населення, хоча найвища частка жертв традиційно припадає на вікову групу 45–64 роки. Дані щодо психологічного впливу є вражаючими: 92 відсотки опитаних жертв шахрайства відчули емоційні або психічні симптоми, 57 відсотків — фізичні симптоми, а 63 відсотки зазнали зміни поведінки. Серед підприємств, що постраждали від шахрайства, 8 відсотків відчули себе стримуваними у здійсненні запланованої майбутньої ділової діяльності.

Стовп RESPOND охоплює заходи щодо реагування, підтримки жертв та правосуддя. Центральними елементами є запуск нового сервісу Report Fraud як єдиної точки повідомлень для жертв; введення Хартії жертв шахрайства (Fraud Victims Charter) у другому кварталі 2027 року, яка встановить мінімальні стандарти підтримки від усіх залучених організацій; а також зміцнення кримінального та цивільного правосуддя через вдосконалення судових процедур і розгляд запровадження додаткових цивільно-правових санкцій. Важливою складовою є також планована реструктуризація правоохоронної відповідальності: відповідно до реформи поліції, загальна відповідальність за шахрайство, економічну злочинність та кіберзлочинність передаватиметься до Національної поліцейської служби (NPS) та Національного агентства з боротьби зі злочинністю (NCA). Стратегія також виділяє промисловий масштаб сучасного шахрайства як ключову характеристику сучасної загрози: злочинці використовують VPN та VoIP-технології для маскування місцезнаходження та підробки британських номерів, AI-діпфейки для соціальної інженерії, злому електронної пошти для переадресації платежів, а темна та сіра мережа надають готові шахрайські інструменти у форматі fraud-as-a-service.

Розуміння та пом'якшення ризиків офшорних VASP: новий звіт FATF [5]

Звіт FATF є першим спеціалізованим дослідженням у сфері ПВК/ФТ/ФР, повністю присвяченим проблематиці офшорних VASP. Його поява обумовлена результатами шостого цільового оновлення FATF щодо імплементації Рекомендації 15, в якому зафіксовано, що юрисдикції систематично повідомляють про складнощі із пом'якшенням ризиків офшорних VASP. Документ покликаний заповнити регуляторну прогалину, яка виникає через відмінності у тому, як різні юрисдикції визначають та регулюють VASP, що надають послуги клієнтам за межами країни своєї реєстрації. Поняття офшорного VASP (oVASP) визначається як постачальник послуг віртуальних активів, створений за законодавством однієї юрисдикції, з фізичною присутністю або без неї, що надає послуги клієнтам, які перебувають в іншій юрисдикції.

Методологічно документ базується на аналізі конкретних прикладів того, яким чином oVASP структурують свою діяльність з метою уникнення або ухилення від регуляторних зобов'язань, а також того, як злочинні актори використовують вразливості, породжені цією структурою. FATF виділяє два типи oVASP: ненавмисні — що стають офшорними через особливості ведення бізнесу або регуляторного середовища без свідомого наміру ухилення від нагляду; та навмисні — що цілеспрямовано обирають юрисдикцію реєстрації, виходячи з мінімальних регуляторних вимог або недостатнього нагляду. Звіт з аналітичною точністю констатує, що різниця між двома

[5] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Understanding-Mitigating-Risks-Offshore-VASPs.pdf.coredownload.inline.pdf

категоріями на практиці може бути розмитою, оскільки ненавмисні oVASP можуть нічим не відрізнятися від навмисних з точки зору функціонального регуляторного впливу.

Ключовою статистичною знахідкою звіту є те, що лише менше половини юрисдикцій — 46 відсотків — прийняли підхід на основі діяльності (activity-based approach) до регулювання та нагляду. Цей підхід передбачає поширення вимог щодо ліцензування або реєстрації на VASP на основі діяльності, яку вони провадять у юрисдикції, незалежно від того, де ці VASP зареєстровані або розташовані. Решта юрисдикцій використовують підхід, заснований на місці реєстрації або фізичній присутності, що автоматично виключає oVASP з-під їхнього нагляду. Цей регуляторний розрив є ключовим вектором ризику, який документ прагне усунути. Як позитивний приклад наводиться регулювання ЄС у рамках MiCA, яке застосовує саме підхід на основі діяльності, вимагаючи від будь-якого VASP, що обслуговує клієнтів у ЄС, отримання відповідного дозволу, незалежно від місця реєстрації.

Документ детально аналізує механізми, через які oVASP уникають регуляторних зобов'язань. По-перше, це відсутність або мінімальна фізична присутність у юрисдикції клієнтів: персонал, ключові управлінці та інфраструктура даних можуть перебувати в зовсім інших країнах, що ускладнює як реєстрацію, так і нагляд. По-друге, схеми вкладених відносин (nested relationships), за яких неліцензований oVASP отримує доступ до ліквідності та шлюзів фіатного переведення через рахунки у регульованих VASP, видаючи себе за приватного клієнта. Такі схеми можуть бути цілком легітимними, але вони також здатні приховувати особистість і діяльність реальних клієнтів та обмежувати видимість транзакційних потоків для регульованого VASP. По-третє, документ фіксує, що регуляторний арбітраж залишається серйозною проблемою: офшорні платформи можуть переміщуватися або маршрутизувати клієнтські операції через юрисдикції зі слабшими вимогами ПВК/ФТ, перетворюючи нижчі витрати на комплаєнс на конкурентну перевагу в ціноутворенні.

Конкретні кейси, наведені у звіті, ілюструють реальний злочинний потенціал oVASP. В одному з них аналіз нігерійського ПФР у справі про масштабне інвестиційне шахрайство виявив, як oVASP та непрозорі корпоративні структури використовувалися для транскордонного переміщення злочинних доходів та заплутування фінансового сліду, причому кошти жертв спрямовувалися через численні проміжні «воронкові адреси», а офшорні VASP слугували кінцевими точками обготівковування. В іншому кейсі oVASP використовувалися для конвертації злочинних доходів з шахрайських центрів та фінансування терористичних угруповань. Ці приклади підтверджують, що oVASP — це не абстрактний теоретичний ризик, а конкретний і

Висновки:

- **Юрисдикціям, що досі не прийняли підхід на основі діяльності до регулювання VASP, необхідно терміново переглянути нормативні рамки**: без поширення ліцензійних вимог на VASP, що обслуговують клієнтів на їхній території незалежно від місця реєстрації, будь-який внутрішній нагляд за криптоактивами залишатиметься структурно незавершеним.
- **Фінансові установи та регульовані VASP мають запровадити спеціальні процедури оцінки ризику вкладених відносин**: перевірка контрагентів на предмет наявності ліцензії / реєстрації у відповідних юрисдикціях, аналіз транзакційних профілів на ознаки прихованого нагромадження клієнтської бази третіх сторін є обов'язковими елементами комплаєнсу.
- **Підрозділи ПВК/ФТ/ФР мають включити oVASP як окрему типологію ризику до своїх секторальних оцінок ризиків та систем транзакційного моніторингу**, зокрема додаючи перевірки на ознаки регуляторного арбітражу при роботі з VASP-контрагентами з юрисдикцій зі слабким наглядом.

задокументований канал обходу системи фінансового моніторингу.

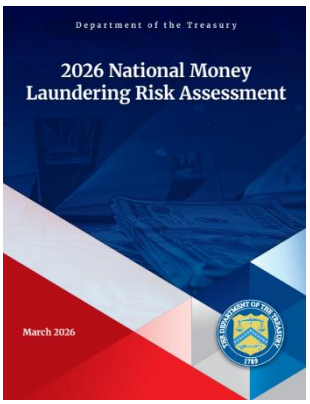
У розділі, присвяченому рекомендаціям, FATF формулює конкретні заходи для трьох груп стейкхолдерів. Для всіх юрисдикцій — включення діяльності oVASP до національних оцінок ризику, навіть у випадку надання послуг без фізичної присутності, та застосування ризик-орієнтованого підходу до нагляду. Для юрисдикцій реєстрації oVASP — забезпечення ефективного ризик-орієнтованого нагляду за VASP, що провадять глобальну діяльність, включаючи повноваження отримувати інформацію про транскордонні операції та співпрацювати з іноземними регуляторами через обмін інформацією та підтримку примусових заходів. Для юрисдикцій перебування клієнтів — розгляд вимог щодо реєстрації або ліцензування офшорних постачальників, а також чітке визначення того, що означає активне надання послуг. Для приватного сектору — оцінка впливу oVASP, застосування ризик-орієнтованих контролів, моніторинг вкладених відносин та відмова від встановлення ділових відносин із неліцензованими або незареєстрованими постачальниками.

Важливим інституційним контекстом є те, що цей звіт виходить одночасно із шостим цільовим оновленням FATF та Довідником про кращі практики нагляду за Travel Rule. Станом на квітень 2025 року 73 відсотки зі 117 юрисдикцій, що дозволяють роботу VASP, ухвалили законодавство щодо Travel Rule, але реальне правозастосування суттєво відстає від формального дотримання. Зв'язок між неефективністю нагляду за oVASP та недостатнім виконанням Travel Rule є нерозривним: без охоплення офшорних провайдерів будь-яка система передачі інформації про платника та отримувача матиме структурні прогалини. Звіт завершується закликом президента FATF Еліси де Анда Мадрасо до всіх держав та приватного сектору діяти відповідно до виявлених кращих практик, зазначаючи, що «oVASP створюють сліпі зони, якими явно користуються злочинці».

Міністерство фінансів США опублікувало національну оцінку ризиків ВК/ФТ/ФР

У березні 2026 року Міністерство фінансів США опублікувало одночасно три взаємопов'язаних документи, що утворюють комплексну офіційну оцінку ризиків ВК/ФТ/ФР в американській фінансовій системі: Національну оцінку ризику відмивання коштів (NMLRA), Національну оцінку ризику фінансування тероризму (NTFRA) та Національну оцінку ризику фінансування розповсюдження зброї масового знищення (NPFRA). Разом ці документи формують основу для майбутньої Національної стратегії протидії незаконним фінансовим потокам (National Illicit Finance Strategy 2026) та слугують орієнтиром як для державних регуляторів, так і для приватного сектору при формуванні власних ризик-орієнтованих програм комплаєнсу. Звітний період охоплює 1 січня 2024 — 31 грудня 2025 року.

Частина I. Національна оцінка ризику відмивання коштів (2026 NMLRA) [6]



П'ята за рахунком NMLRA констатує тривожну динаміку: медіанна сума збитків у справах про відмивання коштів зросла більш ніж на 150 відсотків за п'ять років — з 208 000 доларів США у 2019 році до 526 000 доларів у 2024 році. При цьому частка справ зі збитками понад 1,5 мільйона доларів майже подвоїлася: з 17 відсотків у 2019 до 32 відсотків у 2024 році. Ця тенденція відображає якісну зміну у структурі загроз: від переважно дрібних схем до індустріалізованих, транснаціональних операцій, що здатні завдавати збитків на мільярди доларів. Провідними загрозами залишаються шахрайство та наркоторгівля, які щорічно генерують сотні мільярдів доларів

[6] https://home.treasury.gov/system/files/246/2026-NMLRA.pdf

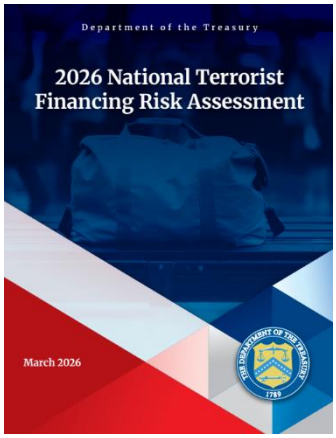
злочинних доходів. Кіберзлочинність, торгівля людьми, контрабанда людей та корупція також генерують мільярди доларів. Оцінка Internet Crime Complaint Center (IC3) ФБР свідчить, що у 2024 році 859 532 скарги жертв на злочини в Інтернеті спричинили збитки на понад 16 мільярдів доларів — зростання на 33 відсотки порівняно з 2023 роком. Втрати через шахрайство, за оцінками Федеральної торгової Комії (FTC), сягали 195,9 мільярда доларів.

Окреме місце в документі посідає аналіз інвестиційного шахрайства. У 2024 році жертви повідомили про збитки від інвестиційного шахрайства на загальну суму 6,57 мільярда доларів — зростання на 44 відсотки, переважно за рахунок схем шахрайства з цифровими активами, відомими як pig butchering. Транснаціональні злочинні організації (ТЗО) провадять ці схеми в індустріальному масштабі, переважно з шахрайських центрів у Камбоджі, М'янмі та Лаосі, із прогнозованим розширенням в Африку, Південну Азію та Південну Америку. У 2024 році жертви повідомили про 5,8 мільярда доларів збитків від шахрайства з цифровими активами — зростання на 47 відсотків. Особливу тривогу викликає зростання схем «ramp-and-dump» з акціями китайських компаній VIE на американських біржах: у першому півріччі 2025 року IC3 зафіксував зростання скарг таких схем на 300 відсотків.

NMLRA виявляє наскрізну вразливість, що пронизує всі сектори: зростаюче використання штучного інтелекту злочинцями для масштабування та удосконалення шахрайств, зокрема для генерування шахрайських комунікацій, синтетичних особистостей та переконливих вебсайтів. Серед секторальних вразливостей документ виокремлює: банківський сектор та MSB (постачальники грошових послуг); брокери-дилери та інвестиційні радники, що піддаються ризику шахрайських інвестиційних схем; казино та ігровий бізнес; страхування. Щодо цифрових активів оцінка фіксує: стейблкоїни становлять більшість незаконної криптоактивності; КНДР вчинила найбільшу одиничну крадіжку в екосистемі цифрових активів, викравши 1,46 мільярда доларів з Bybit. Серед китайських мереж відмивання коштів (CMLN) документ виокремлює особливо небезпечну групу «Huione Group» — камбоджійський фінансовий конгломерат, що був відключений від американської фінансової системи рішенням FinCEN у жовтні 2025 року і допоміг КНДР відмити щонайменше 37 мільйонів доларів.

У сфері нерухомості та дорогоцінних активів NMLRA підтверджує, що ці сектори залишаються стійкими каналами відмивання коштів, зокрема через практику купівлі без іпотеки (all-cash purchases), використання LLC та трастів для приховування реального бенефіціарного власника, а також через арт-ринок та ринок предметів розкоші. Висновки оцінки мають суттєве значення для впровадження вимог щодо корпоративної прозорості (Corporate Transparency Act), виконання яких залишається предметом активної регуляторної уваги.

Частина II. Національна оцінка ризику фінансування тероризму (2026 NTFRA) [7]



NTFRA 2026 розроблялася в середовищі кардинально зміненого глобального безпекового ландшафту. Ключовими контекстуальними чинниками є: середовище після 7 жовтня 2023 року, яке виявилося «родючим ґрунтом для радикалізації та екстремізму»; падіння режиму Асада в Сирії, яке породило нестабільність і нові можливості для терористичних угруповань; а також безпрецедентне рішення адміністрації Трампа у січні 2025 року призначити 15 транснаціональних злочинних організацій і наркокартелів із Західної півкулі іноземними терористичними організаціями (FTO) та Specially Designated Global Terrorists (SDGT). Цей крок вперше об'єднав аналіз ризиків фінансування тероризму та відмивання коштів в єдиному

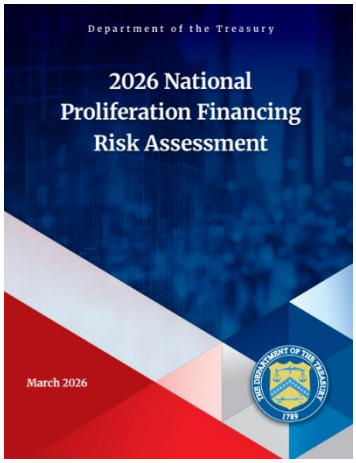
[7] https://home.treasury.gov/system/files/246/2026-NTFRA.pdf

документі — NTFRA тепер включає аналіз ТЗО поряд з традиційними терористичними групами.

ІДІЛ залишається найбільш летальним та активно представленим в США суб'єктом фінансування тероризму. Попри загибель третього лідера у 2025 році та тривалий антитерористичний тиск, організація демонструє стійкість і диверсифікацію джерел фінансування. Грошові резерви ISIS Core скоротилися до 10 мільйонів доларів (порівняно з 500 мільйонами на піку «халіфату»), однак африканські філії — ISIS-Сомалі, ISIS-ДРК та ISIS-Західна Африка — генерують сотні тисяч доларів щомісяця через схеми вимагання. ІДІЛ активно розширює використання цифрових активів: у рамках атаки на залу Crocus Hall у москві у 2024 році ISIS-K переказав щонайменше 2 000 доларів у цифрових активах нападникам. Конкретні кейси, наведені в документі, ілюструють типові механізми: справа Мохаммеда Азхарудділа Чхіпи (засуджений у травні 2025 до 30+ років ув'язнення) — збирав кошти онлайн, конвертував у цифрові активи та відправляв до Туреччини для подальшого контрабандного переміщення до членів ISIS в Сирії; Victoria Jacobs (18 років ув'язнення) — відмила 12 000 доларів через цифрові активи та подарункові карти на користь «Malhama Tactical», пов'язаної з Аль-Каїдою.

NTFRA виокремлює специфічну та відносно нову категорію загроз: внутрішні насильницькі екстремісти (Domestic Violent Extremists, DVE) та самостійно радикалізовані особи (HVE). Для цих гравців характерне самостійне фінансування: вони здійснюють атаки із власних коштів, не вдаючись до залучення зовнішніх фінансових потоків, що принципово обмежує можливості виявлення через інструменти фінансового моніторингу. Новорічна терористична атака в Новому Орлеані 1 січня 2025 року, натхненна ISIS, служить конкретним ілюстративним прикладом цієї загрози. Серед вразливостей фінансової системи документ виділяє: MSB (зокрема, реєстрація без ефективного моніторингу); онлайн-фандрейзинг та P2P-платежі; цифрові активи; неприбуткові організації (НПО), які продовжують піддаватися ризику зловживань з боку терористів. Щодо Хізбалли та ХАМАС — обидві організації, попри суттєвих збитків у ході ізраїльсько-хамасівського конфлікту, зберігають здатність зловживати банківською системою США, використовуючи охоплення операцій у доларах США по всьому світу, та продовжують отримувати значні кошти від Ірану.

Частина III. Національна оцінка ризику фінансування розповсюдження ЗМЗ (2026 NPFRA) [8]



NPFRA 2026, четверта за рахунком подібна оцінка (США опублікували першу у 2018 році), фіксує підвищений рівень загрози від суб'єктів, що прагнуть фінансувати розповсюдження або використання біологічної, хімічної, ядерної або радіологічної зброї чи відповідних матеріалів. Геополітичний контекст 2024–2025 років суттєво ускладнив архітектуру протидії: росія у березні 2024 року заблокувала поновлення мандату Групи експертів Комітету 1718 ООН (ГЕ 1718) щодо КНДР, ліквідувавши унікальний інструмент відстеження санкційних порушень; водночас у вересні 2025 року на Іран були автоматично поновлені всі попередні санкції ООН через «суттєве невиконання» Тегераном зобов'язань за спільним всеосяжним планом дій (СВПД).

КНДР залишається найбільш активним і технологічно просунутим суб'єктом ФР у глобальному вимірі. Диверсифікація каналів генерування доходів є визначальною рисою корейської стратегії: розгортання ІТ-спеціалістів у американських компаніях з підробленими або вкраденими документами для отримання зарплат; кіберкрадіжки цифрових активів (включаючи крадіжку 1,46 мільярда доларів з Bybit — найбільша одинична крадіжка в цифровій екосистемі); відправлення будівельних робітників до росії для заробітку в іноземній валюті; торгівля зброєю,

[8] https://home.treasury.gov/system/files/246/2026-NPFRA.pdf

наркотиками та іншими незаконними товарами. Щодо Ірану, попри нещодавніх невдач ядерної програми та мережі проксі-організацій, країна продовжує використовувати складні схеми ухилення для підтримки програм зі створення балістичних ракет та БПЛА, а також ядерної програми. Відповіддю є кампанія «максимального тиску» адміністрації Трампа, оголошена у лютому 2025 року. Зміцнення росією економічних та військових зв'язків з КНДР є серйозним ФР-ризиком, водночас москва ухиляється від експортного контролю для отримання товарів подвійного призначення з метою розробки зброї для використання в Україні.

Дві широкі типології, виокремлені NPFRA, мають особливу практичну цінність. Перша — «Зловживання глобальною технологічною екосистемою» (Typology 1) — охоплює цілеспрямовану діяльність КНДР щодо IT-сектору та використання цифрових активів для приховування та переміщення коштів. Ця типологія безпосередньо впливає на практику onboarding в IT-компаніях та у VASP: необхідні додаткові перевірки осіб, що претендують на IT-контракти з нетипових юрисдикцій, а також посилений моніторинг транзакцій з ознаками відмивання коштів від кібершахрайства через стейблкоїни та DEX. Друга — «Використання технік відмивання коштів для підтримки діяльності з розповсюдження» (Typology 2) — охоплює залучення посередників для ухилення від санкцій та обходу експортного контролю, а також використання підставних компаній. Документ особливо акцентує роль китайських фізичних та юридичних осіб у сприянні ухиленню від санкцій, що набуває дедалі більшого поширення. Серед секторальних вразливостей виокремлюється недостатній рівень ПВК/ФТ/ФР-контролів у секторі цифрових активів у глобальному масштабі, а також деякі недоліки у відповідності всередині США.

Висновки:

- **Штучний інтелект є наскрізним множником загрози у всіх трьох оцінках**: від генерування переконливих шахрайських комунікацій до deepfake-особистостей IT-працівників з КНДР. Програми комплаєнсу фінансових установ мають бути скориговані на включення AI-орієнтованих індикаторів ризику.
- **Цифрові активи (і насамперед стейблкоїни) є провідним вектором у всіх трьох категоріях** — ВК, ФТ та ФР. Відключення Huione Group від фінансової системи США та визначення відмивання криптоактивів КНДР як пріоритетної загрози формують чіткий регуляторний сигнал: СПФМ, що взаємодіють з VASP, мають застосовувати поглиблену перевірку контрагентів.
- **Визначення 15 ТЗО іноземними терористичними організаціями розширює коло суб'єктів, щодо яких застосовуються найсуворіші заходи ЦФС**: фінансові установи мають переглянути санкційні скринінгові списки та охопити наркокартелі у своїх сценаріях моніторингу транзакцій.
- **Ліквідація ГЕ 1718 ООН і неповна імплементація CPF-контролів у менш ніж 20% юрисдикцій (за оцінкою FATF) формують критичний розрив у глобальній архітектурі протидії ФР**. Це вимагає від відділів комплаєнсу більшої самостійності у проведенні власних оцінок ризиків за транзакціями з товарами подвійного призначення.

Регулювання

Законодавство та регулювання щодо блокчейн та криптовалют [9]

Видавництво Global Legal Insights (GLI) — авторитетне британське юридично-аналітичне видання, що спеціалізується на порівняльному правовому аналізі для бізнес-аудиторії та правників — у жовтні 2025 року опублікувало восьме видання щорічного збірника «Blockchain & Cryptocurrency Laws and Regulations 2026». Збірник охоплює 40 глав та містить аналіз правового регулювання блокчейну та криптовалют у 29 юрисдикціях. У числі ключових юрисдикцій, представлених у виданні, — США, ЄС, Сполучене Королівство, Сінгапур, ОАЕ (Дубай), Гонконг, Японія, Швейцарія, Канада, Австралія, Бразилія, Індія, Україна та інші. Крім оглядів .hbclbrwsq, збірник містить тематичні аналітичні розділи від провідних правових фірм (Holland & Knight LLP, Davis Polk & Wardwell, Cleary Gottlieb Steen & Hamilton, Fenwick & West та інших) з питань стейблкоїнів, оподаткування, санкцій та DeFi. Ключовими глобальними трендами, відображеними у виданні, визначені: революційна зміна регуляторного підходу США після повернення адміністрації Трампа; прийняття першої комплексної федеральної криптовалютної рамки в США (Закон GENIUS, підписаний 18 липня 2025 року); повна імплементація MiCA в ЄС; та інституційне прийняття (ETF на Bitcoin з активами під управлінням 150–170 мільярдів доларів США до кінця вересня 2025 року).

Глава щодо України охоплює поточну правову рамку та зміни, запропоновані Законопроєктом № 10225-д. Ключовою характеристикою поточного стану є регуляторна двоїстість: з одного боку, Україна з 2020 року імплементує Рекомендацію 15 FATF, законодавчо визначила поняття VASP та впровадила вимоги AML/KYC для постачальників послуг з обігу віртуальних активів; з іншого боку, ліцензійний режим для VASP відсутній через те, що спеціалізований Закон про віртуальні активи № 2074-IX від 17 лютого 2022 року так і не набрав чинності. Це породжує правовий вакуум, у якому торгівля, обмін та зберігання криптоактивів дозволені, але не ліцензовані та не знаходяться під спеціалізованим наглядом.

Нормативна основа поточного режиму визначається трьома ключовими елементами. По-перше, Цивільним кодексом України, стаття 179-1 якого класифікує віртуальні активи як «цифрові речі» (цифровий об'єкт), що існують виключно в цифровому середовищі та мають майнову цінність. Ця класифікація встановлює за замовчуванням статус товару, що дозволяє як фізичним, так і юридичним особам володіти та передавати цифрові об'єкти. По-друге, законодавством з ПВК, яке відображає визначення FATF та обов'язки щодо моніторингу: суб'єкти, залучені до обміну, переказу або зберігання віртуальних активів, кваліфікуються як VASP та підпадають під вимоги фінансового моніторингу. Поріг обов'язкової ідентифікації для переказів — 30 000 гривень; для транзакцій понад приблизно 400 000 гривень — обов'язкове повідомлення до Держфінмоніторингу. По-третє, Кабінет Міністрів України Постановою № 856 від 18 вересня 2019 року визначив Міністерство цифрової трансформації уповноваженим органом з розвитку ринку віртуальних активів. Саме цьому міністерству наразі підзвітні VASP щодо виконання зобов'язань з ПВК.

Законопроєкт № 10225-д, поданий 24 квітня 2025 року та прийнятий у першому читанні, є ключовим вектором трансформації, спрямованим на приведення українського регулювання у

[9] https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/

відповідність до європейських стандартів, насамперед MiCA. Найбільш значущою зміною концептуального характеру є запровадження ширшого технологічно-нейтрального визначення віртуальних активів: вони трактуються як тип цифрових речей, створених, збережених і переданих з використанням технології розподіленого реєстру або аналогічних технологій. Це визначення усуває прив'язку до конкретних технологій та забезпечує стійкість рамки до інновацій. Законопроєкт вводить класифікацію токенів, яка відображає структуру MiCA: токени, прив'язані до активів; токени електронних грошей (EMT); та інші віртуальні активи, — з диференційованим регуляторним режимом для кожної категорії.

Законопроєкт запроваджує дворівневу регуляторну архітектуру: Національний банк України (НБУ) встановлює правила авторизації для послуг з обміну віртуальних активів на грошові цінності; другий регулятор, призначений Кабінетом Міністрів, матиме повноваження щодо інших видів послуг VASP. VASP визначається як юридична особа (ТОВ, АТ або іноземна юридична особа), що на професійній основі надає послуги з обігу віртуальних активів та отримала відповідну авторизацію. Перелік послуг, що потребують ліцензування, є вичерпним і охоплює: зберігання та адміністрування віртуальних активів від імені клієнтів; операції торгових платформ; обмін криптоактивів на фіатну валюту та між собою; виконання клієнтських доручень; а також інші визначені послуги. Іноземні VASP матимуть право обслуговувати клієнтів в Україні лише за умови «спрощеної авторизації» і за умови, що базуються у юрисдикціях, схвалених регулятором (зокрема, в ЄС або інших юрисдикціях із white-list).

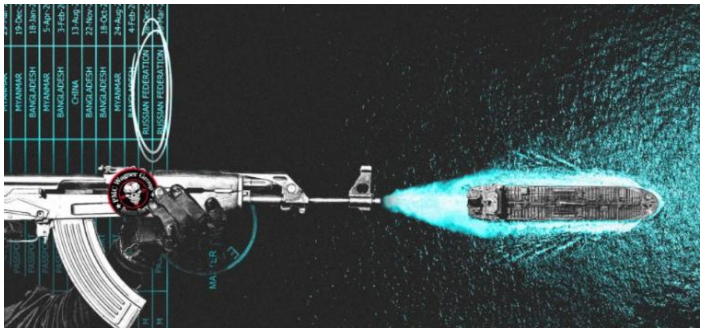
Податкова реформа, запропонована Законопроєктом № 10225-д, є одним із найбільш практично значимих елементів для учасників ринку. Поточна ситуація характеризується застосуванням загальних податкових принципів: доходи фізичних осіб від обміну криптоактивів на фіатну валюту оподатковуються за ставкою 18% ПДФО + 5% військовий збір без будь-яких спеціальних пільг. Законопроєкт змінює цю ситуацію принципово: фізичні особи оподатковуватимуться на основі чистого річного доходу (продажі мінус задокументовані витрати на придбання); звільнення від оподаткування передбачені для обміну крипто-в-крипто, для річних продажів до одного мінімального розміру заробітної плати, а також для токенів, отриманих через майнінг, аірдропи та первинне розміщення. Передбачений перехідний пільговий режим у перший рік дії закону: активи, придбані до набрання законом чинності, можуть оподатковуватися за зниженою ставкою 5% ПДФО (плюс 5% військовий збір). Юридичні особи підпадають під стандартний 18% корпоративний податок з обов'язковим окремим розрахунком прибутків і збитків від операцій з криптоактивами. VASP можуть ставати резидентами спеціального правового та податкового режиму Diia.City, що дозволяє суттєво знизити податкове навантаження на фонд оплати праці (до 5%), однак зобов'язані використовувати стандартну ставку 18% для операцій з віртуальними активами, а підприємці на спрощеній системі оподаткування ("єдиному податку") позбавлені права здійснювати операції з криптоактивами під загрозою переведення на загальну систему.

AML-рамка для VASP в Україні є операційно дієвою вже з 2020 року. У рамках поточного законодавства VASP зобов'язані: мати AML-програми; здійснювати ідентифікацію та верифікацію клієнтів; зберігати записи; призначати відповідальних працівників. Принцип Travel Rule щодо передачі інформації про відправника та отримувача при переказах вже відображений у AML-рамці. Після набрання чинності Законопроєктом № 10225-д нагляд за дотриманням AML-вимог перейде до профільних фінансових регуляторів, що матимуть повноваження встановлювати додаткові вимоги, накладати санкції та відкликати ліцензії. Важливим елементом інноваційного середовища є функціонуюча регуляторна пісочниця для блокчейну та AI, запроваджена Постановою Кабміну № 1238 від 29 жовтня 2024 року, що діє до жовтня 2026 року та дозволяє стартапам тестувати технології у контрольованих умовах за підтримки Міністерства цифрової трансформації, Ukrainian Startup Fund та UK DIGIT. Законопроєкт №

10225-д явно не передбачає нових регуляторних пісочниць, однак поточний механізм продовжує функціонувати у перехідний період.

Звіти окремих інституцій та експертів

Тіньовий флот: Як ветерани ГРУ та «Вагнера» перетворюють нафтові танкери на інструмент гібридної війни [10]



У холодних водах Балтійського моря, де останнім часом зростає кількість провокацій з боку російської авіації, а напруга між росією і НАТО сягнула рівня, якого Європа не бачила з часів Карибської кризи, розгортається нова, прихована фаза конфлікту. Її головними дійовими особами стали не бойові кораблі, озброєні крилатими ракетами, не ескадрильї бомбардувальників, що патрулюють кордони, і не диверсійні групи, які вночі висаджуються на безлюдні береги. Натомість, роль передового загону гібридної війни кремля виконують старі нафтові танкери, які щодня перевозять підсанкційну російську нафту через один із найбільш стратегічно важливих морських шляхів світу.

Однак, як з’ясували журналісти Delfi, Helsingin Sanomat, iStories та OCCRP у своєму масштабному розслідуванні, під палубами цих непоказних плавучих посудин ховається дещо набагато небезпечніше, ніж просто «чорне золото», що живить воєнну машину. росія системно і цілеспрямовано перетворює свій так званий «тіньовий флот» на мілітаризовану силу стримування, розміщуючи на борту ветеранів із бойовим досвідом, кадрових співробітників Головного розвідувального управління (ГРУ) та колишніх найманців сумнозвісної приватної військової компанії «Вагнер». Це явище, яке західні аналітики вже охрестили "плавучими форпостами кремля", кардинально змінює баланс сил та ризиків у регіоні, де проходять життєво важливі комунікаційні артерії Європи.

Аналіз двадцяти танкерів, що виходили з російських портів на Балтиці, зокрема з ключового терміналу в Усть-Лузі, виявив тривожну закономірність, яка простежується з липня 2025 року. Починаючи з цього періоду, на борту майже кожного такого судна, незалежно від його країни реєстрації, віку чи типу вантажу, почали з'являтися додаткові пасажири. У офіційних документах, які подаються портовій владі, вони значаться як «понаднормові» (supernumeraries) — технічний термін для позначення осіб, які не входять до стандартного екіпажу судна, але тимчасово перебувають на борту. Навпроти їхніх імен у графі «кваліфікація» або «наявність морського диплома» красується лише суха і красномовна позначка: NA — not available, тобто "відсутня". Вони не мають жодних морських документів, не вміють керувати судном у шторм і не знають правил міжнародного судноплавства, але мають те, що є набагато ціннішим в нинішніх умовах: бойовий досвід, навички ведення розвідки та прямі зв'язки з найпотужнішими силовими структурами російської федерації. Примітно, що у обмеженій вибірці суднових маніфестів для танкерів, які ходили Чорним морем чи Тихим океаном у той самий період, такої практики виявлено не було, що вказує на цілковиту унікальність балтійського напрямку як арени гібридного протистояння.

[10] https://www.occrp.org/en/investigation/from-wagner-to-gru-russian-military-men-are-manning-moscows-shadow-fleet

Історія танкера «Kira K», який у грудні 2025 року завантажував чергову партію сирої нафти, що належить підсанкційному російському гіганту «Лукойл», у порту Усть-Луга, що глибоко в східній частині Фінської затоки, є найбільш яскравою і показовою ілюстрацією цієї нової стратегії Кремля. Судно мало змішаний інтернаціональний екіпаж з моряків з М'янми, Китаю та Бангладешу — типова практика для тіньового флоту, який наймає дешеву робочу силу з країн, що не приєдналися до санкцій. Однак, окрім них, у списку команди фігурували двоє громадян росії — 45-річний Олександр Каменєв та 48-річний Денис Єнін. Обидвоє, як вдалося встановити журналістам, є ветеранами «Групи Вагнера» — тієї самої сумнозвісної приватної армії, яка майже десятиліття виконувала найбрудніші та найскладніші завдання кремля у найгарячіших точках планети, від донецького аеропорту та сирійської Пальміри до віддалених куточків Центральноафриканської Республіки, Лівії та Малі, де таких бійців офіційно звинувачують у масових порушеннях прав людини, стратах і мародерстві.

Показовою є реакція фігурантів на спроби журналістів отримати коментар. Єнін, із яким зв'язалися через Telegram, спочатку категорично заперечував свою присутність на судні, а після отримання незаперечних доказів просто припинив спілкування. Його співвітчизник Каменєв взагалі проігнорував усі запити, надіслані на його електронну пошту.

Однак присутність на борту «вагнерівців» — це лише вершина величезного айсберга, який становить собою гібридна загроза в Балтійському морі. Журналістам міжнародного консорціуму вдалося ідентифікувати щонайменше 17 росіян, які перебували на борту різних підсанкційних танкерів, не маючи при цьому належних морських кваліфікаційних документів. З цього числа тринадцять осіб мають безпосереднє документально підтверджене відношення або до ПВК «Вагнер», або до елітних державних органів безпеки, зокрема до Головного розвідувального управління (ГРУ) Генштабу ЗС РФ.

Джерела в європейських спецслужбах, які побажали залишитися анонімними через чутливість інформації, підтвердили кореспондентам, що ці люди є частиною системи, а не випадковими пасажирами. Так, 50-річний Олександр Малахов, який здійснював рейси на танкері, виявився ветераном 22-ї окремої гвардійської бригади спеціального призначення ГРУ — елітного підрозділу військової розвідки, дислокованого в Ростовській області, який брав участь у найсекретніших операціях росії за кордоном. Факт його служби підтверджується не лише даними європейської розвідки, а й витоками даних, які вказують, що його зареєстрована адреса збігається з розташуванням цієї військової частини. Разом з Малаховим на борту іншого танкера працював його напарник — колишній найманець «Вагнера» Віктор Александров, чиє минуле легко підтверджувалося його власними фотографіями в соціальних мережах, де він позує в камуфляжній формі на тлі сирійського ландшафту.

Розслідування виявило ще глибші зв'язки з офіційними структурами. На танкері «Kira K» в серпні 2025 року була помічена ще одна пара: 50-річний Дмитро Фролов та 38-річний Юрій Цвєтков. Згідно з даними прикордонної служби, які опинилися у розпорядженні журналістів, ці двоє не просто випадково опинилися на одному судні. Вони мають давню історію спільних подорожей, зокрема, у 2022 та 2023 роках вони разом літали військово-транспортними літаками ВПС росії. Коли журналісти вийшли на зв'язок із Фроловим, він спочатку також відкинув факт свого перебування в морі, але отримавши докази, зреагував украй агресивно, пригрозивши співрозмовнику здачею органам ФСБ. Це свідчить не лише про обізнаність цих людей про свою причетність до державних таємниць, а й про специфічну "корпоративну етику" мовчання, яка панує в цих колах.

Інший підсанкційний танкер, відомий під назвою «Lebre», перевозив на своєму борту "техніків", які, за даними Служби зовнішньої розвідки України, мали пряме відношення до роботи в Міністерстві оборони рф та в оборонному відомстві самопроголошеної невизнаної

Придністровської молдавської республіки, яка фактично перебуває під військовою окупацією росії.

Менеджер судна, компанія Anchor Elite Shipmanagement, намагалася мінімізувати значення цих фактів. У своїй заяві вони запевняли, що не можуть підтвердити "звинувачення", висунуті в статті, і що присутність цих людей на борту "жодним чином не пов'язана з військовою діяльністю чи діяльністю приватних військових компаній". Натомість, за версією менеджменту, ці особи були залучені виключно для виконання "камбузних обов'язків" та "робіт, пов'язаних з палубою". Ці заяви виглядають щонайменше наївно і викликають лише іронію на тлі бойового минулого їхніх "працівників кухні" та зв'язків з військовою розвідкою. Цікаво, що один із фігурантів, якого українська розвідка пов'язувала з Міноборони рф, у коментарі журналістам також усе заперечив, назвавшись кухарем, проте підтвердив, що інший росіянин, який перебував на борту як "технік", справді ніс там охоронні функції.

Навіть французька влада, яка у вересні 2025 року затримала один із танкерів тіньового флоту біля свого узбережжя, не уникнула зіткнення з цим новим явищем. За даними офіцера розвідки з країн Балтійського регіону, який погодився говорити на умовах анонімності, на борту того судна перебував діючий (на той час) десантник російської армії Станіслав Бабичев. Журналісти виявили його профіль у соціальних мережах, де як освіту було вказано 332-гу школу прапорщиків Повітряно-десантних військ — елітний навчальний заклад, що готує командний склад для ВДВ. Бабичев на запити не відповів, але сама по собі присутність військовослужбовця ВДВ на цивільному танкері є грубим порушенням міжнародних норм і свідчить про високий рівень координації між тіньовим флотом та міністерством оборони рф.

Навіщо ж росії знадобилося перетворювати звичайні нафтові танкери на плавучі казарми для спецпризначенців, розвідників і найманців? Відповідь на це питання лежить у площині складної комбінації гібридної війни, економічного виживання та геополітичного шантажу. Балтійське море є критично важливим маршрутом для експорту російської нафти. За даними Київської школи економіки, близько 40% всього обсягу сирої нафти, яку росія продає за кордон, проходить саме через цей вузький шлях, оточений країнами НАТО. Ці гроші, які надходять до бюджету щодня, є буквально кров'ю, що живить воєнну машину кремля і дозволяє їй продовжувати загарбницьку війну проти України.

Однак після запровадження безпрецедентних санкцій з боку Заходу, включаючи нафтове ембарго та механізм обмеження ціни (price cap), росія змушена використовувати для експорту так званий "тіньовий флот". Це сотні старих, часто технічно несправних суден з непрозорою структурою власності, які ходять під "зручними прапорами" (Ліберія, Маршаллові Острови та інші) і не користуються західними страховими та транспортними послугами. Саме ці судна стають вразливою мішенню для контролю з боку країн НАТО, які мають право і можливість інспектувати підозрілі судна у своїх економічних зонах.

За даними офіцерів розвідки з кількох європейських країн, саме для захисту цього життєво важливого економічного артеріалу на борт суден і були відправлені загони, які на Заході вже отримали назву "суднові охоронні команди" (vessel protection teams). Їхнє головне завдання — не стільки захист від піратів, скільки фізичне ускладнення або повне унеможливлення будь-якої спроби дострокової інспекції, блокування чи арешту танкера європейською владою або військово-морськими силами країн Балтії.

Як зазначив керівник розвідувального центру Сил оборони Естонії полковник Антс Ківісельг, мета цієї діяльності полягає в захисті дохідної бази російської федерації від потенційних загроз, будь то диверсії, чи будь-яке інше втручання з боку Заходу. «Наявність на борту двох потенційно озброєних осіб з бойовим досвідом, безумовно, кардинально змінює наш розрахунок ризиків, коли ми повинні приймати рішення, чи зупиняти танкер, чи проводити його огляд», — визнав у розмові з журналістами високопоставлений європейський офіцер розвідки. За його словами, в

кремлі свідомо роблять ставку на те, що країни НАТО на Балтиці будуть значно обережнішими у своїх діях, побоюючись збройного опору та можливої ескалації, яка може призвести до людських жертв і міжнародного скандалу.

Втім, колишній високопосадовець ЦРУ, спеціаліст з російських спецслужб та збройних сил Шон Вісессер вважає, що версія про виключно оборонну функцію цих "техніків" є надто спрощеною і наївною. На його думку, розміщення на борту кадрових військових розвідників та бойових офіцерів перетворює ці судна на ідеальні платформи для проведення розвідувально-диверсійних операцій. Він звертає увагу на разючий факт: за останні два роки в Балтійському морі сталося більше пошкоджень підводних кабелів, ніж будь-де в світі за аналогічний період. "Тіньовий флот" може бути безпосередньо причетний до цих диверсій на критичній підводній інфраструктурі Європи. Танкер, який щодня повільно перетинає ключові морські шляхи, має ідеальне прикриття для скидання підводних дронів, ведення гідроакустичної розвідки узбережжя, картографування дна, або навіть для підготовки диверсій на газопроводах та енергетичних кабелях. У цьому контексті нафта стає не лише метою, а й ідеальним прикриттям, яке дозволяє цим суднам безперешкодно перебувати в чутливих водах.

Аналітики фінської служби безпеки SUPO припускають, що озброєні групи на борту виконують ще одну важливу функцію, яку можна назвати "політичним наглядом". Вони є своєрідними комісарами та наглядачами для найманих іноземних екіпажів. Моряки з Південно-Східної Азії, які масово працюють на російських суднах через низьку зарплату, не мають жодної лояльності до режиму і можуть не підкорятися наказам іноземної влади або навіть саботувати накази капітана під час кризової ситуації. Охоронці з бойовим досвідом, озброєні і готові застосувати силу, гарантують, що судно йтиме туди, куди скаже москва, і що жоден член екіпажу не стане співпрацювати з владою ЄС. Крім того, вони можуть виступати в ролі "зв'язкових" для російських військових кораблів, які часто супроводжують ці танкери, забезпечуючи координацію дій.

Окремо слід звернути увагу на кадровий конвеєр, який постачає цих "фахівців". За даними Служби зовнішньої розвідки України, найманням персоналу для тіньового флоту займаються дві російські приватні охоронні компанії: RSB Group та Moran Security Group. RSB Group, на сайті якої зазначено, що вона "захистила десятки торгових і наукових російських та іноземних суден", відома наймом колишніх офіцерів російської розвідки та інших військовослужбовців. Обидві компанії вже потрапили під санкції США та ЄС за надання послуг російським державним підприємствам та підготовку підрозділів для війни в Україні. Вони не відповіли на запити журналістів про коментарі, що є стандартною практикою для структур, які працюють у тіні.

Таким чином, масштабне розслідування OCCRP та його партнерів малює перед нами цілісну і глибоку картину, де економічні

Висновки:

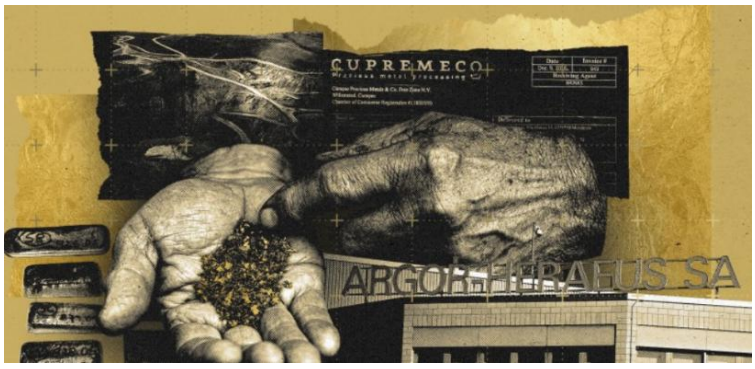
- **Мілітаризація тіньового флоту:** росія системно розміщує на борту танкерів, що перевозять санкційну нафту через Балтійське море, додаткові "команди захисту суден", до складу яких входять ветерани ПВК "Вагнер" та кадрові співробітники ГРУ.
- **Стримування Заходу через ескалацію:** Головною метою присутності військових на борту є фізичне ускладнення або унеможливлення інспекцій, блокування чи арешту танкерів з боку країн НАТО на Балтиці.
- **Багатофункціональність "техніків":** Окрім охоронних функцій, ветерани спецслужб на танкерах, ймовірно, виконують розвідувальні завдання, зокрема збір даних про військову інфраструктуру країн НАТО.
- **Системність та державна координація:** Виявлені зв'язки з ГРУ, Міноборони рф та ПВК "Вагнер", а також їхнє пересування військовими літаками, доводять, що ця практика не є випадковою, а координується на державному рівні.

санкції, військове протистояння, розвідувальна діяльність та гібридні загрози переплелися в один тісний і небезпечний вузол.

росія, відрізана від традиційних фінансових потоків і зіткнувшись із потужною військовою підтримкою України з боку Заходу, не просто контрабандою вивозить свою нафту в обхід санкцій. Вона створює принципово новий, багатофункціональний інструмент гібридної війни, системно мілітаризуючи власний торговельний флот і перетворюючи звичайні танкери на багатоцільові платформи: розвідувальні судна, диверсійні бази, об'єкти стримування, будь-яке затримання яких загрожує прямим військовим зіткненням.

У Балтійському морі, де інтенсивність судноплавства є однією з найвищих у світі і де проходять життєво важливі комунікації між країнами-членами НАТО, ця нова стратегія створює постійний, небезпечний фон для потенційних інцидентів, остаточно стираючи тонку межу між мирним торговельним судном і військовим об'єктом, що несе загрозу. І поки західні уряди та військові альянси намагаються знайти адекватні юридичні, дипломатичні та військові способи протидії цьому явищу, танкери з ветеранами ГРУ та «Вагнера» на борту продовжують свій небезпечний шлях, перевозячи через вразливі води Європи не лише заборонену нафту, а й нові, досі небачені гібридні загрози, перетворюючи кожен рейс на акт гібридної агресії.

Криваве золото Венесуели: Як мільярди доларів потрапляють на світовий ринок [11]



Протягом останнього десятиліття міжнародна спільнота, здавалося б, доклала титанічних зусиль, щоб перекрити кисень збройним конфліктам, які фінансуються за рахунок видобутку так званих "конфліктних мінералів". Були запроваджені багатосторонні угоди, розроблені детальні рекомендації Організацією економічного співробітництва та розвитку (ОЕСР), створені системи сертифікації на кшталт Лондонської асоціації ринку дорогоцінних металів (LBMA). Однак гучне розслідування, проведене OCCRP та його партнерами, з безжальною ясністю демонструє, як ця, здавалося б, міцна система дає глибокі тріщини, дозволяючи величезним обсягам "брудного" металу не просто просочуватися, а безперешкодно вливатися в легальний світовий обіг.

В епіцентрі цього розслідування опинилися десятки тонн венесуельського золота, яке, пройшовши складний, багатоступеневий маршрут через карибський острів Кюрасао та одну з швейцарських афінажних фабрик, осіло в кінцевому підсумку в продуктах глобальних технологічних гігантів — Apple, Tesla та Nvidia. Ця історія є не просто розповіддю про злочини, а кричущою ілюстрацією системних вад, які продовжують існувати в індустрії.

Все починається з доволі несподіваного спостереження, яке, втім, для досвідчених аналітиків одразу стало "червоним прапорцем". Кюрасао — невеличкий острів, загублений у Карибському морі, з населенням близько 150 тисяч осіб, відомий насамперед своїми мальовничими краєвидами, колоніальною архітектурою та як улюблене місце для весільних подорожей і круїзних лайнерів.

[11] https://www.occrp.org/en/investigation/conflict-tainted-venezuelan-gold-entered-world-market-through-caribbean-island-documents-indicate

Це типовий туристичний рай, але аж ніяк не промисловий центр. Тому для фахівців LBMA стало шокуючим відкриттям, коли в статистичних звітах вони побачили, що цей клаптик суші, де немає жодної золотої шахти і ніколи не було розвиненого ювелірного виробництва, раптово перетворився на одного з ключових гравців світового ринку золота. За даними бази даних ООН Comtrade, з острова було експортовано понад 110 метричних тонн золота, сукупна вартість якого сягала 4,5 мільярда доларів.

Щоб усвідомити масштаб цих цифр, досить сказати, що це майже вдвічі більше за річний видобуток Колумбії — однієї з найбільших золотодобувних країн Південної Америки. "Не було жодної розумної причини, чому такі величезні потоки мали б проходити через Кюрасао. Якщо ми подивимося на обсяги, то там просто не може бути стільки ювелірних магазинів, щоб виправдати їх. Для нас було абсолютно очевидно, що це нелегітимне джерело, і ми неодноразово наголошували на цьому", — зізнається у розслідуванні Алан Мартін, керівник відділу постачання LBMA.

Розгадка цієї географічної аномалії крилася зовсім поруч — лише за 70 кілометрів на південь, на узбережжі Південної Америки, де розташована Венесуела. Країна, яка колись пишалася своїми нафтовими багатствами, на той час переживала катастрофічне падіння економіки та стрімке сповзання у прірву гуманітарної кризи. Після націоналізації золотодобувної галузі президентом Уго Чавесом у 2011 році, яка де-юре зробила все золото державною власністю, де-факто настав період хаосу. З падінням світових цін на нафту та запровадженням міжнародних санкцій, режим Ніколаса Мадуро почав розглядати золото як "нову нафту" — єдиний рятівний актив, здатний приносити валютну виручку в обхід фінансової системи. У 2016 році було створено так звану Гірничодобувну дугу Оріноко — колосальну територію площею 112 тисяч квадратних кілометрів, яку було фактично віддану на поталу нелегальному та напівлегальному видобутку золота та алмазів. Це рішення спровокувало екологічну катастрофу планетарного масштабу та розв'язало руки криміналітету.

Тисячі квадратних кілометрів венесуельської Амазонії були вирубані та спалені, річки отруєні ртуттю, яка використовується для амальгамації золота, що призвело до отруєння риби та знищення джерел прісної води для місцевих громад. Але найжахливішими були соціальні наслідки. За даними детальних звітів Управління Верховного комісара ООН з прав людини та Державного департаменту США, шахти дуги Оріноко перетворилися на зони беззаконня, де колумбійські партизани, міжнародні злочинні синдикати та корумповані підрозділи венесуельських військових вели криваву боротьбу за контроль над територіями. У цьому пеклі процвітала масова експлуатація дитячої праці, сексуальне рабство тисяч жінок і дівчат, тортури та позасудові страти незгодних або тих, хто намагався втекти. За оцінками місцевого відділення Transparency International, близько 70 відсотків усього золота, видобутого в країні в цей період, вивозилося контрабандно, оскільки уряд зробив незалежну торгівлю цим металом незаконною, намагаючись монополізувати всі фінансові потоки.

Саме в цьому кривавому контексті на сцені з'являється компанія Curaçao Precious Metals & Co., відома під скороченою назвою Cupremeco. Зареєстрована у вільній економічній зоні Кюрасао, яка пропонувала податкові пільги та спрощені митні процедури, Cupremeco ідеально підходила для відмивання брудного золота. Заснована венесуельським брокером Ектором Оскаром Кастельйоном та Маріо Патаро, представником впливової італійської родини, яка мігрувала до Панами після Другої світової війни і стала великим гравцем на регіональному ринку дорогоцінних металів. Як згодом пояснив Патаро в інтерв'ю, Cupremeco була створена як торговельна фірма, що транспортувала вантажі золота від "клієнтів" з Південної Америки для продажу в Швейцарію.

Однак прямий продаж золота з Венесуели до Швейцарії, навіть через Кюрасао, викликав би надто багато запитань у служб комплаєнсу великих афінажних заводів. Тому була вибудована

складна, багаторівнева і, як показав час, вкрай ефективна схема, яку один з її учасників у судовому засіданні цинічно назвав "комплаєнс-рішенням". Офіційно золото продавалося не Cupremeco безпосередньо, а швейцарській компанії-посереднику PMS SA (Precious Metals Services), якою володів бізнес-партнер Патаро, Марко Бріккола.

PMS SA, технічно виступаючи прямим постачальником престижного швейцарського афінажного заводу Argor-Heraeus, ніколи фізично не отримувала і не бачила золота. Його доставляли логістичною компанією Brink's просто з Кюрасао до воріт заводу в Мендрізіо. Уся ця конструкція була потрібна лише для того, щоб створити паперовий слід, який би влаштовував аудиторів.

Як недвозначно пояснив у суді Ектор Кастельйон, така структура була необхідна, щоб обійти складну і тривалу процедуру "Знай свого клієнта" (KYC), яку Argor-Heraeus застосовував до нових прямих постачальників. «Для того, щоб різні люди могли відкривати великі рахунки на різних афінажних заводах, потрібно пройти процедуру ідентифікації клієнта. Це дуже довгий і важкий процес, і не кожному це вдається. Тому ми вирішили піти іншим шляхом... Ми вирішили йти через Маріо [Патаро], а сам Маріо йде через іншу компанію, яка і доставляє товар до Argor-Heraeus у Швейцарії... Це така комплаєнс-штука», — свідчив Кастельйон.

Argor-Heraeus, один з найпрестижніших афінажних заводів світу, який пишається своєю репутацією, входить до списку "Good Delivery" LBMA і постачає золото для центробанків та інвестиційних фондів, стверджує, що діяв у повній відповідності до всіх чинних на той час правил. Юристи компанії наголошують, що вона не мала жодних ділових відносин з Cupremeco і проводила належну перевірку лише щодо свого безпосереднього контрагента — PMS SA. Вони визнають, що їм було відомо про венесуельське походження металу, але наполягають, що це було виключно "скрапове" золото — переплавлені ювелірні вироби, зубні коронки, старі монети чи промислові відходи.

За даними рахунків-фактур, отриманих журналістами, між 2012 та 2018 роками через цей сконструйований ланцюжок від Cupremeco до Argor-Heraeus надійшло золота на суму близько 2,2 мільярда доларів. Банківські записи свідчать, що PMS SA отримала від Argor-Heraeus близько мільярда доларів, залишаючи собі комісію за транзит, а решта йшла далі — на рахунки компаній, пов'язаних з венесуельськими постачальниками, їхніми родинами та наближеними особами. Один з таких постачальників, Марко Антоніо Флорес Морено, згодом став фігурантом кримінальної справи в Бразилії за звинуваченням у створенні організації, яка займалася незаконним видобутком золота у Венесуелі, контрабандою його через кордон та фальсифікацією документів, видаючи його за "скрап".

Саме питання про те, чи було це золото дійсно вторинним, чи свіжовидобутим із шахт, є ключовим для розуміння всієї схеми. Юристи Argor-Heraeus наполягають на першому, стверджуючи, що криміналістичні тести та аналіз, проведений незалежним експертом GeoBlock International на їхнє замовлення, "підтверджують поза будь-яким сумнівом, що не було жодних доказів походження з первинних джерел".

Однак цій версії суперечать одразу кілька фактів. По-перше, самі постачальники вказують на інше. Маріо Патаро у відповідь на пряме запитання журналістів відповів: "Звідки воно береться я не знаю". Натомість його бізнес-партнер Ектор Кастельйон був значно більш відвертим під присягою: "Частково з ломбардів, але переважно з копалень". По-друге, журналістам вдалося отримати результати 469 власних досліджень Argor-Heraeus, проведених для 6,5 тонн золота, імпортованого через Кюрасао, переважно у 2016 році. Ці дані містять інформацію про вміст золота та срібла в сировині, яка надійшла на завод до афінажу. Шестеро незалежних експертів-геологів, включаючи чотирьох університетських професорів, які вивчили ці дані, дійшли одностайного висновку: показники чистоти та характерні домішки з високою ймовірністю вказують на те, що це суміш рудного (шахтного) та переробленого золота.

Ця суперечка навколо хімічного складу оголює фундаментальну, глибоку ваду в системі саморегулювання золотої індустрії, яка базується на стандартах, встановлених Лондонською асоціацією ринку дорогоцінних металів (LBMA). Правила LBMA, які діяли протягом усього періоду, що розслідується, створюють дві паралельні реальності. Для первинного, рудного золота, яке видобувається з надр, діють жорсткі вимоги: афінажні заводи зобов'язані проводити комплексну перевірку всього ланцюжка постачання, починаючи від самої шахти, і негайно припиняти співпрацю, якщо виявляють будь-які порушення прав людини чи зв'язки з конфліктами.

Однак для "скрапового" золота правила були значно м'якшими: достатньо було перевірити лише безпосереднього постачальника. Логіка полягала в тому, що скрап вже був у обігу і не міг фінансувати конфлікти безпосередньо. Ця прогалина виявилася настільки широкою, що створила гігантський стимул для шахрайства: свіжовидобуте золото можна грубо переплавити в найпростіші прикраси, а потім здати як ювелірний брухт, або, що ще простіше, просто вказати в документах неправдиву інформацію про походження.

Саме тому золото, яке надходило від Cupremeco, декларувалося саме як скрап, і завдяки проходженню через швейцарського посередника PMS SA, Argor-Heraeus мав формальні підстави не копати глибше. У своїх звітах перед LBMA компанія вказувала, що отримує скрап від швейцарського імпортера, жодним чином не згадуючи ні Венесуелу, ні Кюрасао. Представники LBMA визнають, що обсяги золота з Кюрасао виглядали вкрай підозріло, і близько 2018 року вони неофіційно попросили своїх членів припинити приймати метал з цього острова. Однак на той момент "карибський коридор" уже пропрацював на повну потужність понад шість років. Лише у 2019 році, після того як британське Національне агентство з боротьби зі злочинністю (NCA) спільно з владою Каймановых островів конфіскувало чергову велику партію золота Cupremeco, визнавши її "доходами від злочину", зв'язок між Argor-Heraeus, PMS SA та Cupremeco було нарешті розірвано.

Висновки:

- **Масштабне шахрайство з походженням золота:** Протягом 2012–2018 років близько 70 тон венесуельського золота вартістю понад 2,2 мільярда доларів було вивезено через острів Кюрасао під виглядом "скрапу" (вторинної сировини).
- **Прогалини в системі сертифікації дозволили легалізувати "брудний" метал:** Швейцарський афінажний завод Argor-Heraeus, попри свою репутацію, зміг прийняти це золото завдяки прогалині в правилах LBMA, яка вимагала ретельної перевірки лише для рудного золота, але не для скрапу.
- **Золото з конфліктних зон безперешкодно потрапило до продуктів світових техно-гігантів:** Після афінажу в Швейцарії золото втратило будь-яку історію походження та було продане компаніям Apple, Tesla та Nvidia.
- **Проблема зберігається, незважаючи на заяви про реформи:** Незважаючи на те, що схему було викрито, а ланцюжок поставок розірвано у 2019 році, експерти та Єврокомісія констатують, що система саморегулювання галузі залишається недосконалою, що залишає можливості для подібних маніпуляцій.

Однак головна трагедія і головний системний ризик полягає в тому, що золото, яке вже пройшло афінаж на такому поважному заводі, як Argor-Heraeus, стає магічним чином "чистим" і легітимним. Воно отримує тавро "Good Delivery", яке є золотим стандартом якості та законності для світового ринку. Після цього воно повністю втрачає свою ідентичність і зникає в загальній масі металу, що обертається на біржах, у сховищах банків і на промислових підприємствах. Як тільки афінажний завод переплавляє його в зливки зі своїм фірмовим штампом, воно стає легітимним, і втрачається будь-яка можливість його відстежити. Воно вливається в міжнародну монетарну

систему, в побутову електроніку, ювелірні вироби та все інше. Це кінець шляху для інформації про походження.

І саме це стало фінальним, логічним завершенням маршруту венесуельського золота. Десятки тонн металу, який, за всіма ознаками, фінансував репресивний режим Ніколаса Мадуро, врешті-решт осіли в найсучасніших продуктах світових технологічних лідерів.

У своїх щорічних звітах для Комісії з цінних паперів і бірж США (SEC) такі компанії, як Apple, Tesla та Nvidia, відкрито вказували Argor-Heraeus як частину свого ланцюжка постачання золота саме в той період, коли туди надходило золото з Венесуели через Кюрасао. Жодних звинувачень на адресу цих компаній, звісно, немає. Вони діяли в межах чинних правил, сумлінно купуючи сертифікований метал у перевіреного, сертифікованого LBMA постачальника з бездоганною репутацією. Однак саме цей факт — бездоганна поведінка кожного окремого гравця в межах хибних правил гри — робить цю історію особливо показовою.

Оцінка Європейської Комісії, опублікована у 2025 році, показала, що навіть після низки реформ та оновлень стандарти LBMA залишаються лише "частково узгодженими" з більш жорсткими нормами Європейського Союзу. Експерти ЄК дійшли невтішного висновку, що система внутрішнього контролю, на якій базується саморегулювання галузі, "не працює ефективно на практиці". Це визнання того, що покладання на добру волю корпорацій та їхні власні аудити не є достатньою гарантією.

Історія з венесуельським золотом є не просто історією минулого. Це суворий і невблаганний сигнал про те, що без докорінної зміни правил гри — запровадження обов'язкового, незалежного комплексного аудиту всього ланцюжка постачання, незалежно від типу сировини, повної заборони на використання офшорних зон для маскування походження товарів та встановлення реальної юридичної відповідальності для всіх учасників ринку — подібні схеми процвітатимуть і надалі. Вони продовжуватимуть перетворювати далекі, невидимі для більшості катастрофи на чистий прибуток для глобальних корпорацій, водночас дозволяючи споживачам залишатися у щасливому невіданні щодо справжньої ціни речей, якими вони користуються щодня.

Тиха адаптація: Як європейський кокаїновий ринок змінює правила гри [12]

Європейський ринок кокаїну, який десятиліттями вважався відносно стабільним і прогнозованим сегментом транснаціональної організованої злочинності, вступив у фазу глибокої та фундаментальної трансформації.

Те, що ще нещодавно функціонувало за відносно зрозумілими правилами — з визнаними центрами імпорту, усталеними маршрутами та ієрархічно структурованими злочинними угрупованнями — сьогодні перетворилося на надзвичайно адаптивну, децентралізовану та, що найважливіше, неймовірно стійку до зовнішнього тиску екосистему.

Документ GI-TOC, заснований на польових дослідженнях, інтерв'ю з представниками правоохоронних органів і безпосередньо кримінального середовища, а також на моніторингу даркнет-платформ та зашифрованих

[12] https://globalinitiative.net/wp-content/uploads/2026/03/Observatory-of-Organized-Crime-in-Europe-European-Drug-Trends-Monitor-Issue-4-GI-TOC-March-2026.pdf

месенджерів, малює картину ринку, який не просто виживає в умовах безпрецедентного тиску, а процвітає, радикально змінюючи свою структуру, географію та бізнес-моделі. В основі цього аналізу — п'ять ключових тенденцій, які у своїй сукупності вказують на тектонічний зсув: від падіння видимої ефективності правоохоронної діяльності до формування нового, гнучкішого і небезпечнішого обличчя європейського наркобізнесу.

На перший, поверхневий погляд, офіційна статистика може створити оманливе, але політично привабливе враження беззаперечних успіхів у боротьбі з наркотрафіком. Протягом 2024 та 2025 років обсяги вилученого кокаїну в головних морських воротах Європи — бельгійському порту Антверпен та нідерландському Роттердамі — зазнали різкого падіння після рекордних показників, досягнутих у 2023 році. Для неуважного спостерігача це могло б стати сигналом про ефективність посилених заходів безпеки, вдосконалення скануючих систем та міжнародної координації. Однак, як переконливо доводять автори звіту, ці оманливі цифри аж ніяк не відображають реального скорочення масштабів ринку, а є яскравим свідченням його глибокої стратегічної адаптації до нових умов.

Кримінальні мережі, які контролюють трансатлантичні потоки, зробили чіткий прорахунок і свідомо відмовилися від стратегії гігантських, консолідованих партій, які були зручною мішенню для правоохоронців, на користь дроблення вантажів на значно менші, вагою до 100 кілограмів. Це призвело до парадоксальної, але дуже показової ситуації: загальна тоннажність вилучень впала, проте кількість окремих випадків конфіскації зросла. Така фрагментація логістики — це не ознака слабкості чи вимушеної поступки, а геніальний у своїй цинічності прорахований ризик-менеджмент. Концепція "розрахованих втрат" (calculated losses) стала новою операційною нормою для європейських наркоторговців. Злочинці тепер свідомо закладають можливі конфіскації окремих дрібних партій у свої бізнес-моделі, прагнучи не захистити кожен окремий вантаж ціною неймовірних зусиль, а забезпечити безперервність і передбачуваність загального потоку товару, зберігаючи стабільність постачання навіть у разі часткових втрат.

Найпереконливішим та неспростовним доказом того, що європейський ринок аж ніяк не відчуває дефіциту, а навпаки, переповнений пропозицією, є динаміка ціноутворення, яка набула безпрецедентного характеру. Якщо на оптовому рівні ціни в Бельгії, Нідерландах та Іспанії впали до історичних мінімумів, сягнувши позначки €15 000–16 000 за кілограм порівняно з €25 000+ лише кілька років тому, то на роздрібному ринку вартість одного граму для кінцевого споживача залишилася напрочуд стабільною, міцно тримаючись у коридорі €45–65 залежно від міста, країни та особистих зв'язків. Цей унікальний розрив між оптовою ціною, що стрімко падає, і роздрібною ціною, що застигла на місці, створив безпрецедентну маржу прибутку для всіх посередників у ланцюжку, особливо на рівні дрібних гуртовиків та роздрібних дилерів.

Водночас, ця зовнішня стабільність ціни приховує під собою іншу, не менш важливу зміну в структурі споживання. За ті самі умовні €50 покупець сьогодні отримує значно меншу фізичну кількість речовини — лише 0.6–0.7 грама, тоді як у період 2021–2024 років це було 0.9–1 грам. Однак цей менший обсяг із лишком компенсується драматичним стрибком чистоти продукту. Якщо раніше вміст чистого кокаїну в "вуличних" зразках, які перевірялися службами моніторингу в Бельгії, Нідерландах, Франції, Іспанії та Італії, коливався на рівні 30–40%, то тепер він стабільно сягає 70–80%, а в Бельгії медіанний показник чистоти взагалі становить вражаючі 82%, причому в окремих зразках, вилучених у кур'єрів, цей показник наближається до 97%. Ринок, перенасичений високоякісним, майже лабораторним продуктом, більше не потребує сильного розрідження дешевими домішками, або ризикованого підвищення цін, щоб компенсувати дефіцит. Навпаки, він функціонує в умовах хронічної надлишкової пропозиції, яка дозволяє диктувати умови та максимізувати прибуток не за рахунок дефіциту, а за рахунок обсягів.

Саме цей структурний надлишок призводить до ще одного визначального зрушення: значна, і дедалі більша, частка доданої вартості тепер створюється безпосередньо на європейському

континенті. Якщо вирощування листя коки, звісно, залишається виключною прерогативою Андського регіону Південної Америки, то ключові етапи вторинної обробки, що раніше відбувалися переважно в країнах походження — розрідження, перекристалізація, пресування в стандартні блоки та навіть створення впізнаваних кримінальних брендів через нанесення логотипів — дедалі частіше виконуються на території Європи. У 2024 році лише в Нідерландах було виявлено та ліквідовано 24 об'єкти, прямо пов'язані з промисловим виробництвом або обробкою кокаїну, що на три більше, ніж роком раніше. Іспанія, Бельгія, а останнім часом навіть Франція та Польща фігурують у зведеннях Європолу як місця розташування підпільних лабораторій, де латиноамериканські «кухарі» діляться своїми знаннями з місцевими злочинцями.

Особливістю цього нового етапу локалізації стало масове та стрімке використання нового наповнювача — прокаїну. Цей відносно дешевий місцевий анестетик, який у промислових масштабах імпортується з Китаю, має унікальну властивість: при кристалізації він майже ідеально імітує характерний перламутровий блиск високоякісного, добре очищеного кокаїну, а при тестуванні невеликою кількістю на ясна викликає схоже оніміння, вводячи в оману навіть досвідчених покупців. Його використання в європейських лабораторіях зросло настільки, що в Нідерландах у 2024 році прокаїн став найпоширенішим наповнювачем, уперше випередивши традиційні левамізол, фенацетин та кофеїн.

Ця локалізація виробництва дає змогу злочинним мережам бути неймовірно гнучкими: швидко реагувати на дії поліції, змінювати рецептуру залежно від наявності прекурсорів та створювати кілька різних "сортів" продукту з різною чистотою, максимізуючи прибутки за рахунок сегментації ринку. Як цинічно зазначило одне з джерел у кримінальному середовищі під час інтерв'ю, "кокаїн прибуває так швидко і в таких обсягах, що ми навіть не встигаємо його розрізати на березі", і тепер "кожен займається власною кухнею" вже на місці, перетворюючи звичайні гаражі та склади на міні-заводи.

Така професіоналізація ринку супроводжується його безпрецедентним демографічним та організаційним ускладненням. На зміну чітко окресленим, територіальним монополіям, які домінували в минулому, прийшов неймовірно строкатий ландшафт етнічно визначених гравців, які діють у рамках гнучкої моделі "злочин як послуга". Албанські, італійські, турецькі, марокканські, нігерійські, домініканські, сербські та навіть балтійські мережі не просто співіснують, а активно співпрацюють, часто укладаючи тимчасові альянси для виконання конкретних завдань, займаючи різні, чітко визначені ніші в складному ланцюжку постачання.

На найнижчих, найбільш ризикованих рівнях кримінальної ієрархії дедалі частіше фігурують неповнолітні та молодь, які виконують роль "вантажників" портових терміналів, що свідчить про високий рівень експлуатації найбільш вразливих верств населення. Це багатонаціональне середовище більше не обмежується Європою. Спостерігається унікальна двостороння інтеграція: європейські мережі глибоко вкорінюються в латиноамериканських країнах-виробниках, створюючи там свої осередки та налагоджуючи прямі контакти з постачальниками, тоді як латиноамериканські "кухарі" та емісари картелів дедалі частіше з'являються в підпільних лабораторіях Нідерландів та Бельгії, приносячи з собою унікальні знання з хімічної обробки та екстракції.

Арешт восени 2025 року високопоставленого члена найбільшого бразильського угруповання PCC у розкішному кондомініумі в португальському Кашкайші є яскравим свідченням того, як латиноамериканські гравці прагнуть не просто використовувати Європу як ринок збуту, а й фізично закріпитися на її території, інвестуючи при цьому в легальну економіку — нерухомість, бізнес і навіть футбольні клуби, прагнучи до повної інтеграції та відмивання грошей.

Зростаючий, майже нестерпний тиск на головні північно-західні порти змусив наркоторговців шукати нові, менш захищені, але не менш ефективні шляхи. Особливого геополітичного та

логістичного значення в цьому контексті набуло західне Середземномор'я, зокрема так званий Мароккансько-Іспанський коридор. Багатовікова, добре налагоджена інфраструктура контрабанди гашишу в горах Ер-Риф у Марокко сьогодні успішно і з вражаючою ефективністю використовується для перекидання кокаїну. Мережі, що мають у своєму розпорядженні цілі флоти швидкісних катерів, розгалужені системи спостереження на узбережжі та, що найважливіше, міцні, перевірені десятиліттями зв'язки з величезною марокканською діаспорою в Іспанії та Франції, ідеально пристосовані для проведення складних "гібридних" операцій. Вони здатні одночасно перевозити тонни гашишу, невеликі групи мігрантів і багатокілограмові партії кокаїну, використовуючи добре знайомі маршрути через Гібралтарську протоку та море Альборан, де кожен мис, бухта і течія відомі місцевим лоцманам.

Кокаїн, що потрапляє до південної Іспанії, звідти блискавично переправляється далі на північ автомобільними шляхами — через Країну Басків, де активність контрабандистів різко зросла за останні два-три роки, далі через південно-західну Францію, оминаючи основні митниці, до насичених ринків Парижа, а звідти — до Нідерландів та Бельгії, де його вартість зростає в декілька разів.

Ще далі на схід, у складних географічних умовах центрального Середземномор'я, набирає обертів інша, технологічно складніша тактика — так званий "дроп-офф", або скидання за борт. У Сицилійській протоці, де щодня перетинаються жваві міжнародні судноплавні шляхи, великі торговельні судна, що прямують з Латинської Америки, скидають водонепроникні партії кокаїну в заздалегідь визначених точках відкритого моря, звідки їх оперативно підбирають невеликі, координовані через супутниковий зв'язок рибальські човни або швидкісні катери. Цей витончений метод дозволяє майже повністю розділити величезні ризики трансатлантичного перевезення та ризики прибережної логістики, уникаючи необхідності проходження через високотехнологічні, нашпиговані сканерами порти. Після успішної доставки на берег, десь на безлюдному узбережжі південно-східної Сицилії, наркотики негайно дробляться на невеликі партії і переправляються на сусідню Мальту звичайними поромами або приватними суднами, використовуючи щоденний пасажирський та автомобільний трафік як природне прикриття.

Підсумовуючи, сьогоднішній європейський ринок кокаїну — це неймовірно складна, багатовимірна, адаптивна система, яка не просто виживає, а процвітає завдяки розумній фрагментації логістики, стратегічній локалізації виробництва

Висновки:

- **Падіння вилучень не дорівнює скороченню ринку, а є ознакою його адаптації.** Зменшення тоннажу конфіскованого кокаїну в головних портах Європи є результатом свідомої стратегії злочинних угруповань з фрагментації вантажів. Перехід на менші партії дозволяє їм розподіляти ризики та зберігати безперервність постачання.
- **Надлишок пропозиції та зростання чистоти при стабільних цінах свідчать про структурну кризу перевиробництва.** Ринок перенасичений високоякісним кокаїном: оптові ціни впали до історичних мінімумів, тоді як роздрібні ціни залишаються стабільними. Це дозволяє злочинцям отримувати надприбутки без підвищення цін для кінцевого споживача.
- **Виробництво "високої" якості локалізується в Європі.** Ключові етапи створення доданої вартості дедалі частіше відбуваються безпосередньо в ЄС.
- **Середземне море стає новим "сірим" коридором для наркотрафіку.** Посилення контролю в портах Атлантики змушує активізовувати альтернативні маршрути. Кокаїн дедалі частіше надходить через Мароккансько-Іспанський коридор та шляхом у Сицилійській протоці, використовуючи прогалини в системі безпеки.

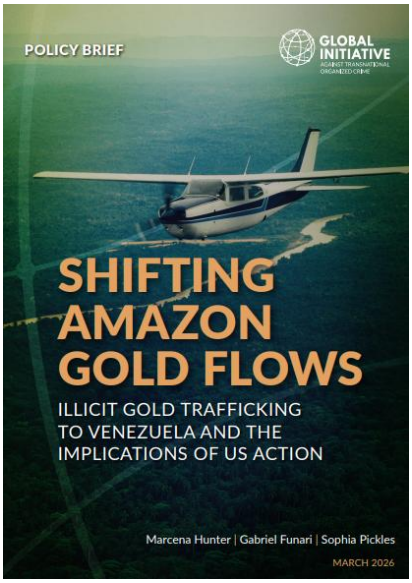
з високою доданою вартістю, безпрецедентному етнічному різноманіттю учасників та їхній вражаючій здатності до кримінального синтезу.

Драматичне падіння оптових цін, яке відбувається на тлі стабільних, майже незмінних роздрібних цін і стрімко зростаючої чистоти кінцевого продукту, є не просто статистичним курйозом, а найпотужнішим і незаперечним доказом того, що пропозиція не просто зберігається на стабільному рівні, а значно перевищує реальний платоспроможний попит.

Для європейських правоохоронних органів, політиків і аналітиків це означає нагальну необхідність радикального переосмислення всіх стратегій і методів оцінки. Замість примітивної гонитви за рекордним тоннажем вилучень, яка дедалі більше втрачає сенс, потрібна комплексна, багатофакторна система оцінки загроз, що обов'язково враховуватиме динаміку цін на всіх рівнях, коливання чистоти, зміни в соціальному складі злочинних угруповань та стрімке географічне розповзання маршрутів постачання, яке робить марними точкові удари по окремих портах.

Європейський кокаїновий ринок більше не схожий на жорстку вертикально інтегровану корпорацію зі штаб-квартирою в джунглях; він перетворився на децентралізовану, мережеву структуру, яка кидає виклик традиційним, часто застарілим, методам стримування і вимагає від Європи такої ж міри гнучкості, адаптивності та інтелекту, яку демонструють самі злочинці.

Золота лихоманка: Як Амазонка стала епіцентром незаконної торгівлі золотом [13]



Останні два роки показали драматичну трансформацію ринку золота в басейні Амазонки. Якщо раніше Венесуела була переважно країною-постачальником нелегального золота, яке вивозилося через Бразилію та Гаяну до міжнародних покупців в обхід санкцій, то сьогодні ситуація кардинально змінилася. В результаті жорсткішого регулювання в Бразилії та унікальних економічних умов, створених військово-політичним керівництвом Венесуели, країна перетворилася на потужний магніт, що притягує потоки золота з сусідніх держав.

Дослідження, опубліковане Global Initiative Against Transnational Organized Crime детально аналізує механізми функціонування цього ринку, його ключових гравців та можливі наслідки нещодавніх політичних змін у регіоні.

За оцінками експертів, ще у 2025 році золотодобувний сектор Венесуели генерував понад 2,2 мільярда доларів США щорічно, ставши фінансовим рятівним колом для режиму Ніколаса Мадуро в період колапсу нафтових доходів через міжнародні санкції, неефективне управління та хронічне недоінвестування нафтової галузі. Золото фактично замінило нафту як головне джерело твердої валюти для режиму, дозволяючи йому утримувати владу та фінансувати лояльні силові структури.

Ключову роль у цьому відіграло створення так званої Оріноцької гірничої дуги у 2016 році. Проголошена «механізмом формалізації гірничодобувної промисловості та залучення іноземних інвестицій», ця територія площею 112 000 квадратних кілометрів, багата на золото, алмази та інші стратегічні мінерали, перетворилася на зону беззаконня та середовище для незаконного видобутку. Цей процес відбувався під наглядом і за безпосередньої участі вищих військових чиновників, які забезпечували "дах" і логістику, колумбійських партизанських

[13] https://globalinitiative.net/wp-content/uploads/2026/03/Marcena-Hunter-Gabriel-Funari-Sophia-Pickles-Shifting-Amazon-gold-flows-Illicit-gold-trafficking-to-venezuela-and-the-implications-of-us-action-GI-TOC-March-2026.pdf

угруповань, що поширили свій вплив на венесуельську територію, та потужних місцевих кримінальних структур, таких як сумнозвісне Трен де Арагуа.

Військова операція США «Absolute Resolve» у січні 2026 року, яка усунула Мадуро від влади та призвела до арешту багатьох високопосадовців, хоч і завдала відчутного удару по політичному керівництву країни, не змогла демонтувати глибоко вкорінені криміналізовані структури управління золотим ринком. Як слушно зазначають автори доповіді, ключові фігури колишнього уряду, особливо з силових структур та військового командування, які десятиліттями наживалися на золоті через корупційні схеми, збори данини та прямий контроль над копальнями, зберегли значний вплив на інститути, що контролюють територію та торгівлю через насильство. Будь-який перехідний сценарій, який загрожуватиме їхньому доступу до надприбутків від золота, може спровокувати жорсткий опір або сприяти формуванню нових кримінальних альянсів з іншими угрупованнями, що матиме катастрофічні наслідки для безпеки всього регіону, потенційно поширюючись на сусідні Бразилію та Гаяну. Ситуація ускладнюється безпрецедентним зростанням цін на золото на міжнародних ринках, які у січні 2026 року перетнули психологічну позначку в 5000 доларів за унцію, що лише підігріває апетити злочинних угруповань та робить незаконний видобуток ще більш привабливим, незважаючи на зростаючі ризики.

Головним відкриттям доповіді став детальний опис інверсії традиційних маршрутів контрабанди, яка відбулася за останні два роки. Сьогодні золото з Бразилії та Гаяни активно перетікає до Венесуели, а не навпаки. Це стало прямим і швидким наслідком регуляторних змін, запроваджених у Бразилії у 2023 році, які суттєво обмежили можливості продажу золота всередині країни та посилили моніторинг пунктів скуповування. Бразильська влада запровадила жорсткіші вимоги до легальності походження металу, що зробило неможливим збут золота з відомих нелегальних копалень. Подальші масштабні рейди федеральних сил проти незаконного видобутку, особливо на території Яномамі, призвели до падіння кустарного виробництва на вражаючі 84% та скорочення офіційного експорту золота на 29% у 2024 році. Брокери, трейдери та афінажні заводи почали відмовлятися купувати золото з відомих "гарячих точок" незаконного видобутку, навіть якщо продавці намагалися підкріпити його підробленими сертифікатами походження. Зіткнувшись із неможливістю легалізувати здобуте, бразильські злочинні угруповання швидко переорієнтували свої логістичні ланцюжки на сусіда, де попит і ціни були значно привабливішими.

Аналогічна ситуація склалася і з Гаяною. Історично венесуельське золото контрабандою вивозилося до Гаяни для доступу до ринків у доларах США та уникнення санкцій. Тепер, однак, починаючи з 2024 року і особливо у 2025-му, золото з Гаяни переправляється до Венесуели для продажу, причому значні обсяги транспортуються через прикордонний перехід Летем до Бразилії, а звідти — через Боа-Вісту до Венесуели. Це є разючою ілюстрацією того, як зміна регуляторного середовища в одній країні може миттєво змінити напрямки транскордонних злочинних потоків.

Центральним хабом нової золотої лихоманки стало місто Боа-Віста, столиця бразильського штату Рорайма. Розташоване лише за 100 кілометрів від кордонів з Венесуелою та Гаяною, це місто з відносно розвиненою дорожньою інфраструктурою та десятками нелегальних злітно-посадкових смуг перетворилося на головний агрегаційний пункт для всього регіону. Золото з бразильських штатів Пара, Амазонас, Рондонія та власне Рорайма, а також із сусідньої Гаяни, доставляється сюди малими літаками або далекобійними вантажівками. Місцеві брокери та ювелірні магазини, часто пов'язані з корумпованими політиками та правоохоронцями, які історично покладалися на доходи від незаконного видобутку, скуповують ці партії готівкою або криптовалютою, організовують їхнє тимчасове зберігання, консолідацію та подальше транспортування через кордон до Венесуели.

Малі літаки відіграють ключову роль у цій логістиці, дозволяючи швидко і непомітно переміщувати товар на величезні відстані через джунглі, уникаючи наземних блокпостів та річкових патрулів. Цей вид транспорту забезпечує безпрецедентну гнучкість, дозволяючи злочинним мережам миттєво реагувати на дії влади та змінювати маршрути. Яскравим прикладом цього став випадок у грудні 2025 року, коли бразильська федеральна поліція перехопила приватний літак у Боа-Вісті, який прибув з Ітаітуби в регіоні Тапажос, та конфіскувала 51 кілограм нелегального золота, заарештувавши пілота та відставного армійського сержанта. З Боа-Вісти золото зазвичай відправляється вантажівками до прикордонного містечка Пакарайма, головного наземного шляху до Венесуели. Партії, що коливаються від 20 до 100 кілограмів, майстерно ховаються в автомобілях, демонструючи високий рівень організації контрабанди.

Але що саме робить Венесуелу настільки неймовірно привабливим ринком збуту для цих злочинців? Відповідь криється у величезному попиті, який формує венесуельське військове керівництво, що перетворило золото на головний інструмент збагачення та накопичення капіталу. За даними джерел GI-TOC з бразильських правоохоронних органів, військовослужбовці, дислоковані в районі Оріноцької гірничої дуги, включаючи генералів високого рангу, скуповують левову частку золота, що надходить із Бразилії. Вони пропонують ціну, що на 8% перевищує світову, — пропозиція, від якої місцеві трейдери просто не можуть відмовитися, адже це значно вище за ставки, доступні в Бразилії.

Гроші за золото іноді надходять у формі криптовалюти Tether (USDT), стейблкоїна, прив'язаного до долара США, що дозволяє ефективно обходити міжнародні санкції та уникати традиційної банківської системи. Такий механізм оплати створює додатковий рівень захисту для обох сторін угоди. Подальша доля цього металу залишається значною мірою неясною, оповитою таємницею: частина, ймовірно, осідає в приватних резервах військової верхівки як страховий актив, інша експортується через складні транзакційні мережі до Туреччини, яка стала одним із ключових напрямків для венесуельського золота за останні п'ять років, або до Китаю, чи використовується для розрахунків з іноземними контрагентами за імпортні товари в обхід фінансової системи.

Сполучені Штати намагаються розробити комплексну відповідь на ці виклики. У Сенаті проходить обговорення законопроєкту "United States Legal Gold and Mining Partnership Act", який пропонує багаторічну стратегію боротьби з нелегальним видобутком та торгівлею золотом у Західній півкулі. Документ, зокрема, містить положення, що безпосередньо стосуються Венесуели, і звертає особливу увагу на діяльність Трен де Арагуа, яке вже визнано в США іноземною терористичною організацією з лютого 2025 року, та колумбійського ELN, чия присутність на венесуельській території дозволяє їм контролювати ключові маршрути наркотрафіку та контрабанди корисних копалин.

Цей законопроєкт, що базується на попередніх законодавчих ініціативах, передбачає посилення збору розвідданих про злочинні мережі та фінансові потоки, жорсткіший нагляд за діяльністю афінажних заводів та трейдерів, а також активнішу співпрацю з місцевими партнерами в країнах-виробниках. Визнання Трен де Арагуа терористичною організацією відкриває перед американським урядом безпрецедентні інструменти для тиску: будь-яка особа чи компанія у світі, яка веде справи з цією групою, навіть несвідомо, ризикує потрапити під санкції або кримінальне переслідування з боку США, що створює значні ризики для всіх учасників золотого ринку, пов'язаного з Венесуелою.

Паралельно з цими законодавчими зусиллями, на початку березня 2026 року, США опосередковано визнали економічну вагу венесуельського золота, сприяючи укладенню знакової угоди про постачання до 1000 кілограмів золота від державної компанії Minerven на американські ринки через компанію Trafigura, що підкреслює складність політики: намагаючись

боротися з нелегальним сектором, Вашингтон водночас прагне отримати доступ до стратегічних мінеральних ресурсів країни.

Однак, як попереджають автори, будь-які односторонні або недостатньо продумані дії США несуть у собі значні ризики та можуть призвести до непередбачуваних негативних наслідків у всьому регіоні. Посилення тиску та військова нестабільність можуть призвести не до бажаного реформування сектору, а до ще більшої нестабільності, вакууму влади та спалахів жорстокого насильства між злочинними угрупованнями за контроль над територіями та ресурсами. Зростання політичної невизначеності в Каракасі підвищує стимули для територіальної конкуренції, оскільки старі захисні домовленості можуть руйнуватися.

Бразильські гіганти організованої злочинності, такі як Primeiro Comando da Capital (PCC) та Comando Vermelho (CV), які вже мають зв'язки з Трен де Арагуа та контролюють окремі копальні на кордоні, можуть спробувати скористатися кризою та значно розширити свою присутність і сферу впливу у венесуельській Амазонії, приносячи з собою ще більш витончені методи насильства та відмивання грошей. В той же час, якщо система стабілізується під новим політичним керівництвом, яке зможе запропонувати аналогічні або навіть кращі "умови співпраці" криміналітету, існуючі злочинні групи лише консолідуються та інтенсифікують видобуток, адаптувавшись до нових реалій.

Аналітики GI-TOC наполягають на необхідності виключно тонкого, багатогранного та доказового підходу до вирішення проблеми, який обов'язково враховуватиме швидку адаптивність та гнучкість злочинних ринків, здатних миттєво реагувати на будь-які зміни регуляторного чи політичного середовища.

Висновки:

- **Внаслідок посилення регулювання в Бразилії, регіональні маршрути контрабанди золота кардинально змінили напрямок:** замість вивезення венесуельського золота через сусідні країни, сьогодні спостерігається масовий приплив нелегального золота з Бразилії та Гаяни до Венесуели, яка пропонує ціну на 8% вищу за світову.
- **Зрощення держави та злочинності.** Золотий ринок Венесуели функціонує як "добре змащений механізм", що об'єднує вище військове керівництво, політичну еліту та транснаціональні злочинні угруповання.
- **Логістична революція в Амазонії.** Малі літаки та мережа нелегальних злітно-посадкових смуг стали головним інструментом транспортування золота, а місто Боа-Віста (Бразилія) перетворилося на ключовий хаб, через який проходять потоки металу з трьох країн перед відправкою до Венесуели.
- **Вашингтон одночасно застосовує два різновекторні підходи:** жорсткі законодавчі ініціативи та прагматичні економічні угоди, що свідчить про відсутність цілісної стратегії.

Ключовим елементом будь-якої стратегії має стати безперервний моніторинг не національних ринків, а саме регіональних ланцюгів постачання, з особливою увагою до критичних логістичних вузлів, таких як Боа-Віста, прикордонні переходи та мережі нелегальних аеродромів, які часто є ранніми індикаторами змін ринкової кон'юнктури.

Надзвичайно важливо уникати політики, яка необережно криміналізує звичайних неформальних старателів (garimpeiros), для яких видобуток золота є єдиним джерелом існування в регіоні з хронічно високим рівнем бідності та відсутністю альтернатив, інакше це лише штовхне їх прямо в обійми організованої злочинності, яка запропонує "захист" і роботу. Як показує сумний досвід впровадження Секції 1502 закону Додда-Франка щодо "конфліктних мінералів", такі заходи можуть мати руйнівні непередбачувані наслідки

для місцевих громад, не зачепивши при цьому великих трейдерів та корумповані уряди, які є справжніми бенефіціарами системи.

Потрібні скоординовані міжнародні зусилля, спрямовані на викриття та нейтралізацію корумпованих військових, трейдерів, фінансових посередників та постачальників техніки, а також на посилення належної перевірки (due diligence) для всього ланцюга постачання, включаючи не лише первинне золото, а й вторинну сировину (брухт), щоб перекрити всі можливі канали для відмивання незаконно отриманих коштів.

Лише поєднання інтелектуально обґрунтованих дій, тісної міжнародної координації та глибокого розуміння місцевої соціально-економічної та політичної специфіки зможе зупинити цей згубний потік, який не лише живить регіональні конфлікти, знищує унікальну екосистему Амазонки та підриває верховенство права, але й збагачує найнебезпечніші транснаціональні злочинні угруповання світу. Майбутнє золота Амазонки залежить від здатності міжнародної спільноти діяти рішуче, але розумно, не повторюючи помилок минулого.

Криптовалютна злочинність у 2025 році: нові масштаби шахрайства, відмивання коштів та обходу санкцій [14]

Документ, підготовлений аналітичною компанією Chainalysis, є масштабним дослідженням еволюції криптовалютної злочинності та її інтеграції у глобальну фінансову систему. У звіті аналізуються ключові типи незаконної діяльності, пов'язані з використанням цифрових активів, включаючи відмивання коштів, шахрайство, кіберзлочинність, торгівлю наркотиками через даркнет-платформи, фінансування тероризму, торгівлю людьми та обходження міжнародних санкцій. Автори наголошують, що криптовалюти стали невід'ємною частиною сучасної фінансової інфраструктури, оскільки забезпечують миттєві, транскордонні та відносно дешеві перекази коштів. Водночас ключовою особливістю блокчейн-технології є прозорість: транзакції зберігаються у незмінному реєстрі, доступному для аналізу, що створює унікальні можливості для фінансових розслідувань та виявлення кримінальних мереж. Таким чином, хоча криптовалюти використовуються злочинцями, їхня технологічна архітектура водночас створює інструменти для боротьби з фінансовими злочинами.

У вступній частині звіту підкреслюється, що сучасна криптовалютна злочинність перейшла на новий рівень організації. Якщо на початкових етапах розвитку цифрових активів незаконні операції здебільшого здійснювалися окремими кіберзлочинцями або невеликими групами, то сьогодні сформувалася ціла кримінальна екосистема, яка функціонує за принципами повноцінної економіки. У цій екосистемі існують спеціалізовані постачальники інфраструктури, брокери, платіжні посередники, оператори сервісів відмивання коштів, розробники шахрайських інструментів та навіть маркетплейси для незаконних фінансових послуг. Таке структурування злочинної діяльності призводить до її професіоналізації та масштабування, оскільки різні учасники кримінальної мережі виконують окремі функції у загальному ланцюгу незаконних фінансових операцій.

[14] https://www.chainalysis.com/wp-content/uploads/2026/03/the-2026-crypto-crime-report-release.pdf

Згідно з оцінками дослідників, у 2025 році адреси, пов'язані з незаконною діяльністю, отримали щонайменше 154 мільярди доларів у криптовалюті, що означає приблизно 162-відсоткове зростання порівняно з попереднім роком. Основним фактором такого зростання стало різке збільшення активності суб'єктів, які перебувають під міжнародними санкціями, оскільки обсяг транзакцій, пов'язаних із санкційними адресами, зріс майже на 694%. Однак, попри ці значні показники, частка незаконної активності у загальному обсязі криптовалютних транзакцій залишається відносно невеликою і становить менше одного відсотка від усіх транзакцій, що підкреслює домінування легального використання криптовалют у світовій економіці.

Звіт також демонструє суттєві зміни у структурі активів, які використовуються у незаконних операціях. Якщо раніше більшість таких операцій здійснювалася у Bitcoin або Ether, то сьогодні переважну роль відіграють стейблкоїни, на які припадає близько 84% незаконного криптовалютного обороту. Це пояснюється тим, що стейблкоїни мають стабільну прив'язку до традиційних валют, що зменшує ризик втрати вартості під час переміщення коштів. Крім того, вони забезпечують швидкі міжнародні платежі та часто використовуються у різних фінансових сервісах, що значно полегшує їх інтеграцію у глобальні фінансові потоки.

Окрему увагу автори приділяють ролі державних суб'єктів у криптовалютній злочинності. У звіті зазначається, що у 2025 році значно зросла активність держав, які використовують криптовалюти для обходу санкцій або фінансування стратегічних операцій. Найбільш помітним прикладом є діяльність Північної Кореї, пов'язаних із якою хакерських груп. За оцінками дослідників, вони викрали понад 2 мільярди доларів у результаті атак на криптовалютні платформи та інші цифрові сервіси. Однією з найгучніших подій став масштабний злам криптовалютної біржі Bybit, під час якого було викрадено приблизно 1,5 мільярда доларів, що стало одним із найбільших криптовалютних пограбувань в історії.

Іншим прикладом є використання криптовалют росією для обходу міжнародних санкцій. У звіті зазначається, що у 2024 році було прийнято законодавчі зміни, які сприяли використанню цифрових активів для міжнародних розрахунків, а у 2025 році було запущено спеціальний токен A7A5, прив'язаний до російського рубля. За менш ніж один рік через цей токен було проведено транзакції на суму понад 93 мільярди доларів, що демонструє потенціал криптовалют як інструменту для обходу обмежень традиційної фінансової системи. Аналогічно, іранські мережі, пов'язані з проксі-організаціями, використовують криптовалюти для фінансування закупівель зброї, торгівлі нафтою та підтримки таких організацій, як Hezbollah, Hamas і Houthi. Таким чином, криптовалюти поступово стають важливим інструментом геополітичної фінансової конкуренції.

Значна частина звіту присвячена аналізу інфраструктури відмивання коштів у криптовалютному середовищі. Особливо важливу роль у цій системі відіграють так звані Chinese Money Laundering Networks (CMLN) — китайськомовні мережі відмивання коштів, які забезпечують обслуговування великої кількості кримінальних операцій. У 2025 році ці мережі обробили приблизно 16,1 мільярда доларів незаконних криптовалютних потоків і стали відповідальними приблизно за 20% відомої діяльності з відмивання криптовалют у світі. При цьому загальний обсяг відмивання коштів у сфері криптовалют зріс із 10 мільярдів доларів у 2020 році до понад 82 мільярдів доларів у 2025 році, що демонструє швидке розширення цієї кримінальної інфраструктури.

Ці мережі мають складну організаційну структуру і включають різні типи сервісів, які забезпечують переміщення коштів через численні транзакції та платформи. До них належать посередники, що вербують осіб для використання їхніх банківських рахунків або криптовалютних гаманців, мережі «грошових мулів», які здійснюють багаторівневе переміщення коштів між рахунками, неформальні обмінні сервіси, що працюють без процедур ідентифікації клієнтів, а також спеціалізовані сервіси для продажу криптовалютних активів, отриманих у результаті незаконної діяльності, зі знижкою. Значну роль у цій екосистемі

відіграють також онлайн-платформи гарантійних сервісів, які функціонують як маркетплейси для кримінальних фінансових послуг і забезпечують механізми репутації, рейтингу та ескроу-платежів між учасниками незаконного ринку.

Дослідження показує, що ці мережі застосовують традиційні методи відмивання коштів, адаптовані до цифрового середовища. Зокрема, широко використовується дроблення транзакцій (smurfing), коли великі суми розбиваються на численні дрібні платежі для уникнення виявлення, а також агрегування коштів, коли численні невеликі транзакції об'єднуються у великі суми перед їх інтеграцією у легальну фінансову систему. В окремих випадках автоматизовані системи дозволяють переміщувати великі обсяги коштів між гаманцями за кілька хвилин, що значно ускладнює їхнє блокування або відстеження.

Окремий розділ звіту присвячений криптовалютному шахрайству, яке залишається одним із найприбутковіших видів незаконної діяльності у цифровій економіці. У 2025 році шахрайські операції принесли щонайменше 14 мільярдів доларів, але дослідники прогнозують, що після уточнення даних ця сума може перевищити 17 мільярдів доларів. Особливо швидко зростає сегмент шахрайства, заснованого на імітації або шахрайських атаках із видаванням себе за іншу особу, коли злочинці видають себе за представників державних установ, банків або криптовалютних платформ. У 2025 році обсяг таких схем зріс більш ніж на 1400%, що свідчить про їхню високу ефективність.

Звіт також описує масштабні фішингові кампанії, які використовують SMS-повідомлення та фальшиві вебсайти для обману користувачів. Однією з найбільш резонансних стала кампанія, що імітувала систему оплати доріг E-ZPass. У межах цієї операції мільйони користувачів отримували повідомлення з посиланням на підроблені вебсайти, які виглядали ідентично офіційним сторінкам державних установ. За оцінками дослідників, ця схема могла охопити понад один мільйон жертв у більш ніж 120 країнах світу, що демонструє глобальний масштаб сучасних криптовалютних шахрайств.

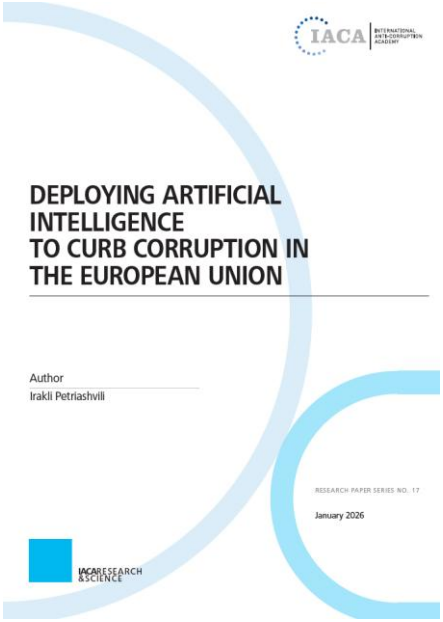
Висновки:

- **Криптовалюти стають ключовим інструментом обходу санкцій та геополітичних фінансових операцій.** Державні суб'єкти (Північна Корея, росія, Іран) активно використовують криптовалюти для обходу санкцій та фінансування стратегічних операцій. Це означає, що системи ПВК/ФТ повинні інтегрувати санкційний моніторинг блокчейн-операцій як один із пріоритетних напрямів.
- **Китайські мережі відмивання коштів перетворилися на глобальну «кримінальну фінансову інфраструктуру».** CMLN фактично виконують функцію міжнародних підпільних банків, що обслуговують шахрайство, кіберзлочинність, санкційні операції та організовану злочинність. Для їхнього виявлення необхідне поєднання OSINT, HUMINT і блокчейн-аналітики.
- **Криптовалютні шахрайства переходять у фазу індустріалізації та сервісної економіки.** Поява платформ надання злочинних послуг дозволяє навіть технічно непідготовленим злочинцям запускати складні фішинг-операції. Це суттєво підвищує масштаби шахрайства та знижує бар'єр входу до кримінального ринку.
- **Штучний інтелект радикально підвищує ефективність фінансових злочинів.** AI дозволяє масштабувати шахрайство, створювати реалістичні фейки та обробляти тисячі жертв одночасно. Для протидії необхідне впровадження AI-інструментів для виявлення шахрайства, а також активна співпраця між приватним сектором, правоохоронними органами та криптокомпаніями.

Важливою тенденцією, на яку звертають увагу автори звіту, є активне використання штучного інтелекту у шахрайських операціях. Технології генерації тексту, синтезу голосу та створення діпфейк-відео дозволяють злочинцям створювати переконливі імітації реальних осіб або організацій. За оцінками дослідників, шахрайські схеми, що використовують AI, отримують у середньому у 4,5 раза більше доходів, ніж традиційні шахрайські операції. Крім того, штучний інтелект дозволяє автоматизувати комунікацію з великою кількістю потенційних жертв і значно збільшити масштаб шахрайських кампаній.

У підсумку звіт робить висновок, що криптовалютна злочинність поступово перетворюється на високотехнологічну та глобально інтегровану систему, у якій поєднуються кіберзлочинність, організована злочинність та геополітичні інтереси держав. Кримінальні мережі використовують складні цифрові інфраструктури, міжнародні платіжні канали та автоматизовані інструменти для приховування походження коштів і масштабування своєї діяльності. Водночас прозорість блокчейн-технологій створює нові можливості для фінансових розслідувань, оскільки дозволяє відстежувати рух коштів і встановлювати зв'язки між різними типами кримінальної діяльності. Автори наголошують, що ефективна протидія криптовалютній злочинності потребує тісної співпраці між державними органами, фінансовими установами, правоохоронними структурами та приватними компаніями, які спеціалізуються на блокчейн-аналітиці, а також розвитку міжнародних механізмів обміну інформацією та спільних розслідувань.

Алгоритми проти корупції: вплив штучного інтелекту на ефективність антикорупційних систем у країнах ЄС [15]



Документ, підготовлений у межах дослідницької серії Міжнародної антикорупційної академії (IACA), присвячений системному аналізу ролі штучного інтелекту у зміцненні антикорупційної політики та механізмів доброчесності у державах Європейського Союзу. Дослідження має емпіричний характер і поєднує картування реальних технологічних рішень, що використовуються державами, із кількісним аналізом змін у показниках корупційних правопорушень. Його основною метою є перевірка гіпотези про те, що впровадження AI-інструментів у системи державного контролю та нагляду може сприяти реальному зниженню рівня корупції та фінансових втрат державного сектору. У цьому контексті дослідження формує одну з перших системних спроб на рівні Європейського Союзу поєднати технологічний аналіз цифрових інструментів управління з конкретними показниками корупційних правопорушень і економічних збитків.

У вступній частині автор підкреслює, що корупція залишається однією з найбільш складних і системних проблем для Європейського Союзу, оскільки вона підриває ефективність використання публічних ресурсів, знижує рівень довіри громадян до інституцій та негативно впливає на економічну стабільність держав. За оцінками Європейського парламенту, щорічні втрати від корупції в ЄС можуть становити від приблизно 179 до 990 млрд євро, що еквівалентно близько шести відсоткам сукупного валового внутрішнього продукту Союзу. Статистичні дані Eurostat демонструють, що лише у період 2018–2023 років правоохоронними органами країн

[15] https://www.iaca.int/media/attachments/2026/02/02/iaca-research-paper-series_irakli-petriashvili1.pdf

ЄС було зафіксовано понад 607 тисяч корупційних правопорушень, що становить приблизно 101 тисячу випадків щороку. Додатково ці дані підтверджуються інформацією Європейської прокуратури (EPPO), яка у своєму звіті за 2024 рік повідомила про 2 666 активних розслідувань, що стосуються зловживань з бюджетом ЄС, із потенційними фінансовими втратами на рівні 24,8 млрд євро, з яких 1,64 млрд євро припадає саме на корупційні правопорушення. Середня економічна шкода одного корупційного випадку у цих розслідуваннях становила приблизно 8,25 млн євро. Ці дані формують емпіричну основу для подальшого аналізу ефективності антикорупційних інструментів.

На цьому тлі автор підкреслює, що публічне управління у Європейському Союзі переживає глибоку цифрову трансформацію, у межах якої все більшого значення набувають технології штучного інтелекту, машинного навчання та аналізу великих масивів даних. Такі технології здатні обробляти величезні обсяги інформації, ідентифікувати складні аномалії у транзакціях, виявляти нетипові поведінкові патерни та формувати ранні сигнали ризику, які неможливо або дуже складно виявити традиційними методами контролю. Саме тому Європейська Комісія у своїх стратегічних документах — зокрема Digital Decade Policy Programme 2030, Digital Europe Programme та Interoperable Europe Act — визначає цифровізацію та впровадження AI-інструментів як один із ключових напрямів модернізації державного управління. У цьому контексті штучний інтелект розглядається не лише як технологічна інновація, але і як інструмент посилення прозорості, підзвітності та ефективності державних інституцій.

Однією з центральних ідей дослідження є існування значної наукової прогалини у розумінні того, як саме технологічні інструменти впливають на реальні результати антикорупційної політики. Хоча сучасна академічна література містить багато теоретичних робіт щодо потенціалу цифрових технологій у сфері державного управління, вона майже не містить системних емпіричних досліджень, які б демонстрували прямий зв’язок між впровадженням AI-інструментів і фактичними змінами у рівні корупції. Більшість попередніх досліджень обмежувалася окремими кейсами або аналізом етичних та правових ризиків використання алгоритмів. Саме тому автор ставить перед собою завдання створити першу системну карту застосування AI-інструментів для антикорупційних цілей у державах ЄС і перевірити, чи існує статистичний зв’язок між їх впровадженням і зменшенням кількості корупційних правопорушень.

Методологія дослідження поєднує кілька аналітичних підходів. По-перше, було здійснено системне картування AI-інструментів, що використовуються у публічному секторі ЄС, на основі бази даних EU Public Sector Tech Watch. Загалом ця база містить інформацію про 1 640 AI-систем, що застосовуються у державному управлінні, однак лише 47 із них були ідентифіковані як інструменти, безпосередньо спрямовані на боротьбу з корупцією. Ці системи використовуються у 17 державах-членах Європейського Союзу. Водночас десять країн ЄС не впровадили жодного AI-інструменту для антикорупційних цілей, що створює можливість для порівняльного аналізу між державами, які застосовують технології штучного інтелекту та державами, які не застосовують такі технології.

Функціонально ідентифіковані AI-системи охоплюють різні сфери державного контролю. До них належать системи автоматизованого виявлення шахрайства, інструменти моніторингу державних закупівель, алгоритми аналізу конфліктів інтересів у державних реєстрах, системи виявлення аномалій у фінансових транзакціях, інструменти аналізу повідомлень викривачів, автоматизований аналіз контрактів і документів, алгоритмічний аналіз мереж бенефіціарної власності та системи прогнозного оцінювання корупційних ризиків. Кожен із цих інструментів здатний обробляти великі масиви даних і формувати автоматизовані сигнали ризику, що значно підвищує ефективність діяльності аудиторів, антикорупційних органів та правоохоронних структур.

Емпіричний аналіз зосереджується на порівнянні країн із найвищим рівнем впровадження AI-інструментів і країн, де такі інструменти відсутні. До першої групи належать Італія, Нідерланди та Німеччина, які мають найбільшу кількість антикорупційних AI-систем. До другої групи входять Болгарія, Хорватія та Румунія, де подібні технології не використовуються. Порівняльний аналіз демонструє чітку відмінність у тенденціях розвитку корупційних правопорушень. У країнах які застосовують технології штучного інтелекту спостерігається стабільне зниження кількості зареєстрованих корупційних випадків. Найбільш яскравим прикладом є Італія, де кількість таких правопорушень зменшилася з понад 21 тисячі випадків у 2016 році до приблизно 3 тисяч у 2023 році, що означає скорочення на понад 86 відсотків. У Нідерландах за цей період зафіксовано зниження приблизно на 21 %, а у Німеччині — приблизно на 18 %. Хоча на ці показники можуть впливати й інші фактори, часовий збіг між впровадженням AI-інструментів і зниженням рівня корупційних правопорушень дозволяє припустити наявність позитивного ефекту від технологічної модернізації систем контролю.

Висновки:

- **Штучний інтелект стає ключовим інструментом сучасних антикорупційних систем.** Країни ЄС, які впровадили AI-системи для моніторингу закупівель, аналізу ризиків і виявлення шахрайства, демонструють стабільне зниження кількості корупційних правопорушень. Це підтверджує доцільність інвестування держав у технологічні системи аналітики даних.
- **Найбільш ефективними є AI-системи, інтегровані у фінансовий контроль і державні закупівлі.** Практичні приклади показують, що системи виявлення аномалій у закупівлях, мережевого аналізу бенефіціарів та автоматизованого ризик-скорингу дозволяють виявляти корупційні схеми на ранніх етапах і зменшувати фінансові втрати.
- **Відсутність цифрових інструментів контролю пов'язана з погіршенням антикорупційних показників.** Країни, які не впровадили AI-технології, демонструють зростання або нестабільність корупційних правопорушень, що свідчить про необхідність модернізації систем нагляду.
- **Інвестиції у AI-інструменти мають значний економічний ефект.** Зменшення кількості корупційних правопорушень у країнах-адоптерах AI, які застосовують технології штучного інтелекту може означати збереження десятків або навіть сотень мільярдів євро публічних ресурсів, що робить такі інвестиції економічно виправданими.

Кореляційний аналіз також підтверджує наявність статистичного зв'язку між використанням AI-систем і змінами у показниках корупції. У Нідерландах було зафіксовано дуже сильну негативну кореляцію між кількістю AI-інструментів і рівнем корупційних правопорушень ($r = -0{,}92$), що свідчить про значну узгодженість між технологічними інноваціями та покращенням результатів у сфері доброчесності. В Італії кореляція є помірною ($r = -0{,}39$), а у Німеччині — слабкою ($r = -0{,}08$), що може пояснюватися високим рівнем інституційної зрілості цієї країни, де антикорупційні механізми вже були відносно ефективними ще до впровадження AI-технологій.

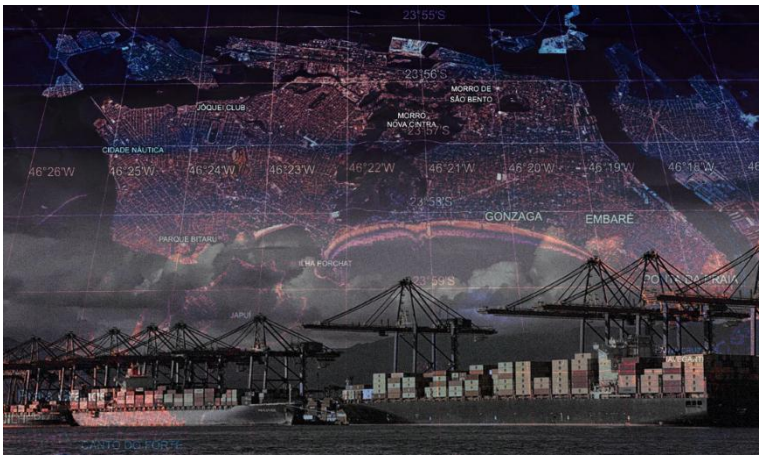
На відміну від цього, країни, які не використовують AI-інструменти для боротьби з корупцією, демонструють менш позитивні тенденції. У Болгарії кількість корупційних правопорушень зросла з 223 випадків у 2016 році до 572 у 2023 році, що означає збільшення приблизно на 156 %. У Румунії кількість таких правопорушень зросла більш ніж удвічі — з 1 401 до 3 246 випадків. У Хорватії ситуація характеризується значною нестабільністю та коливаннями показників, що може свідчити про недостатню ефективність систем виявлення корупційних правопорушень. Таким чином, дослідження демонструє, що відсутність технологічної модернізації систем контролю може бути пов'язана із зростанням або нестабільністю корупційних показників.

Важливим елементом дослідження є економічна оцінка потенційного ефекту від впровадження AI-інструментів. Автор використовує оцінки середніх втрат від одного корупційного правопорушення, які, за розрахунками, становлять від 1,8 до 9,8 млн євро. На основі цих показників було оцінено потенційну економічну вигоду від скорочення кількості корупційних правопорушень у країнах, які застосовують технології штучного інтелекту. Загалом зменшення 17 592 випадків корупції у цих державах може відповідати збереженню публічних ресурсів у межах приблизно від 31,7 до 172,4 млрд євро. У випадку трьох країн із найвищим рівнем впровадження AI цей ефект може становити від 38,7 до 210,6 млрд євро. Ці розрахунки демонструють значний потенційний економічний ефект від використання технологій штучного інтелекту у сфері державного контролю.

У підсумку дослідження робить висновок, що штучний інтелект поступово стає одним із ключових інструментів сучасних систем забезпечення доброчесності у публічному секторі. Його використання дозволяє значно підвищити спроможність державних інституцій виявляти корупційні ризики, аналізувати великі масиви даних і запобігати фінансовим зловживанням. Водночас автор наголошує, що технології не можуть замінити інституційні реформи і повинні використовуватися у поєднанні з ефективними механізмами правового регулювання, аудиту, підзвітності та міжінституційної співпраці. Загалом результати дослідження свідчать, що інтеграція штучного інтелекту у системи державного нагляду може стати одним із ключових факторів підвищення ефективності антикорупційної політики у Європейському Союзі та визначатиме розвиток систем забезпечення доброчесності у публічному секторі в найближчі десятиліття.

Інші новини

Сантус: Чому Бразилія, вигравши битву з наркотрафіком, програла війну[16]



Порт Сантус — це не просто 16 кілометрів причалів, які розділяють навпіл густонаселений промисловий регіон Баїшада-Сантіста. Це дзеркало, в якому відображається вся складність, суперечливість і часто марність глобальної війни з наркотиками.

Крізь його термінали проходить третина всього бразильського валового внутрішнього продукту — зерно, залізна руда, автомобілі, кава, апельсиновий сік. Але разом із легальними вантажами десятиліттями пливли й нелегальні — тонни кокаїну, виробленого в Андах, що прямували до найприбутковіших ринків світу, насамперед до Європи, де ціна зростає в десятки разів. Історія боротьби за Сантус — це історія про те, як держава може виграти битву, але продовжувати програвати війну, спостерігаючи, як вогонь перекидається на нові території.

Картина, яку спостерігає відвідувач порту, оманливо ідилічна. Велетенські судна повільно заходять у канали, де їх уже чекають десятки портових кранів. Ці крани із математичною точністю переставляють різнокольорові контейнери, складаючи їх у неймовірно складні комбінації просто неба. Внизу можна побачити крихітні дерев'яні човни. У них — місцеві

[16] https://insightcrime.org/news/brazil-biggest-port-winning-fight-against-traffickers/

рибалки, для яких води гирла є годувальницею. Але правоохоронці знають: ці ж самі човни, ці ж самі люди, а часто й ті, хто лише прикидаються рибалками, є критично важливою ланкою в ланцюгу контрабанди. Саме вони вночі, під прикриттям туману та корупції, підпливають до якірних стоянок, щоб прийняти на борт вантаж, який згодом за допомогою підкуплених докерів або через недогляд охорони опиниться глибоко в трюмі, захований серед тисяч тонн вантажів.

А на пагорбах над портом тісно ліпляться одна до одної халупи фавел. Звідти відкривається ідеальний огляд на всю акваторію. Ці халупи — не просто житло, це сторожові вежі Першого столичного командування (Primeiro Commando da Capital — PCC), наймогутнішої кримінальної структури Бразилії, яка перетворила наркоторгівлю на індустрію з корпоративною структурою та глобальною логістикою.

У 2019 році Сантус став символом поразки держави в нарко-війні. Майже 21 тонна кокаїну, вилученого лише за один рік, була водночас і доказом роботи поліції, і мовчазним свідченням справжніх масштабів трафіку. Адже правоохоронці добре знають правило «десяти відсотків»: вилучається лише незначна частина від того, що реально проходить. Це означало, що через Сантус щороку йшли сотні тонн наркотиків. Європа захлиналась від кокаїну, і його дедалі більше надходило саме з Бразилії, через її головні морські ворота. А потім статистика несподівано пішла на спад. До 2025 року обсяги вилучень у Сантусі скоротилися до 7,4 тонни. Європейські порти, як-от Антверпен, Роттердам чи Гамбург, продовжували вилучати тонни, але тепер вони дедалі частіше знаходили кокаїн у контейнерах, які прибували не з Бразилії. Щось змінилося.

Ця зміна не була випадковою. Вона стала результатом тихої, але жорсткої інституційної революції, яку провела бразильська влада. Ключову роль відіграла Федеральна служба доходів — структура, яку через її всеосяжний контроль жартома називають «тіткою» (A Tia). Усвідомивши, що традиційні методи роботи — вибіркові перевірки, орієнтація на арешти дрібних дилерів — не працюють, служба змінила філософію безпеки в порту. Замість того щоб намагатися контролювати хаос, вона його структурувала. Було створено трикутник взаємодії: Федеральна поліція (Policia Federal) зосередилася на кінцевому результаті — арештах і безпосередньому захопленні вантажів; власне Служба доходів взяла на себе аналітику, розвідку та профілактику, тобто роботу до того, як наркотики потраплять на борт; а Портова адміністрація відповідала за фізичний периметр. Але найгеніальнішим ходом стало залучення приватного сектору на умовах жорсткого диктату.

Влада зрозуміла просту річ: держава фізично не може перевірити кожен із мільйонів контейнерів, які щороку проходять через Сантус. На це немає ні ресурсів, ні часу. Але вона може змусити це робити приватні компанії, які зацікавлені в роботі в порту. Було запроваджено систему сертифікації. Жодна приватна компанія не може отримати доступ до роботи в Сантусі без підписання угоди про безпеку, яка фактично перетворює її на продовження правоохоронної системи.

Сьогодні кожен контейнер, що прямує до Європи чи Африки, в обов'язковому порядку проходить через стаціонарний чи мобільний сканер. Ті, хто намагається заощадити або заплющити очі, швидко втрачають бізнес. Термінали обнесені подвійними парканами під напругою, обладнані сотнями камер нічного бачення та тепловізорів. Кожен докер, кожен водій вантажівки, кожен співробітник має електронний бейдж із чітко визначеним рівнем доступу. Будь-який в'їзд у заборонену зону миттєво генерує сигнал тривоги в ситуаційному центрі. І найважливіше: інформація з усіх цих приватних систем — відео, дані сканерів, логи перепусток — у режимі реального часу стікається до Федеральної служби доходів. Там аналітики зіставляють цю інформацію з даними поліцейської розвідки, відомостями з-за кордону та супутниковими знімками. Вони шукають аномалії: контейнер, який прибув з регіону, де активний PCC, але був завантажений на терміналі, який мав би обслуговувати іншу продукцію;

судно, що різко змінило маршрут; водій, який надто часто заїжджає на територію без видимої причини.

Окрім високих технологій, влада не цурається і перевірених методів. І ось тут виходять на сцену собаки. Вони знаходять те, що не бачить людина, і роблять це з точністю, недоступною жодному сканеру».

Але найбільшим проривом стала зміна мислення. Замість безплідних спроб перекрити весь неймовірно довгий кордон, влада застосувала логістичний підхід. Відомо, що PCC — це раціональний гравець. Він не возитиме кокаїн через джунглі, якщо є пряма асфальтована дорога. Аналітики вирахували кілька ключових транспортних артерій, якими наркотики з Болівії, Перу та Колумбії стікаються до Сантуса. Це так звані «воронки» — вузькі місця, які неможливо обійти. І це спрацювало. Статистика вилучень на підходах до порту різко зросла. Це була блискуча тактична перемога.

Але саме тут криється пастка, в яку потрапляють майже всі, хто намагається аналізувати ефективність боротьби з наркотрафіком. Вони плутають тактичний успіх із стратегічним . Те, що сталося після затягування навколо Сантуса, ідеально ілюструє концепцію «ефекту гідри», відомого ще з давньогрецьких міфів: відрубаєш одну голову — виростуть дві нові. PCC — це не примітивне вуличне угруповання, це транснаціональна корпорація з розгалуженою розвідкою, аналітичним відділом і здатністю прораховувати ризики наперед. Коли вартість транзиту через Сантус через посилення безпеки різко зросла (більше хабарів, більше ризику втратити вантаж), компанія просто почала диверсифікувати логістику.

Першим напрямком диверсифікації стала Африка. Бразильська влада, зосередившись на Європі, на початку 2020-х років приділяла менше уваги контейнерам, які прямували до портів Західної Африки — Ломе, Котону, Лагосу. Наркоторговці почали використовувати Африку як пункт призначення, але самі наркотики, принаймні їхня переважна більшість, в Африці не залишалися. Їх знову запаковували в контейнери, вантажили на інші судна, і вони пливли далі до Європи. Так виник складний, багатоступеневий маршрут, який ускладнював відстеження вантажу. Бразильська митниця зреагувала, поширивши обов'язкове сканування на всі африканські напрямки, але час було втрачено, і канали постачання встигли налагодитись.

Однак справжній вибух стався значно ближче. Поки влада святкувала перемогу в Сантусі, по всій Бразилії почали спалахувати нові точки напруги. У порту Сальвадор, столиці штату Баїя, вилучення кокаїну пішли вгору. У порту Паранагуа, в штаті Парана, так само. На кордоні з Венесуелою в штаті Рорайма почали знаходити цілі склади. PCC, витіснений із власної фортеці, почав агресивно інвестувати в розширення впливу на інші портові потужності країни. Це був не просто пошук альтернатив — це була стратегія захоплення нових ринків.

У Баїї PCC не намагався діяти самотужки у ворожому середовищі. Він зробив те, що робить будь-яка розумна корпорація: знайшов місцевого партнера. Таким партнером стало угруповання Bonde do Maluco (BDM) — жорстоке бандитське формування, яке контролювало низку фавел у Сальвадорі. PCC запропонував BDM зброю, гроші та доступ до міжнародних каналів збуту в обмін на контроль над логістикою в порту. Цей альянс виявився смертоносним. BDM, відчувши фінансову підтримку та нові амбіції, розпочав тотальну війну зі своїми одвічними ворогами, перш за все з угрупованням Caveira. Вулиці Сальвадора та інших міст Баїї перетворилися на поле бою. Штат, який колись славився своїми пляжами та культурною спадщиною, став одним із найнебезпечніших у Бразилії за рівнем смертей.

І це не межа. За даними розвідки, PCC вже фактично контролює один із ключових терміналів у порту Паранагуа, другому за значенням порту Бразилії, через який експортується величезна кількість зерна. Ведуться перемовини і, за деякими даними, уже здійснено спроби проникнення в порт Масейо, столиці штату Алагоас. Кожен новий порт — це нова логістична головна біль для

влади і нове джерело насильства для місцевого населення, оскільки контроль над портовою інфраструктурою неминуче супроводжується залякуванням, вбивствами і тотальним проникненням у місцеву економіку та поліцію.

Нарешті, бразильська криза виплеснулась за межі країни, запустивши ефект доміно по всій Латинській Америці. Найдраматичніше це проявилося в Еквадорі. Порт Гуаякіль, головні морські ворота країни, за кілька років перетворився на новий світовий центр наркоторгівлі. У 2024 році саме в Еквадорі було вилучено найбільшу у світі партію кокаїну — 22 тонни, які готувалися до відправлення в США та Європу. Це стало символічним маркером передачі «кокаїнової корони» від Бразилії до Еквадору. Ціна для цієї невеликої країни виявилася катастрофічною. Гуаякіль та сусіднє місто Дуран, через яке проходить основна маса вантажів, стали одними з найнебезпечніших міст планети. Рівень вбивств злетів до астрономічних висот, в'язниці перетворилися на філії пекла, де угруповання влаштовують різанини, а кандидатів у президенти розстрілюють просто після передвиборчих мітингів. Мирний Еквадор перетворився на поле битви картелів, які зійшлися в боротьбі за контроль над новим транзитним хабом.

Подібна, хоч і менш кривава, історія розгортається в Уругваї. Порт Монтевідео, завдяки своєму ліберальному законодавству, стає дедалі привабливішим для експорту кокаїну до Європи. Аналітики фіксують більше випадків використання Уругваю як складу для величезних партій наркотику, що очікують на відправку. Існують обґрунтовані підозри, що PCC, слідуючи своїй експансіоністській стратегії, вже закріпився в Монтевідео, використовуючи країну для відмивання грошей та організації безпечних логістичних ланцюжків. Влада Уругваю, не звикла до такого рівня організованої злочинності, намагається дати раду, але стикається з корупцією та погрозами на адресу суддів і прокурорів.

То чи виграв Сантус війну з наркотрафіком? Відповідь на це питання залежить від кута зору. Якщо дивитися на карту порту, на графіки вилучень безпосередньо на його терміналах, на кількість заарештованих корумпованих службовців, то відповідь буде ствердною. Так, Сантус виграв. Коаліція державних органів і приватного бізнесу створила захисний мур, який виявився занадто високим для PCC. Злочинці більше не почуваються там господарями. Вони змушені платити більше, ризикувати більше, помилятися частіше. Це безсумнівне досягнення, яке рятує тисячі життів у Європі та Бразилії, не даючи тоннам наркотиків дістатися споживача.

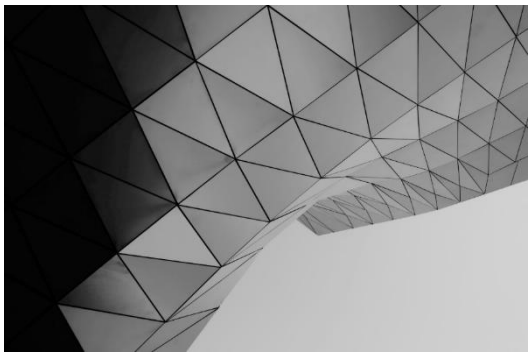
Але якщо піднятися над картою порту й подивитися на карту континенту, відповідь буде невтішною. Бразилія програє, тому що вона просто перемістила проблему. Вона виграла битву за одне місто, але програла війну за цілі регіони — Баїю, Парану, Алагоас. І більше того, вона експортувала проблему сусідам, дестабілізувавши Еквадор і загрожуючи стабільності Уругваю. Поки в Болівії, Перу та Колумбії вироблятимуть сотні тонн кокаїну, поки в Європі та США існуватиме стабільний і платоспроможний попит, доти існуватиме й трафік. Він, мов вода, знайде собі шлях. Перекриєш одне русло — вода проб'є собі десять нових. І кожне нове русло нестиме з собою корупцію, насильство і смерть туди, де їх раніше не було.

AMLA проведе перше публічне слухання щодо двох проєктів RTS [17]

9 березня 2026 року Орган із протидії відмиванню коштів та фінансуванню тероризму (AMLA), що базується у Франкфурті-на-Майні, оголосив про проведення 24 березня 2026 року свого першого публічного слухання. Захід організований у форматі двох окремих сесій та присвячений двом проєктам регуляторних технічних стандартів (RTS), розробка яких є частиною мандату AMLA відповідно до нового пакету законодавства ЄС у сфері ПВК/ФТ. Перша сесія (10:00–12:00 CET) охоплює проєкт RTS за статтею 19(9) Регламенту (ЄС) 2024/1624 щодо критеріїв

[17] https://www.amla.europa.eu/amla-hold-public-hearing-two-draft-rts_en

ідентифікації ділових відносин, разових та пов'язаних транзакцій, а також нижніх порогових значень. Друга сесія (13:30–15:30 CET) присвячена проєкту RTS за статтею 28(1) щодо належної перевірки клієнтів. Обидва консультаційні документи відкриті для публічного обговорення до 8 травня 2026 року (23:59 CEST). Участь у слуханні є відкритою для всіх зацікавлених сторін, однак потребує попередньої реєстрації — кількість місць обмежена.



Консультаційний документ AMLA щодо проєкту RTS за статтею 19(9) AMLR, датований 9 лютого 2026 року, реалізує мандат, що охоплює дві взаємопов'язані, але аналітично відмінні задачі. По-перше, розробку критеріїв ідентифікації ділових відносин, разових транзакцій та пов'язаних транзакцій по всьому Союзу для забезпечення першого кроку у застосуванні рамок ПВК/ФТ. По-друге, визначення суб'єктів, секторів або транзакцій підвищеного ризику, до яких повинні застосовуватися знижені порогові значення для заходів CDD. Принципово важливим методологічним посилом документа є те, що критерії RTS не є вичерпними або умовними щодо законодавчих визначень AMLR: ділові відносини або пов'язані транзакції можуть існувати навіть за відсутності будь-якого з критеріїв, передбачених RTS. Іншими словами, RTS надає операційні орієнтири без звуження правового стандарту.

Стаття 1 проєкту RTS визначає разові транзакції негативно — як транзакції, що не відповідають визначенню ділових відносин. Це важливе концептуальне роз'яснення, оскільки AMLR розглядає ці поняття як взаємовиключні. Стаття 2 надає критерії ідентифікації ділових відносин, звертаючи особливу увагу на специфіку різних категорій підзвітних суб'єктів. Для суб'єктів нефінансового сектору, що зазвичай не проводять транзакції самостійно, але надають послуги, пов'язані з транзакціями (нотаріуси, юристи, ріелтори, бухгалтери, постачальники послуг трастам і компаніям, інвестиційні консультанти), встановлені два специфічні критерії елемента повторюваності: надання послуг з різними інтервалами (наприклад, адвокат, що управляє банківськими рахунками або коштами клієнта), та надання різних видів послуг (кілька різних категорій послуг у межах ПВК/ФТ-рамки одному клієнту). Щодо секторів з підвищеним ризиком — обміну валюти та грошових переказів, а також аналогічних послуг CASP — AMLA встановлює конкретний кількісний критерій: три транзакції протягом ковзного 12-місячного періоду вважаються достатнім критерієм для елемента повторюваності, що слід враховувати при ідентифікації ділових відносин. Ковзний період означає, що облік ведеться безперервно і не скидається в кінці календарного року.

Стаття 3 проєкту RTS детально регламентує критерії ідентифікації пов'язаних транзакцій, що є ключовим інструментом запобігання обходу порогових значень CDD шляхом дроблення транзакцій. Критерії охоплюють: ідентичне або схоже походження, призначення та мету (наприклад, транзакції, пов'язані з однією накладною, номером бронювання або замовленням, а також розстрочені платежі); «інші релевантні характеристики» (наприклад, кругообіг коштів між рахунками чи юрисдикціями, синхронізовані транзакції, використання однієї IP-адреси, однакового ідентифікатора пристрою або геолокації, участь у програмі лояльності); а також «конкретний часовий проміжок», тривалість якого, як підкреслює AMLA, варіюється залежно від характеру бізнесу суб'єкта. Важливим нюансом є те, що ряд критеріїв застосовується лише на основі інформації, вже доступної підзвітному суб'єкту, — останній не зобов'язаний запитувати у клієнта додаткову інформацію виключно для цілей цього RTS.

Щодо нижніх порогових значень AMLA приймає принципово консервативний підхід: на даному етапі не вводяться жодні додаткові знижені пороги для CDD при разових транзакціях. AMLR вже містить спеціальні пороги для певних секторів і транзакцій (1 000 євро для CASP; 3 000 євро для готівкових транзакцій; 2 000 євро для провайдерів азартних ігор), і AMLA не виявила

беззаперечних доказів необхідності введення додаткових порогів, які б були пропорційними пов'язаному навантаженню на суб'єктів та клієнтів.

Консультаційний документ за статтею 28(1) AMLR, також датований 9 лютого 2026 року, є більш масштабним і концептуально складним. Він реалізує мандат AMLA щодо розробки RTS, що визначають вимоги та інформацію для збору з метою стандартної CDD, спрощеної CDD (SDD) та посиленої CDD (EDD). Процесуальна передісторія документа є важливою для розуміння його змісту: 12 березня 2024 року Єврокомісія звернулася до Європейського банківського органу (EBA) за технічними порадами для забезпечення оперативного старту AMLA. EBA провів тримісячне публічне консультування та публічне слухання у квітні 2025 року (понад 600 учасників), отримав 170 відповідей та 30 жовтня 2025 року подав до Єврокомісії відповідь на Запит, що включала проєкт RTS щодо CDD. AMLA прийняла роботу EBA як сильну відправну точку, дотримуючись п'яти принципів EBA: пропорційний ризик-орієнтований підхід; орієнтація на ефективні та практичні результати; технологічна нейтральність; максимальна гармонізація між наглядовими органами, державами-членами та секторами; та мінімізації регуляторних збоїв шляхом використання існуючих стандартів EBA, одночасно узгоджуючись із глобальними стандартами ПВК/ФТ.

AMLA внесла точкові модифікації до тексту EBA, зосередившись на двох пріоритетах: розширення застосування до нефінансового сектору (суб'єкти якого не охоплювалися фокусом EBA) та уточнення формулювань для усунення потенційної двозначності. Зокрема, AMLA вдосконалила положення щодо верифікаційних заходів у форматі non-F2F та положення щодо розуміння структури власності та контролю клієнта у випадку складних корпоративних структур і ідентифікації PEP. Щодо SDD — AMLA підтвердила, що існуючі положення статті 33 AMLR вже є достатньо гнучкими для охоплення необхідних спрощених заходів, і не ідентифікувала можливостей для введення додаткових спрощень без перевищення мандату та без створення виключень із основних зобов'язань, що суперечило б AMLR. Концептуально важливою є стаття, що визначає умови, за яких підзвітний суб'єкт може здійснювати ідентифікацію старших керівних посадовців (SMO) замість бенефіціарних власників: це допускається лише після вичерпання всіх можливих засобів ідентифікації КБВ або за наявності сумнівів у тому, що ідентифіковані особи є реальними КБВ. Стандарт «виснаження всіх можливих засобів» є значно вищим, ніж звичайна ускладненість корпоративних структур, що фактично закриває поширену лазівку для відмови від ідентифікації КБВ. Документ також врегульовує порядок ідентифікації КБВ для колективних інвестиційних суб'єктів (CIU) при розподілі через посередницькі установи, дозволяючи у визначених умовах покладатися на посередника при ідентифікації кінцевих інвесторів.

Ваша думка важлива!

1. Якою, на вашу думку, мала б бути інституційна конфігурація публічно-приватного аналітичного хабу в Україні для боротьби з онлайн-шахрайством — і які конкретні правові, технічні та координаційні бар'єри сьогодні унеможливлюють або ускладнюють його створення?
2. Яким чином Держфінмоніторинг та українські СПФМ могли б адаптувати типологічний підхід NTFRA для ідентифікації транзакцій, пов'язаних з фінансуванням збройних формувань, — і яких правових та операційних інструментів для цього бракує в нинішній українській системі ПВК/ФТ?
3. В умовах, коли значна частина уваги Сил безпеки та оборони України прикута до лінії фронту, наскільки вразливою стає портова інфраструктура та західні кордони для транзиту нелегальних товарів, включаючи наркотики? Чи не створює війна «відкритого вікна» для міжнародних злочинних синдикатів?
4. Як війна впливає на структуру попиту та пропозиції синтетичних наркотиків в Україні? Наскільки існує ризик перетворення України на регіональний хаб для виробництва синтетичних наркотиків через менший контроль за хімічними прекурсорами під час війни?
5. Яким чином держави можуть забезпечити ефективне регулювання криптовалютного ринку та протидію ВК/ФТ у цифрових активах, не стримуючи при цьому розвиток інновацій і фінансових технологій, і яку модель регуляторної політики доцільно формувати Україні в умовах інтеграції до фінансової системи ЄС?
6. Які нові ризики для глобальної безпеки та систем протидії ВК/ФТ можуть виникнути у зв’язку з використанням кримінальними мережами нових технологій транспортування (наприклад, автономних морських апаратів, дронів або напівзанурюваних суден), і як міжнародна спільнота, включаючи Україну, повинна адаптувати регуляторні та оперативні механізми для реагування на ці загрози?

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-2026-11

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].