Методологічний бюлетень

Серійний номер: МінФін-AML-2026-03

Січень 2026

“Ким би ви не були, будьте кращими!”

сентенція XIX століття

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

Використання віртуальних активів для фінансових злочинів [1]

Публічний звіт Підрозділу фінансової розвідки Об’єднаних Арабських Еміратів щодо віртуальних активів за грудень 2025 року є комплексним аналітичним документом, який поєднує елементи секторальної оцінки ризиків, регуляторного керівництва та стратегічної комунікації з міжнародною AML/CFT/CPF-спільнотою. На відміну від багатьох національних звітів, що обмежуються описом загальних тенденцій крипторинку, цей документ чітко вбудований у архітектуру ризик-орієнтованого підходу FATF і демонструє, яким чином віртуальні активи інтегруються у загальну систему фінансового моніторингу без створення паралельних або спрощених режимів регулювання. Базова теза звіту полягає в тому, що віртуальні активи не створюють принципово нових типів фінансових злочинів, однак істотно змінюють їх масштаб, швидкість та складність виявлення, що потребує якісно іншого рівня аналітичної та інституційної спроможності.

[1] https://www.uaefiu.gov.ae/media/sjsfchg1/uaefiu-report-on-vas-public-version-dec-2025.pdf

Методологічна основа звіту заслуговує на окрему увагу, оскільки ПФР ОАЕ прямо демонструє, що аналіз ризиків у сфері віртуальних активів не може ґрунтуватися виключно на статистичних даних або окремих кейсах. Документ базується на поєднанні кількох масивів інформації: звітності про підозрілі операції (STR/SAR), отриманої від VASP, результатів фінансових розслідувань, даних міжнародного обміну фінансовою розвідкою, а також аналітики з використанням інструментів блокчейн-розвідки. Такий підхід дозволяє регулятору не лише ідентифікувати типові сценарії зловживань, але й оцінити ефективність самих механізмів фінансового моніторингу у цьому секторі. Фактично звіт виконує функцію зворотного зв'язку для піднаглядних суб'єктів, демонструючи, які саме елементи їхніх систем управління ризиками працюють неналежним чином.

Змістовно звіт детально аналізує ключові категорії AML/CFT/CPF-ризиків, пов'язаних із віртуальними активами, зокрема відмивання доходів від кіберзлочинів, інвестиційного шахрайства, використання криптоактивів у схемах обходу санкцій, а також у фінансуванні терористичної діяльності та інших форм організованої злочинності. При цьому регулятор послідовно наголошує, що найбільш уразливими є не окремі типи токенів або технологічні рішення, а бізнес-моделі та операційні практики VASP. У звіті прямо вказується, що слабкі процедури ідентифікації клієнтів, формальний підхід до оцінки ризиків, недостатній контроль за транзакціями та низький рівень розуміння клієнтської поведінки створюють умови, за яких віртуальні активи стають зручним інструментом обфускації фінансових потоків.

З юридичної точки зору документ є важливим прикладом того, як регулятор інтерпретує та застосовує національне законодавство у сфері ПВК/ФТ/ФР до динамічних і гібридних моделей бізнесу. ПФР ОАЕ чітко артикулює підхід, відповідно до якого визначальною є економічна сутність операцій, а не формальний статус компанії або технологічний характер послуг. Це дозволяє поширювати AML/CFT-вимоги на широкий спектр діяльності, включно з платформами, що намагаються позиціонувати себе як «чисто технологічні» або такі, що не здійснюють безпосереднього зберігання активів. У контексті глобальних дискусій щодо регулювання DeFi цей підхід є особливо показовим, оскільки демонструє небажання регулятора залишати поза наглядом будь-які сегменти ринку, здатні бути використаними для фінансових злочинів.

Окремий блок звіту присвячений міжнародному виміру ризиків, що має критичне значення для ОАЕ як транзитної фінансової юрисдикції. ПФР ОАЕ прямо визнає, що віртуальні активи активно використовуються у транскордонних схемах, пов'язаних із високоризиковими юрисдикціями та суб'єктами, які перебувають під санкціями. У цьому контексті наголошується на необхідності посиленого міжнародного співробітництва, своєчасного обміну фінансовою розвідкою та гармонізації підходів до регулювання VASP. Фактично звіт слугує інструментом демонстрації того, що ОАЕ не лише імплементують стандарти FATF формально, але й прагнуть відігравати активну роль у глобальній системі протидії фінансовим злочинам.

У підсумку, публічний звіт ПФР ОАЕ формує чіткий регуляторний сигнал для ринку: сектор віртуальних активів розглядається як повноцінна складова фінансової системи з відповідним рівнем відповідальності, наглядового контролю та санкційних ризиків. Для інших юрисдикцій документ є практичним прикладом того, як можна поєднати підтримку фінансових

Висновки:

- VASP інтегруються в систему фінансового моніторингу ОАЕ на рівні, еквівалентному традиційним фінансовим установам.
- Основні AML/CFT/CPF-ризики пов'язані з якістю процедур управління ризиками, а не з технологією блокчейн як такою.
- Регулятор застосовує підхід економічної сутності, що дозволяє охоплювати гібридні та нові бізнес-моделі.
- Віртуальні активи розглядаються як значущий інструмент у транскордонних схемах фінансових злочинів, включно з обходом санкцій.

інновацій із жорстким і послідовним підходом до AML/CFT/CPF, не створюючи регуляторних «сірих зон».

Цифрова стратегія ESMA 2026-2028 [2]

Цифрова стратегія Європейського органу з цінних паперів та ринків (ESMA) на 2026–2028 роки є програмним документом, який визначає не лише напрями внутрішньої цифрової трансформації регулятора, але й контури майбутньої моделі фінансового нагляду в Європейському Союзі. Хоча документ не позиціонується як спеціалізований AML/CFT-акт, його положення мають прямий і системний вплив на архітектуру протидії фінансовим злочинам, зокрема у секторах із підвищеним рівнем технологічних та транскордонних ризиків. ESMA виходить з базового припущення, що традиційні, переважно документарні та ретроспективні моделі нагляду більше не відповідають реаліям цифрових фінансових ринків, де швидкість операцій, складність продуктів і обсяг даних унеможливлюють ефективний контроль без використання сучасних аналітичних інструментів.

Методологічним ядром стратегії є концепція data-driven supervision, яка передбачає перехід від фрагментованого аналізу звітності до системного використання великих масивів структурованих і неструктурованих даних. Для AML/CFT-сфери це означає поступову трансформацію підходів до виявлення підозрілих операцій і схем, де ключову роль відіграватимуть автоматизовані аналітичні моделі, алгоритми виявлення аномалій та міжвідомча інтеграція даних. ESMA прямо визнає, що здатність регулятора аналізувати дані в реальному або близькому до реального часу стає критичним фактором ефективності нагляду, особливо в умовах поширення цифрових активів, платформних бізнес-моделей та інноваційних фінансових сервісів.

З правової точки зору стратегія тісно пов’язана з імплементацією нових регуляторних рамок ЄС, включно з MiCA, DORA та AML-пакетом Європейського Союзу. ESMA позиціонує себе як ключового координатора гармонізованого наглядового підходу, покликаного мінімізувати регуляторний арбітраж між державами-членами. У контексті AML/CFT це має особливе значення, оскільки різний рівень цифрової зрілості національних регуляторів і неоднакові підходи до нагляду створюють прогалини, які можуть використовуватися для відмивання коштів та інших фінансових зловживань. Стратегія прямо вказує на необхідність уніфікації стандартів збору, обробки та аналізу даних на рівні ЄС.

Висновки:

- Майбутній фінансовий нагляд у ЄС ґрунтуватиметься на системному аналізі даних.
- AML/CFT-контроль дедалі більше інтегруватиметься у загальну модель цифрового нагляду.
- Гармонізація підходів зменшить можливості регуляторного арбітражу.
- Технологічна спроможність стає фактором наглядової оцінки.

Окрему увагу ESMA приділяє внутрішній трансформації власної інституційної спроможності. Йдеться не лише про інвестування в IT-інфраструктуру, але й про переосмислення ролі людського капіталу в регуляторі.

[2] https://www.esma.europa.eu/sites/default/files/2026-01/ESMA65-955014868-12887_ESMA_Digital_Strategy_2026_-_2028.pdf

У документі наголошується на потребі формування міждисциплінарних команд, здатних поєднувати правову, фінансову та технічну експертизу. Для AML/CFT-нагляду це означає поступовий відхід від формального контролю відповідності до аналітично орієнтованого підходу, де якість внутрішніх систем управління ризиками стає одним із ключових об'єктів наглядової оцінки.

У стратегічному вимірі документ ESMA відображає загальноєвропейський зсув у бік проактивного регулювання, де регулятор прагне не лише реагувати на порушення, але й формувати поведінку ринку через технологічні та методологічні інструменти. Для AML/CFT/CPF-спільноти це означає, що у найближчі роки зростатимуть очікування щодо цифрової зрілості піднаглядних установ, якості даних та здатності пояснювати логіку прийняття рішень у системах фінансового моніторингу.

Глобальні економічні перспективи [3]

Аналітичний огляд звіту Світового банку «Global Economic Prospects», оприлюдненого у січні 2026 року, вимагає відходу від традиційного сприйняття макроекономічних показників виключно як індикаторів ділової активності. Для спільноти AML/CFT (Anti-Money Laundering / Combating the Financing of Terrorism) цей документ є картою вразливостей глобальної фінансової архітектури. Він вказує на зони, де економічний тиск може призвести до послаблення регуляторних бар'єрів, зростання корупційних ризиків та активізації тіньових схем переміщення капіталу.

1. Макроекономічний контекст: Стагнація як драйвер тіньової економіки

Світовий банк прогнозує, що глобальне економічне зростання у 2026 році стабілізується на рівні 2,6%, з незначним підвищенням до 2,7% у 2027 році. На перший погляд, це свідчить про так звану "м'яку посадку" (soft landing) світової економіки після турбулентності попередніх років. Однак, детальна декомпозиція цих показників виявляє тривожні тенденції, які мають безпосереднє значення для оцінки ризиків клієнтів та транзакцій.

По-перше, звіт констатує, що 2020-ті роки ризикують стати десятиліттям з найнижчими темпами зростання з 1960-х років. Для країн з ринками, що формуються, та країн, що розвиваються (EMDE — Emerging Market and Developing Economies), це означає суттєве уповільнення темпів конвергенції доходів з розвиненими економіками. Прогнозується, що зростання в EMDE (за винятком Китаю) утримуватиметься на рівні 3,7% у 2026 році.

Аналітичний висновок для СПФМ: Історичний досвід та кримінологічні дослідження свідчать про чітку обернену кореляцію між темпами легального економічного зростання та обсягами тіньової економіки. В умовах стагнації легальних ринків, суб'єкти господарювання схильні до оптимізації витрат через ухилення від сплати податків та використання схем переведення коштів у готівку. Це означає, що у 2026 році СПФМ повинні очікувати зростання попиту на послуги конвертаційних центрів та "податкових ям", особливо в секторах, найбільш чутливих до економічного циклу (будівництво, рітейл).

[3] https://openknowledge.worldbank.org/server/api/core/bitstreams/f53549d4-6c5b-43b8-ae8e-9432ab8917b9/content

По-друге, звіт підкреслює "розчаровуючу нерівномірність" відновлення. Якщо розвинені економіки майже повністю відновили свій докризовий рівень, то чверть країн, що розвиваються, залишаються біднішими, ніж у 2019 році.

Ризик-індикатор: Такий розрив у добробуті є потужним драйвером для нелегальної міграції та, відповідно, для функціонування неформальних систем переказу коштів (типу Hawala), які обслуговують мігрантів. Крім того, низький рівень життя в країнах EMDE розширює базу для вербування так званих "грошових мулів" (money mules) — фізичних осіб, які за невелику винагороду надають свої банківські рахунки для транзиту злочинних коштів. СПФМ слід посилити моніторинг рахунків фізичних осіб з ознаками транзитної активності, особливо якщо джерелом надходжень є юрисдикції з низьким рівнем доходу, зазначені у звіті Світового банку.

2. Торговельна фрагментація та протекціонізм: Ренесанс схем TBML

Однією з наскрізних тем звіту є зростання торговельної напруженості та невизначеності торгової політики. Світовий банк відзначає, що глобальна торгівля стикається з безпрецедентною кількістю нових тарифів, експортних обмежень та санкційних бар'єрів. Це явище, яке у звіті описується як "фрагментація", має фундаментальні наслідки для методології виявлення відмивання коштів через торгівлю (Trade-Based Money Laundering — TBML).

Механіка ризику: В умовах вільної торгівлі ціни на товари вирівнюються, що полегшує виявлення аномалій (завищення або заниження вартості в інвойсах). Однак, введення високих тарифів та ембарго створює штучні цінові викривлення та стимулює контрабанду.

- **Схеми обходу санкцій:** Звіт вказує на те, що експорт Китаю залишається стійким завдяки переорієнтації на треті країни. Це підтверджує гіпотезу про використання юрисдикцій-транзитерів (transshipment hubs) для приховування країни походження товарів. СПФМ повинні приділяти підвищену увагу аналізу коносаментів та сертифікатів походження, особливо якщо маршрут постачання є економічно нелогічним (наприклад, постачання високотехнологічних товарів через країни Центральної Азії або Кавказу).
- **Over-invoicing та Under-invoicing:** Високі імпортні тарифи стимулюють імпортерів до заниження митної вартості (under-invoicing) для ухилення від податків. Водночас, жорсткий валютний контроль у деяких країнах EMDE стимулює експортерів до заниження експортної вартості для залишення валютної виручки за кордоном. СПФМ мають інтегрувати у свої автоматизовані системи моніторингу дані про актуальні митні тарифи та торговельні обмеження, щоб виявляти транзакції, економічний сенс яких полягає виключно в регуляторному арбітражі.

3. Фіскальні правила: Інституційна стійкість чи декорація для корупції?

Особливої уваги заслуговує третій розділ звіту, присвячений фіскальним правилам. Світовий банк провів комплексний аналіз ефективності бюджетних обмежень у країнах, що розвиваються, де державний борг досяг 55-річного максимуму.

Методологічний аналіз: Дослідження базується на використанні методу локальних проекцій (Local Projections), розробленого Jordà (2005), для оцінки динамічного впливу фіскальних правил на циклічно скоригований первинний баланс. Ця методологія дозволяє очистити бюджетні показники від впливу економічного циклу і побачити реальні зусилля уряду щодо консолідації. Звіт показує, що понад 55% країн EMDE запровадили фіскальні правила (обмеження дефіциту, боргу, видатків). Однак, ключова проблема полягає у їх виконанні.

Юридичні нюанси та ризики ПВК/ФТ: З точки зору фінансового моніторингу, наявність та дотримання фіскальних правил є індикатором якості державного управління.

- **Ризик розкрадання (Embezzlement):** У країнах, де фіскальні правила відсутні або існують лише на папері ("де-юре", але не "де-факто"), ризик нецільового використання

бюджетних коштів та корупції при державних закупівлях є критично високим. Відсутність стримувань дозволяє політичним елітам роздувати видатки під час виборчих циклів або створювати непрозорі позабюджетні фонди.

- **"Escape clauses" (Застереження про винятки):** Звіт звертає увагу на часте використання урядами механізмів призупинення дії фіскальних правил під час криз. Хоча це може бути економічно виправданим, аналітики ПВК повинні розглядати періоди призупинення правил як періоди підвищеного ризику. Саме в цей час, під прикриттям "надзвичайної необхідності", часто реалізуються масштабні корупційні схеми з виведення державних коштів через фіктивні контракти.
- **Боргова стійкість:** Високий рівень боргу в EMDE створює тиск на фінансову систему. Уряди можуть вдаватися до фінансових репресій або маніпуляцій з борговими інструментами. Для банків це означає необхідність ретельного due diligence при роботі з суверенними облігаціями високоризикових юрисдикцій, оскільки вторинний ринок таких паперів може використовуватися для легалізації коштів PEPs (політично значущих осіб).

4. Прикордонні ринки: Нова географія відмивання коштів

Цей розділ звіту фокусується на "прикордонних ринкових економіках" (Frontier Market Economies). Це група країн, які є більш розвиненими за країни з низьким доходом, але ще не

Висновки:

- **Необхідність рекалібрування ризик-профілів юрисдикцій.** Традиційні списки FATF та ЄС є необхідним, але недостатнім інструментом. СПФМ повинні інтегрувати у свої внутрішні методики оцінки ризиків макроекономічні індикатори, висвітлені у звіті Світового банку. Зокрема, країни з категорії "прикордонних ринків" та країни з критичним рівнем державного боргу і слабкими фіскальними правилами повинні автоматично отримувати підвищений скоринг ризику. Транзакції з контрагентами з таких юрисдикцій вимагають посилених заходів належної перевірки (EDD), спрямованих на виявлення ознак виведення національного багатства.
- **Посилення нагляду за операціями з цінними паперами та інвестиціями.** Враховуючи прогнозовану волатильність на ринках капіталу EMDE та активізацію інвестицій у технологічний сектор, регуляторам та банківському сектору слід зосередитися на виявленні схем відмивання коштів через інструменти фондового ринку. Це включає аналіз джерел походження коштів, що інвестуються в корпоративні права та венчурні фонди, особливо якщо об'єктом інвестування є компанії з "модних" секторів (AI, зелена енергетика) без підтвердженої історії діяльності.
- **Адаптація до торгової фрагментації.** Українським СПФМ слід враховувати, що глобальне підвищення тарифів та санкційних бар'єрів неминуче призведе до ускладнення схем постачання товарів в Україну та з України. Це вимагає впровадження просунутих аналітичних інструментів для виявлення TBML, таких як автоматизована звірка цінових параметрів контрактів з ринковими бенчмарками та аналіз мереж контрагентів для виявлення фіктивних посередників у юрисдикціях-хабах.
- **Фокус на фіскальній прозорості як елементі ПВК.** В умовах післявоєнної відбудови України, висновки Світового банку щодо фіскальних правил набувають особливої ваги. Забезпечення прозорості використання міжнародної допомоги та бюджетних коштів є пріоритетом. СПФМ повинні розглядати будь-які операції, пов'язані з державними видатками, які здійснюються в обхід стандартних процедур (наприклад, через спрощені процедури закупівель без належного обґрунтування), як високоризикові та інформувати про них Держфінмоніторинг.

досягли статусу ринків, що розвиваються. Вони характеризуються зростаючою фінансовою відкритістю, але все ще обмеженою ліквідністю та інституційною слабкістю.

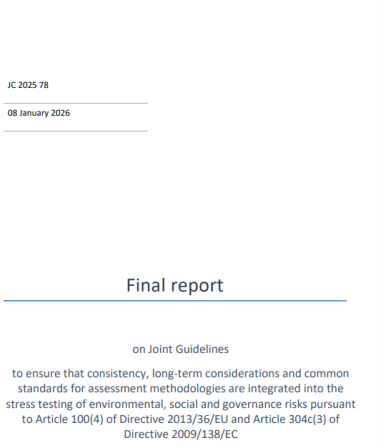
Аналіз вразливостей: Світовий банк зазначає, що ці країни активно інтегруються у глобальні фінансові ринки, залучаючи портфельні інвестиції. Проте, їх регуляторні системи (включаючи органи фінансового нагляду) часто не встигають за темпами лібералізації капіталу.

- **Інституційний розрив:** Приплив капіталу в "прикордонні ринки" часто випереджає розвиток наглядових технологій. Це робить їх ідеальними "пральнями" для міжнародних злочинних синдикатів. Злочинці можуть використовувати низьку ліквідність місцевих фондових ринків для маніпулювання цінами активів (market manipulation) та легалізації доходів через фіктивний прибуток від інвестицій.
- **Волатильність потоків:** Звіт попереджає про ризики раптової зупинки припливу капіталу (sudden stops). У періоди фінансового стресу регулятори таких країн можуть заплющувати очі на походження капіталу, аби лише утримати ліквідність у системі. Це створює вікно можливостей для розміщення сумнівних активів.

5. Технологічний фактор: Штучний інтелект як об'єкт та інструмент інвестицій

Світовий банк окремо виділяє роль інвестицій у штучний інтелект як фактора, що підтримував економічну активність у 2025 році, особливо в США. **Вплив на ПВК:** Бум інвестицій у AI створює специфічні ризики. Оцінка вартості стартапів у цій сфері часто базується на суб'єктивних прогнозах майбутніх прибутків, а не на реальних активах. Це відкриває простір для відмивання коштів через венчурне фінансування. Злочинні кошти можуть бути інвестовані у підставні AI-стартапи під виглядом легального венчурного капіталу. Крім того, нематеріальна природа продуктів AI (код, алгоритми) ускладнює перевірку реальності їх створення та вартості, що робить цей сектор вразливим до схем фіктивного надання послуг.

Вбудовування ESG-ризиків у наглядову архітектуру ЄС [4]


JC 2025 78

08 January 2026

Final report

on Joint Guidelines

to ensure that consistency, long-term considerations and common standards for assessment methodologies are integrated into the stress testing of environmental, social and governance risks pursuant to Article 100(4) of Directive 2013/36/EU and Article 304c(3) of Directive 2009/138/EC

Документ є фінальним звітом щодо Спільних настанов, ухвалених Європейськими наглядовими органами — EBA, ESMA та EIOPA — з метою забезпечення єдності, довгостроковості та методологічної узгодженості під час інтеграції екологічних, соціальних та управлінських ризиків (ESG) у наглядові стрес-тести, що здійснюються компетентними органами держав-членів Європейського Союзу. Настанови розроблено відповідно до статті 100(4) Директиви 2013/36/EU (CRD VI) та статті 304c(3) Директиви 2009/138/EC (Solvency II) і вони застосовуються до органів нагляду у банківському, страховому та інвестиційному секторах, починаючи з 1 січня 2027 року

Ключова ідея документа полягає в тому, що ESG-ризики визнаються структурними та потенційно системними факторами фінансової нестабільності, які повинні бути послідовно інтегровані в наглядові інструменти, зокрема у стрес-тестування. Водночас настанови чітко підкреслюють, що вони не створюють нового обов’язку для компетентних органів проводити стрес-тести з урахуванням екологічних, соціальних та управлінських ризиків, а встановлюють єдині принципи, очікування та методологічні орієнтири для тих випадків, коли

[4] https://www.eba.europa.eu/sites/default/files/2026-01/60ba0389-2d7a-46b7-96e8-9072c481d8ce/EIOPA-BoS-25-602%20-%20ESAs%20Final%20Report%20-%20Joint%20Guidelines%20on%20ESG%20Stress%20Testing.pdf

такі тести вже здійснюються в межах чинного секторального законодавства або або як разові (цільові) наглядові оцінки, що проводяться для конкретного випадку. Таким чином, документ спрямований насамперед на усунення фрагментації підходів між країнами та секторами і на підвищення прозорості та передбачуваності наглядових практик у ЄС.

Зміст настанов вибудувано навколо чіткого розмежування цілей ESG-стрес-тестування. З одного боку, йдеться про короткострокові наглядові стрес-тести з горизонтом до п’яти років, які мають оцінювати стійкість капіталу, ліквідності та здатність фінансових установ поглинати збитки у разі реалізації ESG-шоків. З іншого боку, значний акцент зроблено на довгостроковому сценарному аналізі з горизонтом щонайменше десять років, призначеному для перевірки життєздатності бізнес-моделей і стратегій фінансових установ у різних траєкторіях розвитку ESG-ризиків. Такий підхід відображає усвідомлення того, що більшість кліматичних та екологічних ризиків мають поступовий, кумулятивний характер і не можуть бути адекватно оцінені в межах традиційних короткострокових наглядових циклів.

Документ закріплює ризик-орієнтований та пропорційний підхід як фундамент ESG-стрес-тестування. Компетентні органи повинні починати з оцінки суттєвості, яка має визначити, які саме ESG-ризики є найбільш релевантними з урахуванням бізнес-моделі фінансових установ, структури їхніх портфелів, географічної присутності та секторної концентрації. При цьому підкреслюється, що оцінка суттєвості має бути динамічною та перспективною, здатною враховувати еволюцію ризиків, розвиток регуляторних вимог і вдосконалення доступних даних. Особлива увага приділяється ідентифікації каналів передачі ESG-ризиків у традиційні фінансові ризики, зокрема кредитний, ринковий, страховий, операційний, репутаційний та стратегічний.

Настанови передбачають поступове розширення охоплення ESG-факторів. На першому етапі компетентним органам рекомендовано зосередитися на екологічних ризиках, насамперед кліматичних, охоплюючи як фізичні ризики, пов’язані з екстремальними погодними явищами та хронічними кліматичними змінами, так і трансформаційні ризики, що виникають унаслідок змін у політиці, технологіях та ринкових переоцінках активів. Водночас документ визнає, що інші екологічні, а також соціальні та управлінські ризики мають бути інтегровані в майбутньому, коли рівень методологічної зрілості та якість даних дозволятимуть здійснювати такі оцінки на надійній основі.

Значна частина документа присвячена принципам побудови сценаріїв та методологічним аспектам проведення ESG-стрес-тестів. Компетентні органи заохочуються використовувати сценарії, розроблені міжнародно визнаними організаціями, такими як IPCC, NGFS чи IEA, та адаптувати їх до регіональних і секторальних особливостей. Особливо наголошується на необхідності врахування комбінованих негативних впливів, другорядних ефектів та непрямих каналів передачі, які можуть посилювати початкову реалізацію екологічних, соціальних та управлінських ризиків. Документ визнає обмеження кількісного моделювання на довгих часових горизонтах і допускає ширше використання якісних оцінок, наративних сценаріїв і експертного судження для аналізу стратегічної стійкості.

Окремо аналізується доцільність застосування централізованого та децентралізованого підходів, а також їх поєднання в межах комбінованих методологічних моделей. При цьому підкреслюється, що незалежно від обраного підходу наглядові органи повинні забезпечувати порівнянність результатів, уникати надмірної складності та водночас зберігати достатній рівень деталізації для адекватного відображення фізичних і трансформаційних ризиків. Аналогічно, підхід до балансових припущень має еволюціонувати від статичних моделей у короткострокових вправах до більш динамічних у середньо- та довгострокових сценаріях, за умови критичної оцінки реалістичності управлінських дій і перехідних планів фінансових установ.

Важливим блоком документа є вимоги до організаційних і управлінських аспектів. Компетентні органи повинні мати достатні людські ресурси, експертизу та IT-інфраструктуру для збору, обробки та аналізу ESG-даних, а також забезпечувати чіткі часові рамки, які дозволяють фінансовим установам якісно підготуватися до участі у процедурах наглядового стресового тестування. Наголошується на необхідності постійного діалогу між наглядовими органами та фінансовими установами, а також на важливості міжсекторальної та транскордонної координації для запобігання регуляторним прогалинам і врахування системних ефектів.

Висновки:

- **ESG-стрес-тестування закріплюється як системний наглядовий інструмент, а не експериментальна вправа:** компетентні органи зобов'язані вбудовувати результати таких тестів у капітальні, стратегічні та наглядові рішення, а не використовувати їх лише для інформаційних цілей.
- **Матеріальність і пропорційність — ключові фільтри:** наглядові органи мають концентруватися на найбільш значущих ESG-ризиках і портфелях, що дозволяє уникнути формального виконання вимог та зменшити надмірний регуляторний тиск.
- **Довгостроковий горизонт (≥10 років) стає обов'язковим мінімумом** для аналізу кліматичних і екологічних ризиків, що фактично змінює логіку наглядового мислення з реактивної на стратегічно-прогнозну.
- **Фінансові установи повинні бути готові обґрунтовувати свої управлінські та перехідні плани у межах ESG-сценаріїв:** необґрунтовані припущення щодо переорієнтації портфелів або зниження ризиків підлягатимуть критичній оцінці з боку наглядових органів.

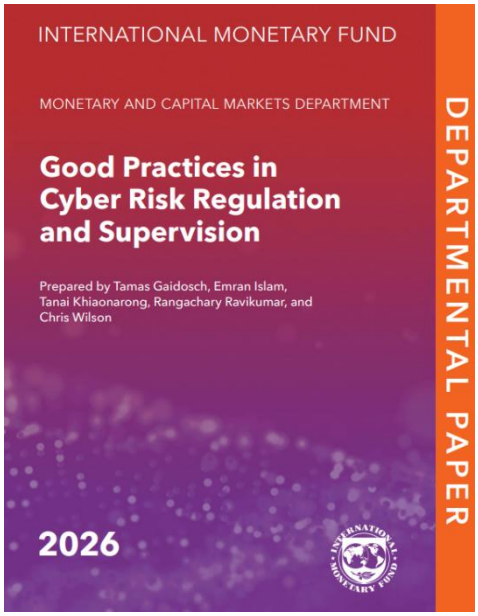
Завершуючи, документ підкреслює, що результати ESG-стрес-тестів мають бути інтегровані у ширший наглядовий процес і використовуватися для формування наглядових пріоритетів, капітальних оцінок та стратегічного діалогу з фінансовими установами. Публічне розкриття результатів повинно здійснюватися обережно, з урахуванням якості даних і методологій, щоб підвищувати прозорість і ринкову дисципліну, не створюючи при цьому небажаних ринкових викривлень. Загалом настанови формують рамкову, але водночас чітку модель еволюції наглядового мислення в ЄС, у якій ESG-ризики розглядаються як невід'ємна складова фінансової стійкості, а не як допоміжний або суто нефінансовий фактор.

Регулювання кіберризиків у фінансовій системі: уроки та кращі практики МВФ [5]

Документ, підготовленний МВФ, є комплексним аналітичним узагальненням практичного досвіду Фонду у сфері регулювання та нагляду за кіберризиками у фінансовому секторі, накопиченого з 2017 року в межах програм FSAP, технічної допомоги та співпраці з міжнародними органами стандартизації. Його ключове завдання полягає не у формуванні нових обов'язкових стандартів, а у виокремленні тих підходів і практик, які на практиці довели свою ефективність у зміцненні кіберстійкості фінансових установ і фінансових ринкових інфраструктур у різних юрисдикціях

У центрі документа перебуває теза про те, що кіберризик трансформувався з технічної або допоміжної проблеми в один з ключових системних ризиків для фінансової стабільності. Це зумовлено одночасним зростанням цифровізації фінансових послуг, залежності фінансової системи від складних ІКТ-екосистем та ескалацією кіберзагроз за масштабом, частотою й складністю. Автори послідовно показують, що фінансовий сектор є особливо привабливою

[5] https://www.imf.org/-/media/files/publications/dp/2026/english/gpcrrsea.pdf



ціллю для кіберзлочинців і державних або квазідержавних учасників через концентрацію чутливих даних, критичну роль платіжної та розрахункової інфраструктури та високий потенціал ланцюгових ефектів. Окремий акцент зроблено на системних сценаріях, коли серйозний кіберінцидент у системно важливій фінансовій установі або фінансовій ринковій інфраструктурі може призвести до втрати довіри, збоїв у наданні незамінних фінансових послуг і, зрештою, до макрофінансової дестабілізації.

Документ детально розкриває концептуальні засади кіберризику відповідно до лексикону ключових понять, що сформовані Фінансовою радою зі стабільності. Кіберризик трактується широко, охоплюючи не лише зловмисні атаки, а й інциденти, спричинені помилками персоналу, недоліками процесів або технологічними збоями. Такий підхід має принципове значення для регулювання, оскільки МВФ аргументує, що спроби жорстко відокремити ІКТ-ризик від кіберризику у нормативних вимогах створюють фрагментацію, дублювання та прогалини. Натомість пропонується інтегрована модель управління технологічними ризиками, у межах якої кібербезпека, операційна стійкість та управління ІКТ розглядаються як взаємопов'язані елементи єдиної системи контролю.

Важливою складовою аналізу є опис еволюції загрозового ландшафту. Автори фіксують різке зростання кількості кіберінцидентів і фінансових втрат, особливо після 2020 року, а також зміну їх природи — від відносно простих атак до складних багатовекторних операцій. Значну увагу приділено ролі штучного інтелекту, який одночасно підвищує ефективність кіберзахисту і радикально розширює можливості атак, зокрема через діпфейк-технології, автоматизовані фішингові кампанії та більш точне таргетування жертв. Паралельно розглядаються довгострокові виклики, пов'язані з розвитком квантових обчислень, що потенційно можуть підірвати основи сучасної криптографії та поставити під загрозу конфіденційність і цілісність фінансових даних.

Окремий розділ присвячено ролі МВФ у формуванні національних підходів до кіберризиків через інструменти фінансового нагляду і технічної допомоги. Документ демонструє, як кіберризик поступово інтегрується у Програму оцінки фінансового сектору, насамперед у частині аналізу регуляторних і наглядових рамок. При цьому наголошується, що на відміну від традиційних фінансових ризиків, кіберризик складно кількісно вимірювати, а отже ключову роль відіграють якісні оцінки, зрілість інституційних механізмів, ефективність нагляду та готовність до реагування і відновлення. Значна увага також приділяється технічній допомозі країнам з ринками, що формуються, де цифровізація часто випереджає розвиток наглядових спроможностей, що створює структурні вразливості.

Найбільш прикладною частиною документа є розгорнутий виклад «кращих регуляторних практик». МВФ підкреслює, що ефективне регулювання кіберризиків починається з якісного процесу розробки нормативних актів, який має включати аналіз потреб, оцінку альтернатив, консультації з ринком та усвідомлення регуляторного навантаження. Центральним принципом є поєднання принципо-орієнтованого та приписового підходів залежно від рівня зрілості фінансового сектору, з перевагою результативних і технологічно нейтральних вимог. Регуляторні очікування мають охоплювати корпоративне управління, внутрішній контроль, управління ризиками, життєвий цикл ІТ-систем, операційну кібербезпеку, реагування на інциденти, відновлення діяльності, регулярне тестування та незалежну оцінку.

Особливо наголошується роль органів управління фінансових установ, насамперед рад директорів, у формуванні культури кіберстійкості, визначенні ризик-апетиту, забезпеченні ресурсів та інтеграції кіберризиків у загальну систему управління ризиками. Документ детально описує практичні елементи управління, включно з контролем доступу, управлінням ідентифікацією, резервним копіюванням, тестуванням на проникнення, кібернавчаннями та управлінням ризиками третіх сторін, підкреслюючи, що аутсорсинг технологічних функцій не знімає відповідальності з фінансової установи.

У частині, присвяченій нагляду, МВФ робить чіткий акцент на тому, що реальна ефективність регулювання визначається не формальними вимогами, а якістю наглядової практики. Ефективний нагляд має бути безперервним, ризик-орієнтованим і пропорційним, поєднуючи дистанційний моніторинг, інспекції на місці, тематичні огляди та контроль за кібернетичним тестуванням. Водночас принцип пропорційності трактується не як зниження стандартів для менших установ, а як адаптація вимог з урахуванням системної значущості, з усвідомленням того, що в умовах взаємопов'язаної фінансової системи навіть невелика установа може стати джерелом серйозного системного ризику.

Завершуючи аналіз, документ виходить на рівень системних кіберризиків і підкреслює роль фінансових ринкових інфраструктур та необхідність координації між регуляторами, центральними банками, іншими органами влади та приватним сектором. Кіберстійкість розглядається як публічне благо, яке неможливо забезпечити виключно зусиллями окремих установ. Саме тому МВФ наголошує на важливості інформаційного обміну, спільних навчань, кризового планування та довгострокових інвестицій у наглядові спроможності як фундаменті фінансової стабільності в цифрову епоху.

Висновки:

- **Регулювання кіберризиків має інтегрувати ІКТ і кібербезпеку в єдину рамку управління технологічними ризиками,** оскільки їх штучне розмежування знижує ефективність контролів і ускладнює наглядову оцінку.
- **Найбільший практичний ефект дають чіткі регуляторні очікування щодо тестування, кризових навчань і управління ризиками третіх сторін,** особливо з огляду на концентрацію ризиків у великих технологічних провайдерів.
- **Активна, глибока і послідовна наглядова присутність (дистанційний нагляд + виїзний нагляд + тематичні огляди + нагляд за кібернетичним тестуванням)** є критично важливішою для кіберстійкості фінансового сектору, ніж формальне існування навіть якісних нормативних актів.
- **Пропорційність не означає зниження стандартів,** оскільки в умовах високої взаємозалежності фінансової системи найменш захищений учасник може стати тригером системного кіберінциденту з макрофінансовими наслідками.

Ризик-орієнтований підхід у дії: застосування спрощеної перевірки клієнтів у CIS [6]

Документ, підготовлений ПФР Мальти у співпраці з Управлінням з фінансових послуг Мальти та опублікований у грудні 2025 року, є комплексним аналітичним і практичним дослідженням того, як колективні інвестиційні схеми (CIS) застосовують режим спрощеної належної перевірки клієнтів (SDD) у відносинах з регульованими клієнтами, що здійснюють релевантну фінансову діяльність, як від власного імені, так і як номінали від імені базових інвесторів

[6] https://fiaumalta.org/app/uploads/2025/12/Application-of-Simplified-Due-Diligence-by-Collective-Investment-Schemes-22.12.2025.pdf

У центрі документа лежить прагнення регулятора чітко окреслити межу між допустимим ризик-орієнтованим спрощенням заходів фінансового моніторингу та небезпечною практикою формального застосування SDD, яка фактично нівелює принцип оцінки ризиків ВК/ФТ. Вихідною тезою звіту є те, що сектор CIS, попри високий рівень регуляторного нагляду, масштабність операцій і залученість до транскордонних фінансових потоків, залишається вразливим до складних схем відмивання коштів і фінансування тероризму, особливо через використання номінальних структур та зведених рахунків. Саме тому FIAU наголошує, що SDD не може розглядатися як стандартний або «дефолтний» режим для клієнтів-регульованих установ.

Тематичний огляд, покладений в основу документа, було проведено у четвертому кварталі 2023 року і він охопив двадцять CIS різних типів, включно з професійними інвесторськими фондами, альтернативними інвестиційними фондами та роздрібними схемами. Аналіз ґрунтувався на поєднанні інтерв'ю з MLRO, перегляді внутрішніх політик і процедур, а також детальному вивченні 124 клієнтських файлів і 97 транзакцій, спеціально відібраних для того, щоб охопити широкий спектр транзакційних сценаріїв, зокрема незвично великі операції, швидкі рухи коштів «in-out», одноразові транзакції, операції після тривалих періодів неактивності та трансфери третім особам. Такий підхід дозволив регулятору не лише оцінити формальну відповідність вимогам законодавства, а й проаналізувати реальну якість застосування ризик-орієнтованого підходу.

Аналізуючи практики оцінки ризику клієнтів, ПФР Мальти визнає, що переважна більшість CIS формально здійснюють оцінку ризику клієнта (CRA) і в значній частині випадків присвоєння низького ризику було обґрунтованим з точки зору наявності базових критеріїв, таких як регульований статус клієнта, його реєстрація в ЄС або еквівалентній юрисдикції та відсутність негативної регуляторної інформації. Водночас документ чітко фіксує системну проблему поверхневого підходу до CRA. Низький ризик часто сприймається як постійна характеристика клієнта, а не як результат аналітичної оцінки, що має переглядатися протягом усього ділового зв'язку. У багатьох випадках CRA не оновлювався роками, навіть за наявності змін у транзакційній поведінці або бізнес-моделі клієнта, що прямо суперечить логіці ризик-орієнтованого підходу.

Суттєва частина документа присвячена проблемі недостатнього розуміння мети та передбачуваного характеру ділових відносин між CIS і їхніми клієнтами. ПФР Мальти констатує, що лише в незначній частині проаналізованих кейсів CIS реально збирали інформацію, яка дозволяла оцінити, чи є фактичний рівень активності клієнта співмірним із заявленим бізнес- і ризиковим профілем. Особливо критично оцінюється практика формального підходу до джерела коштів, коли в досьє фігурують загальні та змістовно порожні формулювання на кшталт «кошти клієнтів», без аналізу того, хто саме є базовими інвесторами, у яких юрисдикціях вони знаходяться, які сегменти ринку вони представляють і який рівень інвестицій для них є економічно обґрунтованим. На думку ПФР Мальти, така інформаційна порожнеча фактично унеможливлює ефективний транзакційний моніторинг, оскільки CIS не має референтної моделі «нормальної» поведінки клієнта.

Розділ, присвячений безпосередньо застосуванню SDD, є одним з ключових у документі. Регулятор детально пояснює, що хоча законодавство Мальти та імплементовані норми ЄС дозволяють застосування SDD у відносинах з певними категоріями регульованих клієнтів, це допускається виключно за умови, що сукупність факторів підтверджує низький ризик ВК/ФТ.

Документ показує, що хоча у 95% перевірених випадків застосування SDD було формально обґрунтованим, існують тривожні приклади, коли SDD продовжував застосовуватися навіть після перекласифікації клієнта у середній або високий ризик. Це розглядається ПФР Мальти як серйозне порушення логіки ризик-орієнтованого підходу та свідчення того, що SDD сприймається деякими CIS як зручний стандарт, а не як виняток.

Окрему увагу у документі приділено використанню листів-підтверджень щодо дотримання вимог у сфері ПВК/ФТ та інших письмових підтверджень. ПФР Мальти наголошує, що такі документи мають бути не просто формальними, а змістовними та юридично релевантними, і походити безпосередньо від клієнта, з яким CIS має ділові відносини. Практика покладання на листи, підписані адміністраторами фондів або зберігачами активів без прямого підтвердження з боку самого клієнта-номінала, розглядається як слабке місце системи контролю, яке може призвести до втрати реальної відповідальності та прозорості.

Завершальна частина документа присвячена постійному моніторингу ділових відносин і транзакцій. Саме тут ПФР Мальти фіксує найбільш системні та критичні недоліки. У значній частині CIS або відсутні докази того, що транзакційний моніторинг реально здійснюється, або ж він зводиться до поверхневого перегляду окремих операцій без зіставлення їх із клієнтським профілем і попередньою історією. Часто великі або нетипові транзакції пояснюються як «очікувані» лише на підставі масштабу клієнта, без належного аналізу причин таких змін. ПФР Мальти підкреслює, що навіть у випадках застосування SDD саме постійний моніторинг має відігравати ключову роль у своєчасному виявленні змін ризикового профілю та прийнятті рішення про необхідність посилення заходів перевірки або подання STR.

У підсумку документ формує чітке регуляторне послання: спрощена належна перевірка є інструментом ризик-орієнтованого підходу, а не механізмом зменшення контролю. Без глибокого розуміння бізнесу клієнта, його базових інвесторів, джерел і логіки руху коштів, а також без ефективного і задокументованого транзакційного моніторингу, застосування SDD не лише втрачає сенс, але й створює суттєві вразливості для системи ПВК/ФТ та фінансової стабільності загалом.

Висновки:

- **Регульований статус клієнта не є автоматичною підставою для SDD.** CIS повинні документально доводити низький ризик ВК/ФТ на основі бізнес-моделі, типів базових інвесторів і географії, а не покладатися на сам факт ліцензування.
- **CRA має бути динамічним інструментом, а не одноразовою формальністю.** Низький ризик повинен регулярно переглядатися з урахуванням змін у транзакційній поведінці, структурі інвесторів або регуляторному середовищі; у разі зростання ризику SDD має негайно припинятися.
- **Розуміння джерела коштів і очікуваної активності є критичним для номінальних структур.** Узагальнені формулювання на кшталт «кошти клієнтів» є недостатніми; CIS мають співвідносити обсяги та частоту інвестицій із профілем базових інвесторів і запитувати пояснення при будь-яких суттєвих відхиленнях..
- **Транзакційний моніторинг залишається повною відповідальністю CIS, навіть за SDD.** Делегування операційних функцій фонд-адміністраторам не звільняє CIS від обов'язку мати докази аналізу транзакцій, належного управління повідомленнями та, за потреби, своєчасного подання STR до ПФР.

Новий кримінальний код цифрової епохи: як кіберпростір змінює природу злочинності [7]

Документ є концептуально цілісним і водночас багатовимірним аналітичним дослідженням того, як цифрова трансформація докорінно змінює природу злочинності, механізми завдання шкоди та самі засади кримінальної відповідальності у XXI столітті. Його наскрізна ідея полягає в тому, що кіберпростір більше не може розглядатися як допоміжне або вторинне середовище для злочинів: він перетворився на активний, структуроутворюючий фактор, який формує новий «кримінальний код» цифрової епохи — сукупність практик, інструментів, ролей і прогалин, що випереджають традиційні правові та інституційні реакції

У вступній частині бачення UNICRI підкреслює, що сучасні цифрові технології — від штучного інтелекту й автоматизованих систем до онлайн-платформ і глобальних мереж — одночасно посилюють законні суспільні функції та створюють принципово нові можливості для злочинної діяльності. Ключовим зсувом є те, що цифрове середовище не просто підвищує ефективність злочинів, а знижує поріг входу до них, дозволяє масштабувати шкоду майже безмежно, приховувати бенефіціарів і розмивати персональну відповідальність. Це породжує фундаментальну напругу між технологічною інновацією та людською відповідальністю, оскільки алгоритмічні системи, навіть найскладніші, не здатні до етичного судження, оцінки пропорційності чи врахування людської гідності, що є базовими категоріями кримінального права та прав людини

Центральне місце у виданні займає аналіз злочинності, пов'язаної зі штучним інтелектом. Документ детально демонструє, що AI вже використовується не епізодично, а системно — для автоматизації хакерських атак, створення адаптивного шкідливого програмного забезпечення, фішингу, шахрайства, маніпуляції інформацією та генерації синтетичних ідентичностей. Запропонована типологія злочинів — проти машини, з використанням машини, всередині машини та злочини, вчинені самою машиною — дозволяє побачити, що AI виступає одночасно інструментом, середовищем і потенційним «учасником» злочину. Особливий акцент зроблено на відсутності гармонізованих визначень і статистики AI-злочинів, що означає фактичну сліпоту держав і міжнародних організацій до реальних масштабів та динаміки цієї загрози і унеможливлює формування обґрунтованої політики протидії

Окремий, концептуально важливий блок присвячено явищу jailbreaking AI — навмисному обходу вбудованих обмежень і захисних механізмів моделей шляхом маніпуляції мовою, контекстом і логікою запитів. Документ переконливо показує, що такі атаки відрізняються від класичних кіберінцидентів, оскільки спрямовані не на код чи інфраструктуру, а на когнітивний рівень системи. Особливо небезпечними ці практики є для неурядових організацій і гуманітарних структур, які дедалі частіше використовують AI для роботи з вразливими групами населення. У таких випадках компрометація AI-систем може призвести не лише до витоку даних, а й до реальної фізичної шкоди людям, повторної віктимізації жертв насильства, втрати довіри та зриву життєво важливих соціальних сервісів

[7] https://unicri.org/sites/default/files/2026-01/F3%20The%20New%20Criminal%20Code%20-%20Deciphering%20Emerging%20Threats%20in%20Cyberspace.pdf

Значна частина видання присвячена генеративному штучному інтелекту як новому каталізатору онлайн-сексуальної експлуатації та насильства над дітьми. Документ фіксує різке зростання матеріалів сексуального насильства, згенерованих із використанням штучного інтелекту, включно з синтетичними зображеннями, створеними із застосуванням технологій глибинної підміни, практиками штучної зміни вікових ознак осіб, додатками для цифрового створення оголених зображень без згоди відповідних осіб, а також використанням синтетичних цифрових аватарів. Підкреслюється, що AI не лише масштабував виробництво забороненого контенту, а й радикально розширив коло жертв, охоплюючи дітей, дорослих і навіть самих підлітків як нову категорію правопорушників. При цьому правові системи більшості країн не встигають адаптуватися до цієї реальності, що створює небезпечний регуляторний вакуум

Водночас документ уникає одновимірного підходу до технологій і пропонує збалансований погляд на діпфейки як технологію подвійного призначення. Поряд із детальним описом її зловживань у сфері дезінформації, шахрайства та фабрикації доказів, автори показують недооцінений потенціал про-соціальних застосувань діпфейків для реалізації прав людини. Йдеться про свободу вираження, доступ до освіти, охорону здоров'я, захист приватності через синтетичні дані, а також підтримку правосуддя і безпеки. Таким чином, діпфейки постають не лише як загроза, а і як інструмент, що потребує тонкого, пропорційного та контекстно чутливого регулювання

Подальші розділи розширюють аналіз до ширшого безпекового контексту, демонструючи, як цифрові технології використовуються недержавними збройними групами для рекрутингу, пропаганди та координації насильства, як супутниковий інтернет одночасно сприяє розвитку і створює нові ризики у крихких державах, як кіберпростір стає полем інформаційних операцій у збройних конфліктах, а також як криптоактиви та цифрові платформи експлуатуються для незаконних фінансових потоків і обходу контролів. У сукупності ці кейси показують, що сучасні загрози мають гібридний характер і стирають межі між кіберзлочинністю, організованою злочинністю, тероризмом і фінансовими злочинами.

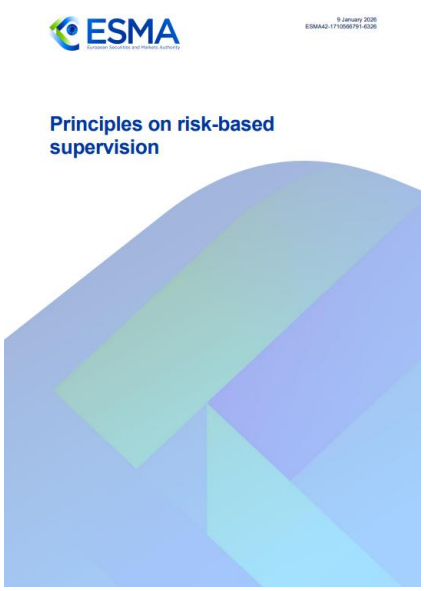
Загальний висновок документа полягає в тому, що протидія новим кіберзагрозам не може зводитися виключно до технічних рішень. Вона потребує збереження людини в центрі прийняття рішень, чіткого розподілу відповідальності, міжнародної координації та інтеграції прав людини у всі стратегії кібербезпеки й кримінальної юстиції. Видання фактично закладає інтелектуальну основу для переосмислення кримінального права і

Висновки:

- **Без уніфікованих визначень і збору даних про AI-злочини держави залишаються «сліпими» до реального масштабу загрози.** Необхідно терміново стандартизувати категорії AI-злочинів і інтегрувати їх у національні та міжнародні системи кримінальної статистики.
- **Jailbreaking AI є не технічною, а системною управлінською проблемою.** Організації, особливо ті, що працюють із вразливими групами населення, повинні впроваджувати процедури імітаційного тестування систем AI з використанням сценаріїв дій зловмисників, обов'язкові перевірки безпеки систем AI під час процедур закупівель, а також системне навчання персоналу ризикам, пов'язаним із використанням AI.
- **Генеративний AI радикально змінює ландшафт сексуальної експлуатації дітей, випереджаючи чинне законодавство.** Країнам необхідно оновлювати кримінальні норми, розширюючи поняття CSAM на AI-згенерований контент та інвестувати у спеціалізовані інструменти виявлення.
- **Діпфейк-технології потребують регулювання як інструментів подвійного призначення, а не суто як загроз.** Політика має одночасно мінімізувати зловживання і зберігати про-соціальні застосування у сфері прав людини, медицини та правосуддя.

політик безпеки в умовах цифрової епохи, де швидкість технологічних змін системно випереджає традиційні регуляторні механізми.

Ризик-орієнтований нагляд у ЄС: принципи ESMA як основа сучасної моделі фінансового регулювання [8]



Документ формує цілісне бачення того, яким має бути сучасний ризик-орієнтований нагляд у сфері ринків цінних паперів Європейського Союзу, та закладає спільні концептуальні й операційні орієнтири для ESMA і національних компетентних органів. Його центральна ідея полягає в тому, що в умовах стрімких змін фінансових ринків, зростання інноваційності, цифровізації, транскордонної діяльності та взаємозалежності учасників традиційний формально-правовий підхід до нагляду, який зосереджується на рівномірній перевірці дотримання всіх норм, втрачає ефективність. Натомість нагляд має бути побудований навколо системного розуміння ризиків, їх відносної значущості та потенційного впливу на інвесторів, фінансову стабільність і впорядковане функціонування ринків.

ESMA розглядає ризик-орієнтований нагляд як безперервний, динамічний і випереджальний процес, який не ставить за мету повне усунення ризиків, а натомість спрямований на їх усвідомлене управління. Документ підкреслює, що ризики є невід'ємною частиною фінансових ринків, а ключове завдання нагляду полягає у визначенні того, які ризики є прийнятними, а які – потребують пріоритетного втручання. Такий підхід передбачає неминучість компромісів і наявність чітко окресленого рівня ризикової толерантності з боку наглядових органів. Водночас наголошується, що ризик-орієнтований нагляд не є виправданням бездіяльності, а навпаки, вимагає чіткої аргументації рішень щодо концентрації ресурсів на певних напрямах та прозорості у визначенні наглядових пріоритетів.

Значну увагу документ приділяє формуванню спільної наглядової культури в межах ЄС. Принципи мають нефінансово обов'язковий характер і не створюють уніфікованої «єдиної моделі» для всіх держав-членів, однак вони встановлюють спільну логіку та мову ризик-орієнтованого нагляду. Передбачається, що національні органи адаптуватимуть ці принципи до власних правових систем, структур ринків і організаційних можливостей, використовуючи професійне наглядове судження. Таким чином, документ одночасно спрямований на підвищення конвергенції наглядових практик і збереження гнучкості, необхідної для врахування національної специфіки.

У концептуальному вимірі ESMA детально описує ключові характеристики ризик-орієнтованого нагляду. Він має бути пропорційним, тобто інтенсивність і глибина наглядових дій повинні відповідати рівню ризику, який несе конкретна установа, продукт або діяльність. Нагляд має бути орієнтований на майбутнє, із фокусом на виявлення ризиків до моменту їх матеріалізації, а не лише на реагування на вже допущені порушення. Важливою рисою є його комплексність: ризики розглядаються не ізольовано, а з урахуванням взаємозв'язків між секторами, ринками та юрисдикціями. Документ окремо наголошує на транскордонному характері сучасних

[8] https://www.esma.europa.eu/sites/default/files/2026-01/ESMA42-1710566791-6326_Principles_on_Risk-Based_Supervision.pdf

фінансових ризиків і необхідності тісної координації, обміну даними та спільних дій між наглядовими органами на рівні ЄС і за його межами.

Фундаментальною основою ефективного ризик-орієнтованого нагляду визначено наглядову стратегію. Вона повинна бути чітко сформульованою, узгодженою із загальними цілями органу та відображати баланс між різними наглядовими завданнями, такими як захист інвесторів, забезпечення стабільності та підтримання чесних і впорядкованих ринків. Центральним елементом такої стратегії є визначення ризикової толерантності або ризикового апетиту, що дозволяє відмежовувати прийнятні ризики від неприйнятних і спрямовувати ресурси на найбільш критичні напрями. Відповідальність за реалізацію та комунікацію цієї стратегії покладається на керівні органи наглядових установ, що підкреслює стратегічний, а не суто технічний характер ризик-орієнтованого підходу.

Операційною опорою RBS виступає структурована рамка оцінки ризиків, яка охоплює належне управління процесом, узгоджені методології та моделі, використання релевантних даних і регулярну оцінку ефективності наглядових дій. ESMA підкреслює важливість стандартизованих підходів до ідентифікації та оцінки ризиків у межах одного органу, що забезпечує порівнянність результатів між секторами та суб'єктами нагляду, водночас не заперечуючи необхідність гнучкості та адаптації методів до конкретного контексту.

Сам процес ризик-орієнтованого нагляду розглядається як послідовність взаємопов'язаних фаз, які можуть адаптуватися залежно від національної практики. Ідентифікація ризиків здійснюється як на галузевому рівні, так і на рівні окремих суб'єктів або їх кластерів. Галузевий аналіз спрямований на виявлення зовнішніх і системних ризиків, що формуються під впливом макроекономічних, технологічних, політичних, регуляторних чи соціальних факторів, тоді як суб'єктний рівень зосереджується на бізнес-моделях, системах управління, внутрішніх контролях, IT-інфраструктурі та операційній стійкості конкретних установ. Такий подвійний підхід дозволяє поєднати «широку картину» ринку з детальним розумінням поведінки та вразливостей окремих учасників.

Висновки:

- **Ризик-орієнтований нагляд має бути стратегічно керованим, а не лише технічним інструментом:** без чітко визначеної наглядової стратегії та ризикової толерантності органи нагляду не здатні обґрунтовано розподіляти ресурси та приймати усвідомлені компроміси.
- **Механічне застосування моделей ризик-скорингу є недостатнім і потенційно небезпечним:** ESMA прямо підкреслює необхідність поєднання кількісних індикаторів із професійним судженням та якісним аналізом першопричин ризиків.
- **Системна інтеграція галузевих і суб'єктних оцінок ризику є критичною для виявлення транскордонних і міжсекторальних загроз,** особливо в умовах зростаючої фінансової інтеграції та цифровізації ринків.
- **Ефективність нагляду визначається не кількістю перевірок, а здатністю трансформувати пріоритетні ризики у цілеспрямовані наглядові плани,** які є гнучкими, регулярно переглядаються та узгоджуються з реальними змінами ризикового середовища.

Оцінка ризиків базується на аналізі ймовірності їх виникнення та потенційного впливу, які разом формують рівень критичності ризикових сценаріїв. Документ визнає цінність кількісних методів, матриць ризиків і скорингових моделей для порівнянності та візуалізації, але водночас застерігає від їх механістичного застосування. ESMA прямо наголошує, що числові показники не здатні повністю відобразити складність фінансових ринків і можуть створювати хибне відчуття точності. Тому професійне

наглядове судження, якісний аналіз і розуміння першопричин ризиків залишаються критично важливими елементами процесу.

Завершальним етапом є пріоритизація ризиків і визначення наглядових дій у відповідь. Пріоритети мають встановлюватися з урахуванням серйозності та терміновості ризиків, появи нових або інноваційних явищ, стратегічних цілей органу та необхідності забезпечення належного охоплення всіх сфер мандату. Процес пріоритизації розглядається як динамічний, що потребує постійного перегляду в умовах зміни ризикового середовища. Результатом цього процесу повинні ставати гнучкі наглядові плани, які поєднують поточний дистанційний нагляд із цільовими перевірками та іншими інструментами втручання. Окремо підкреслюється важливість внутрішньої та зовнішньої комунікації наглядових пріоритетів, що підвищує підзвітність органів і сприяє більш ефективній взаємодії з піднаглядними суб'єктами.

У підсумку документ ESMA формує цілісну рамку ризик-орієнтованого нагляду як стратегічно керованого, аналітично обґрунтованого та гнучкого процесу, який має забезпечити більш ефективне використання наглядових ресурсів і підвищити стійкість та доброчесність фінансових ринків Європейського Союзу.

Глобальна мережа смерті: як китайські прекурсори, мексиканські картелі та фінансові схеми формують кризу синтетичних наркотиків в США [9]

На тлі глибокої та триваючої кризи громадського здоров'я, що спричинена незаконними синтетичними опіоїдами, звіт Рахункової палати США (GAO) розкриває складну та похмуру картину глобальної індустрії, яка живиться сотнями тисяч смертей.

В її центрі — мексиканські картелі, які перетворилися з регіональних наркоторговців на керуючі ланки масштабних транскордонних операцій, що постачають на американський ринок практично весь фентаніл і метамфетамін — дві речовини, які стали головними каталізаторами епідемії передозувань. За останні п'ять років ця криза забрала життя сотень тисяч американців, причому лише за дванадцять місяців від синтетичних опіоїдів померло понад 42 200 осіб.

Серцевину цієї смертельної економіки становить глобальний ланцюг поставок, що бере свій початок у хімічних лабораторіях Китаю. Мексиканські транснаціональні злочинні організації (ТЗО) вдосконалили логістику закупівель прекурсорних хімікатів, необхідних для синтезу фентанілу та метамфетаміну, до рівня високоефективного бізнесу. Після того як у 2019 році Китай запровадив контроль за фентанілом та його аналогами, картелі швидко адаптувалися, переорієнтувавшись з імпорту готового наркотику на імпорт його складових. Тепер вони отримують прекурсори через безліч каналів: безпосередньо від китайських хімічних компаній, що часто є лише фасадом; через мережу посередників у США, включаючи компанії з перепакування та свідомих співучасників; а також через незалежних брокерів, які діють у тіні.

Особливо важливу роль відіграють фірми-одноденки та схеми з використанням підставних компаній, які дозволяють приховувати справжніх бенефіціарів. Хімічна промисловість Китаю, частина якої готова працювати в сірій зоні, відкрито рекламує свої послуги на публічних електронних майданчиках, у соціальних мережах та на зашифрованих маркетплейсах. Розслідування GAO виявило, що ці компанії використовують цілу мову натяків, щоб залучити клієнтів, які шукають хімікати для незаконних цілей. Пропозиції про «непомітну доставку»,

[9] https://files.gao.gov/reports/GAO-26-107918/index.html?_gl=1*1qca46t*_ga*MTIzMTk2MzY5Ni4xNzY4MjA4MTU0*_ga_V393SNS3SR*czE3NjgyMDgxNTQkbzEkZzAkdDE3NjgyMDgxNTQkajYwJGwwJGgw

готовність змінити маркування на упаковці на назву безневинного товару та гарантії «подвійного митного очищення» є стандартними практиками. Більш того, компанії, готові до таких схем, пропонують зразки та партії хімікатів у обсягах, у десятки разів перевищуючи максимально доступні у легальних, респектабельних постачальників, що прямо вказує на їх спрямованість на промислове виробництво наркотиків, а не на законні дослідницькі цілі.

Оплата цієї нелегальної сировини відбувається в цифровому просторі, що ускладнює відстеження. ТЗО активно використовують електронні перекази коштів та криптовалюту. Електронні перекази, згадані в 80% звітів про підозрілу діяльність, пов'язаних з фентанілом, часто структуровані як численні дрібні транзакції від різних відправників, щоб уникнути порогів звітності, встановлених Законом про банківську таємницю, і замаскувати зв'язок із наркоторгівлею. Криптовалюта, зокрема біткоїн, набуває дедалі більшої популярності через сприйняту анонімність. Зростання її використання приголомшливе: обсяг криптовалюти, що надійшла на гаманці, пов'язані з китайськими виробниками прекурсорів, зріс більш ніж на 600% з 2022 по 2023 рік і продовжив збільшуватися в 2024 році. Фінансові потоки проходять через мережі кореспондентських банків і агентів грошових служб, часто за участю тих самих підставних компаній, що й у логістичних схемах.

Доставка прекурсорів із Азії до Мексики — це майстер-клас з ухилення від правоохоронних органів. Незважаючи на те, що основним шляхом для великомасштабних поставок залишаються морські порти Мексики, значна частина матеріалів потрапляє авіавантажем або через міжнародні поштові служби, що використовують експрес-доставку. ТЗО та їхні постачальники використовують цілий арсенал методів для приховування: вони розбивають партії на дрібні посилки, щоб потрапити під поріг безмитного ввезення (de minimis); змішують прекурсори з більшими обсягами легальних товарів; помилково маркують контейнери як корм для домашніх тварин або побутові товари; і навіть відправляють вантажі неочевидними шляхами, наприклад, спочатку в США, а потім через кордон до Мексики, щоб створити видимість внутрішньої торгівлі. Ця складність логістики робить перехоплення хімікатів до їх попадання в секретні лабораторії надзвичайно важким завданням.

Саме в Мексиці відбувається трансформація хімічних речовин у смертоносні наркотики. Лабораторії, розкидані по всій країні, варіюються від примітивних у міських квартирах до великих «супер-лабораторій» у віддалених сільських районах. Вони не потребують високотехнологічного обладнання, а їхня структура дозволяє швидко змінювати місце розташування. Картелі демонструють вражаючу хімічну гнучкість: у відповідь на заборони конкретних прекурсорів вони переходять на менш регульовані альтернативні хімікати. Хоча це призводить до зниження чистоти фентанілу на вулицях, небезпека не зменшується, оскільки американські дилери часто «розбавляють» або посилюють суміші ще більш небезпечними речовинами, такими як ксилазин — потужний ветеринарний седатив, який не реагує на налоксон (засіб для усунення передозування опіоїдами) та спричиняє важкі шкірні виразки, або нітазени — синтетичні опіоїди, що можуть перевершувати фентаніл за силою дії. Особливою загрозою стало масове виробництво підроблених рецептурних таблеток (переважно оксикодону, відомого як «М30»), які містять фентаніл. Ці таблетки, виготовлені за допомогою пресів і штампів, що незаконно імпортуються з Китаю, імітують справжні ліки, вводячи в оману як людей, які шукають рекреаційні наркотики, так і тих, хто вживає справжні рецептурні препарати, що призводить до ненавмисних смертей. Соціальні мережі та зашифровані платформи стали основним ринком збуту цих підробок.

Проникнення готових наркотиків в США — це чітко відпрацьована схема. Мексиканські ТЗО контролюють транспортні маршрути в Мексиці та підтримують розгалужені дистриб'юторські мережі в США. Більшість фентанілу та метамфетаміну перетинає кордон не таємними стежками, а через офіційні пункти пропуску на південному заході, де вони приховуються у вантажних автомобілях, приватним транспортом або навіть на тілах «мулів». Згідно з даними МВБ, більше

90% вилучених партій фентанілу зупиняються саме в цих пунктах. Картелі рідко беруть участь у вуличних продажах; натомість вони постачають наркотики потужним дистриб'юторським хабам у таких містах, як Лос-Анджелес, Фінікс, Х'юстон, Чикаго, Атланта та Маямі, які, у свою чергу, обслуговують менші місцеві групи та банди. Локальна торгівля все більше переміщається в онлайн: даркнет-маркетплейси, соціальні мережі (де продавці можуть відкрито рекламувати товар) та зашифровані месенджери, такі як Telegram або Signal, стали основним каналом комунікації з покупцями, обговорення цін та організації доставки, часто через поштові служби. GAO в рамках свого розслідування безпосередньо вступала в контакт із такими продавцями, які пропонували наркотики через соціальні мережі, а потім переходили до зашифрованого спілкування для уточнення деталей. Платежі на цьому рівні здійснюються готівкою, через P2P-додатки (на кшталт Cash App або Venmo) та, що все частіше, через криптовалюту, що додає ще один шар анонімності.

Однак справжній прояв генія цих злочинних організацій лежить не в логістиці наркотиків, а в логістиці грошей. Мільярди доларів прибутку, отримані в США, потрібно «відмити» — приховати їх кримінальне походження та інтегрувати в легальну економіку. Традиційні методи, такі як контрабанда готівки через кордон (перевезення великих сум фізичних грошей у вантажівках, автомобілях або навіть літаках), використання «концентраційних» рахунків (коли численні особи вносять дрібні суми готівки на один рахунок, з якого потім здійснюється масштабне зняття) та відмивання через торгівлю (маніпуляції з цінами, кількістю або описом товарів в експортно-імпортних документах), все ще широко використовуються.

Але ключовою тенденцією останніх років, яку детально документує звіт, є масове звернення мексиканських ТЗО до професійних китайських мереж відмивання грошей (CMLN). Ці мережі, часто децентралізовані та побудовані на діаспорі китайських громадян у США, Мексиці та самому Китаї, пропонують послуги, що є набагато ефективнішими, швидшими та дешевшими, ніж у традиційних колумбійських або мексиканських відмивачів. Їхня унікальна бізнес-модель ґрунтується на двох стовпах: обслуговуванні потреб картелів та допомозі багатим китайським громадянам у виведенні капіталу за кордон, обходячи суворі валютні обмеження Китаю.

Найелегантнішою та найнебезпечнішою схемою є так звана «дзеркальна транзакція». Вона працює так: представник ТЗО передає готівку від продажу наркотиків (у доларах США) члену CMLN в США. Незабаром після цього спільник ТЗО в Мексиці отримує еквівалентну суму в мексиканських песо від іншого учасника тієї ж CMLN. Фізично гроші не перетинають кордон — відбувається лише обмін зобов'язаннями всередині мережі. Потім CMLN продає отримані долари в США китайським громадянам, які, наприклад, хочуть купити нерухомість або інші активи в Америці, а ті, у свою чергу, переводять еквівалент в юанях на рахунки мережі в Китаї. Таким чином, злочинні кошти «очищаються», потреби китайських клієнтів у валюті задовольняються, а CMLN отримує комісію з обох кінців операції. Це геніальна система, яка забезпечує ліквідність усім учасникам і нейтралізує один з ключових інструментів правоохоронних органів — відстеження міжнародних грошових потоків.

Крім цього, CMLN активно використовують і традиційні банківські канали. Вони вербують громадян Китаю, які проживають у США (іноді надаючи їм підроблені паспорти), для відкриття рахунків, які потім використовуються як ті ж концентраційні рахунки для швидкого внесення та зняття готівки з подальшою купівлею дорожніх чеків. За даними FinCEN, у звітах про підозрілу діяльність часто фігурують мережі кур'єрів — громадян Китаю, які здійснюють великі внески готівкою, купують чеки або роблять P2P-перекази через рахунки, номінально пов'язані з ресторанами, салонами краси чи іншим малим бізнесом. Також CMLN займаються відмиванням через торгівлю, скуповуючи в США електроніку, предмети розкоші або навіть прекурсорні хімікати (замикаючи цикл), які потім експортуються та продаються в Китаї, генеруючи «чисті» прибутки. Масштаби діяльності CMLN вражають: за даними слідчих, у фінансовому 2023 році

більшість з приблизно 600 справ, пов'язаних із фентанілом і Китаєм, стосувалися саме цих мереж.

Боротьба з цією «гідрою», що має безліч голів, вимагає не менш складних та інтегрованих зусиль. Федеральні агенції США координують дії через щільну мережу інституційних механізмів. Спеціальні оперативні групи (task forces), такі як колишні Цільові групи з боротьби з організованою злочинністю та наркотиками (OCDETF) або нова група ФБР з боротьби з опіоїдами (J-CODE), об'єднують слідчих, прокурорів та аналітиків з різних відомств для конкретних розслідувань, дозволяючи об'єднувати повноваження та уникати дублювання. Робочі та консультативні групи, такі як Міжвідомча координаційна група з синтетичних наркотиків або Консультативна група з Закону про банківську таємницю, забезпечують постійний стратегічний діалог та обмін інформацією на високому рівні. Спільна дислокація фахівців, наприклад, у Національному цільовому центрі CBP або в Спеціальному оперативному відділенні DEA, забезпечує оперативну взаємодію та швидкий аналіз даних про вантажі, подорожі та фінансові операції. Міжнародна співпраця є життєво необхідною: угруповання «Five Eyes» об'єднує розвідувальні та правоохоронні служби п'яти англомовних країн, а програма Trade Transparency Unit МВБ співпрацює з 19 країнами-партнерами, аналізуючи митні дані для виявлення аномалій, що вказують на відмивання грошей.

FinCEN, як ключовий регулятор фінансової безпеки, видає детальні рекомендації для банків і грошових служб, описуючи «червоні прапорці» для виявлення підозрілої активності, пов'язаної з ланцюгами поставок фентанілу та діяльністю CMLN.

На початку 2025 року адміністрація Президента США впровадила новий набір рішучих, але суперечливих політичних заходів, спрямованих на перелом тенденції. Виконавчий наказ 14159 передбачає створення Цільових груп національної безпеки в усіх 50 штатах для ліквідації присутності картелів і ТЗО на території США. Однак найбільш радикальним кроком став Виконавчий наказ 14157, який визнає міжнародні картелі та ТЗО іноземними терористичними організаціями або спеціально позначеними глобальними терористами. У лютому 2025 року Державний департамент скористався цими повноваженнями, позначивши вісім ТЗО західної півкулі, включаючи картелі Сіналоа та Халіско. Це надає правоохоронним органам нові могутні інструменти: можливість застосовувати санкції, заморожувати активи, а також пред'являти звинувачення не лише в наркоторгівлі, а й у матеріальній підтримці тероризму або наркотероризмі, що тягне за собою значно суворіші вироки. Міністерство фінансів уже почало застосовувати санкції проти лідерів картелів на підставі законів про боротьбу з тероризмом. Одночасно було запроваджено високі мита на широкий спектр товарів з Китаю, Мексики та Канади, використовуючи економічний тиск для боротьби з притоком наркотиків.

Висновки:

- **Синтетичні наркотики є рушійною силою епідемії передозувань в США.** Їхнє виробництво контролюється мексиканськими ТЗО, які створили глобальний, високоадаптивний ланцюг постачання — від закупівлі прекурсорів у Китаї до дистрибуції в США.
- **Ключовою ланкою у відмиванні мільярдних прибутків картелів стали професійні китайські мережі відмивання грошей (CMLN).** Вони пропонують ефективні, дешеві та важкі для відстеження послуги, які дозволяють обходити фізичне переміщення коштів через кордон.
- **Нова політика адміністрації США спрямована на радикалізацію відповіді,** включаючи визнання картелів терористичними організаціями, запровадження економічних санкцій і мит, а також створення нових правоохоронних цільових груп.

Однак ці нові повноваження несуть і серйозні виклики. Представники МВБ висловили занепокоєння, що статус терористичної організації може ускладнити або навіть зробити небезпечною роботу під прикриттям та використання інформаторів, оскільки такі дії можуть бути витлумачені як «матеріальна підтримка тероризму». Також виникають складні питання щодо обміну розвідувальною інформацією з прокурорами в рамках кримінальних справ, що вимагає ретельного узгодження, щоб не розкрити джерела та методи розвідки. Крім того, запровадження мит може мати непереборні економічні наслідки та викликати торгові спори. Представники агенцій відзначили, що поки що надто рано оцінювати реальний вплив цих політик, і їхня ефективність залишається питанням майбутнього.

Таким чином, звіт GAO малює образ системної та багаторівневої загрози, з якою зіткнулися США. Це не просто проблема наркотиків; це проблема глобальної логістики, міжнародних фінансів, кіберзлочинності та геополітики. Мексиканські ТЗО та їхні китайські партнери створили високоадаптивну, технологічно підковану та жорстоку систему, здатну швидко реагувати на будь-які спроби її порушити. Відповідь США ґрунтується на масштабній внутрішній координації, міжнародній співпраці, посиленні фінансового моніторингу та агресивній, експериментальній політиці, яка розмиває кордони між боротьбою з наркотиками та боротьбою з тероризмом.

Безпілотне майбутнє — еволюція правоохоронної системи в епоху машин [10]

Звіт Європолу — фундаментальне стратегічне дослідження, екзистенційний виклик і водночас докладний план дій для всієї європейської правоохоронної спільноти в епоху, коли технологічна сингулярність перестає бути фантастикою і стає проблемою оперативного планування.

Документ, підготовлений Інноваційною лабораторією Європолу, пророкує не поступове вдосконалення існуючих практик, а революційний розрив шаблону, повну трансформацію операційного середовища, в якому злочинність і правопорядок існували протягом століть. Його головна теза полягає в тому, що ми стоїмо на порозі переходу від «охорони речей» до «охорони середовища, насиченого автономними суб'єктами», де традиційні поняття відповідальності, приватності, державного кордону та навіть фізичної досяжності злочинця втрачають свій класичний зміст.

Суть змін описується через чітке протиставлення «ситуативної» та «системної» парадигм. Зараз безпілотні системи — це переважно дрони, роботи для розмінування або підводні апарати — використовуються правоохоронцями саме ситуативно: їх привозять на конкретний інцидент, як спеціальний інструмент, використовують і забирають. Однак, згідно зі звітом, ця модель вже застаріває. На зміну їй йде системна інтеграція, коли безпілотники, автономні транспортні засоби, гуманоїдні помічники та роботи-кур'єри стануть такою ж органічною і постійною частиною міського та соціального ландшафту, як сьогодні автомобілі, ліфти або світлофори. Вони будуть буквально ткати соціальну та економічну тканину: доставляти їжу та ліки, прибирати вулиці, охороняти об'єкти, супроводжувати дітей, розважати, надавати медичні послуги. У цьому насиченому машинами середовищі правоохоронці вже не можуть діяти як зовнішня сила, що тимчасово застосовує технологію. Вони змушені будуть існувати всередині цього середовища, постійно взаємодіючи з автономними системами, які будуть одночасно об'єктами поліцейського контролю, потенційними знаряддями злочину, джерелами доказів і

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/The-Unmanned-Future-Report.pdf

навіть колегами. Це вимагає не просто нового обладнання, а нової філософії, нової операційної культури та абсолютно нової правової онтології.

Якщо системна інтеграція задає контекст, то чотири взаємопов'язаних мегатренди, детально описані в звіті, визначають динаміку та ризики цього переходу. Перший і найпотужніший тренд — це конвергенція штучного інтелекту (AI), сенсорних технологій, нових матеріалів та модульних архітектур. AI тут виступає не як окрема функція, а як центральна нервова система, що перетворює безпілотник з ретельно запрограмованого автомата на адаптивну систему, що вчиться. У звіті прямо говориться про наближення моменту — коли робот, інтегруючи мовні, візуальні та навігаційні моделі, зможе отримати складну вербальну інструкцію на кшталт «знайди в тому будинку на другому поверсі підозрілий предмет, схожий на вибухівку, і сфотографуй його, уникаючи контакту з людьми», самостійно розкласти її на підзадачі, виконати і звітувати. Це вже не автоматизація рутини, це делегування складних місій. Але така ж потужність стає доступною і зловмисникам. Уявіть терористичний осередок, що використовує версію відкритої AI-моделі для керування роєм з десятків дешевих дронів, які координуються для одночасної атаки на різні цілі в мегаполісі, здатні обходити перешкоди та адаптуватися до протидії. Це вже не сценарій фільму, а об'єкт обговорення в аналітичних центрах.

Другий тренд, тісно переплетений з першим, — це драматична геополітична та ринкова залежність Європи. Надзвичайно показово, що офіційний документ агентства ЄС, прямо зазначає: ключові технології, особливо в сфері дронів і AI-платформ для робототехніки, контролюються компаніями не Європейського Союзу, переважно з США та Східної Азії. Це створює не просто економічну нерівність, а глибоку стратегічну вразливість. Правоохоронні органи будують критичну інфраструктуру безпеки — системи спостереження, розвідки, протидії дронам — на чужому, потенційно ворожому або просто непідконтрольному, технологічному фундаменті. У звіті використовується термін «vendor lock-in» — технологічна пастка залежності від одного постачальника. Наслідки можуть бути катастрофічними: від прихованих лазівок у програмному забезпеченні, що дозволяють зовнішнім силам моніторити операції поліції, до раптової відмови в сервісі чи постачанні запчастин через геополітичні рішення. Ще більш тонким є ризик цензури через алгоритми: якщо система розпізнавання об'єктів, розроблена іноземною компанією, отримує оновлення, яке раптом перестає «бачити» певні типи об'єктів або дій, це може паралізувати операції. Технологічний суверенітет перестає бути абстрактною ідеєю, а стає питанням операційної незалежності та збереження демократичного контролю над силовими структурами.

Третій тренд має соціальний і навіть антропологічний характер — це глибока інтеграція роботів у соціальні зв'язки та психіку людини. Мова йде вже не про промислових роботів у цехах, а про соціальних роботів, призначених для емоційної взаємодії: роботів-компаньйонів для літніх людей, що борються з самотністю, роботів-терапевтів для дітей з аутизмом, навіть роботів-партнерів. Ці системи, оснащені AI, здатні імітувати емпатію, вивчати уподобання користувача і створювати ілюзію взаємності. І саме ця здатність робить їх потенційно потужним знаряддям кримінальної інженерії. Звіт прогнозує появу нового виду шахрайства або терористичної вербування, де жертвою маніпулює не людина через чат, а віртуозно запрограмований робот, здатний читати емоції та будувати довіру. Крім того, ці роботи, будучи постійно присутніми в приватному житті, збирають безпрецедентні обсяги даних — про здоров'я, звички, страхи, соціальні зв'язки. Це створює безпрецедентне джерело інформації для шантажу, викрадення даних та цілеспрямованих атак. Для правоохоронців виникає парадоксальне завдання: як розслідувати злочин, скоєний роботом, який одночасно є і знаряддям, і свідком, що володіє записом всієї ситуації, але чиї свідчення можуть бути сфабрикованими або зламаними? І як суспільство сприйме поліцейську акцію, в ході якої буде «поранено» або «знищено» робота-пса, до якого місцеві жителі вже встигли емоційно прив'язатися? Це змушує переосмислювати поняття доказу, свідка та навіть психологічної шкоди.

Четвертий тренд, найбільш похмурий, — це войовниче походження інновацій. Звіт однозначно ідентифікує російську війну проти України як найпотужніший за останні десятиліття каталізатор технологічного розвитку в сфері безпілотників. Україна продемонструвала світові модель «народної» війни, де тисячі невеликих майстерень та ентузіастів в гаражах здатні налагодити масове виробництво високоефективних, дешевих FPV-дронів з AI-навігацією, стійких до радіоелектронного придушення завдяки оптоволоконним лініям зв'язку. Вони збираються з доступних на глобальному ринку компонентів, а їх схеми поширюються через Telegram-канали та форуми. Це означає, що технологічний розрив між армією та недержавними акторами різко скорочується. Досвід, здобутий на полі бою — від тактики роїв до методів обходу систем протиповітряної оборони, — тепер може бути упакований у вигляді інструкцій, файлів для 3D-друку та програмного коду і знайти шлях до європейських кримінальних угруповань чи одиноких терористів. Злочинець за кілька тисяч євро отримує можливість організувати дистанційну атаку на критичну інфраструктуру, таку як електропідстанція або нафтопровід, з мінімальним ризиком для себе. Для поліції це суттєво підвищує планку: загроза може прийти не від людини зі зброєю, що прориває кордон, а від маленького, майже непомітного безпілотника, запущеного з території сусідньої країни або навіть зсередини ЄС.

У комплексі ці тренди породжують набір викликів, які змушують переосмислити всі аспекти правоохоронної діяльності. По-перше, це виклик просторової трансформації. Класична поліція контролює вулиці, площі, будівлі — двовимірні, по суті, поверхні. У майбутньому злочинність активно освоїть третій вимір: повітря для доставки наркотиків дронами через кордони або спостереження, підводний простір для контрабанди на безпілотних субмаринах, навіть підземні комунікації для несанкціонованого доступу.

По-друге, виклик атрибуції та відповідальності. У цифрову епоху зловмисника вже важко знайти. Якщо дрон скинув вибухівку, хто винний? Той, хто його зібрав? Той, хто написав код для навігації? Той, хто придбав компоненти? Той, хто надав Wi-Fi для завантаження координат? Або, може, власник облікового запису в хмарному сервісі, через який керували роєм, і який було зламано? Це створює правовий вакуум, який одночасно ускладнює покарання винних і загострює питання страхування та компенсацій жертвам.

По-третє, виклик прозорості та втрати приватності. Звіт вводить образ «прозорого суспільства» як аналога «прозорого поля бою» в сучасних війнах. Коли мільйони приватних і комерційних безпілотників, оснащених камерами високої роздільної здатності, постійно літають над містами, коли роботи-прибиральники фіксують все на своєму шляху для навігації, коли супутники здатні розрізнити обличчя людини з орбіти, — поняття приватного життя в публічному просторі фактично зникає.

У відповідь на цей комплекс апокаліптичних на перший погляд викликів звіт Європолу пропонує не розрізнені заходи, а цілісну програму трансформації європейської правоохоронної системи. Ця програма будується на чотирьох стовпах, кожен з яких є відповіддю на певну групу проблем.

Перший стовп — операційне управління. Необхідно відмовитися від реагування на події і перейти до формування стратегічного бачення. Це означає розробку єдиної європейської доктрини щодо безпілотних систем: коли, як і з якими обмеженнями правоохоронці можуть їх використовувати та протидіти їм.

Другий стовп — компетенції. Технології безкорисні без людей, які здатні їх зрозуміти. Потрібна масштабна інвестиція в освіту та навчання. Мова не лише про курси пілотів дронів. Потрібні нові спеціальності: кібер-криміналісти, здатні аналізувати «мозок» захопленого робота; оператори AI-систем, що керують роями безпілотників; юристи, що спеціалізуються на праві робототехніки; психологи, що вивчають взаємодію людини з автономними системами.

Третій стовп — системи та інфраструктура. Розрізнені рішення окремих країн або навіть відомств приречені на провал. Необхідна інтеграція даних від безпілотних систем в єдині платформи обміну інформацією між правоохоронними органами ЄС.

Нарешті, четвертий стовп — організаційна структура. Жорсткі ієрархічні структури командування не пристосовані для роботи з швидкими, автономними агентами. Звіт пропонує перехід до моделі C3A — Командування, Управління, Співпраця та Автономність (Command, Control, Collaboration, Autonomy). Ця модель визнає, що AI і роботи можуть приймати рішення в реальному часі швидше за людину. Завдання людини-оператора — не управляти кожним кроком, а ставити цілі, визначати рамки прийнятних дій (етичні та правові обмеження) і співпрацювати з машиною як з розумним партнером, коригуючи її дії на основі свого досвіду та інтуїції.

Висновки:

- **Майбутнє правоохоронної діяльності — це моніторинг не лише вулиць, а й повітряного, підводного та підземного простору,** де злочинці використовуватимуть дрони, автономні субмарини та роботів для контрабанди, розвідки та атак.
- **Критична залежність від іноземних постачальників безпілотних систем та AI-платформ створює стратегічну вразливість,** ризики для захисту даних і втрату контролю над критичною інфраструктурою безпеки.
- **Війна стала основним драйвером інновацій, які потрапляють до злочинців**. Досвід України в масовому, децентралізованому виробництві дронів формує новий глобальний стандарт доступних високотехнологічних загроз, які можуть бути швидко адаптовані організованою злочинністю.
- **Існуюче законодавство не вирішує питань відповідальності за дії автономних систем,** що гальмує як ефективне використання технологій поліцією, так і боротьбу зі злочинним їх використанням.

У висновку звіт Європолу констатує, що технологічна революція в сфері безпілотних систем та робототехніки є об'єктивною реальністю, яку неможливо ігнорувати або заблокувати. Вона несе в собі одночасно величезні ризики та колосальні можливості для підвищення безпеки. Головна битва майбутнього розгорнеться не в повітрі між дронами, а в сфері нормотворення, стандартизації, освіти та формування суспільної довіри.

Європа стоїть перед вибором: або пасивно спостерігати, як її безпековий простір формують зовнішні технологічні гіганти, або активно взяти долю у свої руки, об'єднавши зусилля для створення безпечного, етичного та технологічно суверенного майбутнього. Час для початку цієї трансформації вже настав.

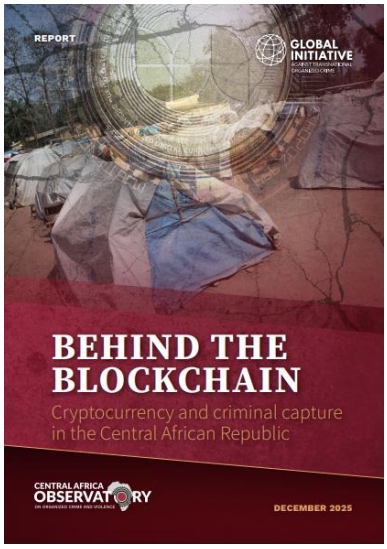
Звіти окремих інституцій та експертів

Комплексний аналіз цифрових експериментів у Центральноафриканській Республіці та їх наслідків для суверенітету та безпеки [11]

Центральноафриканська Республіка, країна втягнута в багаторічні цикли насильства, політичної нестабільності та глибокої гуманітарної кризи, з 2022 року несподівано вийшла на авансцену глобальних фінансових дискусій, проголосивши біткоїн офіційним платіжним засобом. Цей

[11] https://globalinitiative.net/wp-content/uploads/2025/12/Behind-the-blockchain-Cryptocurrency-and-criminal-capture-in-the-Central-African-Republic-Central-Africa-Observatory-on-Organized-Crime-and-Violence-December-2025.pdf

крок, на перший погляд, можна було сприйняти як сміливу спробу модернізації та прориву з фінансової ізоляції.



Однак ґрунтовний аналіз Центральноафриканської обсерваторії з організованої злочинності та насильства, розкриває зовсім іншу, значно похмурішу картину. В ній криптовалютні ініціативи постають не як інструмент розвитку, а як складний механізм державного захоплення, системного збагачення правлячої еліти, обходу міжнародних обмежень та створення нових каналів для впливу транснаціональних злочинних мереж.

Контекст, в якому народжуються ці цифрові експерименти, має вирішальне значення для їхнього розуміння. Після суперечливих президентських виборів 2020–2021 років, які тривали на тлі масштабних військових операцій за участю російських найманців Групи Вагнера, режим президента Фостена-Арканжа Туадери опинився в стані глибокої фінансової та політичної залежності. Вагнер, визнаний низкою країн та організацій транснаціональною злочинною структурою, надав критичну військову підтримку для утримання влади, а в обмін отримав фактично безконтрольний доступ до видобувних та лісозаготівельних концесій країни.

Саме в цій ситуації, коли традиційні західні донори віддалилися, а регіональні фінансові інституції на чолі з Банком держав Центральної Африки (BEAC) виступили рішучими критиками, Туадера зробив ставку на криптовалюту як на панацею. Офіційна риторика про фінансову інклюзію та модернізацію виглядала особливо цинічною з огляду на статистику: лише 15,7% населення має доступ до електроенергії, менш ніж 40% мають мобільний зв'язок, а більшість живе в умовах крайньої бідності з ВВП менше 500 доларів на людину. Очевидно, що ні про яку серйозну участь мільйонів селян у цифровій економіці не могло йти мови. Отже, істинною аудиторією з самого початку були зовнішні гравці.

Перший великий проєкт, Sango Coin, запущений у липні 2022 року, був представлений як фундамент нового валютного режиму та каталізатор токенізації природних ресурсів. Його маркетингова стратегія була однозначно націлена на іноземців: громадянство за 60 000 доларів у криптовалюті, е-резидентство за 6 000, земельні ділянки за 10 000, а також можливість інвестування в гірничодобувний і лісовий сектори. Мрія про «криптомісто» в серці Африки мала залучити мільйони. Однак дуже скоро проєкт наштовхнувся на реальність. Конституційний суд ЦАР, який на той час ще зберігав деякі ознаки незалежності, визнав неконституційним придбання громадянства, резидентства та землі за допомогою криптовалют. Це рішення, проігнороване урядом, виявило фундаментальний конфлікт між непідзвітними цифровими схемами та національною правовою системою. Подальший тиск з боку МВФ, Світового банку та регіональних органів призвів до того, що в березні 2023 року парламент скасував обов'язковий прийом біткоїна як платежу, послабивши закон.

Але це була не поразка, а тактичний відхід. Вже в липні того ж року, майже наперекір судовій владі, було прийнято закон про токенізацію землі та природних ресурсів. Цей документ юридично відкрив шлях до розчленування національного багатства на цифрові токени: від ділянок землі по 10 гектарів до лісових масивів у 500 000 гектарів, з можливістю придбання концесій строком до 99 років іноземними компаніями, зареєстрованими онлайн. Фактично, держава запустила механізм цифрової приватизації найцінніших активів без жодних належних процедур нагляду, екологічної експертизи або консультацій із місцевими громадами. Як зазначила регіональна група з протидії відмиванню коштів (GABAC), уряд не продемонстрував розуміння ризиків, пов’язаних із віртуальними активами, що робить країну магнітом для «токсичного» капіталу.

Фіаско Sango Coin, який зумів продати лише 10% запланованих токенів, не зупинило еліти. Навпаки, воно призвело до радикалізації підходу. У лютому 2025 був анонсований запуск SCAR – мемкоїна, створеного на платформі Pump.fun у мережі Solana. Цей крок сам по собі був символічним: суверенна держава звернулася до інструменту, який у всьому світі асоціюється з інтернет-тролінгом, спекуляціями та швидкими схемами. Запуск супроводжувався низкою подій, що прямо вказували на аматорський підхід та потенційне шахрайство: домен зареєстровано за три дні, сайт заблоковано провайдером, офіційний акаунт тимчасово видалено, а відеозвернення президента визнано підробкою. Проте найсуттєвішим був механізм розподілу токенів. Дані блокчейну Solana показали, що безпосередньо перед публічним запуском анонімний гаманець, пов'язаний із розробником, купив 79,3% усього обігу SCAR за мізерну суму (близько 16 600 доларів), а потім розмістив ці токени в кількох ескроу-гаманцях. Це надало розробнику абсолютний контроль над пропозицією та ціною, створивши ідеальні умови для маніпуляцій ринком. Курс монети різко злетів і так само стрімко впав, що типово для подібних схем, де перші інсайдери фіксують прибуток, а звичайні інвестори залишаються з нічого не вартими активами.

Апофеозом цієї політики став указ президента від травня 2025 року про токенізацію понад 1700 гектарів землі в префектурі Лобає, яку можна було придбати виключно за SCAR. Створена для цього онлайн-платформа пропонує «майже миттєвий» спосіб купівлі землі «без паперової роботи». Для угоди потрібна лише електронна адреса та криптогаманець, без жодної перевірки особи (KYC), процедур протидії відмиванню коштів (AML) або звернення до офіційних земельних кадастрів.

Юридичний статус цифрових сертифікатів власності залишається крайне сумнівним. У більшості юрисдикцій право власності, закодоване в смарт-контракті, не визнається еквівалентом офіційного, що створює юридичний вакуум і ризик безпрецедентних майнових суперечок у майбутньому. Оголошення про плани токенізації наступного етапу – гірничодобувних концесій – загрожує остаточно перетворити національні надри на цифровий товар, контроль над яким може бути втрачений назавжди.

Не менш важливим, ніж технічні механізми, є аналіз осіб, що стоять за цими ініціативами. Вони бездоганно демонструють злиття кримінальних, геополітичних та фінансових інтересів у найближчому оточенні президента. Ключовою фігурою архітектури Sango Coin був швейцарсько-румунський бізнесмен Ніколає Богдан Бузяну. Бузяну підозрюється швейцарською прокуратурою у причетності до масштабної торгівлі тропічним лісом між Сенегалом та Гамбією. Його бізнес-мережа, що простягається Європою та Африкою, за структурою нагадує схеми з приховування активів.

Іншою знаковою фігурою є камерунець Еміль Парфе Сімб, самопроголошений «криптогуру», відомий як «африканський Меддоф» через мільярдні шахрайські схеми, які зачепили сотні тисяч людей в Африці, Європі та Північній Америці. За його спиною – арешти, кримінальні вироки та безліч позовів. Проте Сімб не тільки отримав державну посаду та дипломатичний паспорт ЦАР, а й має тісні зв'язки з російськими пропагандистськими структурами, керуючи проросійським телеканалом Global TV.

Участь таких персонажів не випадкова; вона свідчить про те, що криптовалютні ініціативи розроблялися не фінансовими технократами, а людьми, досвідченими в створенні непрозорих схем, міжнародному шахрайстві та обслуговуванні геополітичних інтересів. Це підриває будь-яку легітимність проєктів і перетворює їх на потенційні канали для відмивання коштів, обходу санкцій та фінансування дестабілізуючої діяльності.

Таким чином, криптовалютна стратегія ЦАР постає як багатошаровий інструмент у системі, яку дослідники називають «режимом Туадери». По-перше, це інструмент фіскального виживання та обходу обмежень. Після відходу західних донорів і регіональної фінансової ізоляції

криптовалюта стала способом отримувати кошти без банківських каналів. Історична зустріч у Сочі 2017 року, протоколи якої оприлюднила Mondafrique, прямо вказує на проблему: російські платежі не могли проходити через французькі кореспондентські рахунки банків ЦАР. Криптовалюта стала запропонованим рішенням цієї проблеми.

По-друге, це механізм приватизації суверенітету. Токенізація землі та ресурсів – це не просто технологічне нововведення; це фундаментальне перетворення державних активів у товар, що легко передається анонімним гравцям на глобальних ринках. Це загрожує втратою довгострокового контролю над стратегічними активами за короткострокову вигоду.

По-третє, це засіб збагачення еліти. Механізми пре-майнінгу, контроль над ліквідністю та внутрішня інформація дозволяють вузькому колу інсайдерів (розробникам, близьким до влади бізнесменам) отримувати мільйонні прибутки від спекулятивних токенів на кшталт SCAR, тоді як державна скарбниця залишається порожньою. Жодних даних про надходження коштів від продажу SCAR до держбюджету не існує.

По-четверте, це інструмент політичного піару та створення видимості інновацій. В умовах міжнародної критики за порушення прав людини та авторитарні, гучні анонси про блокчейн та криптоміста дозволяють формувати образ прогресивного лідера-реформатора, відволікаючи увагу від репресій та кризи.

Наслідки цих процесів є глибоко деструктивними. На внутрішньому рівні вони підривають і без того мізерну довіру населення до держави, остаточно відчужуючи людей від їхніх природних ресурсів. Селяни, які вже страждають, тепер стикаються з ризиком втрати земельних прав через непрозорі цифрові угоди. На регіональному рівні політика ЦАР загрожує фінансовій стабільності Центральноафриканського економічного і валютного співтовариства (CEMAC), порушуючи договірні зобов'язання. На глобальному рівні країна ризикує перетворитися на «чорну діру» для фінансових злочинів – осередок для відмивання коштів, фінансування тероризму та міжнародних шахрайських схем, що використовують оболонку державних криптопроєктів.

Висновки:

- **Криптовалютні ініціативи в ЦАР є інструментом системного державного захоплення (state capture),** спрямованим на обхід міжнародних фінансових обмежень, легалізацію розпродажу національних ресурсів через токенізацію та збагачення вузького кола правлячої еліти.
- **Програми Sango Coin та SCAR не мали на меті реальної фінансової інклюзії чи розвитку** через критичну відсутність інфраструктури та крайню бідність населення. Вони були розраховані на зовнішніх спекулянтів і створювали ідеальні умови для ринкових маніпуляцій, "pump-and-dump" схем та відмивання коштів.
- **Токенізація землі та природних ресурсів без правових гарантій та нагляду становить пряму загрозу національному суверенітету.** Цифрові сертифікати власності сумнівної юридичної сили відкривають шлях для анонімної скупки стратегічних активів іноземними кримінальними мережами, ведучи до втрати довгострокового контролю над країною.

Досвід інших країн свідчить, що без всебічного регулювання, сильних інститутів та прозорості криптоактиви завдають величезної шкоди. У випадку ЦАР, де ці умови відсутні на всіх рівнях, шкода може стати непоправною.

Висновок дослідження є однозначним: замість того щоб бути мостом у майбутнє, криптовалюта в Центральноафриканській Республіці стала сучасним інструментом неоколоніальної експлуатації та кримінального захоплення держави. Вона не служить розвитку чи боротьбі з

бідністю; вона служить збереженню влади авторитарного режиму, який торгує національним суверенітетом для власного виживання та збагачення.

Як союз ELN та режиму Мадуро створив кримінальну наддержаву в серці Латинської Америки [12]

На світанку 16 січня 2025 року, коли туман ще лежав на пагорбах Кататумбо, понад двісті бійців Національної визвольної армії (ELN), озброєних автоматичною зброєю, мінометами та польовими раціями, розпочали скоординований наступ на позиції колишніх союзників — 33-го фронту, що належав до угруповання розколотих Революційних збройних сил Колумбії (FARC).

Операція, яка здалася спостерігачам раптовим спалахом міжусобної війни, насправді була ретельно підготовленим стратегічним маневром, кульмінацією багаторічного процесу проникнення, консолідації та трансформації ELN з колумбійської партизанської організації у могутню транснаціональну гібридну структуру, що функціонує як паралельна держава на обох берегах найдовшого кордону в Південній Америці. Понад 80 осіб загинуло в перші години наступу, а понад 50 тисяч мирних жителів, охоплених жахом, кинули свої домівки, тікаючи від насильства, що розгорталося з неймовірною жорстокістю та ефективністю. Але за цими цифрами — не просто чергова трагедія колумбійського конфлікту, а вияв абсолютно нового феномену: виникнення стабільної, добре фінансованої та політично вбудованої кримінальної держави, яка існує в симбіозі з офіційною владою Венесуели та поширює свій вплив на сусідню Колумбію.

Історія ELN почалася в 1960-х роках, коли група ідеалістів, натхненних кубинською революцією, марксизмом-ленінізмом та теологією визволення, взялася за зброю, щоб повалити колумбійську еліту. Протягом десятиліть вона залишалася менш численною та менш впливовою, ніж FARC, але зберегла свою ідеологічну риторику та структуру. Сьогодні, однак, ELN — це вже не просто партизанський рух. Це складний організм, що поєднує функції збройного формування, кримінального синдикату, політичного суб'єкта та соціальної служби. Її могутність ґрунтується на триєдиній основі: безпрецедентному контролі над наркоторгівлею, стратегічному альянсі з режимом Ніколаса Мадуро та ретельно вибудованій системі соціального управління, що перетворює місцеві громади на лояльні опори партизанської влади.

Офіційна риторика керівництва ELN, особливо її головнокомандувача Елієсера Чаморро, відомого як «Антоніо Гарсія», завжди категорично відкидала будь-які звинувачення у причетності до наркобізнесу, називаючи їх «брехнею». Проте реальність, задокументована розслідуваннями, свідчить про глибоку та всебічну інтеграцію організації у світову торгівлю кокаїном. ELN пройшла еволюцію від стягнення скромного «податку» (грамахе) з селян, які вирощують коку, до повного контролю над усіма ланками ланцюжка доданої вартості — від плантацій до міжнародної логістики. Захоплення Кататумбо в січні 2025 року мало не лише тактичне, але й надзвичайне економічне значення. Цей регіон на півночі департаменту Норте-де-Сантандер є одним з найпродуктивніших кокаїнових басейнів планети. На його 55 тисячах гектарах можна виростити сировину для 400 тонн чистого кокаїну на рік. За колумбійськими внутрішніми цінами це близько 600 мільйонів доларів, але справжнє багатство розкривається

[12] https://insightcrime.org/investigations/peace-never-had-chance-colombia-eln-venezuela/

на міжнародних ринках, де вартість того ж обсягу сягає астрономічних 10 мільярдів доларів. Для ELN контроль над Кататумбо — це гарантія фінансової безпеки, джерело, здатне вічно фінансувати її армію та політичні проекти.

Але ELN не зупинилася на простому зборі данини. Вона створила спеціалізовану фінансово-економічну архітектуру, відому як Estructura de Finanzas y Economías para la Revolución (EFER). Ця структура, підпорядкована Північно-Східному військовому фронту, функціонує як корпоративний штаб, що координує виробництво, переробку, транспортування та відмивання коштів. Вона встановлює внутрішні правила, ціни та квоти, фактично регулюючи ринок як державний орган. Під тиском колумбійської армії та американських спецслужб ELN майстерно використала кордон як захисний бар'єр. Лабораторії з виробництва кокаїну були перенесені у важкодоступні райони венесуельських штатів Сулія та Апуре. Транспортні маршрути пролягли через територію Венесуели, використовуючи озеро Маракайбо, річку Оріноко та безліч крихітних бухт на карибському узбережжі Фалькона. Відкриття наркосубмарин, що будуються в верфях Гуахіри, свідчить про те, що ELN тепер орієнтується на пряму доставку великих партій до Європи, уникаючи проміжних ланок. Ця вертикальна інтеграція та транснаціоналізація бізнесу перетворили ELN на одного з найпотужніших наркокартелів світу, чия діяльність фінансує не лише зброю, але й політичне втручання та соціальні програми.

Співпраця між ELN та венесуельською владою — це не просто таємна угода, а публічний, хоча й офіційно не визнаний, стратегічний альянс. Його коріння сягає часів Уго Чавеса, чия ідеологія «боліваріанського соціалізму» знайшла відгук у марксистсько-ленінській риториці ELN. Однак за правління Ніколаса Мадуро цей ідеологічний флер перетворився на суто прагматичну та життєво необхідну для обох сторін угоду. Для Мадуро, чий режим страждає від глибокої економічної кризи, гіперінфляції, міжнародних санкцій та внутрішньої легітимності, ELN стала багатофункціональним інструментом.

По-перше, ELN виступає як ефективна парамілітарна сила в прикордонних районах, де венесуельська держава традиційно слабка. Класичним прикладом є штат Апуре. У 2020 році венесуельська армія зазнала ганебної поразки в зіткненнях з угрупованням колишніх FARC. Мадуро звернувся до ELN, і партизани Східного військового фронту за кілька тижнів розгромили суперників, встановивши повний контроль над регіоном. Таким чином, ELN взяла на себе функції зовнішньої безпеки та внутрішнього контролю, ставши, за словами експертів, «однією з ліній оборони режиму Мадуро». У контексті періодичної напруженості з Колумбією та США, присутність досвідчених партизанських формувань вздовж кордону служить стримуючим фактором, загрозою асиметричної війни.

По-друге, ELN є ключовим гравцем у системі кримінальної економіки, що живить венесуельську верхівку — так званому «Картелі Сонця» (Cartel de los Soles). Ця система, де генерали та високопосадовці розміщуються в регіонах, багатих на контрабанду, наркотики та незаконну видобуток золота, дозволяє режиму утримувати лояльність силовиків, яких неможливо забезпечити гідною зарплатнею. ELN, контролюючи наркотрафік на кордоні, стає основним джерелом хабарів та спільних операцій для цих корумпованих елементів. Венесуельська влада отримує доступ до потужних фінансових потоків, а ELN — гарантований імунітет та захист. У штаті Тачіра, наприклад, губернатор Фредді Бернал, призначений Мадуро для боротьби з опозицією, у середині 2010-х знайшов у ELN надійного союзника для витіснення колумбійських парамілітарних угруповань «Растрохос». У винагороду ELN отримала можливість закріпитися в регіоні, регулюючи контрабанду та інші види діяльності, а Бернал отримав могутнього політичного союзника, здатного впливати на вибори та забезпечувати «стабільність».

По-третє, ELN активно втручається у політичний процес на місцевому рівні, підтримуючи кандидатів від правлячої партії PSUV. Партизани фінансують кампанії, залякують опозицію та навіть висувають своїх кандидатів, як це мало місце з командиром на прізвисько «Ель Меча» на

муніципальних виборах у Апуре в липні 2025 року. Це перетворює ELN на глибоко вбудованого політичного суб'єкта, інтереси якого тісно переплетені з інтересами венесуельської державної машини.

Крім каральних функцій, ELN також виконує соціальні та адміністративні обов'язки. Коли муніципалітети стикаються з дефіцитом палива або техніки, вони часто звертаються по допомогу до партизан. ELN ремонтує дороги в гірських селищах, фарбує будівлі, організовує спортивні заходи, фінансує дрібні громадські роботи. У Гуахірі, районі з історично слабкою центральною владою, така діяльність дозволила ELN отримати певну легітимність серед населення. Це створює парадоксальну картину: в очах частини жителів ELN є більш передбачуваною, доступною та ефективною владою, ніж далекий уряд у Каракасі або навіть місцеві чиновники. Є свідчення, що навіть представники поліції іноді перенаправляють заяви громадян до командирів ELN, визнаючи їхню юрисдикцію.

Таким чином, ELN будує не просто «кримінальний анклав», а цілу паралельну державність зі своєю економікою, судочинством, соціальною політикою та збройними силами. Ця державність існує в симбіозі з офіційною венесуельською владою, утворюючи те, що експерти називають «гібридною кримінальною державою» (Criminal Hybrid State). У цій моделі кордон між законністю та беззаконням, між державою та організованою злочинністю розмивається до невпізнання.

Висновки:

- **ELN перетворилася з колумбійської партизанської організації на потужну транснаціональну гібридну структуру,** яка функціонує як паралельна держава на обох берегах колумбійсько-венесуельського кордону.
- **Симбіоз ELN з венесуельською владою є системним та багаторівневим.** Він включає військову підтримку, економічну взаємодію та політичне втручання. Це перетворює ELN на одного з опорів правлячого режиму.
- **Соціальний контроль ELN є основою її влади.** Організація не лише завойовує території, але й управляє ними через власні суди, правила поведінки, комендантську годину, систему дозволів, а також виконує соціальні функції.
- **ELN необоротно змінила динаміку безпеки в регіоні.** Кордон більше не є бар'єром, а радше єдиним операційним простором для організації. Це робить її майже невразливою для традиційних військових операцій однієї країни та ставить під загрозу будь-які мирні ініціативи.

Ця реальність має далекосяжні наслідки. Для Колумбії це означає, що мирні переговори з ELN, які були заморожені після наступу в Кататумбо, ведуться вже не лише з внутрішнім повстанським рухом, а з потужною національною силою, що має безпечний тил у сусідній країні.

Для Венесуели — це глибока інституційна деградація, криміналізація держави та завищені ризики в майбутньому, оскільки контроль над такою потужною силою може виявитися тимчасовим. Для регіону в цілому — це загроза подальшої дестабілізації, посилення наркотрафіку та міграційних криз.

ELN не просто вижила після розгрому FARC. Вона використала геополітичний розкол між Каракасом і Боготою, економічний колапс Венесуели та вакуум влади в прикордонних районах, щоб перетворитися на домінуючу силу регіону. Її історія — це історія адаптації, прагматизму та небаченої здатності використовувати слабкості держав для побудови власної альтернативної реальності. Реальності, де партизанський командир часто має більше влади, ніж обраний мер, а чорний ринок — більше значення, ніж офіційна економіка.

Рекомендовані матеріали та події

Віртуальні активи: від основ до національної безпеки. Професійний тренінг [13]

Тема віртуальних активів розвивається шаленими темпами, і разом з новими можливостями з'являються нові ризики. Як фінансовим установам та представникам визначених нефінансових установ та професій (ВНУП) ефективно працювати в цьому полі, дотримуючись міжнародних стандартів та вимог фінмоніторингу?

Цей спеціалізований тренінг, організований Центром фінансів і безпеки (CFS) при RUSI спільно з Центром фінансової цілісності (CFI), покликаний допомогти розібратися у цих питаннях.

Що це за захід? Це комплексний тренінг, який є частиною Програми з розвитку спроможностей України у сфері протидії незаконним фінансовим потокам (за підтримки уряду Великої Британії).

Чому це важливо і кому буде корисно? Захід розроблено спеціально для **фінансових установ та ВНУП**. Ви отримаєте не лише теоретичні знання, а й практичні інструменти для роботи.

На тренінгу ви дізнаєтесь:

- **Основи:** як функціонують віртуальні активи, що таке блокчейн та які існують типи гаманців.
- **Ризики та злочини:** типології відмивання коштів, фінансові злочини та «червоні прапорці», на які варто звертати увагу.
- **Комплаєнс:** найкращі практики належної перевірки клієнтів (CDD), моніторинг транзакцій та оцінка ризиків.
- **Безпека:** як блокчейн-аналітика допомагає виявляти ухилення від санкцій та загрози нацбезпеці.

Хто спікери? Експерти-практики світового рівня та представники українських органів влади:

- **Євгеній Панченко** (Національна поліція України) — про вступ до віртуальних активів.
- **Еллісон Оуен** (RUSI) — про загрози фінансових злочинів.
- **Лукаш Лукашевський** (Chaincomply) — про управління ризиками та комплаєнс.
- **Ендрю Фірман** (Chainalysis) — про загрози нацбезпеці та аналітику.

Коли і де? Дата: 22 січня 2026 року **Час:** 09:30 – 14:40 **Формат:** Гібридний (на вибір):

- **Офлайн:** м. Київ, Київська Школа Державного Управління ім. С. Нижного (вул. Добровольчих батальйонів, 10).
- **Онлайн:** доступно для учасників з усієї України.

Мова заходу: англійська з професійним українським перекладом. Захід проводиться за правилом Chatham House (конфіденційність обговорень).

Як зареєструватися? Реєстрація відкрита до **20 січня** і доступна за посиланням.

[13] https://docs.google.com/forms/d/e/1FAIpQLSdCDAc_dBFFbo3Q2KESiGi5FjqF1XXCtaD5yLb-dn1nDCaPAQ/viewform

Інші новини

У Дубаї набула чинності заборона privacy-tokenів [14]

Запровадження в Об'єднаних Арабських Еміратах, зокрема в еміраті Дубай, заборони на використання так званих privacy-tokenів є показовим кроком у розвитку регуляторної політики щодо віртуальних активів у юрисдикціях, які водночас позиціонують себе як глобальні фінансові та технологічні хаби. Йдеться не про ситуативну або політично вмотивовану заборону, а про логічне продовження вже сформованої в ОАЕ моделі жорсткого ризик-орієнтованого підходу до регулювання сектору VASP, де допустимість фінансових інновацій прямо залежить від рівня прозорості транзакцій та можливості їх подальшого фінансового моніторингу. Privacy-tokeni, такі як Monero, Zcash або Dash у певних режимах використання, за своєю архітектурою створюють структурну несумісність із базовими вимогами AML/CFT/CPF, оскільки унеможливлюють або істотно обмежують ідентифікацію відправника, отримувача та обсягу транзакції.

Регуляторна логіка Дубаю у цьому випадку є не реактивною, а превентивною. Заборона privacy-tokenів вписується у загальну стратегію Virtual Assets Regulatory Authority (VARA), яка послідовно формує режим «контрольованої відкритості»: допуск інновацій можливий лише за умови їх повної інтеграції у систему фінансового моніторингу. На відміну від підходів деяких юрисдикцій, що намагаються адаптувати AML-інструменти до анонімних технологій шляхом компенсаторних заходів, ОАЕ обрали шлях прямого усунення інструментів, які створюють неприйнятний рівень системного ризику. Фактично регулятор визнав, що у випадку privacy-tokenів ризик відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення не може бути ефективно пом'якшений ані технічними, ані процедурними засобами.

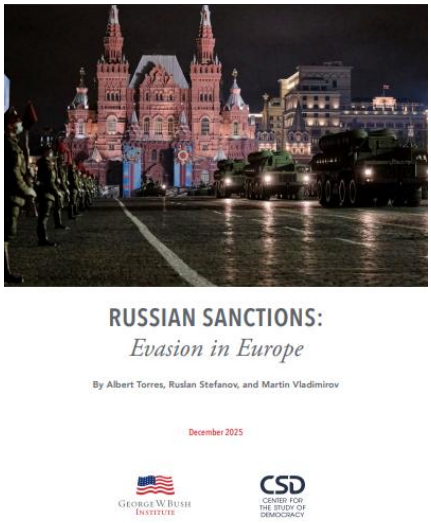
Важливою є і юридична конструкція такого рішення. Заборона не обмежується лише обігом або лістингом відповідних токенів на ліцензованих платформах, а поширюється на ширший спектр діяльності, включно з просуванням, посередництвом та наданням послуг, пов'язаних із такими активами. Це свідчить про розуміння регулятором того, що ризики AML/CFT у сфері віртуальних активів виникають не лише на рівні біржових операцій, але й у межах екосистеми сервісів, які можуть сприяти прихованому переміщенню вартості. Такий підхід корелює з сучасними тлумаченнями FATF щодо поняття VASP, де ключовим є не технологічна форма активу, а економічна сутність операцій та їх здатність бути використаними для нелегальних цілей.

З точки зору глобальної практики ПВК/ФТ/ФР, рішення Дубаю має значення, що виходить далеко за межі національної юрисдикції. ОАЕ тривалий час перебували під пильним наглядом міжнародних організацій у контексті ефективності системи AML/CFT, і останні роки демонструють послідовну політику «нульової толерантності» до високоризикових фінансових інструментів. Заборона privacy-tokenів сигналізує міжнародним партнерам та ринку, що юрисдикція готова жертвувати частиною криптоінновацій заради збереження репутації та відповідності міжнародним стандартам. Для інших країн, які лише формують свої режими регулювання віртуальних активів, цей кейс є практичним прикладом того, як ризик-орієнтований підхід може реалізовуватися не декларативно, а через чіткі та однозначні регуляторні рішення.

[14] https://incrypted.com/ua/u-dubaji-nabula-chynnosti-zaborona-privacy-tokeniv/

Для загального розвитку

Тіні європейської економіки: як росія використовує санкційні прогалини [15]



Сучасний етап протистояння між демократичним Заходом на чолі з Європейським Союзом та авторитарною росією трансформувався з військово-політичного виміру у складну та багаторівневу геоекономічну конфронтацію. Санкції, спочатку сприйняті як безпрецедентний та швидкий інструмент зупинки агресора, з часом виявилися системою з численними прогалинами, через які Кремль не лише продовжує отримувати життєво необхідні ресурси, але й відточує механізми протидії, створюючи паралельні глобальні ланцюги поставок.

Детальний аналіз експертів розкриває не просто окремі випадки порушень, а системну кризу європейських інституцій, їх фрагментацію та нездатність протистояти високоадаптивній гібридній економічній моделі росії, побудованій на десятиліттях інтеграції олігархічного капіталу, корупційних зв'язках та використанні глобальних фінансових інструментів.

На перший погляд, цифри вражають: 18 пакетів санкцій ЄС, тисячі фізичних та юридичних осіб у списках, заблоковані активи, заборона на імпорт енергоносіїв та експорт високотехнологічної продукції. Однак реальність, яку фіксують дослідники, значно складніша та контрастує з публічною риторикою про "відділення". Російська економіка, незважаючи на прогнози про неминучий колапс, продемонструвала гнучкість, переорієнтувавшись на військові рейки та побудувавши нові мости до ринків Азії, Близького Сходу та колишнього радянського простору. Проте, що найважливіше, вона зберегла критичні логістичні та фінансові зв'язки з самою Європою, використовуючи її власні інституційні, правові та політичні розбіжності як зброю. Центральним парадоксом стало те, що чим жорсткішими ставали формальні обмеження, тим витонченішими та розгалуженішими ставали тіньові схеми їх обходу, перетворюючи санкційну політику на складну «гру в кота і мишу».

Основним рушієм цієї паралельної економіки стали не класичні підприємства, а складні, багаторівневі структури фіктивних компаній. Їх унікальність полягає не в новизні як явища, а в масштабах, сміливості та географічній розмаїтості, що стали можливими завдяки глобалізації фінансових послуг. Ці структури створюються не абияк, а з чіткою логістичною та правовою логікою: реєстрація в юрисдикціях зі слабким регулюванням (офшори, деякі країни Азії), використання номінальних директорів та акціонерів, формування ланцюжків із кількох юридичних осіб для розмивання активів, а також інтеграція у легальні торгові потоки як формальні імпортери або експортери товарів широкого вжитку.

Автори наводять низку прикладів, які збираються наче пазл у єдину картину системного явища. Молдовські фірми Airrock Solutions та Aerostage Services, створені буквально під час війни, постачали західні авіазапчастини російським авіалініям. Вірменська TAKO LLC, що належить росіянину, працювала з підсанкційною російською Radioavtomatika для постачання електроніки оборонному сектору. Чорногорська International Business Corporation Bar, зареєстрована в країні, що офіційно прагне до ЄС, фактично контролювалася російським громадянином Сергієм Кокорєвим і постачала обладнання для аерокосмічної галузі підсанкційній російській компанії.

[15] https://gwbushcenter.imgix.net/wp-content/uploads/Russian-Corruption-Paper-2_12.5.pdf

Кожен з цих випадків демонструє, як використовуються прогалини не лише в міжнародному праві, але й у внутрішньо-європейській координації.

Особливо виразно структурна слабкість ЄС виявляється при аналізі механізмів контролю за кінцевою власністю. Формально директиви з протидії відмиванню коштів (AML) вимагають розкриття бенефіціарів, що володіють понад 25% активів. Однак на практиці створення ланцюжка компаній, де кожна наступна володіє менш ніж критичною часткою в попередній, дозволяє ефективно приховувати кінцевого власника. Складнощі посилює те, що сам ЄС не є єдиним правовим полем у цьому питанні: імплементація директив, реєстрація компаній, доступ до даних — все це залишається в юрисдикції держав-членів, які часто керуються протилежними національними інтересами та політичною волю. Яскравим прикладом став скандал навколо латвійської авіакомпанії airBaltic, яку російські ЗМІ звинувачували у закупівлі російського авіа-палива аж до березня 2024 року через складні схеми з участю болгарських нафтопереробних компаній. Цей випадок вказує на ще одну критичну проблему: наявність на території ЄС стратегічної інфраструктури, яка залишається під контролем російського капіталу, як-от нафтопереробний завод Лукойла в Болгарії чи газопровід "Турецький потік". Санкції можуть обмежувати операції, але вони не передають контроль над активами, залишаючи стратегічні ланки логістики потенційно вразливими для маніпуляцій.

Окремої уваги заслуговує феномен Євразійського економічного союзу (ЄАЕС), який за роки війни здійснив метаморфозу з економічно незначної регіональної організації у ключовий геоекономічний інструмент Москви. Союз, що об'єднує росію, білорусь, Казахстан, Киргизстан та Вірменію, а також має низку країн-спостерігачів, виконує роль "санітарного кордону" між Європою та ізольованою Росією. Аналіз торговельних потоків між ЄС та ЄАЕС виявляє шокуючу динаміку: експорт з Європи до Вірменії та Киргизстану виріс у рази після 2022 року, далеко виходячи за рамки логіки нормальної економічної динаміки чи потреб цих невеликих країн. Ці цифри є прямим статистичним відображенням механізму повторного експорту. Європейські товари, особливо обладнання подвійного призначення, електроніка, промислові компоненти, легально експортуються до, наприклад, Вірменії. Потім, вже на території ЄАЕС, де існує митний союз та спрощений режим переміщення товарів, вони "змінюють призначення" і направляються до росії. Таким чином, формально європейські виробники та експортери не порушують прямі заборони на поставки до росії, а країни-транзитери отримують прибуток від логістичних та митних операцій.

Другим критичним напрямком є активізація росією традиційних торговельних партнерів на периферії ЄС, таких як Туреччина, Сербія чи країни Західних Балкан. Ці держави, маючи різний статус у відносинах з ЄС (кандидат, потенційний кандидат), часто демонструють політичну готовність зберігати економічні зв'язки з москвою, використовуючи це як важель у переговорах з Брюсселем. Туреччина, будучи членом митного союзу з ЄС, стала масивним хабом для перенаправлення товарів, особливо машинобудування та електроніки. Сербія ж, не вводячи санкції, відкрито розширює економічне співробітництво, а її компанії, як Ventrade DOO та Soha Info, прямо задокументовані у постачанні технологічної електроніки російським військовим підприємствам. Це створює парадоксальну ситуацію, коли країни, що офіційно прагнуть до європейської інтеграції, одночасно підривають фундаментальну політику безпеки самого ЄС, а Брюссель виявляється безсилим втрутитися у їхню зовнішню торгівлю.

Технологічний аспект проблеми є найбільш болючим, оскільки безпосередньо впливає на здатність російської армії вести війну. Російський ВПК, незважаючи на розмір, залишається глибоко залежним від імпорту високоточної механіки, мікроелектроніки та спеціальних матеріалів. Історія з австрійським виробником пресів GFM є дуже показовою: росія на 100% залежить від його обладнання для виробництва артилерійських стволів. Санкції заборонили прямі поставки, але вже у 2022 році через ланцюжок іспанської та гонконгської компаній старий прес GFM був поставлений на завод в Іжевську. Подібні історії повторились з німецькими

верстатами для обробки металу, чеськими ЧПУ-станками, промисловими ущільнювачами з австрійсько-чеського конгломерату Hennlich Group, який продовжував постачати продукцію на підприємства, що виробляють ракетні двигуни та авіаційні компоненти. Кожен такий випадок — це свідчення наявності стабільних, налагоджених бізнес-зв'язків, які пережили політичні рішення, та існування в Європі цілих прошарків бізнесу, готових до ризикованих операцій задля збереження ринку.

Рекомендації, запропоновані авторами, виходять далеко за межі простих поліпшень і торкаються основ європейської архітектури безпеки. Перший блок пропозицій спрямований на ліквідацію інформаційної та регуляторної фрагментації. Створення єдиної бази даних про бенефіціарну власність під егідою нового органу AMLA та, головне, забезпечення реального доступу до неї для правоохоронних органів, журналістів та громадянського суспільства є фундаментальною умовою. Без прозорості будь-які санкції залишаються грубою силою, застосовуваною наосліп.

Друга, ще більш радикальна пропозиція — створення єдиного європейського органу з реалізації та контролю санкцій за зразком американського OFAC. Це прямо зачіпає національний суверенітет держав-членів у питаннях зовнішньої політики та безпеки, переносячи оперативні повноваження на наднаціональний рівень. Автори обґрунтовано вказують, що саме роздробленість системи дозволяє таким країнам, як Угорщина, блокувати чи розбавляти спільні рішення, роблячи весь санкційний режим "таким же міцним, як його найслабша ланка". Європейська прокуратура (EPPO) розглядається як готовий інституційний каркас для такого органу, оскільки вже має досвід розслідування транскордонної злочинності та фінансових злочинів.

Третій блок стосується зовнішньої політики, зокрема офіційного визнання ключових хабів санкцій (наприклад, країн ЄАЕС) юрисдикціями високого ризику у сфері фінансування тероризму. Це формальний, але потужний інструмент, який автоматично зобов'яже європейські банки та компанії застосовувати посилену перевірку до всіх операцій з цими країнами, фактично ускладнивши механізми обходу.

Висновки:

- **Структурна вразливість ЄС є головною причиною неефективності санкцій.** Фрагментація національних підходів, відсутність єдиного органу на кшталт OFAC, політичні розбіжності між країнами-членами та обмежений доступ до реєстрів бенефіціарної власності створюють ідеальні умови для масштабного обходу обмежень.
- **Росія побудувала паралельну глобальну економічну мережу**, що ґрунтується на ланцюгах фіктивних компаній, транзиті через треті країни та використанні легальних європейських бізнес-структур для постачання критичних технологій, обладнання подвійного призначення та компонентів для ВПК.
- **Євразійський економічний союз (ЄАЕС) перетворився на ключовий хаб для ухилення від санкцій.** Різке зростання експорту з ЄС до Вірменії, Киргизстану та Казахстану після 2022 року безпосередньо фінансує російську військову машину через механізми повторного експорту та фіктивної торгівлі.

Війна в Україні стала стресовим тестом для європейського проекту, і результати, представлені в цій праці, показують, що інституційна конструкція ЄС виявилася не готовою до довготривалої геоекономічної конфронтації з режимом, який не грає за правилами. Ефективна відповідь вимагає більше, ніж нові списки санкцій; вона вимагає переосмислення самих основ європейського суверенітету та готовності передати частину національних компетенцій на загальноєвропейський рівень заради захисту спільної безпеки. Час для таких рішень обмежений, адже кожен день, коли схеми ухилення функціонують, фінансує російську військову

машину, продовжує кровопролиття в Україні та підриває стратегічну стійкість самого Європейського Союзу в боротьбі за стабільність і демократичний порядок на континенті.

Ваша думка важлива!

1. Чи вважаєте ви, що майбутнє глобального AML-регулювання — це сегрегація криптосвіту на 'білий' (повна ідентифікація) та 'чорний' (заборона), чи ми все ще можемо знайти технологічні рішення для деанонімізації privacy-інструментів без їх повної заборони?
2. Наскільки ефективною може бути для України інтегрована модель регулювання кіберризиків, що об'єднує управління інформаційно-комунікаційними технологіями, операційну стійкість та кібербезпеку, з огляду на фрагментовану систему регуляторних повноважень?
3. Як Україна, маючи унікальний практичний досвід масового застосування та інновацій в сфері безпілотників, може трансформувати його з переваги на полі бою в перевагу для внутрішньої безпеки та створення власної технологічної галузі безпілотних систем для правоохоронних органів? Чи може Україна розробити власні прогресивні правові рамки для використання автономних систем?
4. Чи має Україна достатні інструменти та міжнародну підтримку для тиску на країни-хаби обходу санкцій (Туреччина, Сербія, Казахстан тощо), чи ця задача повністю покладається на ЄС та США? Які дипломатичні та економічні важелі може задіяти Україна, щоб перекрити маршрути поставок для російського ВПК?

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-2026-03

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].