Методологічний бюлетень

Серійний номер: МінФін-AML-2026-06

Лютий 2026

“Знати недостатньо – потрібно діяти”

Йоганн Ґете

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Стратегічне управління ІКТ-ризиками при впровадженні систем штучного інтелекту: Орієнтири BaFin та інтеграція в межах DORA [1]

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

У грудні 2025 року Федеральне управління фінансового нагляду Німеччини (BaFin) оприлюднило знаковий документ — "Орієнтовний посібник щодо ІКТ-ризиків при використанні штучного інтелекту". Ця публікація знаменує собою остаточне завершення дискусії щодо того, чи є штучний інтелект (AI) виключно інноваційним інструментом, чи об'єктом пруденційного нагляду. BaFin чітко класифікує AI як систему інформаційно-комунікаційних технологій (ІКТ), яка підпадає під суворі вимоги Регламенту ЄС про цифрову операційну стійкість (DORA).

Методологія дослідження BaFin ґрунтується на аналізі всього життєвого циклу AI-системи, а не лише на окремих випадках використання. Такий підхід дозволяє ідентифікувати вразливості на

[1] https://www.bafin.de/SharedDocs/Downloads/EN/Anlage/neu/dl_Anlage_orientierungshilfe_IKT_Risiken_bei_KI_en.pdf?__blob=publicationFile&v=4

етапах збору даних, розробки моделей, експлуатації та, що вкрай важливо, безпечної деінсталяції. Регулятор підкреслює, що ІКТ-ризики AI виникають не через його місце у ланцюжку створення вартості, а через інтеграцію в IT-ландшафт фінансової установи.

Одним з найскладніших аспектів є управління ризиками генеративного AI та великих мовних моделей (LLM). BaFin зазначає, що ці системи часто функціонують як "чорні скриньки", що ускладнює традиційне тестування. Крім того, залежність від обмеженого кола хмарних провайдерів створює ризики системної концентрації. У разі збою у великого постачальника, такого як CrowdStrike у 2024 році, наслідки для фінансового ринку можуть бути катастрофічними.

Фаза життєвого циклу AI	Ключові механізми виникнення ризику	Регуляторні вимоги та заходи контролю
Придбання даних	Маніпуляція навчальними даними, порушення конфіденційності	Валідація джерел, забезпечення цілісності та якості даних
Розробка та тестування	Використання вразливих open-source бібліотек, "тіньове IT" у підрозділах	Статичний аналіз коду, сертифікація технічної компетенції персоналу
Експлуатація	Дрейф моделі (model drift), змагальні атаки (adversarial attacks)	Безперервний моніторинг виходів моделі, лімітування API для запобігання інверсії моделі
Деінсталяція	Залишкове збереження конфіденційної інформації у параметрах моделі	Процедури безповоротного видалення системи та архівування версій

Причинно-наслідковий аналіз, проведений регулятором, вказує на небезпеку "тіньового IT" (shadow IT). Коли фахівці (наприклад, аналітики ризиків) розробляють складні моделі на Python чи R на власних ноутбуках поза межами централізованого контролю IT-департаменту, це створює некеровані вектори атак. BaFin вимагає, щоб такі розробки (End-User Computing — EUC) підлягали тим самим стандартам версійності та документування, що й основне банківське ПЗ.

Особлива увага приділяється кібербезпеці. Зловмисники можуть використовувати методи "інверсії моделі" для вилучення конфіденційних даних клієнтів, на яких навчалася нейромережа. Для протидії цьому регулятор рекомендує впроваджувати системи виявлення аномалій у запитах до AI-систем та суворе сегментування навчальних і продуктивних середовищ.

Стратегічно BaFin вимагає від керівництва фінансових установ схвалення окремої AI-стратегії, яка має бути узгоджена з загальною IT-стратегією та дорожньою картою технологічних інвестицій. Управлінський орган несе пряму відповідальність за нагляд за ІКТ-ризиками AI, що робить AI-комплаєнс частиною корпоративного управління.

Для України, в умовах воєнного стану, коли кіберзахист є питанням національної безпеки, підхід BaFin щодо суворого контролю за життєвим циклом AI дозволить захистити фінансову систему від специфічних атак на алгоритми, що використовуються для санкційного комплаєнсу та ПВК/ФТ. Крім того, з серпня 2024 року діє Artificial Intelligence Act ЄС, до якого Україна має

адаптувати своє законодавство, інтегруючи вимоги щодо високоризикових систем AI з пруденційними стандартами.

Висновки:

- Штучний інтелект остаточно виведений з "сірої зони" регулювання та класифікований як об'єкт ІКТ-ризиків у межах DORA. Це вимагає від банків включення AI-систем до реєстру інформації та проведення регулярних оцінок ризиків третіх сторін при використанні хмарних сервісів для AI.
- Моніторинг "дрейфу моделі" є критичним для пруденційної стійкості. Зміни в макроекономічному середовищі (наприклад, інфляція) можуть зробити раніше валідні моделі некоректними, що призведе до помилкових рішень або некоректної оцінки капіталу.
- Залежність від зовнішніх постачальників послуг AI вимагає впровадження механізмів цифрового суверенітету. Установи повинні мати плани виходу та процедури безпечного видалення систем, щоб уникнути блокування у постачальника та витоку даних.
- Використання open-source компонентів та генерація коду за допомогою AI прирівнюється до власної розробки з відповідною відповідальністю за безпеку. Необхідно впроваджувати статичний та динамічний аналіз такого коду для виявлення вразливостей.

Постквантова криптографія: Пріоритезація міграції та захист фінансових даних від майбутніх загроз [2]

Звіт Європолу, підготовлений у співпраці з Форумом квантово-безпечних фінансів (QSFF) та FS-ISAC, є фундаментальним аналізом системних викликів, які квантові обчислення створюють для глобальної фінансової стабільності та систем ПВК/ФТ. Регуляторна логіка документа базується на визнанні того, що сучасна криптографічна інфраструктура, яка забезпечує конфіденційність транзакцій, автентифікацію клієнтів та цілісність цифрових контрактів, стає вразливою перед обличчям достатньо потужного квантового комп'ютера. Центральним вектором загрози є алгоритм Шора, який дозволяє квантовим системам експоненціально швидше за класичні комп'ютери розв'язувати задачі факторизації великих чисел та обчислення дискретних логарифмів, що фактично нівелює захист алгоритмів RSA та ECC. Європол наголошує, що перехід до постквантової криптографії (PQC) не є просто технічним оновленням, а є стратегічним мандатом для фінансових установ, оскільки затримка у впровадженні квантово-стійких рішень створює вікно вразливості для атак типу "Harvest Now, Decrypt Later" (HNDL). У межах таких атак зловмисники перехоплюють і накопичують зашифровані дані сьогодні, маючи на меті їх дешифрування в майбутньому, коли квантові технології досягнуть критичної потужності.

Методологія пріоритезації міграції, запропонована Європолом, використовує дворівневу систему скорингу: Quantum Risk Score (показник квантового ризику) та Migration Time Score (показник часу міграції). Квантовий ризик оцінюється через три критичні параметри: тривалість життєвого циклу даних (shelf-life), рівень експозиції та тяжкість наслідків компрометації. Параметр shelf-life є ключовим для ПВК/ФТ, оскільки фінансова звітність, дані

[2] https://www.europol.europa.eu/cms/sites/default/files/documents/Post-quantum-cryptography-report.pdf

про бенефіціарну власність та записи про транзакції повинні залишатися конфіденційними протягом десятиліть. Якщо дані мають shelf-life понад 10 років, вони автоматично отримують найвищий бал ризику. Рівень експозиції враховує доступність криптографічного матеріалу для потенційних атак, зокрема через публічні мережі або фізичний доступ до пристроїв. Тяжкість наслідків оцінює вплив на бізнес, включаючи прямі фінансові втрати, регуляторні санкції та руйнування довіри до цифрових підписів, які є основою юридично значущого документообігу.

Окрему увагу звіт приділяє аналізу конкретних сценаріїв використання (use cases). Наприклад, платіжні термінали (POS-системи) класифікуються як об'єкти з середнім рівнем квантового ризику, але надзвичайно високим показником часу міграції. Це зумовлено тривалими циклами оновлення апаратного забезпечення, складністю ланцюгів постачання та необхідністю координації між багатьма стейкхолдерами — від платіжних систем до виробників чіпів. Натомість публічні веб-сайти мають низький час міграції, оскільки впровадження гібридних PQC-механізмів у протоколах TLS вже підтримується основними браузерами та мережами доставки контенту (CDN). Європол рекомендує фінансовим установам розпочати з інвентаризації всіх бізнес-процесів, що покладаються на асиметричне шифрування, та зосередитися на усуненні "криптографічних антипатернів". До таких антипатернів відносяться ручне управління сертифікатами, жорстко закодовані облікові дані та використання застарілих протоколів, що створює технічний борг та значно ускладнює майбутню міграцію.

Логіка регулятора також підкреслює необхідність формування "криптографічної гнучкості" (crypto-agility) — здатності систем швидко перемикатися між різними алгоритмами без повної перебудови інфраструктури. Це стає критичним у перехідний період, коли будуть використовуватися гібридні схеми, що поєднують класичні алгоритми (для зворотної сумісності) та нові стандарти PQC (такі як CRYSTALS-Kyber для інкапсуляції ключів та Dilithium для цифрових підписів), схвалені NIST. З точки зору ПВК/ФТ, несвоєчасна міграція може призвести до ситуації, коли правоохоронні органи втратять можливість доводити автентичність цифрових доказів у судах, оскільки цифрові підписи минулих років можуть бути підроблені за допомогою квантових обчислень. Тому звіт закликає до негайної дії: створення інвентарю криптографічних активів, оцінки ризиків на основі shelf-life та інтеграції постквантових вимог у цикли модернізації IT-інфраструктури та закупівлі послуг у третіх сторін.

Висновки:

- Фінансові установи повинні негайно розпочати інвентаризацію всіх бізнес-процесів, що використовують асиметричне шифрування, з особливим акцентом на дані з тривалим життєвим циклом (shelf-life >10 років), які є найбільш вразливими до атак HNDL.
- Міграція має відбуватися за гібридною моделлю, що поєднує класичні та квантово-стійкі алгоритми, забезпечуючи криптографічну гнучкість (crypto-agility) для швидкої адаптації до нових стандартів NIST без зупинки операційної діяльності.
- Першочерговими заходами є оновлення публічних веб-інтерфейсів та усунення криптографічних антипатернів (ручне управління сертифікатами), тоді як апаратні системи (POS-термінали) потребують довгострокового планування в межах циклів оновлення обладнання.
- Ризики ПВК/ФТ у квантову епоху зміщуються у площину доказовості цифрових підписів та цілісності історичних даних, що вимагає від регуляторів перегляду вимог до довгострокового зберігання та захисту інформації про клієнтів і транзакції.

Спрощення європейської пруденційної, наглядової та звітної бази [3]

Звіт Високорівневої цільової групи (HLTF) ЄЦБ, оприлюднений у грудні 2025 року, представляє 17 стратегічних рекомендацій щодо спрощення пруденційної та звітної архітектури Європейського Союзу. Документ відображає фундаментальний зсув у логіці регулятора: відхід від екстенсивного накопичення даних до інтенсивного, ризик-орієнтованого моніторингу, що базується на принципах пропорційності та технологічної інтеграції. Основною проблемою, яку ідентифікує ЄЦБ, є надмірна складність європейського "стеку капіталу" (capital stack), який містить значно більше елементів, ніж передбачено глобальними стандартами Базель III. Це створює регуляторний шум, ускладнює капітальне планування та знижує конкурентоспроможність банків єврозони. Рекомендація №1 пропонує радикальне спрощення: об'єднання численних буферів у два блоки — невідкличний (non-releasable), що поєднує буфер консервації капіталу та буфери системної важливості, та відкличний (releasable), що інтегрує контрциклічні та системні ризикові буфери.

У сфері наглядової звітності ЄЦБ пропонує перехід до моделі "Report Once" (звітувати один раз) через впровадження інтегрованої системи звітності (Integrated Reporting System). Ця модель базується на створенні єдиного набору гранулярних даних, який одночасно задовольняє потреби статистичного, пруденційного та резолюційного нагляду. Ключовим інструментом реалізації цієї стратегії є Словник інтегрованої банківської звітності (BIRD), який забезпечує семантичну гармонізацію визначень на рівні внутрішніх систем банків. Це дозволяє уникнути ситуацій, коли один і той самий фінансовий показник звітується за різними методиками для різних регуляторів, що є критичним для забезпечення чистоти даних у системах ПВК/ФТ. Важливою новацією є Рекомендація №14 щодо запровадження "маржі наглядової толерантності" для несуттєвих помилок. Логіка полягає в тому, що банки не повинні бути змушені повторно подавати звіти через технічні похибки, які не впливають на загальну оцінку ризику, що дозволяє комплаєнс-підрозділам фокусуватися на виявленні реальних підозрілих схем, а не на бюрократичних виправленнях.

Окремий вектор реформи стосується посилення пропорційності. ЄЦБ пропонує

Висновки:

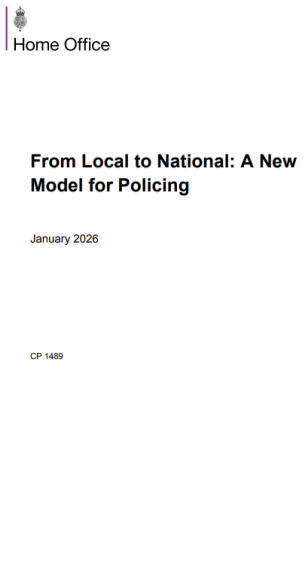
- Перехід до моделі "Report Once" та використання словника BIRD дозволить фінансовим установам значно скоротити операційні витрати на комплаєнс, забезпечуючи при цьому вищу якість та порівнянність даних для цілей ПВК/ФТ.
- Запровадження маржі наглядової толерантності для несуттєвих помилок у звітності зміщує акцент нагляду з формальної перевірки документів на глибокий аналіз матеріальних ризиків та стратегічну стійкість установ.
- Принцип пропорційності через розширення статусу SNCI та спрощення вимог Pillar 3 дозволяє малим банкам залишатися конкурентоспроможними, не знижуючи при цьому загальний рівень захищеності фінансової системи від зловживань.
- Реформа SREP ("Next-level supervision") вимагає від банків посилення внутрішнього управління даними та автоматизації контрольних процедур як передумови для проходження спрощених наглядових процесів.

[3] https://www.ecb.europa.eu/pub/pdf/other/ecb.simplification_supervisory_reporting_framework202512.en.pdf

розширити критерії для "малих та нескладних установ" (SNCI), підвищивши поріг активів (нині 5 млрд євро) та спростивши для них вимоги до звітності та публічного розкриття інформації (Pillar 3). Це відповідає логіці, що інтенсивність нагляду має бути прямо пропорційною системному ризику, який створює установа. У межах проекту "Next-level supervision" ЄЦБ також реформує процес SREP, запроваджуючи фаст-трек для стандартних рішень (наприклад, щодо викупу акцій) та дозволяючи наглядовим групам більше часу приділяти аналізу внутрішніх моделей та стрес-тестуванню у складних випадках. Такий підхід стимулює банки до інвестування у якісну IT-інфраструктуру та автоматизовані системи контролю, оскільки це стає передумовою для отримання статусу SNCI або спрощеного наглядового режиму. Для сфери ПВК/ФТ це означає, що регулятор очікує від банків не просто виконання формальних правил, а наявності зрілої ризик-культури, здатної ідентифікувати аномалії на ранніх етапах.

Реформа поліції як системна трансформація державної спроможності безпеки [4]

Документ, підготовлений Міністерством внутрішніх справ Великої Британії та представлений Парламенту у січні 2026 року, є концептуальним і програмним викладом нової моделі поліцейської системи Англії та Уельсу, яка позиціонується як найглибша та наймасштабніша реформа поліції за майже двісті років. У центрі документа — тверезе визнання того, що сучасна злочинність за своїм характером, швидкістю, транснаціональністю та цифровізацією суттєво випередила інституційну спроможність поліції, організованої за моделлю, що практично не змінювалась із 1960-х років. При цьому Уряд наголошує, що мова не йде про несправну або дисфункціональну поліцію, а про систему, яка структурно не пристосована до нових умов і тому поступово втрачає ефективність, довіру громадян і здатність забезпечувати рівномірно високі стандарти безпеки.


Home Office

From Local to National: A New Model for Policing

January 2026

CP 1489

Вихідною аналітичною рамкою документа є поєднання трьох кризових тенденцій. По-перше, фіксується стале падіння довіри населення до поліції та різке зниження задоволеності потерпілих якістю поліцейських послуг, особливо у частині розслідування «повсякденних» злочинів. По-друге, наголошується на високій фрагментованості та нерівномірності поліцейської системи, де 43 окремі поліцейські сили мають різну спроможність, різний рівень ресурсів і різні результати, що фактично означає нерівність громадян у доступі до безпеки залежно від місця проживання. По-третє, детально описується трансформація злочинності, зокрема домінування шахрайства, кіберзлочинів, злочинів із цифровим компонентом, а також зростання складності розслідувань, які вимагають спеціалізованих навичок, доступу до даних і технологій, що недоступні або фрагментарно доступні на локальному рівні.

У цьому контексті документ вибудовує логіку реформи навколо двох взаємопов’язаних, але чітко розмежованих рівнів поліцейської діяльності. Перший рівень — це поліція на рівні територіальних громад (дільничне поліцейське обслуговування) , яка має бути максимально наближеною до громад, видимою, доступною та сфокусованою на тих проблемах, які громадяни відчувають щодня: антисоціальна поведінка, дрібна та середня майнова злочинність, безпека у громадських просторах, зокрема у центрах міст. Документ підкреслює, що саме занепад видимого дільничного поліцейського патрулювання та роботи з громадами є однією з ключових причин втрати довіри до поліції, оскільки громадяни дедалі рідше бачать

[4] https://assets.publishing.service.gov.uk/media/69779267276692606c013862/260125_White_Paper.pdf

офіцерів на вулицях і дедалі частіше стикаються з відсутністю відчутної реакції на локальні правопорушення.

Відповіддю на це стає концепція Гарантії дільничного (сусідського) поліцейського обслуговування, яка в документі розглядається не як політичний лозунг, а як інституційно закріплений набір зобов'язань держави та поліції перед громадянами. Йдеться про суттєве нарощування кадрової присутності у місцевих патрульних і громадських підрозділах, чітке визначення відповідальних офіцерів для кожного району, стандартизовані строки реагування на звернення громад і бізнесу, обмеження практики «відтягування» дільничних офіцерів на сторонні завдання, а також професіоналізацію ролі офіцерів дільничного поліцейського обслуговування через спеціалізовані програми підготовки. Важливо, що локальна поліція у цій моделі розглядається не лише як інструмент реагування, а як ключовий суб'єкт превенції, спроможний працювати з громадами, місцевою владою, соціальними та освітніми структурами для усунення причин злочинності.

Другий рівень реформи — національний — є значно більш радикальним з інституційної точки зору. Документ прямо констатує, що існуюча національна архітектура поліцейського управління є фрагментованою, перевантаженою координаційними механізмами без реальних повноважень і не здатною ефективно управляти загальнонаціональними викликами. У відповідь пропонується створення Національної поліцейської служби (National Police Service), яка має об'єднати ключові національні поліцейські та квазіполіцейські структури, включно з органами, відповідальними за боротьбу з серйозною та організованою злочинністю, тероризмом, а також за стандарти, навчання та розвиток спроможностей.

Висновки:

- **Створення Національної поліцейської служби є ключовим інституційним зсувом,** спрямованим на подолання фрагментації, концентрацію спроможностей у боротьбі з серйозною та організованою злочинністю та встановлення єдиних обов'язкових стандартів по всій країні.
- **Гарантії дільничного (сусідського) поліцейського обслуговування трансформують локальну поліцію з «резервної» функції у базовий елемент системи,** з чіткими стандартами видимості, реагування та професійної підготовки, що прямо орієнтовано на відновлення довіри громад.
- **Дані, штучний інтелект і національна координація технологій визначаються як критичні інструменти майбутньої ефективності поліції,** а не як допоміжні інновації, що вимагає централізованого управління та єдиного регуляторного підходу.
- **Посилення ролі центрального уряду у встановленні стандартів і нагляді означає відхід від моделі «мінімального втручання»,** з акцентом на вимірювану результативність, швидке реагування на провали та персональну відповідальність керівництва.

Національна поліцейська служба у документі мислиться як єдиний центр стратегічного керівництва, стандартів і ресурсів, здатний забезпечити уніфікований підхід до професійної практики, використання даних, технологій і кадрового планування. Саме на цьому рівні концентруються складні, ресурсомісткі та високоспеціалізовані функції, які не повинні більше «витягувати» ресурси з локальних сил. Таким чином, національний рівень бере на себе захист від серйозних загроз, а локальний — зосереджується на безпеці громад, при цьому обидва рівні пов'язані єдиними стандартами, даними та механізмами підзвітності.

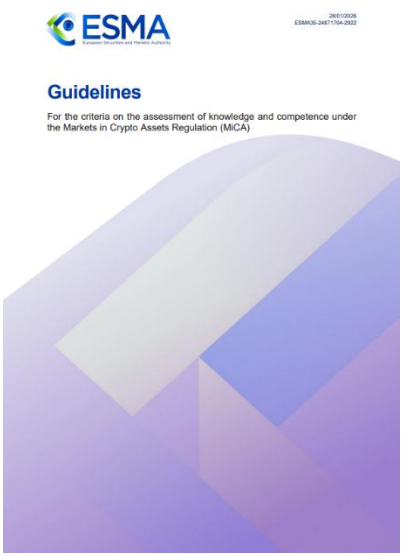
Окремий і наскрізний акцент документа — це відновлення ролі центрального уряду у формуванні стандартів і нагляді за результативністю поліції. Уряд відверто визнає, що попередня модель мінімального втручання призвела до

розмитості очікувань, слабкого контролю за якістю та неможливості оперативно реагувати на системні провали. У зв'язку з цим пропонується нова рамка оцінки ефективності, національні поліцейські гарантії для населення, посилення інструментів втручання у разі погіршення показників, а також підвищення вимог до доброчесності, професійної поведінки та відповідальності індивідуальних офіцерів і керівників.

Значна частина документа присвячена модернізації спроможностей поліції через дані та технології. Автори наголошують, що понад дев'яносто відсотків сучасних злочинів мають цифровий компонент, тоді як поліція часто залишається заручником застарілих IT-систем, несумісних баз даних і дефіциту аналітичних інструментів. Створення національного центру з використання штучного інтелекту в поліцейській діяльності, інвестиції у цифрову експертизу, автоматизацію процесів та єдину інфраструктуру даних подаються як необхідна умова відновлення балансу між державою та злочинними мережами у цифровому середовищі.

У цілому документ формує цілісну візію поліцейської системи, в якій локальний і національний рівні не конкурують за ресурси та повноваження, а взаємно підсилюють один одного. Реформа подається не як сукупність технічних змін, а як оновлення самої філософії поліцейської діяльності — з опорою на принципи поліцейської згоди, але в умовах цифрового, глобалізованого та значно більш складного суспільства XXI століття.

MiCA в дії: як ESMA формує єдині вимоги до знань і компетентності на крипторинку ЄС [5]



Документ Європейського органу з цінних паперів та ринків (ESMA) формує єдину регуляторну рамку щодо оцінки знань і професійної компетентності персоналу, який у межах Регламенту MiCA надає клієнтам інформацію або інвестиційні поради стосовно криптоактивів і послуг із криптоактивами. Його поява є прямою відповіддю на необхідність уніфікації підходів держав-членів ЄС до застосування статей 68 і 81 MiCA, усунення фрагментації наглядових практик та суттєвого посилення захисту інвесторів на ринку, який характеризується високою волатильністю, технологічною складністю та асиметрією інформації.

Керівні настанови адресовані одночасно компетентним органам та постачальникам послуг із криптоактивами (CASPs) і охоплюють усі види криптопослуг, визначені MiCA. Вони мають бути імплементовані у національні наглядові та правові рамки, а також у внутрішні політики самих провайдерів. Документ встановлює чіткий часовий горизонт застосування — через шість місяців після офіційної публікації всіма мовами ЄС, що свідчить про очікування ESMA швидкої інституційної адаптації ринку до нових стандартів.

Ключовою концептуальною основою документа є розмежування двох типів взаємодії з клієнтом: надання інформації та надання порад щодо криптоактивів. ESMA виходить із того, що ці функції мають принципово різний рівень регуляторного ризику та потенційного впливу на інвестора, а отже потребують різної глибини знань, кваліфікації та практичного досвіду персоналу. Надання консультацій розглядається як значно складніша діяльність, що передбачає

[5] https://www.esma.europa.eu/sites/default/files/2026-01/ESMA35-24871704-2922_Guidelines_for_the_criteria_on_the_assessment_of_knowledge_and_competence_under_MiCA.pdf

індивідуальну оцінку клієнта, його фінансового профілю та придатності криптоактивів, і тому до такої діяльності встановлюються підвищені вимоги.

Документ детально визначає зміст поняття «знання та компетентність», розглядаючи його як поєднання відповідної кваліфікації, підтвердженої навчанням або іспитами, та практичного досвіду роботи. Наголошується, що формальна освіта сама по собі не є достатньою: персонал повинен демонструвати здатність застосовувати знання на практиці, з урахуванням специфіки крипторинку та нормативних вимог MiCA. Окремо вводиться поняття роботи «під наглядом», що дозволяє залучати менш досвідчений персонал до взаємодії з клієнтами лише за умови контролю з боку кваліфікованого співробітника, який несе повну відповідальність за надану інформацію або пораду.

Для персоналу, який надає інформацію про криптоактиви або криптопослуги, ESMA встановлює широкий перелік обов'язкових знань. Він охоплює розуміння ключових характеристик криптоактивів, принципів функціонування технологій розподіленого реєстру, механізмів консенсусу, економічних моделей токенів, а також ринкових процесів формування ціни та ліквідності. Особливу увагу приділено ризикам: волатильності, кіберзагрозам, ризикам втрати приватних ключів, програмним помилкам, а також ризикам, пов'язаним із вибором несумісних або небезпечних мереж для переказу криптоактивів. Документ прямо визнає вплив соціальних мереж, інвесторських настроїв і дій великих власників криптоактивів на різкі та важкопрогнозовані цінові коливання. Крім того, персонал повинен чітко розуміти відмінності між режимом захисту інвесторів у межах MiCA та традиційними фінансовими інструментами, регульованими MiFID II, і вміти коректно пояснювати ці відмінності клієнтам.

Для персоналу, який надає інвестиційні поради, ці вимоги не лише зберігаються, а й суттєво розширюються. ESMA вимагає глибокого розуміння правил оцінки придатності, управління портфелем, принципів диверсифікації, повного обсягу витрат і комісій, пов'язаних із криптоактивами, а також механізмів оцінки вартості таких активів. Консультант повинен бути здатним не лише рекомендувати криптоактив, а й обґрунтувати, чому певний актив або стратегія можуть бути непридатними для конкретного клієнта, особливо з урахуванням змін у його фінансовому стані або ринкових умов.

Документ встановлює мінімальні стандарти кваліфікації та досвіду для обох категорій персоналу, передбачаючи різні комбінації професійного навчання, формальної освіти та практичного стажу. Водночас ESMA запроваджує перехідні положення

Висновки:

- **CASPs мають негайно побудувати формалізовану систему оцінки знань і компетентності персоналу,** чітко розділивши ролі «інформування» та «консультування» і встановивши для них різні кваліфікаційні пороги відповідно до MiCA та керівних настанов ESMA.
- **Безперервний професійний розвиток стає обов'язковим елементом комплаєнс-моделі,** а не добровільною практикою: мінімальні CPD-вимоги (10/20 годин на рік) повинні бути інтегровані у внутрішні політики та підтверджуватися оцінюванням знань.
- **Криптоактиви офіційно визнаються високоризиковими з точки зору поведінкових, технологічних і ринкових факторів,** що зобов'язує персонал володіти знаннями з DLT-протоколів, волатильності, ролі великих власників, кіберризиків та питань у сфері ПВК/ФТ на рівні, співставному з традиційними фінансовими ринками.
- **Наглядові органи отримують чіткий інструментарій для перевірки CASPs,** включно з вимогою надання документованих доказів кваліфікації, досвіду та навчання персоналу, що істотно підвищує регуляторні та репутаційні ризики для провайдерів, які ігнорують ці вимоги.

для працівників, які вже виконували відповідні функції до набрання чинності керівними настановами, визнаючи їхній попередній досвід за умови фактичного та безперервного виконання цих функцій протягом визначеного часу.

Окремий системний акцент зроблено на безперервному професійному розвитку. ESMA розглядає безперервний професійний розвиток (CPD) як ключовий інструмент підтримання актуальності знань у середовищі, що швидко змінюється під впливом технологічних інновацій, нових бізнес-моделей та регуляторних змін. Встановлюються орієнтовні мінімальні річні обсяги навчання для різних категорій персоналу, з можливістю їх збільшення залежно від складності продуктів і послуг. Навчання має бути не формальним, а таким, що включає перевірку засвоєних знань і компетентностей.

Значну увагу приділено організаційним вимогам до CASPs. Провайдери повинні чітко визначити ролі та відповідальність персоналу, регулярно оцінювати потреби в розвитку компетенцій, документувати відповідність працівників вимогам керівних принципів і бути готовими надати ці матеріали на вимогу наглядових органів. Документ також підкреслює, що використання автоматизованих або напівавтоматизованих інструментів надання інформації чи порад не звільняє провайдера від відповідальності: персонал, який визначає параметри таких систем, повинен відповідати тим самим вимогам щодо знань і компетентності.

У додатку до керівних настанов наведено практичні приклади, які демонструють межі застосування документа та типові ситуації належної практики. Вони уточнюють, у яких випадках працівники не вважаються такими, що надають релевантні послуги, а також ілюструють очікування ESMA щодо навчання персоналу, управління конфліктами інтересів, контролю якості консультацій та прозорого інформування клієнтів.

У цілому документ ESMA формує комплексну, ризик-орієнтовану модель професійної придатності персоналу крипторинку, яка за своєю логікою та суворістю наближає ринок криптоактивів до традиційних фінансових ринків, водночас прямо враховуючи унікальні технологічні, операційні та поведінкові ризики, притаманні криптоекосистемі.

Від санкцій до мотивації: нова парадигма забезпечення доброчесності бізнесу у публічних закупівлях [6]

Документ, підготовлений UNODC, є ґрунтовним аналітико-практичним дослідженням, присвяченим ролі стимулів як системного інструменту посилення доброчесності бізнесу у сфері публічних закупівель. У центрі документа — ідея переходу від виключно каральної моделі протидії корупції до збалансованого підходу, у якому санкції поєднуються з позитивною мотивацією приватного сектору до впровадження ефективних антикорупційних механізмів. Автори виходять із того, що публічні закупівлі становлять одну з найбільш фінансово значущих і водночас корупційно вразливих сфер діяльності держави, оскільки охоплюють значну частку ВВП, залучають великі грошові потоки та передбачають складні процедури взаємодії між публічними органами і приватними компаніями. Саме тому підвищення рівня

6 https://businessintegrity.unodc.org/bip/uploads/documents/resources/Using_Incentives_to_Strengthen_Business_Integrity_in_Public_Procurement-.pdf

доброчесності бізнесу розглядається як ключовий чинник зниження корупційних ризиків і підвищення ефективності використання публічних коштів.

Документ чітко спирається на міжнародно-правову рамку, насамперед на положення Конвенції ООН проти корупції, зокрема статті щодо публічних закупівель, приватного сектору та відповідальності юридичних осіб, а також на резолюції Конференції держав-членів, які прямо закликають держави створювати стимули для приватного сектору з метою запобігання корупції. У цьому контексті стимули розглядаються не як виняток або пільга, а як легітимний інструмент державної політики, який має бути вбудований у нормативні та процедурні рамки закупівель.

Значна частина документа присвячена детальному аналізу корупційних ризиків на всіх етапах закупівельного циклу — від планування і формування потреб до виконання контрактів. Показано, що ризики мають системний характер і включають маніпуляцію потребами та бюджетами, підготовку технічних вимог під конкретного постачальника, змову між учасниками торгів, хабарництво, фіктивну конкуренцію, зловживання під час оцінки пропозицій, завищення вартості контрактів, підміну або заниження якості робіт і товарів, а також використання додаткових угод для прихованого збільшення вартості проєктів. Автори підкреслюють, що ці ризики виникають у взаємодії публічного і приватного секторів, а отже ефективна протидія неможлива без активного залучення бізнесу до формування культури доброчесності.

Ключовою аналітичною рамкою документа є триєдина модель, що складається зі стандартів доброчесності, оцінки антикорупційних програм та надання стимулів. Стандарти доброчесності розглядаються як фундамент, який визначає мінімальні та підвищені вимоги до поведінки компаній, їхніх внутрішніх політик, систем управління ризиками, контролю, навчання персоналу та механізмів повідомлення про порушення. Оцінка антикорупційних програм подається як критично важливий елемент, що забезпечує об’єктивність і справедливість застосування стимулів, адже без належної перевірки стимулювання може перетворитися на формальність або навіть джерело нових корупційних зловживань. Самі стимули описуються як різноманітний набір інструментів, що можуть застосовуватися як на етапі допуску до закупівель, так і під час оцінки пропозицій або виконання контрактів.

Документ детально аналізує різні типи стимулів, які вже застосовуються в окремих державах і міжнародних організаціях. До них належать пом’якшення відповідальності або звільнення від переслідування у разі саморозкриття та співпраці з органами влади, преференційний доступ до закупівель через кваліфікаційні вимоги або списки доброчесних постачальників, зменшення рівня контролю для компаній із доведено ефективними антикорупційними програмами, використання нефінансових критеріїв

Висновки:

- **Ефективна протидія корупції в публічних закупівлях потребує інституціоналізації стимулів,** інтегрованих у законодавство та процедури закупівель, а не їх використання як разових або декларативних заходів.
- **Трирівнева модель «стандарти – оцінка – стимули» є критичною умовою результативності:** без чітких стандартів і незалежної оцінки антикорупційних програм стимули втрачають легітимність і стають корупційно вразливими.
- **Розкриття кінцевих бенефіціарних власників має розглядатися не лише як контрольний, а й як заохочувальний інструмент,** який може зменшувати адміністративний тиск на доброчесні компанії та підвищувати конкуренцію.
- **Санкції та стимули повинні працювати синхронно:** жорсткі та пропорційні механізми відсторонення і заборони участі в закупівлях формують «червоні лінії», тоді як стимули мотивують бізнес інвестувати в запобігання корупції та сталу доброчесну поведінку.

оцінки пропозицій, які враховують якість комплаєнс-систем, а також програми публічного визнання, рейтинги та сертифікації доброчесності. Ці підходи ілюструються широким колом практичних кейсів із різних правових і економічних контекстів, що дозволяє показати їхню адаптивність і можливість застосування в різних моделях публічного управління.

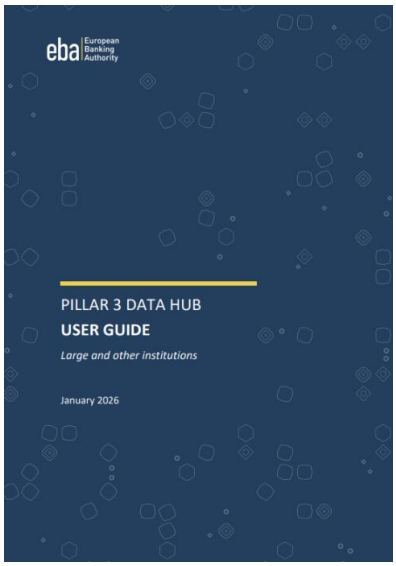
Окремий акцент зроблено на прозорості структури власності як важливому елементі системи стимулів. Розкриття інформації про кінцевих бенефіціарних власників розглядається не лише як інструмент контролю, а й як фактор, який може надавати компаніям конкурентні переваги, знижувати адміністративні бар'єри та підвищувати довіру з боку держави і суспільства. У документі показано, що інтеграція вимог щодо бенефіціарної прозорості в закупівельні системи здатна суттєво зменшити конфлікти інтересів і змови.

Водночас автори послідовно підкреслюють, що стимули не можуть функціонувати ізольовано від санкцій. Санкційні механізми, зокрема тимчасове відсторонення і заборона участі в закупівлях, розглядаються як необхідний елемент забезпечення рівних умов конкуренції та довіри до системи. Документ наголошує, що ефективна система має поєднувати стримувальний ефект санкцій із мотиваційним потенціалом стимулів, створюючи середовище, у якому доброчесна поведінка є економічно доцільною для бізнесу.

Завершальні частини документа присвячені питанням практичної реалізації такої моделі. Особлива увага приділяється ризик-орієнтованому підходу, пропорційності вимог до розміру і сектору компаній, необхідності інституційної спроможності державних органів, регулярного моніторингу ефективності стимулів та запобігання їх зловживанню. Автори також наголошують на важливості супровідних заходів, таких як навчання, підвищення обізнаності та колективні ініціативи, без яких стимули можуть втратити свій трансформаційний потенціал.

У підсумку документ позиціонується як практичний орієнтир для держав, які прагнуть не лише зменшити корупцію в публічних закупівлях, а й вибудувати стійку екосистему доброчесності, у якій держава і бізнес виступають партнерами у захисті публічних фінансів та довіри суспільства.

Pillar 3 Data Hub EBA: технічна інфраструктура нової моделі регуляторної прозорості [7]



Документ Європейського банківського органу присвячений практичному впровадженню та функціонуванню Pillar 3 Data Hub (P3DH) — централізованого цифрового механізму збору, публікації та візуалізації пруденційної інформації, розкриття якої вимагається відповідно до Частини восьмої Регламенту про вимоги до капіталу (CRR) у редакції CRR3. P3DH є елементом ширшого банківського пакета ЄС, спрямованого на посилення ринкової дисципліни шляхом забезпечення єдиного пункту доступу до регуляторних розкриттів Pillar 3, що, у свою чергу, має підвищити прозорість, порівнюваність і аналітичну цінність даних для ринку, наглядових органів та широкої громадськості.

У документі закріплено принципову модель, за якої великі та інші установи, що не належать до категорії малих і не складних (SNCI), зобов'язані подавати всі передбачені CRR розкриття безпосередньо до EBA в електронному форматі. Роль EBA при цьому обмежується технічною публікацією отриманих матеріалів без внесення змін або інтерпретацій, що підкреслює

[7] https://www.eba.europa.eu/sites/default/files/2026-01/988f7061-1afe-4d1f-aa03-ee7d4d620305/EBA%20User%20Guide%20%28Large%20and%20Other%20Institutions%29%20%281%29.pdf

відповідальність самих установ за повноту, точність і узгодженість поданої інформації. P3DH функціонує як публічний регуляторний хаб, який одночасно забезпечує завантаження первинних файлів та доступ до інструментів візуалізації даних.

Значну частину документа присвячено процедурі онбордингу установ до P3DH, яка має чітко формалізований і ієрархічно вивірений характер. Ініціація онбордингу здійснюється EBA на підставі класифікації установ відповідно до CRR і майстер-даних, наданих компетентними органами. Ключовою особливістю цієї процедури є пряме залучення голови органу управління установи, контактні дані якого використовуються як первинна точка взаємодії. Такий підхід відображає логіку Директиви ЄС про пруденційний нагляд за кредитними установами (CRD) щодо відповідальності керівного органу за процеси управління, комунікації та розкриття інформації, і фактично інституціоналізує персональну підзвітність найвищого рівня менеджменту за Pillar 3 розкриття.

Подальші етапи онбордингу включають офіційне індивідуальне повідомлення EBA, визначення установою контактних осіб, створення користувацьких облікових записів та надання доступу до платформи EUCLID. Доступ до системи організований через централізовану інфраструктуру ідентифікації та управління доступом EIAM із обов'язковим використанням багатофакторної автентифікації, що підкреслює високі вимоги до кібербезпеки та захисту регуляторних даних. Документ також описує процедури офбордингу, які застосовуються у разі зміни статусу установи або інших обставин, водночас зберігаючи доступ до платформи для виконання залишкових або повторних зобов'язань щодо подання даних.

Окремий блок присвячений безпосередньо процесу подання Pillar 3 звітності через Централізовану цифрову платформу Європейського банківського органу (EBA) для подання регуляторної звітності банків та фінансових установ (ERRP). Саме ERRP є технічною точкою входу для установ, де здійснюється завантаження, перевірка та моніторинг поданих файлів. Документ чітко фіксує, що звітність Pillar 3 складається з набору модулів, які мають подаватися у визначених форматах і відповідно до чинної моделі точок даних EBA (Data Point Model). Кількісна інформація подається у форматі XBRL-CSV, тоді як якісні розкриття та супровідні наративи оформлюються у PDF-файлах із можливістю машинного зчитування. Такий поділ відображає прагнення EBA поєднати стандартизовану аналітичну обробку даних із збереженням контексту та пояснень, необхідних для правильного розуміння розкриттів.

Документ детально регламентує підходи до застосування принципів суттєвості, конфіденційності та пропрієтарності інформації. Хоча CRR дозволяє за певних умов не розкривати окремі дані, EBA вимагає, щоб кожне таке рішення було чітко обґрунтоване,

Висновки:

- **Централізація Pillar 3 через P3DH радикально змінює роль установ:** банки більше не «публікують» розкриття самостійно, а зобов'язані забезпечити технічно бездоганне та своєчасне подання даних до EBA, яка стає єдиною точкою публічного доступу.
- **Відповідальність керівництва інституцій формалізована на практиці, а не лише нормативно:** процес онбордингу починається з голови органу управління, що підсилює персональну підзвітність за якість і повноту Pillar 3 розкриттів.
- **Технічна готовність стає критичним фактором комплаєнсу, а не допоміжним елементом:** помилки у форматах або структурі можуть фактично заблокувати виконання регуляторних обов'язків.
- **EDAP трансформує Pillar 3 у інструмент порівняльного аналізу та нагляду,** що підвищує репутаційні та ринкові ризики для установ і водночас створює додатковий стимул до високої якості, узгодженості та обґрунтованості розкриттів.

задокументоване та відображене у відповідних шаблонах XBRL-CSV. Таким чином, навіть нерозкриття стає формалізованим і прозорим з точки зору наглядового та ринкового контролю. Аналогічно врегульовано порядок повторних подань, при якому кожне повторне завантаження повністю замінює попередній модуль і повинно містити повний обсяг інформації, а не лише виправлені елементи.

Завершальним компонентом екосистеми P3DH є Портал доступу до даних EBA (EDAP), який забезпечує публічний доступ до всіх поданих розкриттів і надає інструменти візуалізації як на рівні регуляторних шаблонів, так і на рівні окремих точок даних. EDAP перетворює Pillar 3 з формального регуляторного обов'язку на активний аналітичний ресурс, що дозволяє здійснювати міжустановчі та міжкраїнні порівняння, агрегований аналіз і глибоке дослідження окремих показників.

У цілому документ формує цілісну концепцію цифрового, стандартизованого та публічно орієнтованого розкриття пруденційної інформації, у межах якої правові вимоги CRR, технічні стандарти ITS і цифрова інфраструктура EBA інтегровані в єдиний процес із чітко визначеними ролями, відповідальністю та очікуваними результатами, що істотно підвищує значення Pillar 3 як інструменту ринкової дисципліни та наглядової прозорості.

Глибинна трансформація незаконної торгівлі дикою природою в епоху глобалізації та цифровізації [8]

На початку 2026 року Всесвітній фонд дикої природи (WWF) оприлюднив ґрунтовний аналіз сучасних тенденцій у незаконній торгівлі дикими тваринами та рослинами. Звіт не просто фіксує зростання обсягів цієї злочинної індустрії, але й розкриває її якісну трансформацію, спричинену поєднанням технологічних інновацій, змін у споживчих уподобаннях та адаптацією організованих злочинних мереж до міжнародних регуляторних заходів. Сьогоднішня незаконна торгівля — це вже не просто контрабанда окремих трофеїв, а складний, багаторівневий бізнес із високим рівнем спеціалізації, що має всі ознаки транснаціональної злочинної діяльності, яка стає все більш невловимою та руйнівною для глобальної біорізноманітності.

Однією з найбільш тривожних та яскраво виражених тенденцій останнього десятиліття стало активне формування та розширення нових регіональних ринків, де традиційно існував відносно низький рівень попиту на контрабанду диких видів. Найкраще це ілюструє ситуація в Північній Америці, де, за даними WWF, стрімко зростає внутрішня та міжнародна торгівля північноамериканськими птахами. Види, такі як індиговий вівчарик, рожевощокий вівчарик та синій кардинал, які перебувають під охороною федерального законодавства США, стали об'єктом масового браконьєрства. Механізм цього ринку складний: птахів виловлюють із дикої природи, часто використовуючи спеціальні пастки, після чого вони потрапляють як на внутрішній чорний ринок для продажу як екзотичні домашні улюбленці, так і в міжнародні мережі, особливо до Європи та Азії. Окремим споживчим сегментом є організатори нелегальних пісенних конкурсів птахів, де ціна переможця може бути дуже високою. Це свідчить не лише про зростання попиту, але й про диверсифікацію мотивації покупців — від естетичного задоволення до азарту та престижу. Така тенденція демонструє, що загрози можуть виникати несподівано для видів, які раніше не вважалися глобально вразливими через

[8] https://www.worldwildlife.org/news/stories/the-latest-trends-in-the-illegal-wildlife-trade/

торгівлю, що вимагає від природоохоронців постійного моніторингу навіть стійких на перший погляд популяцій.

Паралельно розвивається масштабна міжконтинентальна логістика інших груп тварин, що вказує на глибоку інтеграцію глобальних ринків. Прісноводні черепахи з території США та Мексики, такі як валлартська мулова черепаха, плямиста та деревна черепахи, зазнають колосального впливу через експорт до Азії. Тут попит формується потрійною силою: традиційна медицина приписує їм лікувальні властивості, кулінарна традиція вважає їх делікатесом, а ринок екзотичних домашніх тварин бажає отримувати рідкісні види. Оскільки понад половини видів черепах у світі вже перебувають під загрозою зникнення, такий трансконтинентальний тиск стає фатальним. Цей напрямок ілюструє ще одну сучасну особливість: злочинні мережі все частіше експортують не лише азійські види до Заходу, але й використовують біорізноманіття Америки для задоволення азійського попиту, створюючи двосторонні потоки контрабанди.

Окремої уваги заслуговує драматичне посилення торгівлі приматами, що є прямим наслідком впливу соціальних медіа. Попит на мавп, зокрема ревунів, капуцинів та мармозеток, для утримання вдома як статусних «віртуальних улюбленців» активно культивується через платформи, такі як Instagram та TikTok, де відео з милими дитинчатами приматів набирають мільйони переглядів. Це створює ілюзію прийнятності та простоти догляду. Реальність насправді жахлива: щоб отримати дитинча, браконьєри часто вбивають дорослих тварин у зграї; самих немовлят контрабандою перевозять у жахливих умовах, що призводить до високої смертності. Окрім безпосередньої загрози вимирання для цих видів, така практика несе серйозну небезпеку для здоров'я людей — зоонозні захворювання можуть перейти від приматів до людей, як це сталося з Еболою. Торгівля приматами — це яскравий приклад того, як цифрові технології не лише полегшують зв'язок між продавцем і покупцем, але й активно формують попит, романтизуючи володіння дикими тваринами.

Найбільш несподіваним і показовим явищем останніх років стало масове включення в незаконний обіг рослинного світу, зокрема сукулентів і саговників. У регіонах з унікальною флорою, таких як Капські провінції ПАР та посушливі райони Намібії, браконьєри тепер цілеспрямовано проводять рейди за рідкісними, часто крихітними рослинами, пристосованими до екстремальних умов. Попит на них як на предмет колекціонування та дизайну в інтер'єрі стрімко зріс на ринках США, Східної Азії та Європи. Критично вразливі види, такі як Clivia mirabilis або карликовий сукулент Oophytum nanum, виривaються з природного середовища тисячами. Ключову роль тут відіграли онлайн-маркети, де торгівля ведеться в закритих групах, зашифрованих чатах або під виглядом легального обміну насінням. Це робить рослинну контрабанду надзвичайно складною для виявлення та переслідування, оскільки вона не потребує складних логістичних ланцюгів, як для живих тварин, і може маскуватися під легальну поштову пересилку. Ця тенденція доводить, що жоден компонент екосистеми не застрахований від комерціалізації в умовах глобалізованого ринку.

У водних екосистемах ситуація досягла критичної точки, особливо щодо вугрів та акул. Європейський вугор, вид на межі зникнення, залишається об'єктом масштабного незаконного вилову. Його склоподібні мальки (так звані «скляні вугри») контрабандою вивозяться з Європи тисячами до аквакультурних ферм у Азії, де вони вирощуються до дорослого стану для ринків суші та грілю. Ця незаконна діяльність підриває всі міжнародні зусилля з відновлення популяції регульованої CITES.

Паралельно процвітає нелегальна торгівля акулами, де центральною проблемою стала не лише контрабанда, але й масштабна фальсифікація продукції на легальному ринку. Дослідження в США показало, що переважна більшість проданого м'яса акул маркована неправильно, приховуючи продаж заборонених видів під загальними назвами. Це означає, що споживач, який намагається уникнути покупки незаконного продукту, часто не має можливості зробити

свідомий вибір, оскільки вся система маркування та трасування ланцюгів постачання є корумпованою або недієздатною. Таким чином, легальний ринок часто служить ефективною пральнею для незаконно здобутої продукції, що є однією з найбільших проблем сучасної боротьби з торгівлею.

Незважаючи на похмуру загальну картину, аналіз WWF підкреслює, що посилені та цілеспрямовані зусилля на міжнародному та національному рівнях можуть призводити до реальних позитивних результатів. Зразковим прикладом є вражаюче відновлення популяції сайгака в степах Казахстану, Монголії та Узбекистану. Ця антилопа, яка в 1990-х роках була майже знищена браконьєрами через попит на її роги в китайській медицині, демонструє стрімке зростання чисельності завдяки жорсткій координації між державами, створенню охоронних зон, ефективній роботі спецпідрозділів і, що важливо, програмам залучення місцевого населення до охорони виду. Це доводить, що навіть для видів, що перебувають у критичному стані, шлях до відновлення можливий за наявності політичної волі та сталого фінансування.

Законодавчі ініціативи в ключових країнах також починають давати ефект. Ухвалення в США Закону про громадську безпеку щодо великих котів у 2022 році стало історичною подією, яка закрила значну легальну прогалину для зловживань. Закон забороняє приватне володіння та розведення левів, тигрів та інших великих кішок, вимагаючи від усіх установ отримання федерального дозволу. Це не тільки покращує добробут тварин у неволі та зменшує ризики для громадської безпеки, але і ускладнює потрапляння частин тіла цих тварин на нелегальний ринок. Подальшим логічним кроком став повторний внесок до Конгресу законопроєкту «Про безпеку приматів у неволі», що забороняє приватне володіння мавпами та лемурами. Такі закони безпосередньо впливають на попит, ліквідуючи цілі сегменти ринку екзотичних домашніх тварин.

На оперативному рівні ефективною виявилася тактика управління популяціями, спрямована на зменшення економічного стимулу для браконьєрів. Метод видалення рогів у живих носорогів, що практикується в Намібії, ПАР та Зімбабве, є яскравим прикладом. Безболісна процедура, під час якої залишається лише невеликий залишок рогу, робить тварину непотрібною для браконьєра, значно знижуючи ризик вбивства. Цей захист є тимчасовим, оскільки ріг відростає, але в поєднанні з традиційними патрулями та суворими судовими переслідуваннями він дав значне зниження рівня браконьєрства в ключових регіонах.

WWF та інші організації надалі розвивають багаторівневий підхід до боротьби, працюючи одночасно на рівні джерел, транзиту та попиту. На місцях це означає оснащення рейнджерів сучасними технологіями моніторингу (дрони, тепловізійні камери, системи на основі ШІ для аналізу даних), що підвищує ефективність патрулювання та

Висновки:

- **Незаконна торгівля дикою природою швидко диверсифікується:** окрім традиційних видів (слони, носороги), об’єктами стали птахи, прісноводні черепахи, примати, сукуленти та морські види (вугрі, акули).
- **Цифрові платформи й соціальні мережі стали ключовим драйвером глобалізації цієї торгівлі,** полегшуючи зв’язок між браконьєрами та покупцями, а також формуючи новий попит (наприклад, через відео).
- **Ефективна боротьба можлива лише за умови поєднання** суворого законодавства, технологічних рішень, міжнародної координації та роботи зі зменшенням попиту через просвітницькі кампанії.
- **Навіть в умовах зростання загроз існують позитивні приклади** (відновлення сайгака, закони про великих котів у США, тощо), що доводять ефективність системних та узгоджених дій.

безпеку самих охоронців. У віртуальному просторі ключовим партнерством стала Коаліція за припинення торгівлі дикою природою в мережі, куди входять понад 40 провідних технологічних компаній, таких як Google, Meta та TikTok. Коаліція розробляє та впроваджує алгоритми для автоматичного виявлення та блокування оголошень про продаж заборонених видів, а також проводить навчання модераторів. Однак найважливішою складовою довгострокового успіху залишається робота з суспільною свідомістю. Цільові кампанії в країнах Азії спрямовані на зміну ставлення до продуктів із рогів носорога, кісток тигра або плавників акули, а в країнах Заходу — на підвищення обізнаності про проблему екзотичних домашніх тварин. Такі інструменти допомагають потенційним власникам зрозуміти ризики та етичні наслідки покупки дикої тварини.

Підсумовуючи, сучасна незаконна торгівля дикою природою — це дзеркало глобальних суперечностей: вона використовує інструменти глобалізації та цифровізації для свого розвитку, паралельно експлуатуючи соціальні тенденції та регуляторні прогалини. Вона більше не має чітких географічних або таксономічних меж, загрожуючи як мега-фаунам, так і маловідомим рослинам. Ефективна протидія їй вимагає такого ж динамічного, інноваційного та координованого підходу, що поєднує силові, правові, технологічні та просвітницькі методи. Майбутнє багатьох видів залежатиме від здатності людства усвідомити, що ця торгівля — не лише екологічна катастрофа, але й серйозна загроза економічній стабільності, місцевому розвитку та глобальній безпеці здоров'я, що вимагає найвищого пріоритету на рівні міжнародної політики.

Всесвітній ринок наркотиків у 2025 році: рекордні обсяги, нові загрози та виклики для глобальної безпеки [9]

Всесвітній звіт про наркотики за 2025 рік, опублікований Управлінням ООН з наркотиків та злочинності (UNODC), розкриває панораму глибокої системної кризи, яка переплітається з глобальною нестабільністю, технологічними змінами та соціальними розривами. Цей документ, ґрунтуючись на офіційних даних держав-членів, фіксує момент, коли світова наркосфера перетнула якісну межу: від класичної боротьби з рослинними наркотиками світ перейшов до епохи гіпер-адаптивного, децентралізованого та технологічно оснащеного синтетичного ринку, контроль над яким утворює все більш складну головоломку.

У 2025 році 316 мільйонів людей — майже 6% дорослого населення планети — вживали ті чи інші наркотики, причому цей ріст значно випереджає темпи приросту населення, свідчачи не про кількісне, а про якісне поглиблення проблеми. Це вже не маргінальне явище, а потужний чинник, що формує ландшафт громадського здоров’я, безпеки та соціальної стабільності в кожному регіоні світу, від найбагатших міст Північної Америки до найвразливіших сільських громад Західної Африки.

Однією з найяскравіших ілюстрацій цієї адаптивності є кокаїновий ринок, який продовжує бити власні рекорди. У 2025 році глобальне незаконне виробництво кокаїну досягло неймовірних 3708 тонн, збільшившись на третину лише за один рік. Це зростання зумовлене не лише розширенням площ під кокою в Колумбії, але й технологічними змінами: виробництво концентрується у високоврожайних регіонах, що підвищує ефективність. Паралельно масштаби

[9] https://www.unodc.org/documents/data-and-analysis/WDR_2025/WDR25_B1_Key_findings.pdf

трафіку набувають транснаціонального характеру: хоча основними потоками залишаються маршрути з Андських країн до Північної Америки та Європи, все більш значущими стають африканські та азійські шляхи. Західна та Центральна Європа тепер фіксують більше вилучень кокаїну, ніж Північна Америка, що свідчить про фундаментальний зсув ринку збуту. Але справжньою тривогою є стрімке зростання попиту на кокаїн у регіонах, де він раніше був рідкістю: у Африці та Азії. Хоча абсолютні цифри споживання там ще не досягають європейських чи американських рівнів, темпи зростання у відносному вираженні вражають, а поява кокаїну в системах лікування та в аналізах стічних вод у країнах, що традиційно не асоціювалися з цим наркотиком, сигналізує про глибоке проникнення трафіку в нові суспільства.

Якщо кокаїновий ринок демонструє експансію, то опіатний переживає тектонічний зсув, наслідки якого ще належить усвідомити. Драматичне рішення афганської влади заборонити вирощування маку в 2022 році призвело до різкого, на 72%, скорочення глобального виробництва опіуму. На 2024 рік площі під маком у світі були на 68% меншими, ніж до заборони. Це спричинило не лише зростання цін на опіум у десять разів у самому Афганістані, а й серйозні порушення в глобальних ланцюгах поставок героїну. Вилучення героїну впали майже вдвічі порівняно з 2021 роком. Однак накопичені раніше запаси — експерти оцінюють їх у 13 200 тонн на початок 2023 року — досі дозволяють задовольняти світовий попит, відстрочуючи повномасштабну кризу. Ці запаси, вартість яких становила до чверті ВВП Афганістану, стали буфером, що запобіг негайному економічному колапсу.

Реальна загроза криється в тому, що трапиться, коли запаси виснажаться. Високі ціни можуть спокусити афганських фермерів повернутися до вирощування маку, незважаючи на заборону, але набагато небезпечнішим сценарієм є масовий перехід мільйонів споживачів опіатів по всьому світу на синтетичні замінники. У Європі вже зараз спостерігаються локальні спалахи отруєнь потужними синтетичними опіоїдами з групи нітазенів, які часто продають під виглядом героїну. Ці речовини, що в десятки разів сильніші за фентаніл, становлять екзистенційну загрозу для громадського здоров'я. Система міжнародного контролю, хоч і реагує, додавши 12 нітазенів до списку заборонених, відстає від швидкості, з якою хіміки синтезують нові аналоги.

Саме синтетичні наркотики сьогодні є основним драйвером та символом трансформації всього ринку. Їхня перевага — у незалежності від клімату, сільськогосподарських циклів та географії. Лабораторію можна розташувати поблизу місць споживання, що скорочує логістичні ланцюги та знижує ризики. У 2025 році рекордних значень досягли вилучення стимуляторів амфетамінового типу (ATS), на які припала майже половина всіх вилучених синтетичних наркотиків у світі. Метамфетамін залишається домінантним наркотиком у Східній та Південно-Східній Азії та Північній Америці, де його виробництво сконцентроване в таких потужних хабах, як М'янма та Мексика. Однак найшвидше зростання вилучень метамфетаміну за останнє десятиліття спостерігається не в цих традиційних регіонах, а в Європі, Африці, на Близькому Сході — там, де ринки тільки формуються, що свідчить про стратегічну експансію виробників.

Цікавим феноменом є ринок «каптагону» — фальсифікованих таблеток на основі амфетаміну, що виробляються переважно в Сирії та затопили країни Близького Сходу. Політичні зміни в Сирії 2024 року зробили майбутнє цього ринку невизначеним: були виявлені та знищені великі виробничі майданчики. Однак дані про вилучення у 2024 та на початку 2025 року свідчать, що потік наркотику до Саудівської Аравії, Йорданії та Іраку не припинився, ймовірно, за рахунок реалізації гігантських запасів, накопичених за попередні роки, або швидкого перенесення виробництва в інші локації. Паралельно в регіоні стрімко зростає трафік метамфетаміну, і експерти побоюються, що в разі перебоїв з «каптагоном» споживачі можуть масово перейти на цей ще більш руйнівний стимулятор, що створить додаткове навантаження на і так слабкі системи охорони здоров'я та лікування.

Ринок нових психоактивних речовин (НПР) демонструє, що міжнародна система контролю може бути ефективною, коли мова йде про окремі речовини. Кількість НПР, що спостерігаються на ринку, скоротилася з піку 2021 року, і жодна окрема речовина не стала глобально домінуючою. Проте цей успіх є оманливим. НПР залишаються постійною «лабораторією ринку»: коли одну речовину забороняють, з'являється десяток нових. Більш того, головна небезпека НПР полягає не в їх цільовому споживанні, а в тому, що їх підмішують до інших наркотиків, таких як героїн, кокаїн або каннабіс, без відома покупців. Саме так нітазени, продані під виглядом героїну, викликали спалахи смертельних передозувань в Ірландії, Великій Британії та країнах Балтії. Це створює ситуацію тотальної невизначеності для споживача, коли навіть досвідчений користувач не може бути впевнений у вмісті купленого продукту, що різко підвищує ризик смертельних наслідків.

Окремої уваги заслуговує масове немедичне вживання фармацевтичних препаратів, що стало паралельною епідемією. Трамадол, неконтрольований на міжнародному рівні, є головною наркотичною проблемою Західної та Центральної Африки, де його використовують для підвищення витривалості та пригнічення болю. Кодеїн, контрольований речовина, переживає ренесанс вилучень, головним чином в Азії та Африці. Прегабалін, ліки від нейропатичного болю, стає популярним на Близькому Сході та в Африці завдяки своїм ейфорієгенним та дисоціативним ефектам. Ці ринки живляться або за рахунок «легальних» поставок з аптек (часто через корупцію), або завдяки масовому незаконному виробництву, зокрема в Індії, звідки препарати розповсюджуються по всьому світу. Це вказує на системні прогалини у фармацевтичному регулюванні та контролі за ланцюгами поставок ліків у багатьох країнах, якими майстерно користуються злочинні мережі.

Система кримінальної юстиції у всьому світі, як видно зі звіту, продовжує зосереджуватися переважно на найменш небезпечних ланках нарколанцюга: споживачах. У 2023 році близько 6.1 мільйона людей мали контакт з поліцією через правопорушення, пов'язані з наркотиками, і майже дві третини з них — за вживання або володіння для особистого вживання. Хоча загальна кількість притягнених за ці правопорушення більша, ймовірність бути притягнутим до суду та засудженим значно вища для тих, хто займається трафіком. Це створює парадоксальну картину, коли тисячі людей з розладами вживання, які потребують допомоги, потрапляють у кримінальну систему, водночас великі трафікери, особливо ті, що мають можливість найняти хороших адвокатів або дати хабара, часто уникають правосуддя. Жінки, які становлять лише 10% затриманих за наркозлочини, рідше за чоловіків потрапляють під суд і отримують вирок, що може свідчити про певну поблажливість системи, але також може бути відображенням того, що жінок частіше залучають до нижчих ланок трафіку (наприклад, як перевізників), де довести вину складніше.

У світі спостерігається розкол у правовому підході до канабісу. З одного боку, Канада, Уругвай, 28 штатів США, а також Мальта, Люксембург та Німеччина легалізували або суттєво декриміналізували немедичне вживання, дозволяючи домашнє вирощування та володіння невеликими кількостями. З іншого боку, у більшості країн Африки та Азії особисте вживання залишається кримінальним злочином. Дані з юрисдикцій, що легалізували канабіс, показують неоднозначну картину: серед підлітків зростання споживання не спостерігається (їм доступ до легального ринку заборонений), але серед молоді та дорослих зростає частота щоденного вживання, збільшується споживання продуктів з високим вмістом ТНС, а також кількість госпіталізацій, пов'язаних із розладами вживання канабісу, та випадків психічних розладів. Разом з тим різко скоротилася кількість арештів та ув'язнень за правопорушення, пов'язані з канабісом.

Організована злочинність залишається головним бенефіціаром наркобізнесу. Наркотики приносять сотні мільярдів доларів на рік, становлячи основу фінансування для тисяч груп по всьому світу. Аналіз показує, що ці групи не є монолітом. Одні орієнтовані на «управління»: ієрархічні, прагнуть контролювати території, ринки, політиків та суддів через корупцію та насильство (картелі Мексики, 'Ндрангета в Італії). Інші орієнтовані на «торгівлю»: вони більш мережеві, гнучкі, зосереджені на максимізації прибутку від конкретних операцій, швидко змінюють маршрути та методи (багато груп, що займаються морським трафіком метамфетаміну в Південно-Східній Азії). Ця різниця визначає їхню вразливість. Ієрархічні групи можна порушити, усуваючи ключових лідерів або фінансистів, але це може призвести до спалаху насильства у боротьбі за владу. Мережеві групи важче розбити силовими методами, але вони вразливі до тактик, що руйнують довіру між учасниками, наприклад, залучення інформаторів або цілеспрямоване вилучення ключових «вузлів» мережі — експертів з логістики чи «хіміків». Автори звіту закликають відмовитися від нерозбірливих силових операцій на користь цілеспрямованих, інтелектуально наповнених дій, що враховують специфіку кожної групи.

Висновки:

- **Синтетичні наркотики стали основним драйвером глобального ринку.** Поява надпотужних опіоїдів та стрімке поширення метамфетаміну в нових регіонах створюють непередбачувані загрози для громадського здоров'я.
- **Південно-східний вектор трафіку зміщується до Європи та нових ринків Африки й Азії.** Західна та Центральна Європа тепер фіксують більше вилучень кокаїну, ніж Північна Америка, а стрімке зростання попиту в Африці та Азії свідчить про експансію трафіку.
- **Доступ до лікування наркозалежності залишається катастрофічно нерівним.** Лише 1 із 12 людей з розладами вживання отримує допомогу, а в Африці цей показник сягає лише 3%.
- **Організована злочинність диверсифікується, але наркотрафік залишається її основним доходом.** Ефективна боротьба вимагає цільових, а не масових силових операцій, з урахуванням структури кожної групи.

Всесітній звіт про наркотики 2025 року малює картину світу на роздоріжжі. З одного боку, ми бачимо неймовірно стійку, технологічно просунуту та багатомільярдну індустрію, що користується соціальними розривами, політичною нестабільністю та прогалинами в регулюванні. З іншого боку, ми маємо науково доведені, ефективні та часто недорогі методи запобігання шкоді, лікування та реінтеграції. Майбутнє боротьби з наркотиками залежатиме не від того, скільки тонн буде вилучено або скільки лабораторій знищено, а від здатності суспільств інвестувати в людей, будувати справедливі та здорові громади, забезпечувати рівний доступ до лікування та боротися зі стигмою. Це вимагає переходу від переважно силової парадигми до комплексної, гуманної та науково обґрунтованої політики, що визнає залежність хворобою, а не злочином, а здоров'я та безпеку громад — своєю найвищою метою. У протилежному випадку глобальна наркосфера, як мутагенний вірус, і надалі адаптуватиметься, породжуючи все нові, ще більш небезпечні форми, а людські страждання, задокументовані в цьому звіті, будуть лише множитися.

Звіти окремих інституцій та експертів

Платежі в стейблкоїнах: реальність за цифрами [10]

Аналітична доповідь Boston Consulting Group є найбільш ґрунтовним дослідженням реального економічного імпакту стейблкоїнів, проведеним у партнерстві з Allium Labs. Центральна проблема, яку піднімає BCG, — це "класифікаційний хаос" у блокчейн-даних, де через відсутність метаданих (на кшталт MCC-кодів у традиційних картах) будь-який рух токенів часто помилково трактується як "платіж". Аналіз 62 трильйонів доларів США річного валового обсягу переказів показав, що лише 4,2 трильйона (7%) є органічною економічною діяльністю. Решта 93% — це "технічний шум": арбітражні боти, внутрішнє балансування гаманців бірж, складні маршрутизації через децентралізовані обмінники (DEX) та застава у деривативних протоколах. Методологія BCG базується на ідентифікації патернів: наприклад, виключаються транзакції між адресами з високою частотою (1000+ на місяць) або оборотом понад 10 млн дол. за 30 днів, що вказує на активність ботів.

Сегментація реальних платежів (оцінених у 350-550 млрд дол. США за 2025 рік) демонструє чітку спеціалізацію стейблкоїнів у нішах, де традиційна банківська система є неефективною. B2B платежі займають 40% ринку і зростають на 65% щорічно. Їхня цінність полягає у миттєвій фінальності транскордонних розрахунків, що дозволяє компаніям уникати "замороженої ліквідності" у рахунках ностро/востро та мінімізувати FX-спреди. C2C платежі (25% частки) демонструють найвищий середньорічний темп зростання (CAGR - 75%), що свідчить про масову адаптацію стейблкоїнів для платежів у країнах з нестабільними валютами або дорогими коридорами грошових переказів. Дослідження зафіксувало важливий тектонічний зсув у виборі блокчейнів: хоча TRON все ще домінує за обсягом (60-80%) через свою дешевизну, нові інституційні потоки масово мігрують на Ethereum, Solana та Polygon. Це пояснюється потребою у "регуляторній чистоті", кращій аналітиці та сумісності зі смарт-контрактами для автоматизованого комплаєнсу.

Категорія використання	Частка в реальних платежах	CAGR (24-25)	Основна перевага
B2B (Business-to-Business)	~40%	65%	24/7 розрахунки, швидка фінальність
C2C (Consumer-to-Consumer)	~25%	75%	Дешеві ремітенси, доступ до USD
C2B (Consumer-to-Business)	~25%	55%	Онлайн-сервіси, ігри, гемблінг
B2C (Business-to-Consumer)	~10%	50%	Виплати фрілансерам та кріейторам

[10] https://media.licdn.com/dms/document/media/v2/D4D1FAQEo_H1guSeHEA/feedshare-document-pdf-analyzed/B4DZwg2egQLAAY-/0/1770077679644?e=1771459200&v=beta&t=0UgWzDPdwRmDSRs9YB9ucM7gcUYyeYT57Y7BWJ38yc0

Для фахівців з комплаєнсу висновки BCG мають критичне значення. По-перше, звіт підтверджує, що стейблкоїни стали "практичним мостом" між он-чейн системами та традиційними фінансами, а не просто інструментом для криптотрейдингу. Капіталізація ринку понад 307 млрд дол. США та зростання на 50% за рік підкріплені регуляторною еволюцією в США, ЄС (MiCA) та ОАЕ. По-друге, розрив між валовим та реальним обсягом вказує на те, що системи моніторингу транзакцій повинні вміти фільтрувати "неорганічні" потоки, щоб не перевантажувати аналітиків помилковими спрацюваннями. По-третє, домінування B2B сегмента вимагає від банків

Висновки:

- Реальне використання стейблкоїнів у платежах становить лише 7% від загального обсягу переказів, що вимагає від регуляторів переходу від валового моніторингу до глибокої поведінкової аналітики для розрізнення торгових операцій та комерційних розрахунків.
- B2B сегмент є найбільш динамічним та інституційно значущим вектором росту, що зумовлено здатністю стейблкоїнів оптимізувати ліквідність у транскордонних операціях та забезпечувати розрахунки в режимі реального часу 24/7.
- Спостерігається системна міграція інституційних платежів з блокчейнів з низькою вартістю (TRON) до мереж з розвиненою екосистемою безпеки та регуляторної прозорості (Solana, Ethereum), що вказує на пріоритет надійності над ціною для великого капіталу.
- Зростання сегмента C2C на 75% щорічно демонструє перетворення стейблкоїнів на основний інструмент фінансової інклюзії в регіонах з обмеженим доступом до доларового банкінгу, що створює нові виклики для контролю за переказами.

перегляду своїх стратегій щодо управління казначейством та пропонування клієнтам сервісів зберігання стейблкоїнів, оскільки попит на них з боку корпоративного сектору стає структурним фактором конкурентоспроможності.

Інтероперабельність як умова довіри: стандарти цифрових активів у регульованій фінансовій системі [11]

Документ, підготовлений у межах співпраці SODA та MIT Connection Science, є концептуально й методологічно цілісним аналітичним викладом проблеми фрагментації токенізованих фінансових активів і водночас дорожньою картою створення глобальної системи інтероперабельності для цифрових активів у сфері регульованих фінансів. У центрі документа — твердження, що нинішня хвиля токенізації реальних активів, попри технологічні успіхи та зростаючий інтерес з боку банків, фінансових ринкових інфраструктур і великих інституційних інвесторів, залишається структурно обмеженою через відсутність спільних стандартів, які дозволяли б активам вільно, безпечно та юридично коректно переміщатися між різними технологічними середовищами, блокчейнами та традиційними системами обліку.

Автори виходять з емпіричного спостереження, що більшість проєктів токенізації 2020-х років розвивалися у вигляді ізольованих, часто дозвільних екосистем, створюючи окремі «острови ліквідності». Такі підходи забезпечують лише локальні операційні покращення — швидше

[11] https://soda-services.com/white-paper/

врегулювання, зниження витрат або кращу прозорість у межах конкретної платформи, — але не формують системного ефекту для глобальних фінансів. У результаті мікроефективності на рівні окремих проєктів перетворюються на макронеефективності для фінансової системи загалом. Документ підкреслює, що справжній економічний потенціал токенізованих активів може бути реалізований лише за умови існування спільного «глобального середовища», у якому емітенти й інвестори здатні здійснювати операції з активами незалежно від конкретної технології, мережі чи юрисдикції.

Для обґрунтування цієї тези використано дві історичні аналогії, які пронизують увесь документ. Перша — розвиток Інтернету, де рання стандартизація базових протоколів керування передаванням даних та міжмережевого протоколу у межах відкритої та нейтральної моделі Інженерної робочої групи Інтернету (IETF) створила умови для вибухового зростання цифрової економіки, попри неможливість передбачити майбутні сервіси та бізнес-моделі. Друга — стандартизація морських контейнерних перевезень, яка перетворила фрагментовану логістику на основу глобалізації. У обох випадках ключовим чинником успіху стала не домінуюча технологія або окремий гравець, а узгоджені, мінімальні й універсальні стандарти, що дозволили різним системам працювати разом. Автори прямо проводять паралель між цими прикладами та сучасною токенізацією, наголошуючи, що вікно можливостей для стандартизації відкрито саме зараз, на етапі формування ринку.

Висновки:

- **Без глобальних стандартів взаємної сумісності токенізація не здатна до масштабування:** ізольовані дозвільні рішення та несумісні екосистеми розподілених реєстрів створюють макрорівневі неефективності, які нівелюють потенційні вигоди від токенізації регульованих активів.
- **Стандарти мають бути технологічно нейтральними та юридично орієнтованими:** першочерговим є уніфікований опис активу, його життєвого циклу та правового режиму, а не вибір конкретного розподіленого реєстру чи технічного протоколу.
- **Взаємна сумісність у фінансах = взаємна сумісність + довіра + регуляторна відповідність:** ефективні стандарти повинні одночасно забезпечувати перевірку вимог ПВК/ФТ/ФР на рівні розподіленого реєстру, захист конфіденційної інформації та прозорість для органів нагляду.
- **Роль I-SODA — координувати, а не конкурувати:** створення нейтральної організації зі стандартизації за моделлю IETF є практичним шляхом до консолідації існуючих стандартів і формування спільної інфраструктурної основи для майбутньої глобальної токенізованої фінансової системи.

Центральним інституційним елементом документа є опис еволюції Групи з питань інтероперабельності (IOG) та трансформації цієї ініціативи у Організацію зі стандартизації інтероперабельності цифрових активів (I-SODA). I-SODA позиціонується як нейтральна організація зі стандартизації, що діятиме за моделлю відкритих стандартів і не конкуруватиме з існуючими протоколами чи екосистемами. Її завдання полягає не у створенні «єдиного правильного блокчейну», а у гармонізації вже наявних стандартів, абстрагуванні спільних елементів токенізаційних процесів, виявленні прогалин та, за потреби, розробленні нових технічних і функціональних специфікацій. Важливо, що ця діяльність має здійснюватися у співпраці з системно важливими фінансовими ринковими інфраструктурами, банками, емітентами, постачальниками технологій та регуляторами.

Методологічною основою роботи I-SODA є поділ стандартизації на три взаємопов’язані потоки. Перший зосереджується на моделі даних активу та описі його життєвого циклу

таким чином, щоб ідентичність активу зберігалася незалежно від форми — цифрової чи нецфрової — та від технології зберігання. Другий формує спільний набір цифрових функцій і дій, які мають бути універсально зрозумілими для будь-якого представлення регульованого активу, включно з базовими операціями, ролями учасників і їх взаємодією. Третій потік присвячений правовим і управлінським аспектам, зокрема відображенню чинних регуляторних режимів, юридичних ролей, механізмів ідентифікації, юрисдикційного нагляду та вирішення спорів у токенізованому середовищі.

Особливу увагу документ приділяє темі довіри як фундаменту інтероперабельності. Наголошується, що в регульованих фінансах технічна сумісність не має цінності без правової визначеності, відповідності вимогам комплаєнсу та можливості регуляторного нагляду. Водночас без захисту конфіденційної інформації та комерційних даних інституційна участь у відкритих мережах є неможливою. У цьому контексті значне місце відведено концепції ідентичності на рівні розподіленого реєстру, програмованої приватності та стандартів, які дозволяють токенам самостійно перевіряти дотримання вимог ПВК/ФТ, санкцій, інвесторської придатності чи юрисдикційних обмежень без покладання на позамережеві реєстри або централізовані платформи.

Документ послідовно демонструє, що справжня токенізація — це не технічне «обгортання» активів, а складний міждисциплінарний процес, який вимагає узгодження правових, операційних, податкових і технологічних вимог. На прикладах акцій, облігацій, фондів, депозитів і альтернативних активів показано, що без спільної мови для опису прав, обмежень, корпоративних дій і відповідальності будь-яка токенізована модель залишається крихкою та вразливою до арбітражу, зловживань або правової невизначеності, особливо в умовах міжмережевих операцій.

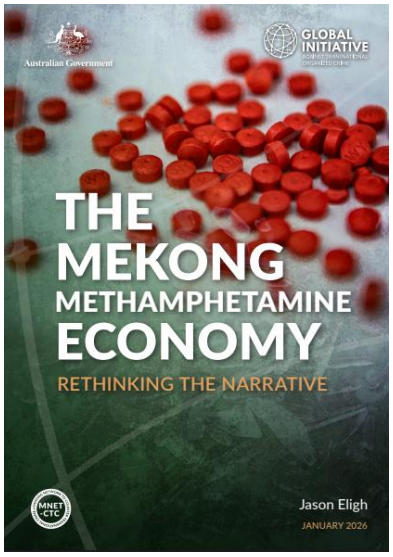
У підсумку аналітичний документ формує чіткий стратегічний меседж: майбутнє токенізованих фінансів залежить не від кількості блокчейнів чи швидкості транзакцій, а від здатності галузі домовитися про спільні, відкриті й нейтральні стандарти, які поєднають інтероперабельність, довіру та регуляторну відповідність. I-SODA пропонується як інституційний механізм для досягнення цієї мети, а сам документ — як концептуальна основа для переходу від фрагментованих експериментів до по-справжньому глобальної інфраструктури цифрових активів.

Метамфетамін Меконгу: як регіональна наркоекономіка стала глобальною індустрією і чому світ дивиться не туди [12]

Аналітичні й політичні уявлення про метамфетамінову економіку регіону Меконгу протягом останніх років формувалися навколо зручної, але методологічно слабкої гіпотези: військовий переворот у М’янмі в лютому 2021 року нібито спровокував різкий і безпрецедентний сплеск виробництва метамфетаміну. Ця версія стала майже аксіомою в заявах міжнародних організацій, урядів і медіа, попри те що вона значною мірою ґрунтується на непрямих індикаторах, припущеннях і некритичному використанні статистики вилучень. Дослідження, опубліковане GI-TOC послідовно й аргументовано демонструє: така інтерпретація не просто спрощує реальність, а системно викривляє розуміння самої природи метамфетамінової економіки Меконгу, її історичної еволюції та сучасної глобальної ролі.

Ключовий аналітичний зсув, який пропонує автор, полягає у відмові від реактивного мислення на користь структурного аналізу. Замість того щоб шукати «тригер» зростання виробництва в

[12] https://globalinitiative.net/wp-content/uploads/2026/01/Jason-Eligh-The-Mekong-methamphetamine-economy-Rethinking-the-narrative-GI-TOC-December-2026.pdf



одному політичному моменті, дослідження показує довготривалу, багаторічну траєкторію індустріалізації наркоринку, що почалася задовго до 2021 року і продовжилася без якісного зламу після перевороту. Зростання обсягів виробництва, удосконалення хімічних процесів, диверсифікація продуктів і глобалізація ланцюгів постачання є результатом поступового накопичення організаційної, технологічної та фінансової спроможності, а не реакцією на короткострокову нестабільність.

Особливу увагу в роботі приділено критиці домінантного використання даних про вилучення наркотиків як проксі-показника виробництва. Автор методично розкладає цю логіку на складові й показує її хибність. Кількість і обсяг вилучень значно більше відображають інтенсивність і пріоритети правоохоронної діяльності, ніж реальний масштаб ринку. Зменшення вилучень у М'янмі після 2021 року, наприклад, цілком логічно корелює з перенаправленням потоків, зміною маршрутів і зниженням внутрішнього перехоплення, а не зі скороченням або, навпаки, стрибкоподібним збільшенням виробництва. Аналогічно, падіння роздрібних цін у Таїланді та інших країнах регіону не є автоматичним доказом «надвиробництва», а може свідчити про підвищену ефективність логістики й менші втрати на етапі транзиту.

Структурна картина, що постає з дослідження, радикально відрізняється від образу хаотичного, фрагментованого наркобізнесу. Метамфетамінова економіка Меконгу функціонує як зріла, високоефективна індустрія з елементами квазідержавного управління. Контроль над територіями, податкові механізми, «орендні» моделі для лабораторій і виробників, гарантії безпеки та логістики — усе це формує систему, де збройні угруповання і пов'язані з державою суб'єкти виступають не стільки виробниками, скільки адміністраторами й бенефіціарами. Перехід до так званої «landlord model», коли місцева влада дозволяє стороннім кримінальним підприємцям виробляти наркотики на своїй території в обмін на податки й захист, значно знизив ризики для ключових гравців і підвищив загальну стійкість системи.

Окремого аналізу заслуговує хімічна еволюція виробництва. Відмова від залежності від ефедрину та псевдо-ефедрину й перехід до використання прекурсорів і пре-прекурсорів, зокрема феніл-2-пропанону (P2P) і метиламіну, стали стратегічною відповіддю на міжнародний контроль. Ця адаптація не лише ускладнила регуляторні зусилля, а й підвищила ефективність синтезу, дозволивши збільшити чистоту продукту та обсяги виробництва. Контроль за такими хімікатами подвійного призначення є значно складнішим, що робить класичні інструменти протидії практично неефективними.

Важливим сигналом глибокої трансформації ринку є диверсифікація продуктового портфеля. Метамфетамін більше не є єдиним або навіть домінуючим товаром у вузькому сенсі. На ринку з'являються синтетичні фармацевтичні препарати, опіоїди, бензодіазепіни та полідрогові суміші на кшталт «happy water», орієнтовані на нові сегменти споживачів і глобальний попит. Це свідчить про підприємницьке мислення учасників ринку та їхню здатність швидко реагувати на зміни споживчих уподобань.

Найбільш тривожний висновок дослідження полягає в тому, що метамфетамін Меконгу вже давно перестав бути регіональною проблемою. Він є повноцінною складовою глобального ринку синтетичних наркотиків поряд із виробничими хабами Мексики та регіону Афганістан–Пакистан–Іран. Його хімічна «універсальність», відсутність географічної прив'язки до сільськогосподарських циклів і здатність інтегруватися в легальні транспортні й фінансові ланцюги роблять його ідеальним глобальним товаром. Фактична присутність меконзького

метамфетаміну в Австралії, Новій Зеландії, Південній Азії, Африці, Європі та навіть Латинській Америці — це не гіпотеза, а емпірично зафіксована реальність, яка досі недооцінюється через аналітичні «сліпі плями».

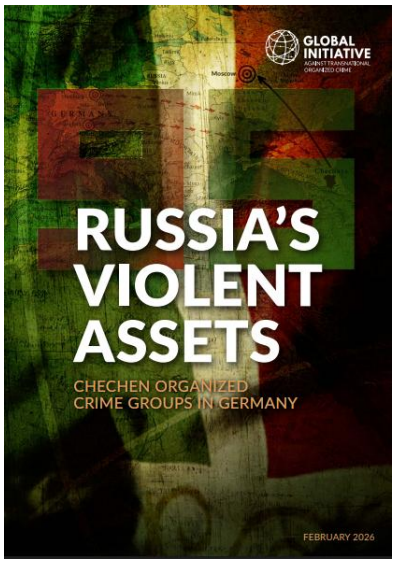
Парадоксально, але саме концентрація уваги міжнародної спільноти на інших загрозах — кокаїні в Європі чи фентанілу в Північній Америці — створює для метамфетамінової експансії особливо сприятливе середовище. Коли правоохоронні органи «не дивляться» в певному напрямку, ринок заповнює вакуум без помітного опору. Згортання програм міжнародної допомоги, скорочення ресурсів антинаркотичних агентств і ослаблення громадянського сектору в регіоні лише посилюють цю тенденцію.

У підсумку, дослідження — це не просто критика хибного наративу, а фундаментальний виклик усталеним підходам до аналізу й протидії синтетичним наркотикам. Воно чітко показує: без переходу до доказово обґрунтованої, транснаціональної та структурно орієнтованої політики міжнародна спільнота й надалі реагуватиме на симптоми, а не на систему. Метамфетамінова економіка Меконгу вже набула індустріального масштабу — і саме в цьому полягає її головна, але досі недооцінена загроза.

Висновки:

- **Твердження про різкий сплеск виробництва метамфетаміну після перевороту в М'янмі у 2021 році не підтверджується доказами** і є результатом хибної інтерпретації даних про вилучення та ціни.
- **Метамфетамінова економіка Меконгу є зрілою, індустріалізованою та інституціоналізованою системою,** яка функціонує за логікою квазідержавного управління, а не хаотичного кримінального бізнесу.
- **Хімічна адаптивність виробництва та диверсифікація синтетичних наркотиків** роблять традиційні підходи контролю прекурсорів і лабораторій структурно неефективними.
- **Регіон Меконгу вже є одним із ключових глобальних хабів синтетичних наркотиків,** а його метамфетамін інтегрований у світові логістичні, фінансові та корупційні ланцюги, але системно недооцінюється міжнародною аналітикою.

Російські «силові активи»: чеченські злочинні угруповання в Німеччині [13]



На тлі складних міграційних потоків, геополітичних зрушень та транснаціональної злочинної діяльності на території Федеративної Республіки Німеччина останнім десятиліттям відбувається тихе, але невпинне формування та укріплення специфічного й небезпечного явища – професійних, жорстоких та надзвичайно згуртованих злочинних мереж, пов'язаних із чеченською діаспорою.

Ці структури, які у звіті GI-TOC визначені як «силові активи» росії, є не просто кримінальними угрупованнями в класичному розумінні, а складними гібридними утвореннями, корені яких сягають глибин історії чеченського народу та інтегровані в сучасні пострадянські політико-кримінальні схеми. Їх діяльність виходить далеко за межі традиційної злочинності, переплітаючись з питаннями безпеки, контролю над діаспорою,

[13] https://globalinitiative.net/wp-content/uploads/2026/02/Russias-violent-assets-Chechen-organized-crime-groups-in-Germany-GI-TOC-February-2026.pdf

дипломатією та впливом зовнішніх державних суб'єктів, що робить їх унікальним викликом для німецької та європейської правової, соціальної та політичної систем.

Щоб зрозуміти сутність чеченських організованих угруповань у Німеччині, необхідно зануритися в колективну пам'ять сформовану століттями опору. Чеченське суспільство, доведене до межі виживання під тиском царської експансії, радянських депортацій та двох кровопролитних воєн за незалежність у 1990-х роках, виробило унікальні механізми адаптації. У цих умовах кланові зв'язки, що базувалися на спільному походженні та родинній вірності, перетворилися з інструменту соціальної організації на єдиний надійний каркас безпеки та взаємодопомоги. Поняття колективної відповідальності та солідарності, життєво необхідні для виживання в умовах зовнішньої агресії та внутрішньої нестабільності, з часом були інструменталізовані. Коли держава або відверто ворожа, або відсутня, або непоправно корумпована, авторитет переходить до неформальних лідерів, які здатні забезпечити захист, ресурси та своєрідну «справедливість».

Цей перехід став критичним у радянських таборах, де чеченці, і так маргіналізовані системою, знаходили спільну мову з кримінальною субкультурою, але, на відміну від інших кавказьких груп, рідко інтегрувалися в неї повністю, створюючи власні, етнічно однорідні спільноти. Тут формувалася альтернатива державній лояльності – вірність своїй групі, своїм поняттям честі («нохчалла») та своїм методам вирішення конфліктів, які часто передбачали внутрішнє насильство як інструмент дисципліни. Після повернення з депортації та під час розпаду СРСР ці вже існуючі мережі вийшли на перший план. Вони заповнили вакуум влади в Чечні, швидко монетизувавши свою репутацію безкомпромісної жорстокості та надійності. Їх еволюція в росії пройшла шлях від контролю над вуличним рекетом, проституцією та валютними до участі у великій нафтовій контрабанді, фінансуванні військових формувань та, зрештою, до симбіозу з політичною владою. Прихід Рамзана Кадирова та побудова його вертикалі не ліквідували ці структури, а інкорпорували їх, перетворивши частину на офіційні чи парадержавні силові підрозділи, а іншу частину – на зовні незалежні, але лояльні транснаціональні мережі, здатні виконувати різноманітні завдання за межами росії.

Масова хвиля міграції чеченців до Німеччини, що посилилася в 2010-х роках, не була лише пошуком безпеки від війни. Це був також процес трансплантації вже сформованих соціальних динамік у новий контекст. Консервативні оцінки говорять про понад 50 000 осіб чеченського походження в країні, але реальна цифра може бути значно вищою через проблеми ідентифікації (багато мають російські паспорти) та постійний новий приплив. Значна частина цих людей перебуває в юридично невизначеному статусі «Duldung». Цей статус – пастка: він дозволяє залишатися в країні, але практично позбавляє легальних шляхів інтеграції – доступу до стабільної роботи, якісної освіти, повноцінного соціального захисту. Така юридична вразливість створює ідеальні умови для розвитку паралельних систем залежності та контролю. Люди зі статусом Duldung природним чином звертаються до своєї етнічної спільноти за підтримкою, роботою та захистом. І саме в цих неформальних спільнотах кримінальні мережі мають найбільший вплив. Вони позиціонують себе не просто як злочинці, а як «постачальники послуг» для спільноти – можуть вирішити проблему з документами, дати заробіток, захистити від зовнішніх загроз або внутрішніх суперечок.

Це формує глибоку залежність і, що важливо, культуру мовчання. Скарга до німецької поліції розглядається не лише як особистий ризик (помсти), але й як зрада спільності, порушення неписаних законів солідарності, а також може мати наслідки для родичів, що залишилися в Чечні, де кадирівський режим відомий практикою колективної відповідальності. Таким чином, сама структура німецької міграційної політики, ненавмисно, створює середовище, де злочинні угруповання можуть не лише існувати, але й процвітати, вербуючи нових членів серед маргіналізованої молоді та отримуючи мовчазну згоду від більшості діаспори.

Організаційна структура цих угруповань є зразком адаптації до умов сучасної правоохоронної діяльності. Вона навмисно відрізняється від вертикальних ієрархій класичної мафії або арабських кланів. Натомість це гнучка, децентралізована мережа, побудована на щільній павутині довіри, родинних зв'язків, спільних військових біографій та пережитих травм. На вершині цієї невидимої піраміди знаходяться так звані «де-факто авторитети». Це рідко колишні вуличні бандити. Часто це люди з бойовим досвідом чеченських воєн, які мають публічну репутацію у діаспорі як успішні бізнесмени, громадські діячі або спортивні функціонери. Їхня справжня сила полягає в гібридності: вони одночасно є неофіційними представниками інтересів кадирівського режиму в Європі, кримінальними брокерами та громадськими авторитетами. Наприклад, Тімур Дугазаєв, колишній житель Кіля, відкрито позиціонував себе як прихильник Кадирова, отримував державні нагороди Чечні, організовував публічні заходи на підтримку режиму, будучи при цьому номінально політичним біженцем у Німеччині. Його соціальні мережі демонстрували зв'язки з силовими структурами Чечні та підтримку російських дій в Україні. Подібну роль, за даними ЗМІ, тепер виконує Саїхан Агаєв з Гамбурга, який фігурував на з'їзді народу Чечні як представник діаспори.

Ці зв'язки є не просто символічними. Вони надають авторитетам доступ до ресурсів, можливість відмивати кошти через напівдержавні структури, а головне – слугують могутнім інструментом залякування. Уявлення про те, що той чи інший лідер має «вихід на Грозний», породжує страх фізичної розправи не тільки в Німеччині, але й розправ з родичами на батьківщині. Це перетворює звичайну кримінальну угоду на акт політичної лояльності. Під цими авторитетами діють координатори – часто німецькомовні представники другого покоління, які є сполучною ланкою між світом діаспори та німецькою реальністю. Вони переводять стратегічні вказівки в практичні дії, ведуть переговори з іншими злочинними групами, керують низовим бізнесом. Ще нижче – операційні ядра, невеликі групи з 2-6 осіб, які безпосередньо планують та здійснюють злочини. І, нарешті, широка периферія – молодь, часто неповнолітня, яку використовують як виконавців дрібних доручень, для залякування, збору боргів та розповсюдження наркотиків. Це одночасно і кадровий резерв, і джерело «вуличного шуму», що привертає увагу поліції, відволікаючи її від вищих ланок.

Економічна модель угруповань різноманітна, але стрижневою залишається сфера вимагання та «захисту». Вони активно входять в такі сфери, як ресторанний бізнес, будівництво, організація азартних ігор. У східних землях, як-от Бранденбург або Саксонія, вони вже домінують на окремих нелегальних ринках, особливо в торгівлі наркотиками. Відмінною рисою є їхня готовність працювати як «підрядники» з безпеки для інших, більш старих кримінальних синдикатів, пропонуючи послуги силового впливу на конкурентів або захисту бізнесу. Ця роль «професійних виконавців» добре вписується в їхню репутацію. Насильство тут – це не емоційний спалах, а розрахований інструмент комунікації та управління. Ця репутація підживлюється культурою бойових мистецтв (ММА, бокс), які є одночасно центрами соціалізації молоді в діаспорі та неформальними майданчиками для вербування та побудови ієрархій.

Проблема чеченських організованих угруповань ставить перед Німеччиною низку складних, взаємопов'язаних викликів. Перший і найголовніший – це виклик для правоохоронної системи. Звичайні методи боротьби з організованою злочинністю тут часто неефективні. Високий рівень конспірації, побудований на довірі та родинних зв'язках, ускладнює вербування інформаторів. Страх жертв повідомляти про злочини через загрозу помсти не стільки собі, скільки родичам в Чечні, створює «стіну мовчання». Навіть коли справа дістається суду, свідки можуть відмовитися від показань. Поліція та прокуратура часто стикаються не з окремими злочинами, а з цілісною системою контролю та залякування, яку важко розірвати окремими арештами.

Другий виклик – політико-безпековий. Гібридний характер угруповань, їхні зв'язки з кадирівським режимом, а через нього – з кремлівськими центрами впливу, перетворюють їх на потенційний інструмент втручання. Вони можуть використовуватися для збору розвідувальної

інформації, контролю над певними сегментами діаспори (наприклад, для виявлення або залякування опозиційних активістів), для впливу на місцеві громади або навіть для здійснення спецоперацій, як це сталося з убивством у Тіргартені в 2019 році. Це розмиває межі між кримінальною поліцією, розвідкою та контррозвідкою.

Висновки:

- **Чеченські організовані злочинні угруповання в Німеччині є гібридними структурами**, які поєднують кримінальну діяльність з політико-силовими функціями.
- **Структура угруповань побудована на історичній травмі та соціальній згуртованості.** Це формує непроникну для правоохоронців систему, засновану на кланових зв'язках, вірності, стратегічному використанні насильства та культурному коді.
- **Юридична вразливість мігрантів створює ідеальні умови для зростання впливу цих мереж.** Обмежений доступ до легальної роботи та соціальних гарантій змушує людей шукати захист у неформальних спільнотах, формуючи глибоку залежність і культуру мовчання.
- **Ефективна протидія вимагає комплексних заходів:** від посилення міжнародної співпраці до програм соціальної інтеграції, уникаючи при цьому стигматизації всієї чеченської діаспори.

Третій виклик – соціальний. Існування таких груп посилює маргіналізацію самої чеченської діаспори. З одного боку, більшість її членів – прості люди, які втекли від війни та репресій і самі страждають від тиску з боку земляків-злочинців. З іншого боку, в суспільстві та в ЗМІ поширюються стигматизуючі стереотипи, що призводить до ксенофобії та соціальної напруги. Це створює підґрунтя для популістських політичних сил та ускладнює роботу з інтеграцією.

Четвертий виклик – стратегічний. У звіті GI-TOC зазначається про відчутну інерцію та запізнілу реакцію німецьких політичних кіл. На ранніх етапах попередження фахівців із правоохоронних органів про зростання впливу цих мереж часто ігнорувалися, а іноді навіть заперечувалося само їхнє існування як окремого явища. Це дозволило групам закріпитися, вибудувати структури та інтегруватися в місцеві кримінальні ринки, перш ніж держава всерйоз взялася за проблему.

Таким чином, чеченські організовані злочинні угруповання в Німеччині являють собою не локальну проблему «етнічної злочинності», а складний багаторівневий феномен на перетині кримінології, міграційної політики, соціальної роботи та геополітики. Їхня стійкість заснована на унікальному поєднанні історично сформованої соціальної згуртованості, експлуатації правової вразливості мігрантів та гібридних зв’язків із авторитарним режимом за кордоном.

Ефективна протидія вимагає такого ж комплексного підходу. Він має включати не лише посилення правоохоронної співпраці на федеральному та європейському рівні, а й створення спеціалізованих слідчих груп та розвиток аналітичного моніторингу зв’язків між злочинністю і зовнішніми політичними суб’єктами. Не менш важливою є «м’яка сила»: цілеспрямована робота з інтеграції чеченської молоді, створення альтернатив кримінальній кар’єрі через освіту, професійне навчання, спорт, надання правової та психологічної допомоги. Критично важливо працювати з самою діаспорою, налагоджуючи довіру через неурядові організації та громадських діячів, щоб розірвати коло страху та мовчання.

Рекомендовані матеріали

Онлайн-захід CGAP: Від хайпу до імпакту — що стейблкоїни значать для фінансової інклюзії [14]

Вебінар CGAP "From Hype to Impact" (січень 2026 р.) став платформою для дискусії між глобальними регуляторами та лідерами індустрії. Спікери — Данте Діспарте (Circle), Дороті Делорт (Світовий банк), Ефайомі Карр (Flourish Ventures) та Люк Тату (MoneyGram) — представили багатогранний аналіз того, як стейблкоїни трансформують фінансовий ландшафт у країнах, що розвиваються (EMDE). Основна тематика заходу фокусувалася на переході від спекулятивного сприйняття криптоактивів до їхнього використання як "програмованої платіжної інфраструктури". Данте Діспарте підкреслив, що завдяки блокчейну кожен смартфон стає вузлом глобальної мережі розрахунків, що дозволяє переказувати вартість так само легко, як електронні листи, але з вбудованим рівнем комплаєнсу та безпеки.

Аналіз AML/CFT тематик на заході виявив кілька критичних напрямів. По-перше, концепція "compliant endpoints" (комплаєнс-орієнтованих кінцевих точок). На відміну від анонімних криптогаманців, сучасні VASP (постачальники послуг віртуальних активів) інтегрують процедури KYC безпосередньо в інтерфейси мобільних додатків. Люк Тату з MoneyGram поділився досвідом імплементації "KYC з нульового долара", що є радикальним кроком у порівнянні з традиційними порогами для переказів. Це дозволяє створювати "прозорі коридори" для переказів, де кожна транзакція відповідає Travel Rule (рекомендація FATF 16). По-друге, обговорювалася проблема "фінансової доларизації". Регулятори висловлюють занепокоєння, що стейблкоїни, прив'язані до долара США, можуть витіснити слабкі національні валюти, що позбавить центральні банки можливості проводити незалежну монетарну політику та контролювати кредитні цикли.

Технологічний імпакт стейблкоїнів був проілюстрований через кейси африканського ринку. Ефайомі Карр зазначив, що в Нігерії стейблкоїни використовуються для розрахунків у реальному секторі економіки через хронічний брак доларової ліквідності в банках. Це створює паралельну платіжну систему, яка працює швидше та дешевше за традиційний SWIFT. Регуляторний погляд на цю проблему, представлений Дороті Делорт, полягає в необхідності поступового впровадження регулювання: спочатку — закриття прогалин у ПВК/ФТ для VASP, потім — розробка стандартів для емітентів стейблкоїнів та захисту прав споживачів. Перегляд заходу є надзвичайно корисним для фахівців, які займаються розробкою національних стратегій цифрових валют (CBDC), оскільки він демонструє реальну конкуренцію між державними та приватними цифровими активами у боротьбі за довіру користувачів.

Інші новини

Запуск збору даних для тестування моделей оцінки ризиків AMLA [15]

Оголошення Управління боротьби з відмиванням коштів (AMLA) про запуск збору даних у березні 2026 року є ключовою подією в розбудові нової європейської архітектури фінансової

[14] https://www.youtube.com/watch?v=86vH-N0P_XY
[15] https://www.amla.europa.eu/amla-launch-data-collection-exercise-test-risk-assessment-models-financial-sector_en

безпеки. Цей захід не є просто статистичним опитуванням; це фундаментальне тестування і калібрування моделей, які визначать майбутнє прямого нагляду в ЄС. Логіка AMLA полягає у створенні доказової бази для відбору 40 найбільш ризикових та транскордонних фінансових установ, які перейдуть під її пряме управління з 2028 року. Методологія вправи передбачає залучення двох груп учасників: установ, що за об'єктивними критеріями (наявність у 6+ країнах ЄС, обсяг активів) можуть потрапити під нагляд, та репрезентативної вибірки установ, що залишаться під національним контролем. Такий підхід дозволяє перевірити "чутливість" моделей та їхню здатність коректно диференціювати рівні притаманного та залишкового ризику в масштабах усього Союзу.

Згідно з проектом Regulatory Technical Standards (RTS) за статтею 40(2) AMLD, AMLA впроваджує гармонізовану структуру оцінки ризиків. Притаманний ризик (inherent risk) аналізується через призму клієнтського профілю, географічної присутності, каналів дистрибуції та типів продуктів. Особлива увага приділяється транскордонній активності: RTS пропонує кількісні пороги (наприклад, понад 20 000 клієнтів або 50 млн євро транзакцій у конкретній країні) для визначення матеріальності присутності установи. Залишковий ризик (residual risk) оцінюється на основі якості систем контролю, ефективності транзакційного моніторингу та готовності IT-інфраструктури. Регулятор очікує від установ переходу до структурованих даних та автоматизованого скорингу, де ручне втручання допускається лише як експертне коригування.

Процес збору даних у 2026 році дозволить AMLA оптимізувати перелік точок даних, які будуть офіційно зібрані у 2027 році для фінального відбору. Важливо, що AMLA також бере на себе роль координатора національних підрозділів фінансової розвідки (ПФР) та наглядових органів, забезпечуючи перенесення мандатів ПВК від EBA до кінця 2025 року. Це означає створення єдиного "аналітичного хребта", де дані про ризики стікаються в централізовану систему, дозволяючи бачити мережеві ефекти та складні схеми відмивання доходів, які раніше були приховані через національну фрагментацію. Для фінансових установ участь у цьому зборі даних є можливістю провести "репетицію" та підготувати свої системи до значно суворішого та консолідованого режиму нагляду, де якість даних стає критичним фактором оцінки їхньої доброчесності.

Криптозлочинність: темна сторона цифрової фінансової революції [16]

Криптовалюти, які ще два десятиліття тому сприймалися як маргінальний експеримент, сьогодні перетворилися на глобальне явище, що об’єднує понад півмільярда користувачів по всьому світу. Вони обіцяли не лише технологічний прорив, але й фінансову емансипацію — свободу від банківських комісій, державного контролю та кордонів. Однак, як показує глибоке дослідження BBC, опубліковане на початку 2026 року, ця свобода виявилася двосторонньою: децентралізовані технології одночасно стали ідеальним середовищем для злочинності нового типу.

У 2025 році обсяг викрадених криптоактивів досяг 3,4 мільярда доларів, і майже чверть цієї суми — 713 мільйонів — припала на атаки на приватних

[16] https://www.bbc.com/news/articles/c93w30gl5jno

інвесторів. Ці цифри не просто статистика; за кожною з них стоять людські долі, втрачені надії та зруйновані плани.

Основним парадоксом, на який вказує дослідження, є суперечливе поєднання прозорості та анонімності в світі криптовалют. Блокчейн, цифровий реєстр усіх транзакцій, робить кожен переказ грошей публічно доступним для перегляду. Жертви можуть у реальному часі спостерігати, як їхні кошти переходять з гаманця в гаманець, назавжди залишаючись у відкритому доступі. Проте ця технологічна прозорість абсолютно неефективна, коли мова заходить про ідентифікацію злочинців. Криптогаманці, на які переводяться викрадені кошти, часто належать анонімним користувачам, чиї реальні особистості неможливо встановити без спеціальних розслідувань, доступу до IP-адрес або помилок самих зловмисників.

За даними аналітичної фірми Chainalysis, у 2025 році кількість атак на приватних криптоінвесторів зросла до 80 тисяч — це вдвічі більше, ніж у 2022 році. Такий стрімкий зріст пояснюється низкою взаємопов'язаних факторів. По-перше, стрімке зростання вартості таких активів, як біткоін та ефіріум, особливо під час пандемії, привернуло увагу мільйонів нових інвесторів, багато з яких не мали достатнього досвіду в кібербезпеці. По-друге, покращення захисту великих криптобірж, таких як Binance чи Coinbase, змусило злочинців переорієнтуватися на менш захищені цілі — приватних власників гаманців, які часто не використовують навіть базові засоби безпеки, такі як двофакторна автентифікація або апаратні гаманці. По-третє, зросла доступність зламаних баз даних, які зловмисники використовують для цілеспрямованого вибору жертв. Найвразливішими виявляються ті, хто не лише володіє значними сумами, але й активно ділиться інформацією про свої інвестиції в соціальних мережах або спеціалізованих форумах. Проте, як зазначають експерти Chainalysis, реальна статистика може бути значно вищою — багато жертв, особливо ті, хто втратив відносно невеликі суми, не повідомляють про крадіжки через відчуття сорому, безнадії або невіри в можливість відновлення справедливості.

Глобальний масштаб криптозлочинності яскраво ілюструють гучні міжнародні справи. У лютому 2025 року північнокорейські хакери, які, за даними розвідки, діють під державною підтримкою, викрали 1,5 мільярда доларів із криптобіржі Bybit. Ця атака стала однією з найбільших в історії, але вона не є винятком — Північна Корея регулярно звинувачується у використанні кібератак для фінансування свого режиму, обходячи міжнародні санкції. Окрім державних суб'єктів, активність проявляють і кримінальні угруповання, такі як Social Engineering Enterprise, члени якого у США визнали себе винними у викраденні 260 мільйонів доларів між 2023 і 2025 роками. Вони використовували складні схеми соціальної інженерії: через зламані бази даних вони ідентифікували заможних власників криптовалют, потім імітували співробітників бірж, переконуючи жертв переказати кошти на «безпечні» адреси. Отримані кошти злочинці витрачали на розкішний спосіб життя — приватні літаки, дорогі автомобілі, люксові аксесуари, якими вони хизувалися в соціальних мережах і роздавали в нічних клубах. Ця безтурботність свідчить не лише про масштаби крадіжок, але й про відчуття безкарності, яке панує серед багатьох злочинців у криптосфері.

Однак найтривожнішим трендом останніх років стало поширення фізичного насильства, відомого в криптоспільноті як «гвинтові атаки» (wrench attacks). Ця назва походить від історій, коли злочинці буквально загрожували жертвам гайковими ключами, щоб отримати доступ до їхніх гаманців. Але реальність набагато жорстокіша: у 2024-2025 роках відбулася низка випадків викрадень, тортур і навіть вбивств, пов'язаних із спробами заволодіти криптоактивами. В Іспанії злочинці викрали пару, поранили чоловіка в ногу і тримали їх у полоні годинами, намагаючись отримати доступ до їхніх гаманців. Жінку було відпущено, а тіло чоловіка знайшли пізніше в лісі. У Франції відбулося кілька спроб викрадення членів сімей криптоекспертів, включаючи співзасника компанії Ledger Девіда Балланда, якого разом із дружиною викрали з дому, а під час спроби вимагати викуп йому відрізали палець. У Великій Британії поліція заарештувала шістьох людей після того, як злочинці зупинили автомобіль на трасі між Оксфордом і Лондоном

та примусили одного з пасажирів переказати криптовалюту на суму 1,5 мільйона фунтів. Філ Apicc, директор з питань зв'язків із державним сектором у TRM Labs, зазначає, що організовані злочинні групи, які вже звикли до насильства, закономірно переходять у криптосферу: «Доки існує життєздатний шлях для відмивання або ліквідації викрадених активів, злочинцю не має великої різниці, чи його ціль — дорогі годинники, чи криптогаманець. Криптовалюта тепер міцно увійшла в мейнстрім, і наше традиційне розуміння фізичної загрози та пограбування має еволюціонувати відповідно».

Ключовим фактором, що полегшує атаки на приватних осіб, є легкість доступу до персональних даних через масштабні витоки інформації з корпоративних баз. Хакер, який дав інтерв'ю BBC на умовах анонімності, розповів, як він купив за 300 тисяч доларів базу даних групи копаній Kering, до якої входять такі бренди, як Gucci та Balenciaga. Ця база містила не лише контакти мільйонів клієнтів, але й інформацію про суми їхніх покупок, що дозволило визначити найбагатших і, отже, потенційно найпривабливіших цілей. Поєднавши ці дані з іншими витоками, хакеру вдалося виманити у користувачів Coinbase понад 1,5 мільйона доларів у криптовалюті.

Регуляторний вакуум у багатьох юрисдикціях значно посилює проблему. У Великій Британії, де криптовалюти залишаються «майже нерегульованими та високоризикованими», за попередженням FCA, жертви крадіжок практично не мають шансів на компенсацію. На відміну від традиційних банків, які часто покривають втрати від шахрайських транзакцій за певних умов, криптобіржі не несуть такої ж відповідальності. Наприклад, Binance, найбільша у світі криптобіржа, яка має близько 1,4 мільйона користувачів у Великій Британії, не надає підтримки жертвам крадіжок, а її сторінки з порадами для постраждалих блокуються на британській території. Біржа не приймає нових клієнтів з 2023 року через відсутність авторизації FCA, але це не заважає злочинцям цілитися в британців, які вже мають рахунки. Така ситуація створює середовище, де правоохоронці та регулятори відстають від технологій, а злочинці користуються міжнародним характером криптовалют, щоб ухилятися від правосуддя.

У відповідь на зростаючі загрози з'являються технологічні рішення, спрямовані на посилення безпеки приватних гаманців. Метью Джонс, засновник компанії Haven, який сам став жертвою крадіжки криптоактивів, розробив гаманець з розширеними функціями захисту: безперервна біометрична перевірка (наприклад, сканування обличчя або відбитків пальців) для підтвердження кожної транзакції, гео-захист, який блокує перекази за межами заздалегідь визначених безпечних зон (дому чи роботи), та «тривожна кнопка», що дозволяє миттєво заблокувати доступ при загрозі. Однак такі інновації поки що залишаються нішевими продуктами, недоступними для широкого загалу користувачів, особливо для новачків, які часто не усвідомлюють ризиків.

Це підводить до фундаментальної дилеми криптосвіту: вибір між свободою «бути своїм власним банком» та повною відповідальністю за власну безпеку. З одного боку, як аргументує Джонс, традиційні фінансові інституції далекі від ідеалу: вони можуть заморожувати рахунки за широкими та часто незрозумілими причинами, втручатися у транзакції та збирати величезну кількість персональних даних. Криптовалюти пропонують альтернативу — фінансовий суверенітет, де користувач сам контролює свої активи без посередників. Але, ця свобода може обернутися катастрофою, якщо користувач не готовий до ролі власного охоронця, слідчого та технічного спеціаліста одночасно.

Майбутнє криптобезпеки залишається невизначеним. З одного боку, розвиток технологій, таких як гаманці з мульти-підписами, децентралізована ідентифікація та покращені протоколи шифрування, може зробити зберігання активів безпечнішим. З іншого — злочинці також вдосконалюють свої методи, використовуючи штучний інтелект для масштабоних фішинг-атак, глибокі підробки (deepfakes) для обходу біометрії та складні схеми для відмивання коштів через децентралізовані біржі (DEX) та міксери транзакцій. Регулятори поступово починають

впроваджувати нові правила, але їх ефективність обмежена глобальним характером криптосфери. Водночас зростає обізнаність користувачів: все більше людей розуміють важливість апаратних гаманців, резервного копіювання seed-фраз та обережності в мережі.

Висновки:

- **Криптовалютна злочинність стрімко зростає:** у 2025 році загальний обсяг викрадених коштів склав понад 3,4 млрд доларів, з яких 713 млн доларів припало на приватних інвесторів.
- **Атаки на фізичних осіб стають все жорстокішими:** злочинці все частіше використовують не лише кіберметоди, але й фізичне насильство — викрадення та тортури.
- **Регуляторний вакуум підсилює ризики:** у багатьох країнах, включаючи Велику Британію, криптовалюти залишаються майже неврегульованими, що робить жертв беззахисними перед злочинцями.
- **Доступ до викрадених даних полегшує цілеспрямовані атаки:** масові витоки даних із корпорацій (наприклад, Gucci, Balenciaga) дозволяють злочинцям ідентифікувати найбагатших власників криптовалют та цілеспрямовано їх обкрадати.

У підсумку, криптозлочинність сьогодні — це не просто побічний ефект нової технології, а складний соціотехнічний феномен, що відображає глибші проблеми: нерівність у доступі до знань про безпеку, міжнародні розбіжності в регулюванні, етичну амбівалентність у світі анонімних технологій та фундаментальну людську вразливість перед обіцянками швидкого багатства. Історія про 713 мільйонів доларів, викрадених у приватних інвесторів у 2025 році, — це лише один розділ у тривалій історії напруженої взаємодії між інноваціями та злочинністю. Майбутнє цієї взаємодії залежатиме не лише від технологій, але й від здатності суспільства виробити нові форми колективної відповідальності, освіти та правової адаптації в епоху цифрових активів, де кожен може бути одночасно і банкіром, і мішенню.

Ваша думка важлива!

1. Наскільки готова правоохоронна система України до переходу від переважно кількісних показників ефективності до моделі, заснованої на даних, аналітиці та цифрових інструментах, і які інституційні запобіжники мають супроводжувати таку трансформацію для захисту прав людини?
2. Як знайти баланс між "регуляторною чистотою" транзакцій у мережах Ethereum чи Solana та збереженням швидкості B2B-розрахунків, враховуючи, що вимоги Travel Rule стають дедалі складнішими для DeFi-сектору?
3. Чи не призведе жорстка стандартизація компетентності персоналу за MiCA до витіснення малих та інноваційних криптопровайдерів з ринку, і як Україна може знайти баланс між захистом інвестора, розвитком фінтеху та доступом до ринку ЄС?
4. Чи здатні традиційні інструменти ПВК/ФТ (аналіз транзакцій та STR) протидіяти системі, де злочинні доходи інтегровані в легальні логістичні ланцюги через прекурсори подвійного призначення, і які нові індикатори "індустріального" наркотрафіку ми маємо впроваджувати вже сьогодні?
5. Чи відповідає українська система фінансового моніторингу та правоохоронної аналітики викликам глобалізованих синтетичних ринків? З огляду на розвиток тіньових платіжних систем, криптовалют, неформальних транснаціональних фінансових мереж — чи достатньо Україна фокусується не лише на речовинах і фізичних поставках, а й на фінансових та сервісних компонентах нарко-економіки?
6. Як фахівці з AML можуть ефективно ідентифікувати платежі за контрабанду дикої природи, якщо вона маскується під легальні онлайн-покупки або пересилку насіння через зашифровані чати?

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-2026-06

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].