Методологічний бюлетень

Серійний номер: МінФін-AML-2025-13

Березень 2025

“Ми - це те, що ми робимо постійно”

Арістотель

Мета

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи 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.

Включає 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

Цифрова трансформація і стійкість платіжної системи Швеції: аналіз звіту ЦБ Швеції «Payments Report 2025»[1]

Звіт, оприлюднений ЦБ Швеції, є ґрунтовним аналітичним документом, присвяченим сучасному стану та викликам у платіжній системі Швеції. Основний наголос зроблено на оцінці безпеки, ефективності та доступності платежів у контексті цифровізації, посилення геополітичної напруги, трансформації споживчої поведінки, а також національної готовності до кризових ситуацій. Документ також включає рекомендації центрального банку до приватного сектора, уряду та парламенту щодо збереження функціональності та інклюзивності платіжної інфраструктури у мирний час і в умовах надзвичайних ситуацій.

Швеція є одним із глобальних лідерів у сфері цифрових платежів: частка готівкових операцій у країні становить лише близько 10%, а карти та мобільні додатки (Swish, Apple Pay, Samsung Pay) переважають як серед громадян, так і серед малого бізнесу. Використання готівки зменшується з року в рік, хоча спостерігалося тимчасове зростання попиту

[1] https://www.riksbank.se/globalassets/media/rapporter/betalningsrapport/2025/engelsk/payments-report-2025.pdf

у 2023 році як реакція на безпекову ситуацію в Європі після повномасштабного вторгнення Росії в Україну. У шведському суспільстві формується «де-факто» безготівкова економіка, що створює як переваги у зручності й швидкості транзакцій, так і ризики у разі технічних або енергетичних збоїв.

Звіт ґрунтується, зокрема, на репрезентативному опитуванні малого бізнесу, результати якого засвідчують, що більшість компаній надають перевагу картковим розрахункам завдяки їх простоті та мінімальному адміністративному навантаженню. Swish використовується як зручний інструмент для миттєвих платежів, особливо для невеликих сум. Разом з тим, значна частина підприємців висловлює занепокоєння тим, що оплата за допомогою карт може надходити із затримкою до трьох днів. Для 50% респондентів миттєве надходження коштів є критично важливим фактором.

Незважаючи на високий рівень цифровізації, система залишається вразливою до низки ризиків: кібератак, збоїв у електропостачанні, порушень телекомунікацій та зростання фінансового шахрайства. За перше півріччя 2024 року втрати від шахрайства з платіжними сервісами перевищили 1 мільярд SEK, причому особливу загрозу становлять авторизаційні шахрайства із застосуванням соціальної інженерії (переважно проти літніх людей). У зв'язку з цим ЦБ Швеції та наглядові органи рекомендують посилити моніторинг транзакцій, обмежити функціональність облікових записів для вразливих груп та підвищити відповідальність платіжних провайдерів за покриття втрат споживачів.

У частині стратегічного розвитку ЦБ Швеції наголошує на необхідності модернізації інфраструктури для пакетних платежів (зокрема Bankgirot), адаптації до міжнародних стандартів (ISO 20022), і впровадження нових послуг миттєвих платежів. Також Швеція має активізувати участь у трансєвропейських ініціативах, таких як TIPS (TARGET Instant Payment Settlement), що дозволяють обробку крос-валютних платежів у реальному часі.

Одним із головних пріоритетів звіту є забезпечення функціонування платежів у кризових умовах. ЦБ Швеції ставить за мету до 1 липня 2026 року забезпечити можливість офлайн-карткових платежів на термін до 7 днів для оплати критичних товарів (їжі, медикаментів, пального). Зараз лише близько 10% компаній здатні приймати такі платежі; серед підприємств життєзабезпечення ця частка трохи вища — 29%. Швеція у цьому контексті орієнтується на досвід Норвегії, Данії та країн Балтії, де вже впроваджено законодавчі або ринкові механізми для забезпечення офлайн-платежів.

Окрема увага приділяється проблематиці готівки. Зменшення її використання загрожує руйнуванням інфраструктури (банкнотомати, точки видачі/інкасації). У

Висновки:

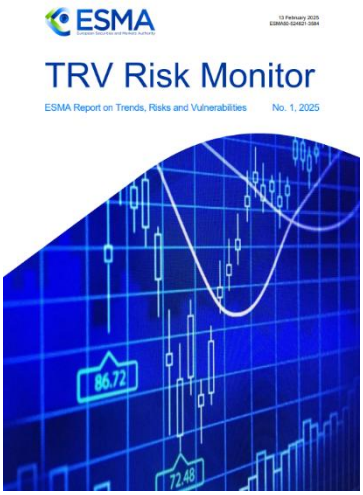
- **Необхідно посилити інфраструктуру для кризових ситуацій.** До липня 2026 року має бути реалізована можливість офлайн-карткових платежів до 7 днів для товарів першої необхідності. Платіжна інфраструктура має стати більш стійкою до тривалих перебоїв.
- **Розширення доступу до базових фінансових послуг.** Банки повинні впровадити рахунки з обмеженим функціоналом, зокрема для осіб без доступу до цифрових інструментів, що також сприятиме зменшенню ВК/ФТ.
- **Потрібна прозорість тарифів на платіжні послуги.** Близько 30% малого бізнесу не знає вартості обслуговування платежів. ЦБ Швеції пропонує уряду ініціювати перевірку та посилити прозорість для стимулювання конкуренції.
- **Підтримка готівки — елемент нацбезпеки.** Запровадження обов'язку приймати готівку для секторів життєзабезпечення, максимальних меж платежів готівкою та модернізація готівкової інфраструктури — необхідні дії для збереження стійкості.

звіті підтримується пропозиція «Готівкового розслідування» (Cash Inquiry) щодо запровадження обов'язкового приймання готівки у секторах життєво важливих товарів, а також встановлення максимального ліміту на розрахунки готівкою (приблизно 5 880 SEK у 2025 році). Це дозволить поєднати протидію відмиванню коштів з інклюзією для незахищених груп.

Ще однією стратегічною темою є взаємозв'язок між цифровим євро (в межах проєкту ЄЦБ) та можливим впровадженням шведської е-крони. Звіт фіксує, що цифровий євро, навіть у разі обмеженого розповсюдження в Швеції, може вплинути на конкуренцію, підвищити стійкість платіжної інфраструктури, а також актуалізувати потребу у запуску е-крони як засобу захисту грошового суверенітету.

Загалом, ЦБ Швеції виступає за системну трансформацію платіжного ринку, яка поєднує цифровізацію, безпеку, інклюзію та готовність до криз. Роль держави, згідно з логікою звіту, полягає не лише у регулюванні, а й у прямому забезпеченні ключових компонентів платіжної системи (готівка, інфраструктура, стандарти, доступність у надзвичайних умовах). Документ має не лише аналітичний характер, а й чітко спрямований на стимулювання публічної дискусії, залучення парламенту та уряду до розробки нормативно-правової бази, здатної забезпечити сталість функціонування системи платежів у будь-яких умовах.

Фінансова стабільність ЄС під тиском: аналіз ключових ризиків і вразливостей у другій половині 2024 року за даними звіту ESMA[2]



Звіт Європейського органу з цінних паперів та ринків (ESMA) є комплексним аналізом фінансової стабільності, вразливостей ринків капіталу та структурних тенденцій, які спостерігались у другій половині 2024 року. Основний меседж звіту полягає в тому, що незважаючи на відносну стійкість фінансових ринків ЄС, загальний рівень ризиків залишається високим або дуже високим. Цей стан зумовлений поєднанням макроекономічних, політичних, технологічних та структурних чинників, які мають як коротко-, так і середньостроковий вплив.

На тлі очікуваного пом'якшення монетарної політики основними центральними банками, ринки функціонували під впливом зростаючої геополітичної напруги (зокрема після виборів у Франції, краху коаліції в Німеччині та зміни адміністрації у США), зниження темпів зростання ВВП у ЄС та ознак глобального економічного фрагментування. Водночас спостерігалася дивергенція між ринками США та ЄС: американські фондові індекси стрімко зростали на очікуваннях дерегуляції, тоді як європейські ринки залишалися переважно стагнаційними. Цей дисбаланс виявився у значному розриві показників P/E, де ринки США досягли рівнів, характерних для стану перегріву, що викликає побоювання щодо переоцінки та ризиків корекції.

На ринку облігацій відзначено подальше звуження спредів, особливо в сегменті високоризикових паперів (high-yield), що є індикатором надмірної схильності інвесторів до ризику та можливої недооцінки кредитних вразливостей. У той же час, у корпоративному секторі спостерігалися певні покращення кредитної якості, зокрема у нефінансових компаній, а також зниження частки «fallen angels» (емітентів, що втратили інвестиційний рейтинг). Однак структурна вразливість у сфері комерційної нерухомості зберігається: ціни на об'єкти

[2] https://www.esma.europa.eu/sites/default/files/2025-02/ESMA50-524821-3584_TRV_1_2025.pdf

знижувались, тоді як вартість портфелів фондів переважно залишалась незмінною, що створює ризик нереалізованих збитків та потенційних масових викупів у разі погіршення умов.

Управління активами характеризувалось зростанням активів переважно за рахунок переоцінки, а не чистих грошових потоків. Особливу увагу викликає факт, що європейські інвестиційні фонди продовжують зміщувати портфелі в бік активів США, що у випадку корекції американського ринку може спровокувати транснаціональний ефект через канал портфельних втрат. Крім того, у структурі фондів зросла питома вага високоризикових активів, зокрема через збільшення фінансового важеля в альтернативних фондах та довший середній строк у портфелях HY-фондів. Окрему увагу ESMA приділяє RE-фондам, які стикаються з істотними ліквідними дисбалансами, особливо у країнах, де фонди мають щоденну ліквідність — як, наприклад, в Австрії, де середній дефіцит ліквідності за один тиждень становить 81% NAV. Ризики ліквідності посилюються через відсутність переоцінки портфелів відповідно до ринкових реалій.

Фінансові інновації, зокрема криптоактиви, у другій половині 2024 року показали стрімке зростання капіталізації — до рекордних 3.3 трлн EUR, що на 27% перевищує історичний пік 2021 року. Цей стрибок пов'язаний із політичними очікуваннями після виборів у США. Зростання охопило як традиційні активи (біткоїн, +30%), так і спекулятивні мем-коїни. У відповідь на це ESMA посилила публічні попередження про надмірну волатильність і спекулятивний характер криптоінструментів. Також було виявлено тісний зв'язок між активністю в соціальних мережах і динамікою цін на окремі інструменти, що створює ризики для некваліфікованих інвесторів, які орієнтуються на контент без належної перевірки.

У сегменті сталого фінансування зберігається невизначеність щодо політик «зеленого переходу», що послаблює апетит інвесторів до ESG-продуктів. Водночас ринок «зелених облігацій» у ЄС залишається активним, зростаючи переважно за рахунок нефінансових корпорацій. Утім, ESMA фіксує зростання скарг і випадків greenwashing, що підриває довіру інвесторів до сегменту.

Висновки:

- Необхідно посилити нагляд за фондами нерухомості, особливо з щоденною ліквідністю, через ризики ліквідності та нереалізованих збитків у разі масових викупів.
- Потрібно моніторити експозиції фінансових установ до ринків США, зокрема в секторі технологій, через високу ймовірність ринкової корекції.
- Необхідно зміцнити кіберстійкість фінансової інфраструктури, зокрема у провайдерів хмарних сервісів, враховуючи зростання гібридних кіберзагроз.
- Потрібно підвищити контроль за маркетингом високоризикових інструментів, зокрема через соціальні мережі, для зменшення шкоди непрофесійним інвесторам та запобігання маніпуляціям.

Споживачі демонструють змішану поведінку. З одного боку, зростає інтерес до облігацій та фондів облігацій як альтернативи депозитам. З іншого — фіксується зниження довіри до ринку, а також зростання кількості скарг (до 6 400 у 3 кварталі 2024 року), пов'язаних переважно з акціями, CFD та фондами. У фінансових послугах посилилися ризики, пов'язані з агресивним маркетингом високоризикових продуктів, впливом штучного інтелекту у клієнтських інтерфейсах та зростанням копі-трейдингу через соціальні мережі. Загрози для інвесторів посилюються через недостатній рівень фінансової обізнаності.

У сфері інфраструктури та ринкових послуг ключовим викликом залишаються кіберризики, зокрема у світлі зростаючої геополітичної напруги. Попри відсутність інцидентів із системним ефектом, випадки,

як-от збій CrowdStrike, підсвітили вразливість фінансових систем до порушень в IT-ланцюгах. Також актуальними залишаються ризики, пов'язані з маржинальними коливаннями, збої в клірингу та надмірна залежність від хмарних сервісів.

Загалом, ESMA підкреслює збереження високого рівня системного ризику та необхідність пильного моніторингу впливу політичних подій, макроекономічної фрагментації, структурних вразливостей у секторах нерухомості, інноваційних фінансових продуктів і кібербезпеки. Регулятори та учасники ринку мають адаптувати свої підходи до управління ризиками з урахуванням вищої чутливості ринків до зовнішніх шоків та взаємозалежності глобальних фінансових систем.

Кіберзагрози для фінансового сектору ЄС: аналітичний огляд ENISA за 2023–2024 роки[3]

Аналітичний звіт є першим цільовим дослідженням Європейського агентства з кібербезпеки (ENISA), яке охоплює стан кіберзагроз у фінансовому секторі ЄС і сусідніх країн (зокрема, Україна, Велика Британія, Швейцарія, Норвегія тощо). Звіт охоплює період із січня 2023 по червень 2024 року і містить глибокий аналіз 488 публічно задокументованих кіберінцидентів, які сталися у фінансовій сфері. Увага зосереджена на кредитних установах, платіжних і електронних грошових організаціях, інвестиційних компаніях, криптоактивних провайдерах, страховиках, органах державної влади, які надають фінансові послуги, а також цифрових постачальниках послуг та інфраструктури.

Основу методології дослідження ENISA становить поєднання OSINT-джерел (відкритої інформації) та системи обов'язкового звітування про інциденти згідно з Директивою NIS2 та Регламентом DORA. Важливим аналітичним інструментом є розмежування інцидентів за типами загроз, наслідками, активами, що постраждали, категоріями цілей та профілями суб'єктів, що здійснюють кібератаки. Також дослідження враховує як технічні аспекти атак, так і ширший контекст – геополітичні фактори, економічні тенденції, поведінку користувачів і прогалини у системах захисту.

Фінансовий сектор став ціллю значної частки зібраних інцидентів – 46% усіх атак були спрямовані проти банківських установ, 13% – на публічні фінансові організації, ще 10% – на індивідуальних клієнтів. Кількість інцидентів поступово зростала у другій половині 2023 року та першій половині 2024 року, зокрема через хвилі DDoS-атак, пов'язаних із підтримкою України, війною на Близькому Сході та іншими політичними подіями. Характерною ознакою стало збільшення активності хактивістських угруповань, зокрема проросійських NoName057(16), Anonymous Russia, UserSec, а також інших геополітично вмотивованих груп, як-от Turk Hack Team або Anonymous Sudan.

Серед основних типів загроз визначено вісім ключових категорій: DDoS-атаки, загрози щодо витоку або зловживання даними (data-related threats), соціальна інженерія (особливо фішинг, смішинг, вішинг, BEC), кібершахрайство, ransomware, ураження шкідливим ПЗ (malware), атаки на ланцюги постачання та інші – включаючи збої IT-систем і помилки персоналу. Найчастіше

[3] https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

використовуваним вектором доступу були фішингові кампанії, що імітували відправників із банківських структур або державних фінансових установ. Особливо небезпечною стала тенденція до використання ШІ (наприклад, deepfake-відео, генерація персоналізованих фішингових повідомлень) для підвищення рівня достовірності атак. Значна частина атак була спрямована на мобільні банківські додатки, зокрема через банківські трояни (Anatsa, Medusa, Godfather, Hydra, Copybara, SpyNote тощо), які отримували контроль над пристроями клієнтів для крадіжки облікових даних і здійснення транзакцій.

Значний інтерес також викликали атаки на ланцюги постачання: у ряді випадків атаки на сторонніх постачальників послуг призводили до вторинного ураження фінансових установ, зокрема через крадіжку даних або поширення ransomware. Під удар потрапили цифрові сервіси, хмарні інфраструктури, платіжні шлюзи. Наприклад, атаки із використанням вразливості MOVEit CVE-2023-34362 призвели до витоку даних кількох великих банків, включно з Deutsche Bank, ING та іншими.

Оцінюючи вплив інцидентів, ENISA зазначає, що найчастіше уражались IT-інфраструктура (31%), операційні дані (28%), персональні дані (25%) і корпоративна інформація (15%). Основними наслідками інцидентів були: фінансові втрати, порушення ділових процесів, викриття конфіденційної інформації, шкода репутації та накладення регуляторних санкцій. Особливу увагу ENISA звертає на той факт, що значна частка серйозних інцидентів, офіційно поданих згідно з вимогами NIS2, мали немалварне походження — причиною ставали збої систем або помилки користувачів (разом 73% офіційно зафіксованих інцидентів із серйозним впливом).

У розділі про учасників загроз проведено системну типологізацію: учасники з державним зв'язком (APT-групи), кіберзлочинні групи, хактивісти, інсайдери та невстановлені суб'єкти. Державні учасники, такі як Lazarus Group або APT29, часто здійснювали шпигунство, крадіжки криптоактивів, використовуючи zero-day вразливості або атаки на постачальників. Кіберзлочинні групи застосовували шантаж, ransomware, підміни вебсайтів, використання ботнетів і соціальну інженерію для фінансової вигоди. Зокрема, група TA505 використовувала Cl0p ransomware, а Akira – новий ransomware як сервіс (RaaS), що спеціалізувався на атаках проти малого і середнього бізнесу. Деякі кампанії, на кшталт Operation Magalenha, були спеціально націлені на банки в окремих країнах (наприклад, Португалії).

У заключному розділі звіту ENISA наголошує на потребі системного посилення кіберстійкості у фінансовому секторі. Зокрема, це включає впровадження регулярних навчань персоналу, побудову ефективних механізмів інцидент-менеджменту, посилення вимог до постачальників, відповідність до вимог DORA, GDPR, NIS2, розвиток механізмів обміну інформацією між фінансовими організаціями та органами влади. Особливо

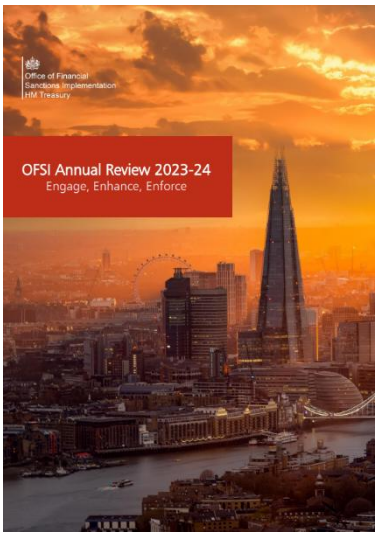
Висновки:

- **Фішинг, смішинг і BEC-атаки стали найчастішими векторами злому.** Рекомендація: впроваджувати багаторівневу автентифікацію (MFA), навчання персоналу та клієнтів, аналітику ШІ для виявлення соціальної інженерії.
- **DDoS-атаки, переважно з боку хактивістів, були координованими та геополітично вмотивованими.** Рекомендація: інвестувати в DDoS-мітинг-сервіси, системи швидкого реагування та співпрацювати з CERT-EU.
- **Ланцюги постачання — критично вразливе місце.** Рекомендація: забезпечити аудит постачальників, включно з хмарними і API-сервісами; впровадити вимоги до безпеки контрактів.
- **Інциденти з втратами даних призводять до регуляторних штрафів і репутаційної шкоди.** Рекомендація: переглянути політики резервного копіювання, контроль доступу до даних, шифрування PII та оцінку впливу (DPIA).

важливо в умовах ескалації геополітичних загроз вживати заходів щодо превентивного виявлення атак, моделювання сценаріїв кризових ситуацій і реагування на інциденти у транскордонному вимірі.

Звіт демонструє високий рівень систематизації загроз, притаманних фінансовому сектору, та дає чіткі вказівки на найбільш вразливі точки в екосистемі цифрових фінансів, актуальні не лише для країн ЄС, але й для фінансових розвідок сусідніх країн, зокрема України.

Річний огляд діяльності Управління з імплементації фінансових санкцій Великобританії (OFSI) за 2023–24 фінансовий рік[4]



Річний огляд є стратегічним звітом, що відображає суттєве посилення спроможностей Великобританії у впровадженні, моніторингу та примусовому забезпеченні дотримання фінансових санкцій. Документ охоплює ключові аспекти діяльності OFSI в межах трьох основних пріоритетів: взаємодія (Engage), вдосконалення (Enhance) та правозастосування (Enforce).

У контексті триваючої збройної агресії Росії проти України та глобальних загроз економічній і національній безпеці, OFSI значно розширило свою діяльність. Зокрема, було здійснено понад 100 національних заходів із представниками бізнесу, 245 міжнародних зустрічей, а також надано технічну допомогу з питань санкцій шістьом країнам. Особливу увагу приділено просуванню принципів дотримання санкцій шляхом публікації роз'яснень, попереджень та рекомендацій у рамках системи е-сповіщень (161 повідомлення) і тематичних червоних прапорців, зокрема щодо обходу санкцій.

Суттєвим досягненням став запуск програми санкцій у межах урядової ініціативи Economic Deterrence Initiative (EDI), що дозволила профінансувати модернізацію внутрішніх процесів, зокрема аналітики, розслідування криптовалютної діяльності, обробки ліцензійних заявок та збільшення штату. Загальна чисельність персоналу OFSI зросла до 135 осіб, із чотириразовим розширенням команд з ліцензування та правозастосування.

OFSI опрацювало рекордну кількість санкційних випадків: 396 нових справ, з яких 242 були закриті, що втричі більше за результат попереднього періоду. Водночас, OFSI запровадило першу грошову санкцію у справі, пов'язаній із російськими санкціями — проти Integral Concierge Services Ltd. Також уперше скористалося правом публічного розголошення порушень без накладання штрафу — у справі Wise Payments Ltd, що стало сигналом до зміни підходів до правозастосування.

Ще одним показником посилення санкційної діяльності стало додавання до Консолідованого списку санкцій 564 нових осіб, внаслідок чого загальна кількість становить 4 331 позицію (зокрема, 2 001 пов'язаних із Росією). Значний обсяг ліцензійної роботи (процес розгляду та надання дозволів (ліцензій) на здійснення певних транзакцій або фінансових операцій, які в інших умовах були б заборонені внаслідок застосування фінансових санкцій) також демонструє ефективність OFSI — за рік було прийнято 1 401 рішення, порівняно з 503 у попередньому періоді. Застосування загальних дозволів, удосконалення процесів (впровадження механізму

[4] https://assets.publishing.service.gov.uk/media/67dc3abcc5528de3aa671215/OFSI_Annual_Review_2023-24.pdf?utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery

Висновки:

- **OFSI зміцнило свою правозастосовчу спроможність** — у 2023–24 рр. проведено рекордну кількість розслідувань (396), із триразовим зростанням кількості закритих справ; OFSI вперше застосувало грошове стягнення за порушення російських санкцій та механізм публічного розголошення без накладення штрафу.
- **Потужне посилення інституційного потенціалу** — завдяки EDI та бюджетному зростанню, OFSI у 4 рази збільшило команди з ліцензування та правозастосування, запровадило сучасні інструменти аналізу для розслідування криптовалют, а також нові формати взаємодії з бізнесом.
- **Підхід до ліцензування став ефективнішим і прозорішим** — кількість оброблених справ зросла майже втричі (1 401 проти 503), оптимізовано процедури завдяки “Return Without Action” та розширено застосування загальних ліцензій для уникнення дублювання або надмірного регулювання.
- **Посилено міжнародну координацію та профілактику обходу санкцій** — OFSI відіграє ключову роль у впровадженні санкцій, розробляє спільні рекомендації з партнерами G7+ і США, та проводить навчання і надає технічну допомогу іншим державам, зміцнюючи глобальну архітектуру санкційної відповідальності.

Return Without Action) та оновлення Делегаційної схеми дозволили оперативніше розглядати заяви.

На геополітичному рівні OFSI активно співпрацює з міжнародними партнерами, насамперед OFAC (США), ЄС, країнами G7+, а також з британськими заморськими територіями для забезпечення узгодженості та ефективності санкцій. У лютому 2024 року було опубліковано спільне попередження коаліції OPC щодо обмежень на російську нафту.

Фінальний розділ документа окреслює зобов’язання OFSI перед бізнесом, спрямовані на забезпечення прозорості, передбачуваності й підтримки дотримання санкцій. Прогнозовані публікації на 2024–25 рік включають запуск блоку Частих Запитань (FAQs), публікацію Звітів з оцінки загроз, оновлення галузевих інструкцій та подальше посилення регуляторного середовища через нові поправки до законодавства.

Ринок наркотиків ЄС: MDMA — поглиблений аналіз[5]

Документ є результатом спільної аналітичної роботи Європейського агентства з питань наркотиків (EUDA) та Європолу, і пропонує глибоку оцінку європейського ринку MDMA — синтетичного психоактивного наркотику, відомого як екстазі. У фокусі аналізу — весь життєвий цикл MDMA: виробництво, торгівля, роздрібний продаж, споживання, ризики для здоров’я і навколишнього середовища, а також рекомендації щодо протидії. Документ підкреслює, що попри відносно невелику вартість порівняно з кокаїном чи канабісом, MDMA є високоприбутковим товаром для організованих злочинних мереж, із щорічним обігом у ЄС на рівні мінімум 594 млн євро.

[5] https://www.euda.europa.eu/publications/eu-drug-markets/mdma_en

Ключовими центрами виробництва залишаються Нідерланди та Бельгія, які відіграють домінантну роль як у внутрішньоєвропейському, так і глобальному ланцюгу поставок. Європейське виробництво вражає масштабами, технічним рівнем, а також адаптивністю до тиску правоохоронців — зокрема, злочинні мережі дедалі частіше використовують дизайнерські прекурсори та змінюють методи синтезу, що ускладнює виявлення та регулювання. При цьому, велика кількість лабораторій функціонує в промислових масштабах із залученням досвідчених виробників і спеціального обладнання, часто придбаного з Китаю.

ЄС також є головним світовим постачальником MDMA у такі регіони, як Океанія, Азія та Латинська Америка. У звіті детально описано нові форми торгівлі, зокрема використання поштових сервісів і darknet-маркетів, а також тенденції до бартерних угод (наприклад, обмін MDMA на кокаїн із латиноамериканськими партнерами). Водночас, окремі країни-члени ЄС, як-от Німеччина та Болгарія, стають новими розподільчими хабами.

Роздрібний ринок у Європі характеризується переважним споживанням MDMA в таблетках, хоча набирають популярності і кристалічна форма, і нові продукти, як-от їстівні цукерки з MDMA. Залишається значною проблема високодозованих таблеток, які становлять загрозу для здоров'я споживачів — зокрема, через ризики гострої токсичності. Попри деяке зниження концентрації MDMA в таблетках з пікових рівнів 2010-х років, ринок зберігає небезпеку у зв'язку з непередбачуваним вмістом, включно зі змішаними продуктами (наприклад, tucibi — MDMA з кетаміном).

Важливу увагу приділено не лише кримінальним, але й екологічним та громадським аспектам: зокрема, очищення відходів після синтезу MDMA пов'язане з серйозними витратами та забрудненням, а незаконне скидання відходів є поширеною проблемою в Нідерландах. Прогресивною є також частина звіту про потенціал використання MDMA в медичних цілях (наприклад, терапія ПТСР), проте на 2024 рік жоден з європейських регуляторів не схвалив його терапевтичне застосування.

У розділі з рекомендаціями підкреслено необхідність:

1. Посилення контролю за прекурсорами. Для зменшення обсягів виробництва MDMA критично важливо розширити нормативно-правове регулювання на так звані дизайнерські прекурсори — хімічні сполуки, подібні до PMK (піперонілметилкетон - хімічна речовина, яка є ключовим прекурсором у нелегальному синтезі MDMA (екстазі), які не мають легітимного використання, але масово імпортуються до ЄС і використовуються у нелегальному синтезі. Запровадження обов'язкового електронного обліку прекурсорів на всіх етапах постачання — від виробництва та імпорту до реалізації та кінцевого споживання — дозволить органам влади забезпечити системний моніторинг їх обігу. Компанії, що займаються хімічною продукцією, мають бути зобов'язані повідомляти про підозрілі замовлення, особливо ті, що включають високотехнологічне обладнання або реактиви подвійного призначення. Паралельно необхідно посилити митний контроль, орієнтуючись на ризик-профілі постачальників з Китаю, який є основним джерелом таких речовин, і виявляти спроби їх переміщення шляхом обходу митного декларування під іншими кодами.
2. Удосконалення транскордонного обміну інформацією. Ефективне реагування на глобалізовані ланцюги постачання MDMA передбачає розширення обміну інформацією між правоохоронними, аналітичними, митними та регуляторними органами. Ключовим завданням є інтеграція профілів ризику, даних про виробників, трейдерів прекурсорів, виробничі лабораторії та канали транспортування до спільних баз даних — таких як SIENA або платформи EMPACT. Варто забезпечити зворотний зв'язок між країнами-членами ЄС щодо підозрілих операцій у режимі реального часу, використовуючи

можливості Європейського ордера на здобуття доказів та інші механізми судово-слідчої взаємодії. Доцільним є проведення спільних транскордонних операцій із виявлення лабораторій, затримання ключових фігурантів та перекриття маршрутів надходження прекурсорів, у тому числі тих, що здійснюються у форматі бартеру з латиноамериканськими наркоорганізаціями.

3. **Інвестицій у новітні технології з виявлення лабораторій.** Зважаючи на промисловий масштаб виробництва MDMA, державам необхідно інвестувати в сучасні інструменти виявлення підпільних лабораторій. Зокрема, доцільним є використання тепловізійного моніторингу, безпілотних літальних апаратів і супутникової зйомки для ідентифікації об'єктів з аномальним енергоспоживанням або тепловиділенням, характерним для хімічних реакцій. Крім того, слід впроваджувати системи моніторингу відходів та забруднення ґрунту й повітря, які можуть вказувати на скидання токсичних речовин після завершення синтезу. Розробка та застосування аналітичних моделей виявлення підозрілих закупівель обладнання та хімікатів на основі аналізу торгових і митних даних дозволить заздалегідь встановлювати ризики. В окремих випадках доцільно застосовувати сенсори та інтернет речей (IoT) для моніторингу покинутих приміщень і складів у сільських або промислових зонах, які часто використовуються для розміщення лабораторій.
4. **Розширення профілактики та програм зниження шкоди.** З огляду на високу токсичність екстазі з підвищеним вмістом MDMA, особливо у змішаних продуктах типу tucibi, важливо забезпечити доступ до інструментів зниження шкоди, зокрема сервісів попередньої перевірки вмісту таблеток (drug-checking), які можуть діяти при нічних клубах, фестивалях або аптеках. Такі сервіси мають не лише зменшувати шкоду для споживачів, а й слугувати джерелом оперативної аналітичної інформації для виявлення нових речовин на ринку. Масштабні інформаційні кампанії у соціальних мережах, орієнтовані на молодь, мають пояснювати ризики вживання сильнодіючих або фальсифікованих форм MDMA. Медичні служби повинні мати алгоритми реагування на випадки гострої токсичності, а працівники розважальних закладів — пройти базову підготовку з надання допомоги. Додатково, мобільні додатки з функцією тривожного повідомлення або базою перевірених зразків можуть стати дієвим інструментом інформування.

Висновки:

- **Нідерланди та Бельгія залишаються головними центрами промислового виробництва MDMA**, із дедалі більш складною технологією синтезу та використанням дизайнерських прекурсорів, що ускладнює правоохоронну протидію.
- **ЄС виступає глобальним постачальником MDMA**, з підтвердженими маршрутами в Океанію, Азію та Латинську Америку, а також зростанням ролі поштових сервісів, darknet-платформ і появою нових розподільчих хабів, таких як Німеччина.
- **Проблема продуктів із високим вмістом MDMA та змішаних продуктів (наприклад, tucibi) зберігає актуальність**, збільшуючи ризики гострої токсичності, включно з летальними випадками — це вимагає посилення попереджувальних заходів і доступу до drug-checking сервісів.
- **Регуляторна та правоохоронна відповідь повинна включати контроль прекурсорів, цифрову аналітику, онлайн-моніторинг і міжнародну співпрацю**, а також супроводжуватися заходами громадського здоров'я, включно з профілактикою і лікуванням.

5. **Цільового навчання правоохоронців.** Комплексна протидія обігу MDMA неможлива без спеціалізованого підготовленого персоналу. Правоохоронці повинні бути навчені ідентифікувати лабораторне обладнання, типові схеми синтезу, а також особливості поводження з прекурсорами та відходами. Особливу увагу слід приділити підготовці до роботи в онлайн-середовищі: розслідування продажу через darknet, соціальні мережі та криптовалютні платформи, а також виявлення фіктивних онлайн-магазинів. Інспектори з охорони довкілля, слідчі, митники та аналітики повинні працювати як мультидисциплінарна команда, що забезпечить комплексне документування всього ланцюга виробництва та збуту. Упровадження стандартизованих посібників, чек-листів і тематичних тренінгів дозволить уніфікувати практики реагування у межах ЄС.

Звіт окреслює MDMA-ринок як приклад високодинамічного, технологічно просунутого, добре інтегрованого в глобальні злочинні мережі явища, що потребує скоординованої відповіді на рівні ЄС та за його межами.

Санкції

Контрабанда в небі: Як Росія рятує авіацію від санкцій [6]

Стаття, опублікована 5 березня 2025 року Радіо Вільна Європа/Радіо Свобода (RFE/RL), розкриває глибоку кризу в російській цивільній авіаційній індустрії, спричинену західними санкціями, запровадженими після початку повномасштабного вторгнення Росії в Україну в лютому 2022 року. Ці санкції перекрили доступ до сертифікованих деталей і обслуговування для літаків Boeing та Airbus, які складають дві третини комерційного авіафлоту Росії та забезпечують перевезення приблизно 90% пасажирів. У тексті детально описано, як російські авіакомпанії, опинившись у безвиході, змушені обирати між припиненням експлуатації літаків, ризикованою їхньою роботою без належного технічного догляду або контрабандою запчастин із США та Європи через треті країни, такі як Туреччина, Вірменія та Казахстан.

Автори наводять конкретний приклад боротьби з контрабандою: 13 лютого 2025 року Міністерство юстиції США заарештувало трьох осіб, пов'язаних із компанією Flighttime Enterprises, американською філією російського постачальника авіазапчастин, за незаконний експорт деталей на суму 2 мільйони доларів. Цей випадок став щонайменше п'ятим за останні три роки, коли США висунули звинувачення у подібних схемах. Експертка Лія Волкер із Берклі зазначає, що реальна кількість таких інцидентів може бути значно більшою через затримки в розслідуваннях, які іноді тривають до двох років, а також через труднощі зі співпрацею з посередницькими країнами. Вона підкреслює унікальність підходу Росії, яка, на відміну від Китаю, що вдається до кібершпигунства для отримання технологій, зосереджується на фізичній контрабанді невеликих партій деталей.

Санкції заборонили обслуговування та оновлення літаків західного виробництва, що призвело до серйозних технічних проблем. Наприклад, російські авіакомпанії не можуть проводити обов'язкові перевірки C Check (кожні 18–24 місяці) та D Check (кожні 6–12 років), які вимагають сертифікованих деталей і співпраці з виробниками, такими як Boeing чи Airbus. У результаті

[6] https://www.rferl.org/a/russia-flight-dangers-sanctions-war-aviation/33323526.html

літаки експлуатуються далеко за межами рекомендованих термінів, що спричиняє різке зростання аварійності. Зокрема, у період із 1 грудня 2024 року по 20 січня 2025 року зафіксовано 11 випадків відмови двигунів, з яких вісім стосувалися літаків Boeing або Airbus, а три — російських Sukhoi Superjet. Один із таких інцидентів стався в січні 2025 року, коли літак Ural Airlines Airbus A321 повернувся в аеропорт Єгипту через несправність двигуна незабаром після зльоту. Експерти прогнозують, що до кінця 2025 року більшість російських літаків вичерпають свій законний термін експлуатації, якщо ситуація не зміниться.

Стаття також висвітлює спроби Росії зменшити залежність від західних технологій. Після анексії Криму в 2014 році та загострення відносин із Заходом Москва інвестувала в розвиток власного авіапрому, зокрема в Sukhoi Superjet та перспективний МС-21. За планом 2022 року, до 2030 року Росія мала б виготовити 1036 літаків, включно з 270 МС-21, однак санкції та війна гальмують ці амбіції. Навіть Superjet, який частково виробляється в Росії, залежить від західних компонентів — двигунів, авіоніки, шасі. Без доступу до них ці літаки також приречені на поступове виведення з експлуатації, хоча й із затримкою приблизно на рік порівняно з іноземними моделями. МС-21, який мав стати альтернативою західним літакам, стикається з проблемами через відсутність власних двигунів і сучасних композитних матеріалів — за словами експертів, Росія відстає в цих технологіях на 40 років. Виробництво затримується, зокрема через переспрямування ресурсів на війну.

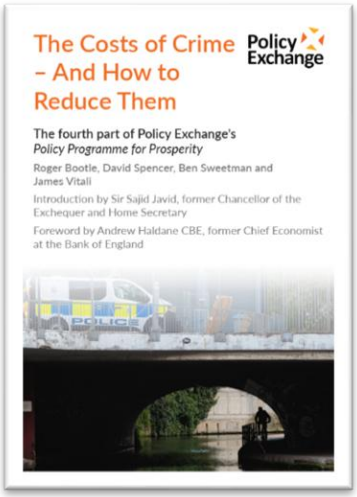
Як потенційне рішення Росія розглядає співпрацю з Китаєм, який розробляє власні авіаційні двигуни. Хоча китайський літак C919 наразі використовує західні двигуни і недоступний для Росії через санкції, Китай планує завершити створення власного двигуна до 2026 року. У разі успіху це може дати Росії шанс частково відновити авіаційну спроможність до 2029 року, однак експерти сумніваються в швидкому прогресі. Стаття завершується песимістичним прогнозом: без прориву в контрабанді, технологіях чи знятті санкцій російська авіація продовжить деградувати, наражаючи пасажирів на дедалі більші ризики, а пілотів — на перевантаження через скорочення флоту.

Висновки:

- **Посилення контролю за контрабандою через посередницькі країни:** Західним урядам варто зосередити увагу на країнах-посередниках (Туреччина, Вірменія, Казахстан), через які Росія отримує авіаційні деталі, та співпрацювати з місцевими органами для блокування таких каналів, враховуючи, що контрабанда є основним способом обходу санкцій.
- **Моніторинг безпеки польотів у Росії:** Міжнародним авіаційним організаціям, таким як ICAO, слід посилити нагляд за російськими авіакомпаніями, які експлуатують літаки без належного обслуговування, та розглянути заборону їхніх польотів у повітряному просторі країн-членів через зростання інцидентів (наприклад, 208 за 11 місяців 2024 року).
- **Прискорення тиску на технологічну залежність:** США та ЄС можуть посилити санкції на постачання авіоніки та двигунів, щоб унеможливити неофіційне обслуговування навіть російських літаків типу Superjet, змусивши Росію шукати менш надійні альтернативи, що пришвидшить деградацію її авіафлоту.
- **Оцінка довгострокового впливу співпраці з Китаєм:** Західним аналітикам варто відстежувати прогрес Китаю у створенні авіаційних двигунів (очікувано до 2026 року), оскільки їхнє постачання Росії може частково відновити її авіаційну спроможність до 2029 року, створюючи нові виклики для санкційного режиму.

Звіти окремих інституцій та експертів

Злочинність і економіка: Невидимий податок, що підриває добробут громадян [7]



Документ «The Costs of Crime – And How to Reduce Them», підготовлений аналітичним центром Policy Exchange, є комплексним дослідженням впливу злочинності на економіку та суспільство Великої Британії. У ньому аналізується сучасний стан злочинності, ефективність правоохоронних органів і кримінального правосуддя, а також розглядаються механізми стримування злочинності та заходи, які необхідно впровадити для зменшення її негативного впливу.

Основною тезою звіту є те, що безпека громадян є основним обов'язком держави, а високий рівень злочинності не тільки порушує громадський порядок, а й підриває основи економічного розвитку. Автори доводять, що реальний стан справ набагато гірший, ніж свідчить офіційна статистика. Хоча загальна кількість зареєстрованих злочинів демонструє спад з 1995 року, спостерігається стрімке зростання окремих категорій правопорушень, зокрема крадіжок, пограбувань, насильницьких злочинів та шахрайства. Поліцейські звіти свідчать, що рівень магазинних крадіжок зріс на 51% із 2015 року, а кількість збройних нападів і пограбувань збільшилася на 64% і 89% відповідно. Злочини, пов'язані з громадським порядком, зросли на 192%, що вказує на кризу в системі правопорядку. Особливо турбує тенденція до зростання шахрайства в системі соціальних виплат, де втрати держави збільшилися у вісім разів з 2006 року.

Окрім аналізу статистичних показників, у документі наголошується на глибоких структурних проблемах у системі кримінального правосуддя. Автори вказують, що рівень розкриття злочинів суттєво знизився – у 2015 році обвинувальні висновки були висунуті у 15,6% випадків, тоді як у 2021 році цей показник впав до 7,3%. Особливо низьким є рівень розкриття таких правопорушень, як крадіжки та пограбування, де лише 3,5% справ щодо зламу будинків та 4,1% справ щодо крадіжок доходять до суду. Дедалі частіше громадяни втрачають довіру до правоохоронних органів і навіть не повідомляють про правопорушення, оскільки вважають це марною справою.

Значну увагу приділено проблемам судової та пенітенціарної системи. Автори наголошують, що кількість нерозглянутих справ у коронних судах досягла рекордного рівня – понад 73 000 справ у 2024 році, з яких 30 000 очікують на розгляд понад шість місяців. Водночас британські в'язниці переповнені – понад 20 000 ув'язнених утримуються в умовах значного перенаселення. Внаслідок цього уряд був змушений вдатися до дострокового звільнення тисяч ув'язнених не тому, що вони виправилися, а через брак місць у пенітенціарних установах.

Окремий розділ дослідження присвячений оцінці економічних наслідків злочинності. Автори підрахували, що загальні витрати на злочинність у Великій Британії становлять приблизно £170 млрд на рік, що еквівалентно 6,5% ВВП. Витрати бізнесу оцінюються у £38 млрд, державного сектору – у £31 млрд, а втрати громадян – у £63 млрд. Однак ці цифри не враховують непрямі витрати, такі як зміна поведінки громадян та підприємств через страх перед злочинністю. Високий рівень правопорушень змушує людей витрачати більше на страхування, уникати певних районів, скорочувати інвестиції в роздрібну торгівлю, що в сукупності посилює економічні проблеми країни. З урахуванням цих чинників загальні витрати на злочинність можуть перевищувати £250 млрд, що становить близько 10% ВВП.

[7] https://policyexchange.org.uk/wp-content/uploads/The-Costs-of-Crime-%E2%80%93-And-How-to-Reduce-Them.pdf

Зважаючи на ці проблеми, автори пропонують комплекс заходів для зменшення рівня злочинності та підвищення ефективності кримінального правосуддя. Однією з ключових рекомендацій є розширення тюремної системи – пропонується будівництво 43 000 нових тюремних місць для усунення перенаселення та забезпечення можливості ув'язнювати небезпечних злочинців. Також необхідно переглянути підхід до поліцейської діяльності – уряд має збільшити фінансування правоохоронних органів, повернути на вулиці більше патрулів та переглянути систему підготовки поліцейських керівників.

Ще одна критична рекомендація стосується перегляду кримінальних вироків. Автори наголошують, що нинішня система є надто поблажливою – багато серйозних злочинців отримують надто м'які вироки або взагалі уникають покарання. Пропонується посилити відповідальність для «гіпер-продуктивних злочинців» – тих 9% рецидивістів, які вчиняють понад 50% усіх злочинів. Для таких осіб має бути запроваджено мінімальні строки ув'язнення не менше двох років та обов'язкові реабілітаційні програми у в'язницях.

Документ також закликає до активнішого використання сучасних технологій у боротьбі зі злочинністю. Автори пропонують створення спеціального фонду у розмірі £200 млн для розвитку технологій розпізнавання облич, інтелектуального аналізу злочинної поведінки та систем превентивного виявлення загроз. Крім того, судова система потребує негайного реформування – для прискорення розгляду справ необхідно залучити більше суддів та адвокатів, а також переглянути систему винесення вироків, щоб вона відповідала очікуванням суспільства.

На завершення автори стверджують, що боротьба зі злочинністю потребує як фінансових вкладень, так і політичної волі. Вони наголошують, що ці заходи можуть окупитися в довгостроковій перспективі, адже безпека громадян є фундаментом економічного зростання. Якщо держава не забезпечить ефективне правосуддя та належний рівень безпеки, суспільна довіра до уряду та державних інституцій буде й надалі знижуватися, що матиме негативні наслідки для всієї країни.

Висновки:

- **Злочинність є ключовим економічним тягарем для Великої Британії** – прямі та непрямі витрати сягають £250 млрд (10% ВВП), що перевищує витрати на NHS.
- **Проблеми у правоохоронній системі сприяють зростанню злочинності** – лише 7% злочинів доходять до суду, а поліція втратила ефективність через зменшення чисельності на 12%.
- **Зростання деяких видів злочинності є критичним** – крадіжки, шахрайство, злочини з використанням ножа та пограбування зросли на 50-90% за останнє десятиліття.
- **Необхідне жорсткіше покарання та системні реформи** – включаючи будівництво нових в'язниць, збільшення чисельності поліції та застосування технологій для запобігання злочинам.

Кількість муніципалітетів Гондурасу, де вирощують коку, досягла рекордної кількості[8]

Стаття від InSight Crime, опублікована 4 березня 2025 року автором Семом Вулстоном, є детальним аналізом безпрецедентного розширення культивації коки в Гондурасі протягом 2024 року, що свідчить про еволюцію від початкових експериментів до створення стабільних комерційних операцій із виробництва кокаїну. У 2024 році гондураські сили безпеки

[8] https://insightcrime.org/news/honduras-sees-record-number-municipalities-growing-coca/

повідомили про виявлення та знищення посівів коки в рекордних 16 муніципалітетах, порівняно з 9 у 2023 році, що є значним стрибком у географічному охопленні цієї діяльності. Кількість рейдів проти плантацій коки також різко зросла — з 29 у 2023 році до 81 у 2024 році, хоча загальна площа виявлених посівів дещо зменшилася до 461 гектара. Ці статистичні дані вказують на зміну стратегії наркотрафікантів: замість концентрації на великих плантаціях вони переходять до фрагментованої моделі, створюючи менші за розміром ділянки, розподілені по значно більшій кількості локацій. Однак автори статті наголошують, що виявлені посіви, ймовірно, є лише верхівкою айсберга, а реальний обсяг культивації коки в Гондурасі може бути набагато більшим, що ускладнює оцінку справжньої ситуації та розробку ефективних контрзаходів.

Основний обсяг вилучень коки припав на департаменти Колон, Оланчо та Атлантіда, які давно відомі як ключові вузли в маршрутах наркотрафіку через Центральну Америку. Ця тенденція не сповільнилася і на початку 2025 року: за перші шість тижнів нового року військові провели 11 рейдів, знищивши майже чверть мільйона кущів коки та виявивши 9 нарколабораторій, що вказує на стійке зростання активності в цій сфері. Культивація коки поступово охоплює нові регіони країни, зокрема департаменти Атлантіда, Йоро і Санта-Барбара, а також західні гірські райони поблизу кордону з Гватемалою, де природні умови — віддаленість і складний рельєф — значно ускладнюють роботу сил безпеки. Анонімний безпековий аналітик, якого цитує InSight Crime, підкреслює, що Гондурас суттєво поступається таким країнам, як Колумбія, у технічних і людських ресурсах для боротьби з культивацією коки. За його словами, величезна територія країни, переважно вкрита горами та джунглями, робить повний контроль над ситуацією практично недосяжним завданням без значного зовнішнього сприяння чи інвестицій у сучасні технології.

Історія культивації коки в Гондурасі почалася відносно недавно: перші посіви виявили у травні 2018 року в муніципалітеті Ескіпулас-дель-Норте в департаменті Оланчо. Тоді силовики знищили чотири гектари плантацій і помітили, що рослини були генетично модифіковані для адаптації до місцевих кліматичних умов, що викликало занепокоєння щодо можливого перетворення Гондурасу на нового гравця у виробництві кокаїну. Відтоді кока стрімко поширилася по всій країні, хоча представники сил безпеки довгий час применшували її значення, називаючи ці спроби експериментальними та стверджуючи, що місцева кока поступається за якістю і врожайністю традиційним південноамериканським сортам. За даними урядових джерел, один гектар коки в Гондурасі виробляє в середньому 2550 кг сухого листя на рік, що значно нижче за колумбійський показник у 6400 кг на гектар, оприлюднений Управлінням ООН з наркотиків і злочинності (UNODC). Проте дослідження 2024 року, опубліковане в журналі Environmental Research Letters, змінило уявлення про потенціал регіону: вчені дійшли висновку, що до 47% території північного Центральної Америки, включно з Гондурасом, мають сприятливі умови для вирощування коки. Більше того, близькість до основного споживчого ринку — Сполучених Штатів — робить цей бізнес фінансово привабливим для наркотрафікантів, скорочуючи логістичні витрати та час транспортування.

У департаментах Колон і Оланчо, де культивація коки зародилася, спроби силовиків придушити її не лише не дали бажаного результату, а й спровокували її поширення на нові території, віддаленіші від зони їхнього впливу. Незважаючи на це, ці два регіони залишаються головними осередками виробництва, на які припадає близько двох третин усіх вилучень коки у 2024 році. Обидва департаменти є переважно сільськими, розташовані вздовж ключового коридору

наркотрафіку і мають найвищі показники вбивств у країні, що створює ідеальні умови для діяльності кримінальних груп. Одним із таких гравців є клан Монтес Бобадільля, який виріс із колумбійського Калі Картелю і перетворився на одну з найвпливовіших наркотрафікантських організацій Гондурасу. Виробництво наркотиків у країні поки що залишається на початковому рівні: місцеві лабораторії, які називають "рустикальними", переробляють листя коки лише в пасту, а подальше виробництво кокаїну гідрохлориду відбувається в Гватемалі чи Мексиці. Тим не менш, у Гондурасі активно розвивається внутрішній ринок наркотиків, зокрема крек-кокаїну, що додає нового виміру до проблеми.

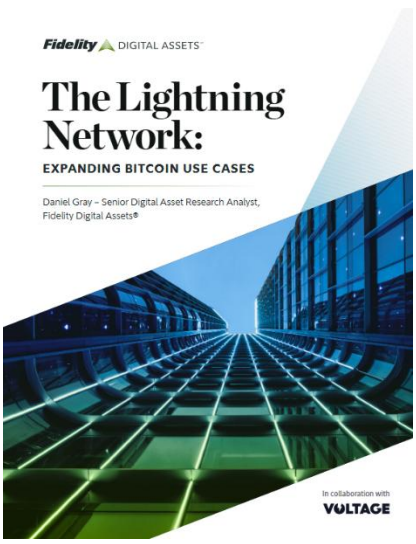
Економічний аспект внутрішнього ринку вражає: за підрахунками, кожен гектар коки може принести до 63 000 доларів США у вигляді креку на місцевих ринках, де один "камінь" коштує 50 лемпір, або приблизно 2 долари США. Споживання креку в Гондурасі стрімко зростає, про що свідчать як слова місцевих жителів, так і офіційна статистика: якщо у 2014 році вилучення креку обчислювалися грамами, то у 2023 році цей показник зріс до 4,3 кг. Громадський лідер із одного з міст розповів InSight Crime, що банди виготовляють крек навіть поблизу поліцейських дільниць, що вказує на слабкість правоохоронної системи та високий рівень корупції чи безсилля перед кримінальними структурами. Цей сплеск внутрішнього попиту супроводжується появою ознак того, що Гондурас поступово стає не лише транзитною зоною чи виробником сировини, а й повноцінним споживацьким ринком наркотиків, що посилює соціальні та безпекові проблеми в країні.

Роль Сполучених Штатів у боротьбі з цією кризою залишається обмеженою. Незважаючи на військову присутність у Гондурасі, американські інституції розглядають проблему коки як "локальну", не надаючи значної підтримки в її вирішенні. Анонімний аналітик зазначає, що США висувають численні вимоги до гондураського уряду, але їхня практична участь у боротьбі з культивацією залишається мінімальною, що ускладнює зусилля місцевих силовиків. Таким чином, Гондурас опиняється в унікальній ситуації: країна, яка тривалий час слугувала лише транзитним пунктом для наркотрафіку з Південної Америки до США, тепер активно трансформується у виробника і споживача кокаїну. Це явище, підкріплене слабкими інституціями, браком ресурсів і зростаючим впливом кримінальних груп, створює серйозний виклик для безпеки як у самому Гондурасі, так і в регіоні Центральної Америки загалом, вимагаючи негайних і скоординованих дій на національному та міжнародному рівнях.

Висновки:

- **Посилення моніторингу віддалених районів:** Уряд Гондурасу має інвестувати в розвідувальні технології (наприклад, дрони чи супутникові знімки) для виявлення коки у важкодоступних гірських регіонах, таких як кордон із Гватемалою, де культивація набирає обертів.
- **Міжнародна співпраця з США та Колумбією:** З огляду на обмежені ресурси Гондурасу, необхідно залучити технічну та фінансову підтримку США і досвід Колумбії для ефективного протистояння фрагментованій культивації коки.
- **Боротьба з внутрішнім ринком креку:** Сили безпеки повинні зосередити зусилля на ліквідації локальних мереж виробництва та збуту креку, особливо в Колоні та Оланчо, де зростає споживання, паралельно із соціальними програмами для зменшення попиту.
- **Удар по кримінальних групах:** Пріоритетним є розрив зв’язків між місцевими кланами (наприклад, Монтес Бобадільля) та міжнародними наркокарт Málaga, через арешти лідерів і конфіскацію активів, щоб зупинити комерціалізацію коки.

Lightning Network: Нова ера масштабованих та миттєвих біткоїн-платежів[9]



Документ, підготовлений Fidelity Digital Assets у співпраці з інфраструктурним провайдером Voltage, є глибоким аналітичним дослідженням сучасного стану, тенденцій розвитку та практичних застосувань мережі Lightning Network (LN) — платіжного рівня другого порядку на базі блокчейну Bitcoin. Мета дослідження полягає у висвітленні того, як Lightning Network еволюціонувала з експериментального рішення до стабільної, масштабованої, надшвидкої платіжної інфраструктури, здатної суттєво змінити ландшафт цифрових транзакцій.

У центрі уваги — аналіз ключових метрик LN: кількість вузлів і каналів, місткість каналів, швидкість обробки транзакцій, розмір комісій, коефіцієнт успішності платежів, а також їх динаміка в період 2020–2024 років. Особливістю цього дослідження є доступ до як відкритих, так і приватних (анонімізованих) даних від Voltage, що дозволяє оцінити ті аспекти роботи мережі, які зазвичай залишаються поза межами публічної статистики.

Звіт констатує, що Lightning Network продовжує демонструвати зростання за всіма ключовими напрямами. Зокрема, середня місткість каналів за останні 4 роки зросла на 214%, а загальна публічна місткість у біткоїнах збільшилася на 384%. Водночас кількість каналів на одного вузла знижується, що свідчить про консолідацію мережі: замість великої кількості дрібних вузлів формується інфраструктура з меншою кількістю, але більш потужних, добре зв’язаних вузлів, здатних обробляти велику кількість транзакцій із високою пропускною здатністю.

Особлива увага приділяється капітальній ефективності: великі канали з вищою ліквідністю забезпечують вищий рівень завершення транзакцій і дають змогу обробляти значні суми без потреби в залученні додаткових маршрутів (хопів). Саме кількість хопів визначає рівень плати за транзакцію та її швидкість: однохопові транзакції мають середню тривалість усього 0.38 секунд й майже 100% успішність, тоді як п’ятихопові — вже близько 5.66 секунд і помітно нижчий рівень успіху. Цей параметр є ключовим для практичного застосування мережі в умовах, де критичними є швидкість та надійність (наприклад, фінансові послуги, мікроплатежі, потокові платежі).

Фінансово Lightning Network виявляється однією з найефективніших платформ у цифровому просторі: при належній конфігурації каналів користувачі можуть здійснювати транзакції з комісіями менше 0.05%, а в деяких випадках — взагалі безкоштовно. Більше того, оператори вузлів можуть отримувати дохід, надаючи пропускну здатність для маршрутизації платежів, що відкриває перспективу створення некостодіального прибуткового середовища, у якому користувачі не передають контроль над своїм капіталом, але отримують дохід за його ефективне розміщення в мережі.

Звіт приділяє увагу також екосистемі сервісів, які вже використовують Lightning Network. Йдеться не лише про великі біржі (Kraken, Coinbase), які інтегрували LN у свої платіжні системи, а й про соціальні мережі (Nostr), стрімінгові платформи (Fountain), експериментальні проєкти (Fedimint, Cashu) і протоколи нового покоління (ARK), що додають нові шари масштабованості. Зокрема, ARK дозволяє використання віртуальних UTXO (vUTXO), що ще більше знижує вимоги

[9] https://fwc.widen.net/s/fxj6fgcwpq/fda_thelightningnetwork_expandingbitcoinusecases_1187503.1.0_v5

до ліквідності при збереженні швидкості транзакцій. Такі інновації розширюють функціональність LN, роблячи її універсальним платіжним рушієм.

У завершенні звіту представлено перспективну концепцію — поєднання Taproot Assets із Lightning Network. Це дає змогу вбудовувати токенізовані активи (у т.ч. стейблкоїни, NFT, цінні папери) у біткоїн-UTXO, з можливістю їх блискавичної передачі через LN. Таким чином, мережа може виступати не лише каналом для передачі BTC, але й універсальною інфраструктурою для обігу різноманітних цифрових активів у глобальному масштабі.

Документ також зазначає, що Lightning може бути не лише peer-to-peer рішенням, а й альтернативою міжбанківським платіжним системам (SWIFT, Fedwire). Потенціал використання LN як інструменту фінального клірингу між установами є суттєвим, з огляду на швидкість, відсутність посередників і можливість розрахунку в режимі реального часу.

Попри очевидні переваги, автори визнають, що перешкодою для масового впровадження Lightning Network може бути так звана «HODL»-ментальність — небажання користувачів витрачати біткоїн як актив, вартість якого очікувано зростає. Водночас інтеграція стейблкоїнів у LN може пом'якшити цей бар'єр, дозволяючи зберігати стабільність вартості та користуватись всіма перевагами протоколу.

У підсумку, Lightning Network позиціонується як фундаментальний інструмент для реалізації Bitcoin як дієздатної платіжної системи, з потенціалом революціонізувати як індивідуальні транзакції, так і інституційні розрахунки. Її еволюція може суттєво вплинути на загальну інвестиційну привабливість Bitcoin, перетворюючи його з переважно «store-of-value» активу на функціональний фінансовий інструмент глобального масштабу.

Висновки:

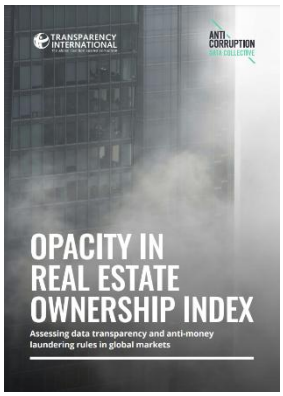
- Підприємствам і фінансовим установам варто розглядати інтеграцію Lightning Network для зменшення витрат на транзакції, прискорення розрахунків і покращення клієнтського досвіду. LN дозволяє досягати практично нульових комісій та субсекундної швидкості платежів.
- Інституціональні провайдери платіжної інфраструктури (банки, біржі, LSP) можуть отримати стратегічну перевагу, впроваджуючи LN для трансграничних розрахунків, обслуговування корпоративних клієнтів або стрімінгу зарплат у реальному часі.
- Для ефективного використання LN потрібна грамотна стратегія керування каналами: оптимізація хопів, правильне підключення до «якісних» вузлів та моніторинг маршрутизації дозволяють суттєво знизити комісії й підвищити надійність.
- Зростаюча роль Taproot Assets у поєднанні з Lightning Network відкриває шлях до токенізації реальних активів, у т.ч. стейблкоїнів, з можливістю їхнього миттєвого обігу без виходу за межі мережі Bitcoin. Це може радикально змінити ринок цифрових платежів.

Індекс непрозорості власності на нерухомість[10]

Цей аналітичний звіт презентує індекс непрозорості у сфері власності на нерухомість (OREO Index), що є першим глобальним інструментом оцінки прозорості даних про нерухомість та належності механізмів з ПВК у цьому секторі. Індекс охоплює 24 юрисдикції, включаючи країни G20 та ключові фінансові хаби (зокрема ОАЕ, Сінгапур, Панаму, Гонконг), оцінюючи їх за двома

[10] https://www.transparency.org/en/publications/opacity-in-real-estate-ownership-index-2025

опорними стовпами: (1) доступність та якість даних про нерухомість і (2) повнота національних режимів з ПВК, що стосуються ринку нерухомості.



Перший стовп індексу виявляє значні прогалини у сфері відкритих даних: хоча більшість країн веде реєстри юридичних власників, інформація про бенефіціарних власників у реєстрах відсутня або фрагментована. У багатьох випадках доступ до даних обмежений виключно державними органами або особами з «легітимним інтересом». Публічність реєстрів, машинозчитуваність даних, можливість масового завантаження або крос-посилання з іншими наборами (наприклад, реєстрами компаній) — у більшості країн або відсутні повністю, або реалізовані обмежено. Показово, що середній бал за відкритість даних становить лише 1,98 з 10, при цьому 9 країн отримали нуль балів за цим критерієм.

Другий стовп - виявляє, що хоча більшість країн накладає певні зобов'язання з ПВК на фахівців, залучених у транзакції з нерухомістю, реальне охоплення є фрагментарним. Особливо часто виключаються девелопери та юристи, навіть якщо вони безпосередньо продають або супроводжують продаж нерухомості. У ряді країн (наприклад, Австралії, Південній Кореї, Канаді, Панамі) юристи або зовсім не зобов'язані подавати повідомлення про підозрілі транзакції, або мають імунітет через захист конфіденційності клієнтів. Окрема проблема - відсутність вимог до ідентифікації бенефіціарних власників іноземних компаній, які набувають права на нерухомість: лише 11 з 24 країн мають такі зобов'язання.

Серед найбільш проблемних практик:

- можливість проведення транзакцій без участі жодного фахівця, зобов'язаного дотримуватись ПВК, що відкриває шлях для необмеженого відмивання коштів;
- грошові розрахунки у готівці, криптовалютах, золоті або інших неформальних засобах - зокрема в Австралії, росії та ряді інших країн;
- роздробленість наглядових органів, як-от у Німеччині (300 органів контролю), що ускладнює ефективний нагляд.

OREO Index демонструє, що навіть найбільш «відкриті» юрисдикції — як-от Франція, Англія та Уельс — мають критичні недоліки. Наприклад, у Великобританії інформація про власників компаній, які володіють нерухомістю через трасти, залишається закритою. А у Франції іноземні компанії не зобов'язані розкривати бенефіціарів. Загалом, ані FATF, ані G20 не розробили всеохопної нормативної рамки щодо прозорості у сфері нерухомості, що створює простір для зловживань.

У висновках автори закликають до:

- повної прозорості власності на нерухомість та обов'язкової реєстрації бенефіціарних власників;

Висновки:

- **Інформація про бенефіціарних власників нерухомості залишається недоступною або фрагментованою в більшості країн**, що дозволяє використовувати нерухомість для відмивання коштів та приховування активів.
- **Зобов'язання з ПВК не охоплюють ключові професії (девелопери, юристи, агенти)** у низці юрисдикцій, що створює системні прогалини в контролі за транзакціями з нерухомістю.
- **Міжнародні стандарти FATF та зобов'язання G20 поки не адаптовані до реального масштабу проблем у секторі нерухомості**, особливо щодо транскордонних транзакцій і використання трастових структур.
- **Відсутність відкритого, безоплатного та машинозчитуваного доступу до даних** про власність на нерухомість та транзакції перешкоджає розслідуванням і контролю з боку громадськості.

- ліцензування та здійснення регулювання у сфері ПВК щодо всіх фахівців, залучених у ринок нерухомості;
- централізації нагляду у руках незалежного державного органу;
- забезпечення безкоштовного, відкритого доступу до даних для громадськості, включаючи журналістів, громадські організації та іноземні правоохоронні органи.

ВНУП

Прозорість власності та офшорні інвестиції в нерухомість[11]

Цей документ є глибоким емпіричним дослідженням впливу запровадження публічного реєстру бенефіціарних власників нерухомості, що перебуває у власності офшорних компаній, на динаміку іноземних інвестицій у ринок нерухомості Великої Британії. Автори аналізують ефективність Economic Crime Act (ECA) 2022 року, ключовою частиною якого стало створення Register of Overseas Entities (ROE) — обов'язкового публічного реєстру для всіх зарубіжних компаній, що володіють нерухомістю у Великій Британії. Закон став реакцією на вторгнення Росії в Україну, але насправді є логічним завершенням тривалих дискусій про роль Британії як глобального хабу для відмивання коштів через ринок нерухомості, особливо в Лондоні, прозваному «Лондонградом».

У дослідженні застосовано метод різниці в різницях (difference-in-differences), що дозволяє ізольовано виміряти вплив реформи на покупки та продажі нерухомості через компанії, зареєстровані в юрисдикціях, які традиційно вважаються офшорними — зокрема, на підставі їхнього рівня прозорості, участі в міжнародних обмінах інформацією та даних із витоків (наприклад, Pandora Papers). Ключовий результат: нові покупки нерухомості через компанії з офшорів знизилися приблизно на 5,7 відсоткових пунктів, а в грошовому вираженні — на 4,8 млн фунтів стерлінгів на місяць на одну офшорну юрисдикцію, що становить загальне зниження на понад 5,6 млрд фунтів за весь досліджуваний період.

Ці ефекти є стійкими навіть після виключення юрисдикцій, які традиційно використовувались російськими інвесторами, що дозволяє авторам стверджувати: саме прозорість, а не лише санкції, стала ключовим чинником зниження попиту. При цьому жодних істотних змін у цінах на нерухомість або масштабних розпродажів не зафіксовано — що свідчить про ефективність антиуникальних положень закону. Водночас автори виявили, що значна частина компаній, які володіють нерухомістю, уникла реєстрації бенефіціарів, скориставшись легальними винятками: розподілом прав менше 25%, використанням номінальних директорів, трастових структур тощо. Це ставить під сумнів повноту дії реформи.

Дослідження особливо цінне тим, що автори провели груповий аналіз для різних "типів ризикових юрисдикцій": офшорів, які переважно використовуються росіянами, мешканцями країн з високим рівнем корупції, а також юрисдикцій, що перебувають у системі автоматичного обміну податковою інформацією (CRS). Для всіх трьох груп було зафіксовано істотне падіння інвестицій після вступу в дію ECA. Це дозволяє зробити висновки не лише про ефективність британської політики, а й про потенціал її адаптації в інших країнах.

Додатково автори оцінюють, наскільки закон вплинув на структуру ринку: зокрема, чи було заміщення офшорного інвестування через сумнівні британські компанії. Жодних ознак такого

[11] https://www.taxobservatory.eu//www-site/uploads/2025/03/The-End-of-Londongrad.pdf

заміщення не виявлено. Проте дослідження підкреслює, що для забезпечення справжньої прозорості необхідна ефективна валідація даних, чого наразі бракує у Companies House (урядова британська агенція, що здійснює реєстрацію компаній та веде їх реєстр). Незважаючи на формальну вимогу підтвердження особи бенефіціара, контроль за достовірністю залишається слабким. Частину проблем сподіваються вирішити за допомогою положень Economic Crime and Corporate Transparency Act 2023, які набули чинності у 2024 році.

На завершення автори підкреслюють, що британський досвід є одним із небагатьох прикладів застосування публічного реєстру в контексті нерухомості, що може бути джерелом навчання для інших країн. Однак навіть такий прогресивний підхід не гарантує повної прозорості без ретельного дизайну політики, правозастосування та врегулювання винятків.

Висновки:

- **Впровадження публічного реєстру бенефіціарних власників призвело до суттєвого скорочення нових покупок нерухомості через офшори**, зниження склало понад £5,6 млрд за два роки - це свідчить про ефективність прозорості як інструменту протидії відмиванню коштів.
- **Закон не викликав масового розпродажу активів**, ані з боку російських бенефіціарів, ані з боку інших офшорів, що свідчить про дієвість положень, що направлені на попередження ухилення від звітності (наприклад, вимога до розкриття інформації перед продажем).
- **Значна частина офшорних компаній змогла уникнути повного розкриття даних**, скориставшись законними винятками (дроблення володіння, трасти, номінальні особи) - це потребує подальшого посилення законодавства та валідаційних механізмів.
- **Британський підхід - приклад для інших країн, які прагнуть обмежити анонімне володіння нерухомістю**, але ефективність подібних реформ залежить не лише від прозорості, а й від якості нагляду, аналітичного супроводу та закриття законних «лазівок».

Нагляд за ВНУП і шлях до відповідності вимогам FATF[12]

Цей аналітичний матеріал присвячений одному з найбільш складних і системно проблемних напрямів у сфері протидії відмиванню коштів і фінансуванню тероризму — ефективному нагляду за визначеними нефінансовими установами та професіями (ВНУП). Документ розкриває, чому саме ця складова стала ахіллесовою п’ятою для багатьох країн у межах четвертого раунду взаємних оцінок FATF (зокрема в межах Безпосереднього Результату 3), і чому в рамках п’ятого раунду — з акцентом на змінений Безпосередній Результат 4 — вона трансформується у ще більш критичний напрям перевірки. Автори проводять глибокий розбір типових прогалин, підкріплений прикладами з практики та системним баченням шляхів виправлення ситуації.

Основна теза полягає в тому, що країни не провалюють оцінку FATF через відсутність законів — вони провалюють її через відсутність ефективного впровадження нагляду. Проблеми носять багатофакторний характер. Однією з ключових є недиференційований підхід до ВНУП, коли до всіх професій (казино, юристи, ріелтори, арт-дилери тощо) застосовують однакові моделі ризику і нагляду, попри їхню об’єктивну відмінність. Другою проблемою є нестача ресурсів та експертизи — регулятори часто мають обмежений персонал, недостатню спеціалізацію в таких складних темах, як трасти, компанії-оболонки, оцінка мистецтва або складні міжнародні структури. Третій блок — недосконалість правової бази: неузгоджені або занадто вузькі визначення ВНУП, правові лазівки (наприклад, щодо короткострокової оренди нерухомості),

[12] https://sites.google.com/view/gemma372dnfbps?usp=sharing

або нечітко виписані обов'язки зі здійснення CDD та подання STR. Особливу увагу приділено професії юриста, де баланс між вимогами з ПВК та адвокатською таємницею часто перешкоджає ефективному виявленню підозрілих транзакцій.

Автори також звертають увагу на фрагментацію регуляторної системи — коли відповідальність за нагляд розподілена між декількома установами (ПФР, міністерства, реєстраційні органи), що ускладнює координацію, створює дублювання або навпаки — зони нерегульованої активності.

Висновки:

- **Ключовою проблемою сектору ВНУП є не відсутність нормативки, а неефективне впровадження нагляду**, зокрема — недиференційований підхід, нестача експертизи та відсутність ризик-орієнтованих пріоритетів.
- **Новий Безпосередній Результат 4 у п'ятому раунді FATF вимагає доведення впливу нагляду на зменшення ризиків ВК/ФТ**, а не просто наявності нормативних документів, що суттєво підвищує вимоги до якості нагляду.
- **Юридичні винятки, розмиті визначення та фрагментованість регулювання створюють системні зони ризику**, які дозволяють ВНУП уникати нагляду, і мають бути усунені через перегляд законодавства та централізацію функцій.
- **Країни мають впровадити трирівневу стратегію: зміцнити правову базу та ресурси, побудувати ефективну ризик-орієнтовану систему нагляду, і запровадити технологічні рішення та міжнародну кооперацію** — лише тоді можливо досягти відповідності новим критеріям FATF.

Перехід до Безпосереднього Результату 4 у межах п'ятого раунду означає не лише зміну нумерації, а й підвищення стандарту доказовості: країни повинні показати не лише наявність правил, але й те, що ці правила призвели до зменшення ризиків ВК/ФТ у секторах ВНУП.

Документ пропонує трирівневу дорожню карту підготовки до п'ятого раунду. На першому етапі (6–12 місяців) країни повинні оновити національну оцінку ризиків із акцентом на ВНУП, переглянути визначення суб'єктів, внести зміни до законодавства, визначити регуляторів та забезпечити їх кадрами і фінансами. На другому етапі (12–24 місяці) акцент робиться на побудові ризик-орієнтованої системи нагляду з чіткими методиками оцінки, інспекцій, дистанційного моніторингу, підвищенням вимог до CDD та якості STR. Також — на підвищенні аналітичної спроможності ПФР до обробки звітів. Третій етап (24+ місяців) передбачає впровадження SupTech-рішень (автоматизований моніторинг, аналітика, цифрова звітність), посилення міжнародної кооперації, регулярний перегляд підходів та вбудовані механізми вдосконалення. Завершується документ тезою, що відповідність FATF — не пункт призначення, а процес, який вимагає стратегічного управління, рішучості та інституційної пам'яті.

Рекомендовані матеріали

Марко Еббен: від європейського наркоторговця до солдата Сіналоаського картелю [13]

Стаття розкриває складний і насичений кримінальний шлях нідерландського наркоторговця Марко Еббена, який відігравав ключову роль у співпраці між європейськими злочинними угрупованнями та мексиканськими наркокартелями. Його історія не лише демонструє транснаціональну природу організованої злочинності, а й піднімає питання про інтеграцію

[13] https://insightcrime.org/news/life-death-sinaloa-cartel-dutch-emissary/

європейських злочинців у структури латиноамериканських картелів, еволюцію наркобізнесу та нові виклики для міжнародних правоохоронних органів.

Марко Еббен походив із сім'ї з давніми кримінальними зв'язками. Його батько, Генк Еббен, ще у 1990-х роках керував наркотрафіком до Великої Британії, але після арешту та ув'язнення намагався відновити свій вплив, залучивши до справи сина. У ранні роки Марко не мав власного капіталу для наркобізнесу, тому він і його батько пропонували знання та зв'язки в порту Роттердама іншим злочинцям, діючи за принципом "злочинність як послуга". Проте амбіції молодого Еббена виявилися значно ширшими. Він був безрозсудним, імпульсивним і прагнув швидких прибутків, що відрізняло його від батька, який діяв обережніше. Така поведінка швидко зробила Марко мішенню як для конкурентів, так і для правоохоронців.

У 2019 році через загрози життю поліція Нідерландів взяла його під охорону, але вже у 2020-му він був засуджений за контрабанду 400 кг кокаїну з Бразилії. Попри це, Еббену вдалося втекти, після чого він став одним із найбільш розшукуваних злочинців Європолу. Протягом наступних років він переховувався у Дубаї, Туреччині та Мексиці, неодноразово інсценуючи власну смерть. У 2023 році він пережив реальний замах і скористався цим, щоб сфабрикувати свою загибель, однак згодом знову з'явився на кримінальній арені.

Його зв'язки із Сіналоаським картелем стали одним із найбільш несподіваних аспектів його кар'єри. Спершу він лише допомагав налагоджувати трафік кокаїну через Роттердам, але згодом отримав статус довіреної особи угруповання Ісмаеля Самбада Гарсії, відомого як "Ель Майо". На відміну від традиційної схеми, коли європейські злочинці виступали лише як покупці латиноамериканських наркотиків, Еббен став частиною внутрішньої структури мексиканського картелю, а пізніше – учасником його збройних конфліктів. Восени 2024 року він опинився у центрі кривавої сутички між фракціями Сіналоаського картелю, після чого з'явилися перші повідомлення про його можливу смерть. Однак тоді вони так і не отримали підтвердження.

Його справжній кінець, якщо це дійсно так, настав у лютому 2025 року, коли його тіло було знайдено у паркінгу в місті Атізапан-де-Сарагоса, штат Мехіко. Він був убитий п'ятнадцятьма пострілами, що вказувало на типову розправу у кримінальному середовищі. Проте обставини його смерті викликали багато запитань: на місці знайшли підроблені документи DEA, а також з'ясувалося, що у грудні 2024 року Еббен зустрічався з агентами США. Це могло свідчити як про його потенційну співпрацю з правоохоронними органами, так і про чергову спробу організувати власне зникнення. Деякі експерти зазначають, що його характер робив можливим будь-який варіант розвитку подій – як реальне вбивство, так і ще одну інсценізацію смерті.

Окрім особистої історії Еббена, стаття також висвітлює загальні тенденції у світовій наркоторгівлі. Якщо раніше європейські злочинці були лише клієнтами мексиканських картелів, то сьогодні вони дедалі більше інтегруються у структури цих угруповань. Крім того, у Європі зафіксовано зростання виробництва метамфетаміну із залученням мексиканських "кухарів", які використовують нідерландську та іспанську інфраструктуру для виробництва наркотиків. Це вказує на те, що мексиканські картелі не просто експортують продукцію, а й активно розширюють свій вплив у Європі.

Врешті-решт, історія Марко Еббена піднімає питання про майбутнє організованої злочинності у світі. Чи стане його випадок прецедентом для інших європейських злочинців, які прагнуть інтегруватися у латиноамериканські картелі? Чи означає це, що насильство, притаманне

мексиканському кримінальному середовищу, невдовзі може поширитися і на Європу? Відповіді на ці питання поки що немає, але очевидно, що подібні випадки привертають дедалі більше уваги правоохоронних органів по всьому світу.

Інші новини

Глобальна криза торгівлі дітьми: виклики, технологічні загрози та шляхи подолання [14]

Доповідь, представлена Раді з прав людини ООН, висвітлює проблему значного зростання кількості дітей, які стають жертвами торгівлі людьми, підкреслюючи глобальні масштаби цього явища та його системний характер. Згідно з доповіддю доктора Наджат Маалла М'жід, спеціального представника Генерального секретаря ООН з питань насильства щодо дітей, сьогодні майже 40% від усіх ідентифікованих жертв торгівлі людьми – це діти, однак реальна кількість постраждалих може бути значно вищою. Основними причинами цього явища є соціально-економічні негаразди, зростання рівня бідності, нестача продовольства, гуманітарні кризи та збройні конфлікти, що змушують мільйони дітей залишати свої домівки та потрапляти у вразливі ситуації. Особливо високим є ризик для дівчат, які стають жертвами сексуальної експлуатації, примусового шлюбу, трудового рабства та залучення у злочинну діяльність.

Доповідь також звертає увагу на проблему безкарності злочинців, які експлуатують дітей. Засудження за торгівлю дітьми залишаються рідкісними, що пояснюється корупцією, страхом жертв перед репресіями, соціальною стигматизацією та недостатньою роботою правоохоронних органів. Злочинні мережі, що займаються торгівлею людьми, дедалі більше вдосконалюють свої методи, використовуючи новітні технології, зокрема штучний інтелект, для оптимізації своїх злочинних схем, зменшення ризиків викриття та зниження витрат на організацію незаконного бізнесу. У цьому контексті підкреслюється важливість міжнародної співпраці та впровадження сучасних технологій для боротьби з цим явищем, включаючи створення цифрових систем моніторингу та відстеження підозрілих дій у кіберпросторі.

Окремий розділ доповіді присвячений питанню дітей у зонах конфліктів. Представник ООН з питань дітей у збройних конфліктах Вірджинія Гамба заявила, що понад одна шоста всіх дітей у світі проживають у регіонах, охоплених війною, що значно підвищує їхню вразливість до вербування у збройні формування, примусової праці та сексуальної експлуатації. У зв'язку з цим державам рекомендується розробити спеціальні програми захисту дітей, які дозволять їм уникнути потрапляння в злочинні мережі та отримати належну допомогу в кризових ситуаціях.

Доповідь також містить аналіз сучасних загроз, пов'язаних із розвитком нейротехнологій. Спеціальний доповідач з питань права на приватність Ана Ноґререс попередила про небезпеку використання цих технологій для незаконного збору нейроданих, маніпуляції свідомістю людей та навіть потенційного "злому" мозку. Вона закликала держави розробити чіткі правові механізми регулювання використання нейротехнологій, щоб запобігти їх використанню в цілях контролю над поведінкою людини або її експлуатації. У доповіді наголошується, що без

[14] https://news.un.org/en/story/2025/03/1161061

належних запобіжних заходів подібні технології можуть становити серйозну загрозу правам людини, включаючи право на приватність, автономію та ментальну цілісність.

Для загального розвитку

Комплаєнс з ПВК для корпоративних постачальників послуг в ОАЕ[15]

Документ є системним і структурованим посібником, що розкриває всі ключові вимоги, які пред'являються до корпоративних постачальників послуг (CSPs) в Об'єднаних Арабських Еміратах у межах національного режиму протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Документ базується на чинному нормативно-правовому полі ОАЕ, а саме — на Федеральному законі №20 від 2018 року, Постанові №10 від 2019 року, а також Постанові №74 від 2020 року щодо реалізації санкційної політики відповідно до Резолюцій Ради Безпеки ООН. Крім того, згадується низка роз'яснень та методичних рекомендацій, виданих відповідними наглядовими органами (Міністерством економіки, FSRA, DFSA та Центральним банком ОАЕ).

CSP в ОАЕ офіційно віднесені до категорії визначених нефінансових установ і професій (ВНУП), отже, зобов'язані дотримуватись режиму ПВК/ФТ/ФР на рівні не нижчому, ніж фінансові установи. Автори посібника надають не лише регуляторні рамки, а й практичні алгоритми впровадження AML-програм у повсякденну операційну діяльність CSP.

Документ починається з визначення ролі CSP у системі ПВК/ФТ/ФР та вказує на їхню особливу вразливість до зловживань у контексті створення компаній, надання послуг номінальних директорів, використання адрес реєстрації, трастових відносин тощо. Оскільки CSP часто є першою точкою входу до корпоративної структури або банківської системи, ризики зловживання їх послугами в схемах ВК/ФТ — надзвичайно високі.

Одним із перших і базових обов'язків CSP є реєстрація в системі goAML, яка є офіційним електронним порталом подання звітності до фінансової розвідки ОАЕ (ПФР). Процедура передбачає попередню реєстрацію в SACM, надання ідентифікаційних документів та призначення відповідального працівника. Останній - центральна фігура системи AML-контролю в межах кожної компанії, відповідальна за реалізацію політик, моніторингу, звітність, навчання персоналу та взаємодію з регулятором.

Суттєве місце у документі займає опис процесу оцінки ризиків на рівні компанії (Enterprise-Wide Risk Assessment, EWRA). Усі CSP мають провести глибоку і структуровану оцінку власних вразливостей до ПВК/ФТ/ФР на основі таких параметрів, як клієнтська база, продукти/послуги, обсяги транзакцій, юрисдикції клієнтів тощо. Результатом є визначення залишкового ризику, співвіднесення з рівнем схильності компанії до ризику та розробка додаткових заходів контролю, де це потрібно.

Далі розкриваються вимоги до розробки політик, процедур і контролів ПВК/ФТ, які повинні відповідати результатам оцінки ризиків, бути гнучкими та враховувати актуальні зміни в законодавстві, типології злочинів, технологічні загрози. Йдеться не лише про документи, але й

[15] https://amluae.com/wp-content/uploads/2024/03/Corporate-Service-Provider-AML-Compliance-eBook.pdf

про внутрішні процеси, пов'язані з перевіркою клієнтів (KYC, CDD), ідентифікацією бенефіціарних власників, перевірками на наявність у санкційних списках (UN, національний список OAE, інші міжнародні реєстри), визначенням статусу PEP, а також наявності негативних згадок у ЗМІ.

Окремий блок стосується постійного моніторингу: інформація про клієнтів та транзакції повинна бути актуалізована та перевірена, особливо у випадках високого ризику. У разі виявлення нетипових або підозрілих операцій відповідальний працівник має ініціювати внутрішнє розслідування та ухвалити рішення про подання відповідного звіту (SAR/STR). Також описано процедури подання спеціалізованих звітів — Funds Freeze Report (FFR), Partial Name Match Report (PNMR), High-Risk Country Report тощо.

Висновки:

- **Реєстрація у goAML є юридичним обов'язком.** Нереєстрація загрожує штрафами до 5 млн AED. CSP повинні забезпечити своєчасну реєстрацію в системі ПФР з належним пакетом документів.
- **Ризик-орієнтований підхід є основою всіх AML-процедур.** CSP зобов'язані проводити повну оцінку ризиків EWRA, що охоплює типи клієнтів, географію, продукти, канали, контрольні заходи — і відповідно адаптувати свою AML-програму.
- **Програма TFS є критично важливою для відповідності** CSP зобов'язані використовувати офіційні списки санкцій (ООН, місцеві), перевіряти всі ідентифікатори клієнтів, подавати FFR або PNMR у випадку виявлення відповідностей.
- **Регулярне навчання персоналу та підтримка AML-культури — необхідність.** Всі працівники CSP мають бути навчені відповідно до своєї ролі. Важливо проводити тренінги, фіксувати участь, оновлювати програми з урахуванням нових ризиків та змін у законодавстві.

У рамках санкційного комплаєнсу документ містить конкретні інструкції щодо цільових фінансових санкцій (ЦФС): від підписки на сповіщення EOCN до дій у випадку виявлення повного чи часткового співпадіння з фігурантами санкційних списків.

Не менш важливою є увага до навчання персоналу — всі співробітники мають бути обізнані про свої обов'язки у сфері ПВК/ФТ. Програма навчання має бути системною, адаптованою до ризиків, містити первинне та оновлювальне навчання, а також фіксуватися в реєстрах.

Завершується документ описом вимог до ведення документації: всі AML-записи, включаючи KYC, звіти до ПФР, результати моніторингу, внутрішні розслідування, мають зберігатися щонайменше 5 років.

Загалом документ формує повне уявлення про те, як CSP в OAE мають будувати свою комплаєнс-функцію у сфері ПВК/ФТ, враховуючи не лише формальні вимоги, але й практичні підходи до їх імплементації. Він може слугувати типовою дорожньою картою для створення або вдосконалення AML-програми в будь-якій нефінансовій установі, зокрема й у національному контексті.

Ваша думка важлива!

1. Чи бачите Ви ризик, що масове скорочення готівки в економіці може створити нові вразливості до ВК/ФТ, особливо в умовах воєнного або техногенного ризику? Чи варто Україні зберігати елементи готівкової інфраструктури як частину фінансової стійкості?

2. Які кроки варто зробити суб'єктам фінансового моніторингу в Україні вже зараз, аби відповідати вимогам нових регламентів ЄС (DORA/NIS2)?

3. У зв'язку з проблемою обходу санкцій Росією через контрабанду, які інструменти міжнародної співпраці могли б ефективніше ідентифікувати та перекривати схеми обходу санкцій через "країни-прокладки"?

4. Як, на вашу думку, слід забезпечити ефективне впровадження ризик-орієнтованого нагляду за різними типами ВНУП в Україні — зокрема за юристами, ріелторами та дилерами з дорогоцінними камінням та металами, а також арт-дилерами? Які ресурси або інституційні зміни для цього потрібні?

5. Чи має Україна створити публічний реєстр бенефіціарних власників нерухомості, зокрема у випадках, коли майно зареєстровано на іноземні компанії? Які механізми валідації інформації могли б запобігти зловживанням?

6. На вашу думку, які категорії нерухомості в Україні (наприклад, курортна, преміальна столична, комерційна) є найбільш вразливими до використання для відмивання коштів через офшорні структури? Як це можна перевірити на практиці?

7. Які елементи національної системи фінансового моніторингу мають бути адаптовані для виявлення транзакцій, пов'язаних із нелегальним виробництвом, логістикою та експортом синтетичних наркотиків, зокрема MDMA?

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-2025-13

Бюлетень є волонтерською розробкою методологічної команди Міністерства фінансів України відповідно до частини 8 статті 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

Щоб отримати доступ до інших Методологічних Бюлетенів – перейдіть за посиланням [офіційний веб-сайт Міністерства фінансів].