Методологічний бюлетень

Серійний номер: МінФін-AML-2026-22

Травень 2026

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

Томас Карлайл

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Цифрова трансформація режиму SAR і нові типологічні загрози у Великій Британії [1]

Черговий, 36-й випуск щоквартального журналу Підрозділу фінансової розвідки Великої Британії (UKFIU) «SARs in Action» (травень 2026 року) охоплює чотири ключові тематичні блоки, що відображають як технологічну трансформацію британського режиму повідомлень про підозрілу діяльність (Suspicious Activity Reports, SAR), так і оперативні результати застосування SAR-аналітики у розслідуванні організованої злочинності. Видання адресоване широкому колу стейкхолдерів — від правоохоронних органів до підзвітних суб'єктів і регуляторів — і виконує функцію інформаційно-аналітичного інструменту для підвищення ефективності режиму фінансової розвідки в цілому.

Центральною інфраструктурною подією випуску є масштабне розширення доступу до нової Цифрової Служби SAR (SARs Digital

[1] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/814-sars-in-action-issue-36/file

Service, SDS): понад 1 600 співробітників правоохоронних органів перейшли до роботи з новою платформою після завершення розширеного тестового етапу. Більше двох третин партнерських організацій пройшли обов'язкові інструктажі та отримали облікові записи. Паралельно з розгортанням нової системи функціональні оновлення впроваджуються щомісяця у відповідь на зворотний зв'язок від перших користувачів. UKFIU підкреслює, що попри поступовий перехід усі старі системи продовжуватимуть паралельну роботу протягом тривалого перехідного періоду, що знижує операційні ризики впровадження для кінцевих користувачів і убезпечує безперервність обслуговування активних справ.

Матеріал Відділу публічно-приватного партнерства Національного центру боротьби з економічними злочинами (NECC) присвячений результатам роботи тимчасової слідчої групи щодо незаконних фінансових потоків між Балканами та Великою Британією. Цей механізм, сформований у рамках Illicit Finance Public-Private Threat Group, проаналізував дані, підтримав чотири активні кримінальні розслідування та залучив до роботи контрагентів у Балканському регіоні. Ключовим продуктом роботи групи стало видання класифікованого Amber Alert, що описує нові типологічні методи організованих злочинних угруповань (ОЗУ), зокрема схеми з поєднанням нелегальної міграції, обходу митного контролю Великої Британії та застосування обмінників (Money Service Businesses, MSB) у Тирані. На підставі отриманих результатів підготовлені рекомендації для державних органів і набір «червоних прапорців» для фінансових установ із метою ефективнішого управління клієнтськими ризиками.

Команда з розвитку SAR-аналітики (SARs Intelligence Development Team, SIDT), заснована у 2020 році в рамках Програми реформування SAR Міністерства внутрішніх справ, надала детальний звіт про результати діяльності, що засвідчує суттєвий внесок у боротьбу з організованою злочинністю. Завдяки SAR-розвідці вжиті заходи призвели до відновлення активів на суму понад £5,8 млн, ще £14,5 млн заморожено в рамках поточних розслідувань. Паралельно SIDT сприяла ідентифікації об'єктів оподаткування та формуванню податкових претензій HMRC на суму понад £500 000. Команда також відіграла ключову або інструментальну роль у майже 150 арештах, з яких 40 вже завершились обвинувальними вироками, а решта справ перебуває у системі кримінального судочинства. Наприкінці звітного періоду Міністерство внутрішніх справ спільно з Казначейством оголосили про значне додаткове фінансування SIDT, що передбачає

Висновки:

- **Розгортання SDS із понад 1600 активними користувачами засвідчує готовність UKFIU до переходу на централізовану платформу аналізу даних**; СПФМ, що подають SAR до британського ПФР, слід очікувати пришвидшення оперативного реагування та розширення можливостей перехресного збагачення даних між різними правоохоронними структурами.
- **Типологічні схеми у контексті Балканського регіону — поєднання нелегальної міграції та операцій MSB у Тирані — формують новий профіль ризику для британських фінансових установ**, що обслуговують клієнтів із зв'язками з цим регіоном; ефективне виявлення таких клієнтів потребує перекалібрування транзакційних сценаріїв із урахуванням специфіки електронних грошових переказів у балканському напрямку.
- **Схема відмивання через міжнародну іпотеку вимагає від відділів комплаєнсу банків переосмислення стандартних підходів до належної перевірки іпотечних клієнтів-нерезидентів:** встановлення джерела початкового внеску, ідентифікація реального власника нерухомості та моніторинг невідповідностей між задекларованим рівнем доходу і розміром транзакцій є мінімальними обов'язковими заходами.

подвоєння чисельності команди і посилення її присутності у структурі регіональних підрозділів боротьби з організованою злочинністю (ROCU).

У рамках Міжнародної робочої групи, що є структурним елементом розширеної версії Спільної оперативно-аналітичної групи з боротьби з відмиванням коштів (JMLIT+), NECC спільно з Мережею фінансової розвідки Джерсі (JFIN) у березні 2026 року видали Amber Alert 0798-NECC, присвячений загрозі зловживання продуктами міжнародної іпотеки з метою відмивання коштів. Документ розкриває типологічну схему, за якою злочинці використовують географічну роз'єднаність між позичальником, кредитором та об'єктом нерухомості для введення незаконних коштів через офшорні юрисдикції в рахунок внесків, орендних доходів і погашення іпотечних платежів. Такий механізм забезпечує щонайменше один додатковий шар обфускації провенансу активу, ускладнюючи відстеження реального джерела капіталу. Alert містить набір ключових типологічних індикаторів і факторів-каталізаторів для фінансових установ.

Практичний розділ журналу містить кейс-стаді щодо застосування механізму Defence Against Money Laundering (DAML) SAR: суб'єкт звітування виявив підозру у нелегальній зайнятості клієнта та закінченні терміну дозволу на перебування у Великій Британії, подав DAML SAR і отримав згоду на блокування залишку на рахунку. На підставі отриманих даних правоохоронний орган ініціював заморожування рахунку та повне розслідування в рамках Закону про доходи від злочинів 2002 (POCA 2002), що завершилось конфіскацією понад £20 000, розподілених на кількох рахунках. Водночас редакційна відповідь UKFIU на актуальне практичне питання стосується автоматичного зв'язку між судовими запитами та обов'язком подання SAR. Позиція UKFIU є принципово чіткою: підозра не може бути «успадкована» від зовнішнього запиту — суб'єкт зобов'язаний самостійно сформувати незалежну підозру у відмиванні коштів, фінансуванні тероризму або злочинному майні, яку він зможе артикулювати в контексті власного ділового зв'язку з клієнтом.

Санкційний комплаєнс у фінансових установах Великої Британії [2]

Опублікована масштабна аналітична доповідь Управління з фінансового регулювання і нагляду Великої Британії (FCA) узагальнює результати проактивного наглядового огляду систем і механізмів санкційного комплаєнсу понад 150 підпорядкованих FCA фінансових установ у різних секторах. Доповідь є логічним продовженням звіту вересня 2023 року і охоплює системи фінансових та торгових санкцій. Обсяг накопичених кількісних і якісних даних, а також деталізація практик, роблять цей документ ключовим орієнтиром для галузі санкційного комплаєнсу.

Контекстуальну основу формує зростання обсягу та складності санкційних режимів Великої Британії після лютого 2022 року: загальна вартість заморожених у Великій Британії активів зросла з £24,4 млрд у 2023–2024 роках до £37 млрд у 2024–2025 роках. Разом із розширенням таргетованих фінансових санкцій суттєво розвинулись секторальні та торгові санкційні режими: вони поширились не лише на традиційні військові та товари подвійного використання, але й охопили ширше коло товарів, технологій, суміжних послуг і технічної допомоги. Для фінансових установ особливого значення набули заборони на надання фінансових послуг і технічної допомоги, пов'язаних із обмеженими товарами, а також автономні санкції щодо конкретних видів послуг.

У сфері повідомлень про можливі порушення FCA фіксує неоднозначну динаміку: попри скорочення кількості повідомлень за 2023–2025 роки, абсолютний рівень залишається суттєво

[2] https://www.fca.org.uk/publications/good-and-poor-practice/sanctions-systems-and-controls-our-firms-our-findings

вищим за допандемічний базовий рівень. Географічно переважна більшість повідомлень стосується Росії, однак регулятор вказує на зростаючу частку повідомлень, пов'язаних із Іраном, Північною Кореєю та тематичними режимами (глобальна антикорупція, права людини, протидія тероризму). Критичним залишається фактор своєчасності: у 2025 році 35% поданих звітів стосувалися подій, що відбулися до року звітування, а середній час між ідентифікацією потенційного порушення та його звітуванням становив 116 днів — лише незначне поліпшення проти 120 днів у 2024 році. FCA особливо звертає увагу на аномально низьке представництво страхового сектору та сектору цифрових активів у загальній масі звітів, попри задокументоване використання криптовалют і «тіньового флоту» для обходу санкцій.

В аналізі систем управління та нагляду FCA виявив суттєву диференціацію між установами: ряд компаній демонстрував застарілі, неточні або внутрішньо суперечливі санкційні політики, що переважно фокусувались на замороженні активів і не відображали секторальних чи торгових санкцій. Практика надмірної залежності від групових угод, провайдерів скринінгу або третіх сторін без адекватного локального нагляду зафіксована у значній частині перевірених установ. Навпаки, установи з найкращими практиками артикулювали власні підходи до прийняття, управління та пом'якшення санкційних ризиків у рамках детальних оцінок юрисдикційного й продуктового ризику, запровадили таргетовані програми навчання з урахуванням специфіки ролей у зонах підвищеного ризику та підтримували актуальну документацію — включаючи змістовні ключові індикатори ризику у звітах MLRO.

Якість оцінок санкційних ризиків варіювалась у широкому діапазоні. Серед системних вад FCA виокремлює: нечітке розмежування між санкційними ризиками та ризиками ВК/ФТ; мінімальну або відсутню увагу до фінансування розповсюдження зброї масового знищення (ФР) як самостійного виду ризику; створення висновків без документованого обґрунтування; надмірну залежність від сторонніх систем рейтингування юрисдикційного ризику без внутрішнього критичного осмислення та зіставлення з

Висновки:

- **Розрив між зрілістю фінансово-санкційного та торгово-санкційного комплаєнсу є критично значущим:** переважна більшість установ не відображає торгові санкції в оцінках ризику, CDD, скринінгу та навчанні персоналу; ліквідація цієї прогалини потребує переосмислення продуктових, клієнтських та юрисдикційних оцінок ризику із включенням специфіки торгових заборон і суміжних послуг.
- **Результати тестування скринінгових систем (SST) виявили системний дефіцит у обробці нелатинських символів, варіацій написання та складних корпоративних структур власності**, що безпосередньо генерує санкційні порушення; установам необхідно провести незалежний аудит конфігурацій скринінгових систем і окремо протестувати сценарії з нелатинським алфавітом та однаковими іменами.
- **Середній час у 116 днів між ідентифікацією потенційного порушення та його звітуванням регулятору є неприйнятним**: санкційне законодавство Великої Британії передбачає звітування у розумні строки; установам необхідно запровадити чіткі правила на всіх етапах від алерту до звіту, включаючи ескалаційні маршрути і визначені строки для кожного рівня прийняття рішення.
- **Надмірна залежність від сторонніх провайдерів скринінгу та CDD без належних механізмів нагляду та валідації формує системний правовий ризик**: FCA недвозначно зазначає, що відповідальність за ефективність санкційного контролю залишається з ліцензованою установою, а не за постачальником послуг.

оцінками FATF. Особливо критичними є прогалини у відображенні торгових санкцій — значна частина установ обмежувала їхню сферу виключно торговим фінансуванням, не поширюючи аналіз на всю бізнес-модель, клієнтську базу та продуктовий портфель.

Аналіз належної перевірки клієнтів (CDD/EDD) виявив системні проблеми у роботі з непрозорими структурами власності: ряд установ зазнавав труднощів з встановленням непрямого бенефіціарного власника в мультирівневих корпоративних структурах. Анкети з оцінки санкційного впливу (SEQ) застосовувались непослідовно, часто мали застарілі питання або використовувались виключно у форматі самоатестації клієнта — що FCA кваліфікує як недостатній контрольний інструмент. Щодо скринінгу: попри поширену практику автоматичного скринінгу (70% установ) та щоденного повторного скринінгу клієнтів (81%), FCA виявив суттєві проблеми калібрування систем — нездатність обробляти імена з нелатинськими символами, хибне відсіювання однакових імен або імен із цифровими елементами, обрізання наддовгих імен без генерування сповіщення. 90% алертів при точному збігу імен коректно ідентифікували підсанкційного суб'єкта, однак цей показник знижувався до 75% при незначних варіаціях написання — що свідчить про системну неповноту нечіткого збігу (fuzzy matching).

Окремий блок доповіді присвячений управлінню замороженням активів і звітуванню про порушення. FCA документує критичні випадки несвоєчасного блокування виведеної ліквідності внаслідок запізнілого оновлення санкційних списків та несанкціонованого продовження банківського обслуговування після ідентифікації клієнта як підсанкційного — через відсутність у персоналу чіткого розуміння процедури блокування рахунків і відповідних подальших дій. Ліцензійне управління також є проблемною зоною: установи демонструють недостатнє розуміння меж ліцензійних дозволів, що призводить до ненавмисних порушень умов ліцензії. У сфері звітування переважна більшість установ усвідомлює обов'язки щодо OFSI, але значна їх частина не має задокументованих процедур звітування до OTSI та HMRC, що суперечить вимогам чинного законодавства.

Торгові санкції формують системний «сліпий кут» для більшості перевірених установ, тоді як методологія виявлення обходу санкцій загалом залишається реактивною. Серед виявлених сценаріїв ухилення FCA виокремлює: переведення коштів із рахунків незадовго після введення санкцій щодо особи; доступ до фінансових послуг через складні структури власності, родичів або близьких осіб; використання третіх сторін і банків-кореспондентів для приховування зв'язків із підсанкційними особами; маршрутизацію коштів через криптоактиви та гаманці електронних грошей; фальсифікацію торгової документації. FCA відзначає найкращі практики у фірм, що запровадили проактивні тематичні перевірки, поєднуючи їх із відкритою розвідкою та спеціалізованими сценаріями транзакційного моніторингу, які зіставляють юрисдикційні ризики з галузевими. Найбільш прогресивні гравці досліджують застосування автоматизації та AI для скорочення ручної обробки торгової документації і виявлення аномалій.

Кібер-вибір 2026: Навігація світом цифрових технологій [3]

У часи, коли цифрові технології пронизують кожен аспект життя — від навчання й розваг до міжособистісної комунікації та майбутньої кар’єри, — проблема правомірного використання цих інструментів стає особливо гострою.

[3] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/810-cyber-choices-brochure-2026-under-12s/file
https://www.nationalcrimeagency.gov.uk/who-we-are/publications/806-cyber-choices-brochure-2026-12-17s/file
https://www.nationalcrimeagency.gov.uk/who-we-are/publications/809-cyber-choices-brochure-2026-teachers/file
https://www.nationalcrimeagency.gov.uk/who-we-are/publications/811-cyber-choices-brochure-2026-parents-1/file
https://www.nationalcrimeagency.gov.uk/who-we-are/publications/807-cyber-choices-brochure-2026-18-plus/file

Саме цій темі присвячена серія інформаційних брошур Cyber Choices 2026, підготовлених Національним агентством з боротьби зі злочинністю Великої Британії (NCA) спільно з регіональною мережею Cyber Choices та місцевими кіберпідрозділами поліції. Брошури пропонують цілісне уявлення про сучасний британський підхід до профілактики кіберзалежної злочинності серед молоді. Програма не лише пояснює юридичні межі, але й пропонує позитивну альтернативу: розвиток технічних талантів у легальному, безпечному та перспективному напрямку.

Головна теза, що червоною ниткою проходить через усі документи, полягає в тому, що допитливість і технічні здібності молодої людини самі по собі не є проблемою. Навпаки, сучасна кіберіндустрія відчуває колосальний дефіцит кваліфікованих кадрів, і тому фахівці з програмування, хакінгу, цифрової криміналістики чи хмарних технологій мають блискучі перспективи працевлаштування. Однак проблема виникає тоді, коли молода людина через брак знань про закон, бажання самоствердитися або під впливом однолітків обирає нелегальний шлях.

Статистика, наведена в брошурах, вражає: середній вік засудженого за кіберзлочини значно нижчий, ніж за іншими видами злочинів, — найчастіше це підлітки. Вони можуть зламувати чужі акаунти, використовувати так звані «стресори» (booters) для атак на інтернет-з’єднання суперників в іграх, поширювати шкідливе програмне забезпечення, навіть не усвідомлюючи всієї серйозності своїх дій. Мотивація може бути різною: виклик власним навичкам, нудьга, бажання довести щось друзям або просто хибне уявлення про те, що «так роблять усі».

Юридичним підґрунтям усіх матеріалів є Computer Misuse Act 1990 (Закон про комп’ютерні зловживання). Закон складається з п’яти ключових розділів.

Перший розділ стосується найпростішого, на перший погляд, порушення — несанкціонованого доступу до комп’ютерних матеріалів. У брошурі наводять приклад: ви спостерігаєте, як ваш друг вводить логін і пароль, запам’ятовуєте їх, а згодом без дозволу заходите в його обліковий запис і читаєте повідомлення. Це вже злочин.

Другий розділ — несанкціонований доступ із наміром вчинити або сприяти вчиненню подальших правопорушень. Ілюстрацією слугує ситуація, коли підліток бере планшет друга без дозволу, заходить у його ігровий акаунт і купує ігрові кредити, використовуючи прив’язану кредитну картку.

Третій розділ — несанкціоновані дії з наміром або через недбалість, що погіршують роботу комп’ютера. Типовий випадок: гравець використовує «стресор» (Booter tool), знаючи, що це вимкне суперника з мережі, щоб виграти матч. Чимало молодих людей вважають це просто «жартом», однак закон кваліфікує таку дію як злочин.

Розділ 3ZA йде ще далі — несанкціоновані дії, що спричиняють або створюють ризик серйозної шкоди. Якщо хакер атакує телефонну компанію, і внаслідок цього деякі люди не можуть викликати поліцію в небезпечній ситуації, то навіть якщо хакер не мав наміру завдати шкоди, він діяв недбало, а це також карається за законом.

Нарешті, розділ 3A говорить про виготовлення, постачання або отримання інструментів для вчинення злочину. Наприклад, завантаження спеціального програмного забезпечення, яке дозволяє обійти логін і пароль, щоб зламати ноутбук друга, — це вже кримінально каране

діяння, навіть якщо ви не встигли скористатися цим інструментом. Таким чином, автори брошур намагаються донести думку, що незнання закону або сприйняття своїх дій як «невинної гри» не звільняє від відповідальності.

Надзвичайно важливо, що програма не обмежується застереженнями. Вона пропонує розгорнуту систему легальних ресурсів і можливостей, які дозволяють молодій людині розвивати свої здібності у безпечному, контрольованому та водночас викликовому середовищі. Для наймолодшої аудиторії (до 12 років) у брошурі рекомендовані міжнародні клуби кодингу, зокрема Code Club, де діти 9–13 років можуть створювати ігри, анімації та вебсторінки за допомогою Scratch, Python або HTML/CSS. Батькам радять пошукати такі клуби у своєму регіоні — вони часто є безкоштовними й працюють при бібліотеках або школах.

Окрему увагу матеріали приділяють кіберспорту (esports). Це невипадково, адже 9 з 10 молодих людей уже грають у відеоігри, і часто саме в ігровому середовищі виникають перші спокуси вдатися до нелегальних дій (наприклад, DDoS-атака на суперника). Замість того щоб ігнорувати або засуджувати захоплення іграми, програма Cyber Choices пропонує інтегрувати його в позитивне русло. Британська організація British Esports, яка детально описується в брошурах, створена для розвитку кіберспортивних талантів на національному та міжнародному рівнях. Таким чином, кіберспорт стає не лише майданчиком для розваг, а й потужним інструментом виховання дисципліни, критичного мислення, командної роботи та юридичної свідомості.

Для батьків і вчителів брошури містять низку практичних порад і ресурсів. Батькам радять не лякатися технічних захоплень дитини, а навпаки — визнати їх, обговорювати з дитиною важливість чесності й законності в цифровому світі так само природно, як вони пояснюють, чому не можна красти в магазині або пошкоджувати чуже майно. Рекомендується шукати гуртки програмування та кібербезпеки у своєму регіоні, заохочувати дитину брати участь у легальних змаганнях (наприклад, Capture the Flag, онлайн-олімпіадах з кібербезпеки) і пояснювати реальні наслідки порушеннь.

Вчителі отримують ще більше інструментів. Брошура для педагогів містить посилання на два безоплатні плани уроків, розроблені спільно з Асоціацією PSHE. Ці плани допомагають говорити з учнями про причини та наслідки кіберзлочинності, а також про те, як її уникнути. Для вчителів також пропонується ознайомитися з поняттям «Bug Bounties» — програм винагороди за виявлення вразливостей. Багато компаній (як великих технологічних гігантів, так і невеликих стартапів) пропонують фінансові стимули хакерам, які знаходять і повідомляють про вразливості в їхніх системах. Це чудовий спосіб для талановитої молоді легально випробувати свої навички, отримати визнання й навіть заробити гроші. Однак брошура застерігає: необхідно ретельно читати умови таких програм і суворо їх дотримуватися; недотримання може призвести до ненавмисного вчинення злочину.

Щодо кар'єрних перспектив, матеріали Cyber Choices пропонують широкий огляд можливостей. Згадуються такі організації, як UCAS (Служба прийому до університетів та коледжів), де можна знайти повну інформацію про університетські курси з кібербезпеки та вимоги до вступу, а також про академічні стажування (apprenticeships). Національний центр кібербезпеки (NCSC) надає інформацію про професійні та академічні кваліфікації. Міжнародна некомерційна організація CREST, яка акредитує та сертифікує фахівців з технічної інформаційної безпеки, пропонує кар'єрні поради для тих, хто хоче стати фахівцем з тестування або аналітиком центру моніторингу безпеки (Security Operations Centre Analyst).

У брошурах наголошується, що попит на такі навички, як хмарні обчислення, штучний інтелект, машинне навчання, мережеві технології, хакінг, цифрова криміналістика та скриптове програмування, є надзвичайно високим, і цей попит лише зростатиме в майбутньому. Іншими словами, інвестиція часу та зусиль у легальний розвиток кібернавичок окупається з лишком.

На завершення варто підкреслити, що матеріали Cyber Choices 2026 — це не набір залякувань, а насамперед система підтримки та навігації. Вони визнають, що молоді люди з технічними здібностями мають величезний потенціал, і суспільству вигідно, щоб цей потенціал реалізовувався легально та етично. Замість того щоб відштовхувати підлітків, які цікавляться хакінгом, потрібно простягати їм руку й показувати шлях до престижної, високооплачуваної професії, де їхні таланти будуть затребувані. Батьки отримують інструменти для розмови з дітьми, вчителі — готові уроки, а молодь — захопливі онлайн-платформи, клуби, кіберспортивні змагання та чітке розуміння юридичних кордонів.

Гасло, яке завершує кожну брошуру, — «Helping you choose a positive and legal path» (Допомагаємо обрати позитивний і легальний шлях) — відображає сучасний підхід до профілактики злочинності, заснований не на покаранні, а на залученні, освіті та розвитку. У світі, де відчувається дефіцит кіберфахівців, а технології стають дедалі складнішими, подібні програми є не просто корисними, а критично необхідними для безпеки та процвітання як окремих молодих людей, так і суспільства загалом. Саме тому матеріали Cyber Choices 2026 заслуговують на увагу, поширення та впровадження не лише у Великій Британії, а й як зразок для наслідування в інших країнах, які прагнуть збалансувати цифрову свободу з правопорядком.

Висновки:

- **Кіберзлочини — це не «жарти», а реальні кримінальні справи.** Згідно з Computer Misuse Act 1990, навіть несанкціоноване читання чужих повідомлень або використання DDoS-атаки в грі може призвести до кримінального запису, вилучення пристроїв та неможливості працевлаштування в майбутньому.
- **Середній вік кіберзлочинця — підлітковий.** Більшість правопорушень вчиняються молодими людьми через брак обізнаності про закон, бажання випробувати свої навички або під впливом однолітків, а не через злий умисел. Це відкриває вікно для профілактики та переорієнтації.
- **Легальна альтернатива існує й активно підтримується.** Уряд Великої Британії створив безоплатні ресурси, які дозволяють розвивати технічні таланти в безпечному, легальному та перспективному середовищі.
- **Ключова роль належить батькам, вчителям і ранньому втручанню.** Документ закликає дорослих не лякатися захоплень дитини, а відкрито говорити про юридичні межі, використовувати готові плани уроків і звертатися до фахівців до того, як ситуація вийде з-під контролю.

Як посилення контролю створює «розумніші» злочинні екосистеми [4]

Коли у 2007 році Болгарія офіційно стала членом Європейського Союзу, євроінтеграційний оптимізм сягнув свого піку щодо багатьох сфер, включно з безпекою кордонів.

Переважна думка серед політиків, аналітиків та громадськості полягала в тому, що членство в ЄС автоматично запустить ланцюг позитивних змін: від модернізації інфраструктури та цифровізації митних процедур до запровадження найвищих стандартів прозорості й боротьби з хабарництвом. Європейські кошти та ноу-хау мали перетворити кордони нової держави-члена

[4] https://baselgovernance.org/blog/how-stronger-borders-can-create-smarter-corruption-lessons-one-europes-most-strategic-border

на зразкові форпости правопорядку. Однак реальність, як це часто буває, виявилася набагато складнішою та менш лінійною.

Дослідження, Базельського інституту врядування (Basel Institute on Governance) на прикладі пункту пропуску «Капітан Андреєво» на кордоні Болгарії з Туреччиною, пропонує глибоко парадоксальний, але вкрай важливий висновок. Корупція на цьому стратегічному переході, одному з найбільш завантажених сухопутних шляхів між Європою та Азією, не просто не зникла – вона трансформувалася, адаптувалася та стала «розумнішою».

Щоб зрозуміти масштаб цієї трансформації, необхідно спочатку зануритися в історичний та інституційний контекст кордону до моменту вступу Болгарії до ЄС. Протягом 1990-х років Болгарія переживала глибоку економічну кризу, що супроводжувалася тотальним дефіцитом споживчих товарів, стрімким падінням державної спроможності та, як наслідок, бурхливим розквітом неформальних, тіньових ринків. У цих умовах контрабанда перестала бути виключно кримінальним явищем – вона стала стратегією виживання для багатьох людей. Кордон перетворився на простір, де дискреційна влада митників, прикордонників та інспекторів досягала колосальної концентрації. Ці посадовці, з одного боку, та торговці, транспортні компанії, мігранти, дрібні контрабандисти й організовані злочинні групи – з іншого, існували в стані симбіозу. Хабарі були універсальним засобом платежу, що дозволяв не помічати недекларовані товари, заплющувати очі на контрафактну продукцію чи сприяти масштабному ухиленню від сплати податків.

Особливим осередком активності стала так звана «нічийна земля» – нейтральна смуга між болгарським та турецьким кордонами, де працювали магазини duty-free. Ці магазини стали не просто точками роздрібної торгівлі, а потужними хабами для оптової контрабанди цигарок, алкогольних напоїв, нафтопродуктів та інших підакцизних товарів.

Дуже важливо, що корупція на пункті пропуску «Капітан Андреєво» ніколи не була хаотичною сукупністю індивідуальних зловживань. Дослідження чітко виділяє два її рівні. На нижчому рівні функціонували повсякденні обміни між водіями вантажівок та рядовими офіцерами, часто засновані на довготривалих особистих зв'язках, взаємному знайомстві та репутації. Але над цим височіла набагато складніша конструкція: зв'язки між політиками, високопосадовцями центральних митних і податкових органів, бізнес-елітами та лідерами організованих злочинних угруповань. Прибутки від контрабанди рухалися вгору цими патронажними системами, забезпечуючи політичний захист і «дах» для контрабандних маршрутів. Без такого захисту масштабна нелегальна діяльність на стратегічному переході була б неможливою.

Вступ Болгарії до Європейського Союзу докорінно змінив юридичне та інституційне середовище, в якому функціонував цей корупційний комплекс. Процес євроінтеграції вимагав від Болгарії не просто косметичних змін, а глибокої гармонізації всього спектру прикордонних правил і процедур. Країна мала імплементувати єдині митні правила ЄС, стандарти оподаткування ПДВ (включно зі складними механізмами його відшкодування при експорті), уніфікувати ставки акцизів, а також запровадити суворі санітарні, ветеринарні та харчові стандарти, які діють на всьому просторі Союзу.

Розпочалася масштабна цифровізація. Стали до ладу такі складні інформаційні системи, як VIES (Інформаційна система обміну даними про ПДВ) та EMCS (Система контролю за переміщенням підакцизних товарів), які дозволили державам-членам в режимі реального часу відстежувати транскордонні потоки товарів і звіряти податкові дані. Міграційний контроль значно посилився через необхідність відповідати Шенгенським вимогам, що надало болгарським прикордонникам доступ до Шенгенської інформаційної системи (SIS) та міжнародних баз даних викрадених документів і транспортних засобів. Однак найбільш візуально помітною зміною стало впровадження сучасних технологій фізичного контролю. На «Капітан Андреєво» з'явилися рентгенівські установки для сканування великовантажних контейнерів, стаціонарні та

портативні сканери, тепловізори для нічного моніторингу, а також системи автоматичного розпізнавання номерних знаків (Automatic License Plate Recognition), здатні фіксувати та перевіряти кожен автомобіль, що перетинає кордон. Поруч із цим були впроваджені сучасні інструменти аналізу ризиків, які дозволяли митникам обирати для поглибленої перевірки саме ті вантажі, які мали найвищі ризики порушень. З погляду технократичного управління, це була беззаперечна історія успіху: європейські гроші та стандарти перетворювали кордон на фортецю законності.

Але саме тут, як стверджують автори дослідження, відбувся перший серйозний теоретичний збій у мисленні реформаторів. Кримінальні та корупційні системи не є статичними. Вони не зникають під тиском нових правил – вони реагують, перегруповуються та шукають нові вразливості. Найбільш парадоксальний висновок дослідження полягає в тому, що після євроінтеграції нелегальний перетин кордону та ухилення від сплати податків стали значно складнішими, ризикованішими та дорожчими. Але ця обставина, замість того щоб зробити корупцію непотрібною, навпаки, кардинально підвищила її стратегічну цінність. Якщо в 1990-х хабарі слугували переважно для прискорення бюрократичних процедур або заплющення очей на очевидні, «грубі» порушення, то тепер вони стали абсолютно необхідним інструментом для прямого маніпулювання складними, багатошаровими контрольними системами.

Випадок із шахрайством з ПДВ є, мабуть, найяскравішою ілюстрацією цієї адаптації. У рамках ЄС діє правило, згідно з яким експорт товарів за межі митної території Союзу оподатковується за нульовою ставкою ПДВ. Більше того, компанія-експортер має право на відшкодування того ПДВ, який вона раніше сплатила своїм постачальникам всередині країни. Здавалося б, це проста та прозора норма, покликана стимулювати торгівлю. Однак саме вона стала основою для витончених злочинних схем, відомих як «карусельне шахрайство» (carousel fraud). На «Капітан Андреєво» дослідники зафіксували випадки, коли корумповані митні офіцери вносили у відомчі інформаційні системи завідомо неправдиві відомості. Вони вручну реєстрували реквізити фіктивних вантажівок, вказуючи, що ті нібито перетнули кордон і виїхали за межі ЄС. Зрозуміло, що жоден реальний перетин кордону не відбувався, і ніякого експорту не існувало. Але на основі цих сфабрикованих даних компанії отримували законне (з точки зору наявних у системі записів) право на відшкодування ПДВ.

Однак навіть цей механізм блідне порівняно з тим, як зловмисники навчилися маніпулювати системами автоматичного розпізнавання номерних знаків. За даними дослідження, корумповані особи іноді просто відключали автоматичне розпізнавання на окремих смугах руху. Потім вони вручну вводили змінені номерні знаки, використовуючи символи кирилиці, які візуально майже не відрізняються від латинських літер. Це дозволяло контрабандистам провести вантажівку з нелегальним товаром через кордон, тоді як в системі фіксувався абсолютно інший, «легальний» транспортний засіб.

Іншою важливою сферою, де адаптація відбулася надзвичайно швидко та болісно, стало застосування європейських харчових та фітосанітарних норм. Вступ до ЄС означав для Болгарії необхідність проводити жорсткий контроль якості та безпеки всіх харчових продуктів, що перетинають її кордон, особливо з третіх країн, таких як Туреччина. Це створило абсолютно нові «вузькі місця» (bottlenecks) і, відповідно, нові форми дискреційної влади. Офіцери, які відповідали за відбір проб, та працівники лабораторій, які проводили аналізи, отримали величезний вплив.

Дослідження описує дві основні маніпулятивні стратегії, що стали рутинною практикою. Перша – це вибіркове взяття зразків. Замість того, щоб відбирати проби відповідно до суворої статистичної методики з різних частин вантажу (включно з підозрілими зонами), корумповані інспектори брали зразки лише з «чистих» ділянок, де продукт свідомо відповідав нормам. Друга стратегія – ще більш зухвала – полягала у прямій фальсифікації результатів лабораторних тестів.

Лабораторії, найчастіше приватні, видавали сертифікати відповідності для небезпечних, зіпсованих або заборонених продуктів, дозволяючи їм безперешкодно потрапити на ринки ЄС.

Ця проблема набула критичного масштабу після того, як частина прикордонних функцій була передана на аутсорсинг приватним компаніям. На «Капітан Андреєво» було приватизовано лабораторне тестування харчових продуктів, послуги паркування вантажівок, а також дезінфекцію транспортних засобів. Ідея полягала в тому, що приватний сектор працює ефективніше та менш схильний до корупції. На практиці ж вийшло навпаки. Приватизація створила гібридні публічно-приватні структури, де підзвітність стала ще більш розмитою, а механізми нагляду – фрагментованими. Висновок, який роблять автори, є надзвичайно важливим для сучасної антикорупційної політики: приватизація публічних функцій жодним чином не є автоматичним рішенням проблеми корупції.

Мабуть, найтривожнішою трансформацією, описаною в дослідженні, є еволюція самої організаційної структури корупції на «Капітан Андреєво». У 1990-х роках система була більш фрагментованою, хоча й пов'язаною патронажними зв'язками. Сьогодні ж, після євроінтеграції, жоден окремий офіцер, навіть високопосадовець, не може самостійно гарантувати безпечне проходження контрабандного вантажу. Занадто багато різних агенцій залучено до процедури: митниця, прикордонна поліція, фітосанітарна інспекція, ветеринарний контроль, податкова служба, а іноді й інші спеціалізовані органи. Процедури передбачають перехресні перевірки, багаторазове сканування, електронне логування кожної дії. У відповідь на це корупція еволюціонувала в бік колективної координації, створюючи складні мережі, що охоплюють представників різних відомств.

Сучасна корупція – це цілісний, інституціоналізований механізм, який функціонує як вбудована екосистема. Дослідники використовують термін «рутинізована корупція» (routinised corruption), щоб описати системи, в яких хабарі не передаються безпосередньо від водія до інспектора, а акумулюються, розподіляються між членами мережі за заздалегідь узгодженими правилами. Існують внутрішні ієрархії, механізми збору та перерозподілу хабарів, а також складні структури політичного та адміністративного захисту.

Водночас дослідження Базельського інституту робить важливе застереження, яке запобігає надто песимістичним висновкам про тотальну корумпованість. Корупція не завжди є оптимальним або навіть можливим інструментом для всіх видів кримінальної діяльності. Найпоказовішим у цьому сенсі є порівняльний аналіз торгівлі наркотиками. На відміну від ухилення від сплати податків чи контрабанди цигарок, сприяння наркотрафіку в межах ЄС тягне за собою не просто адміністративну відповідальність або втрату роботи. Посадовець, спійманий на допомозі перевезенню наркотичних речовин, постане перед судом за звинуваченням в участі в організованій злочинності, що гарантує тривалі терміни ув'язнення у в'язницях суворого режиму. Ризики стають екзистенційними.

Тому, як показують польові дослідження на «Капітан Андреєво», наркозлочинці все частіше відмовляються від стратегії «купити офіцера» на користь стратегій технологічного обману та конспірації.

Автори описують витончену тактику, відому як стратегія «двох вантажівок-близнюків» (twin trucks strategy). Суть полягає в наступному: кілька майже ідентичних вантажівок, що належать одній компанії та перевозять однаковий номінальний вантаж (наприклад, текстиль або металобрухт), під'їжджають до кордону одночасно в годину максимальної завантаженості. Лише в одній з них таємно обладнано схованку з наркотиками. Інша є абсолютно «чистою». Оскільки пропускна спроможність сканерів і кількість інспекторів обмежені, митники змушені проводити поглиблену перевірку лише частки потоку. Імовірність того, що для перевірки буде обрано саме вантажівку з наркотиками, є невисокою, а решта «чистих» вантажівок, що пройдуть огляд, створюють відчуття нормальної роботи кордону.

Цей приклад має величезне концептуальне значення. Він демонструє, що кримінал і корупція – хоч і часто пов'язані, але не є синонімічними поняттями. Ефективна антикорупційна робота (якщо під нею розуміти ускладнення можливості «домовитися» та створення суворих покарань за хабарі) може не знищити нелегальний обіг наркотиків, а лише змінити його тактику – від більш «соціальної» практики хабарництва до суто технічного змагання між методами приховування та методами виявлення.

Отже, головний урок, який виносить дослідження з аналізу еволюції корупції на пункті пропуску «Капітан Андреєво», виходить далеко за межі Болгарії, Туреччини або окремо взятого прикордонного переходу. Він кидає виклик фундаментальним постулатам сучасної державної політики, заснованої на технократичному оптимізмі. Політики та реформатори в усьому світі часто помилково припускають, що існує прямий, лінійний причинно-наслідковий зв'язок між інвестиціями в технології контролю, посиленням регулювання та зменшенням рівнів корупції та нелегальної торгівлі. Мовляв, більше камер, більше сканерів, суворіші закони, більше цифрових систем – і корупція зникне.

Однак досвід демонструє, що злочинні та корупційні системи є фундаментально адаптивними. Вони не зникають – вони швидко реорганізовуються навколо нових вразливостей, які невідворотно створюються кожною реформою. Кожна нова регуляція, кожна нова технологічна система, кожна нова інспекція, замислена як перешкода для злочинності, водночас породжує нові стимули, нові «вузькі місця» та нові можливості для експлуатації з боку криміналітету.

Посилення контролю не зменшує попит на корупцію – воно робить її більш стратегічно цінною, більш складною та, зрештою, більш дорогою для виявлення та розслідування. Це не означає, що реформи взагалі марні. Проте, щоб уникнути того, що автори називають «непередбачуваними наслідками» – тобто посилення стимулів до хабарництва, перенаправлення контрабандних потоків на альтернативні, менш захищені маршрути, витончене технологічне маніпулювання, виникнення нових форм колузійної змови між державними та приватними структурами, або створення непрозорих приватизаційних схем, – політика має будуватися на зовсім інших засадах.

Висновки:

- **Корупція є адаптивною екосистемою, а не статичним явищем.** Посилення контролю та цифровізація не знищують корупцію, а змушують її еволюціонувати, переносячи фокус на маніпулювання технологічними системами та створюючи нові «слабкі місця».
- **Посилення кордонів підвищує стратегічну цінність хабаря.** Коли нелегальний перетин стає більш складним і ризикованим, корупція з інструменту прискорення процедур перетворюється на необхідний засіб для обходу складних багаторівневих систем контролю.
- **Аутсорсинг прикордонних функцій не зменшує, а часто посилює корупційні ризики.** Передача функцій приватним компаніям створює гібридні публічно-приватні структури з розмитою відповідальністю та слабшим наглядом, що відкриває нові можливості для корупції.
- **Сучасна прикордонна корупція стає колективною та організованою.** Через множинність залучених агенцій жоден окремий офіцер не може гарантувати результат, натомість формуються злочинні мережі з механізмами розподілу хабарів, внутрішньою ієрархією та політичним захистом.

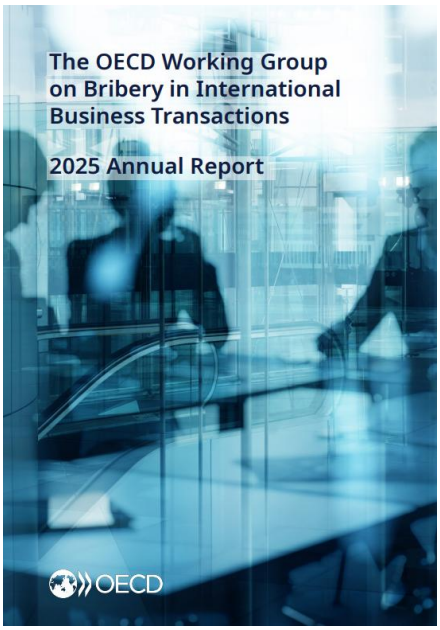
Автори дослідження закликають до так званого «випереджального врядування» (anticipatory governance). Це означає, що перед тим, як впроваджувати будь-яку масштабну реформу – чи то цифровізація митниці, чи то приватизація лабораторного контролю, чи то запровадження системи автоматичного розпізнавання номерів – необхідно ретельно моделювати, яким чином на цю реформу можуть відреагувати

злочинці. Які нові схеми обходу вони створять? Які нові посадові особи отримають критичну владу? Де виникнуть нові можливості для маніпуляцій?

Тільки поєднуючи антикорупційні стратегії з глибоким, міждисциплінарним аналізом адаптивної поведінки злочинних ринків, можна розраховувати на довгостроковий успіх.

Кордони, як слушно підсумовують автори, не є статичними лініями на карті, які захищаються статичними інституціями від статичних загроз. Вони є постійно еволюціонуючими екосистемами, де держави, ринки, технології та злочинці перебувають у стані безперервної, взаємної адаптації.

«Глобальні програми протидії хабарництву та міжнародні розслідування: тенденції 2025 року» [5]



Документ ОЕСР є масштабним аналітичним і звітним дослідженням, присвяченим діяльності Робочої групи Організації економічного співробітництва та розвитку (ОЕСР) з питань боротьби з підкупом у міжнародних бізнес-операціях (WGB), імплементації Конвенції ОЕСР про боротьбу з підкупом іноземних посадових осіб у міжнародних комерційних операціях, глобальним тенденціям у сфері забезпечення дотримання законодавства щодо транснаціонального хабарництва, міжнародній правоохоронній співпраці та розвитку глобальної антикорупційної архітектури. Документ демонструє, що боротьба з транснаціональним хабарництвом поступово перетворюється на один із ключових елементів міжнародної економічної безпеки, захисту доброчесності глобальних ринків та забезпечення добросовісної конкуренції у міжнародній торгівлі. ОЕСР наголошує, що підкуп іноземних посадових осіб більше не розглядається виключно як окремий корупційний злочин, а дедалі більше сприймається як фактор, який безпосередньо впливає на верховенство права, інвестиційний клімат, міжнародну конкурентоспроможність та довіру до глобальної фінансово-економічної системи.

У вступній частині звіту голова WGB підкреслює, що 2025 рік став періодом суттєвого розширення та трансформації діяльності Робочої групи. OECD прямо зазначає, що міжнародне середовище стає дедалі складнішим через зростання геополітичної нестабільності, тиск на демократичні інститути та послаблення довіри до глобальних механізмів управління. На цьому фоні Конвенція ОЕСР про боротьбу з підкупом іноземних посадових осіб позиціонується як один із небагатьох міжнародних механізмів, який поєднує жорсткі юридично обов'язкові стандарти, систему взаємного моніторингу держав та реальні механізми політичного й репутаційного тиску щодо країн, які не забезпечують ефективного розслідування та переслідування транснаціональної корупції. Документ наголошує, що у 2025 році Україна стала 47-м членом WGB, а також фіксує подальший інтерес інших держав — зокрема Індонезії, Маврикію, Таїланду та Саудівської Аравії — до приєднання до Конвенції. ОЕСР прямо підкреслює, що розширення кола учасників формує більш уніфіковану глобальну систему протидії транснаціональному

[5] https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/fighting-foreign-bribery/the-oecd-working-group-on-bribery-2025-annual-report.pdf

хабарництву та посилює міжнародну співпрацю у справах, пов'язаних із транснаціональною корупцією.

Документ детально пояснює правову та інституційну основу діяльності WGB. Конвенція ОЕСР 1997 року визначається як міжнародний договір, що зобов'язує держави криміналізувати підкуп іноземних посадових осіб у міжнародних бізнес-операціях, забезпечити відповідальність юридичних осіб, застосування ефективних, пропорційних і стримувальних санкцій, а також розвиток систем міжнародної правової допомоги у справах про підкуп іноземних посадових осіб. ОЕСР особливо наголошує на тому, що Конвенція має унікальний фокус саме на стороні надання хабарів — тобто на компаніях, посередниках та особах, які надають хабарі іноземним посадовим особам для отримання контрактів, ліцензій або інших комерційних переваг за кордоном. У цьому контексті документ підкреслює, що транснаціональна корупція створює системні викривлення конкуренції, сприяє неефективному розподілу ресурсів, підриває інвестиційне середовище та стимулює розвиток організованої злочинності й незаконних фінансових потоків.

Одним із центральних елементів звіту є детальний опис механізму взаємного моніторингу, який ОЕСР характеризує як один із найжорсткіших міжнародних антикорупційних механізмів у світі. Система моніторингу складається з чотирьох фаз, що включають оцінювання законодавства, аналіз практичної імплементації, оцінку ефективності правозастосування, виїзні оціночні місії, зустрічі з правоохоронними органами, бізнесом, громадянським суспільством та медіа. Документ наголошує, що країна, яка проходить оцінювання, не може заблокувати висновки щодо себе через принцип «консенсус мінус один» (consensus-minus-one – принцип ухвалення рішень консенсусом без урахування голосу держави, що проходить оцінювання). ОЕСР також підкреслює, що після ухвалення звітів за результатами моніторингу Робоча група з питань хабарництва продовжує здійснювати подальший моніторинг, може застосовувати додаткові заходи щодо держав із серйозними недоліками та навіть публічно реагувати на події, які можуть впливати на виконання Конвенції.

Значна частина документа присвячена аналізу глобальних тенденцій у сфері забезпечення дотримання законодавства щодо боротьби з підкупом іноземних посадових осіб. ОЕСР публікує узагальнену статистику застосування законодавства у сфері протидії транснаціональному хабарництву з моменту набрання Конвенцією чинності у 1999 році до 2024 року. Документ демонструє, що хоча рівень правозастосування загалом поступово зростав, ситуація між державами залишається надзвичайно нерівномірною. ОЕСР прямо констатує, що 16 держав-членів Конвенції досі не повідомили жодного випадку обвинувального вироку або застосування санкцій за підкуп іноземних посадових осіб. Водночас у звіті наголошується, що після 2021 року суттєво зросла кількість санкцій щодо юридичних осіб, а компанії дедалі більше стають центральним об'єктом антикорупційного правозастосування. При цьому темпи застосування кримінальних санкцій до фізичних осіб останніми роками знижуються. ОЕСР фактично демонструє, що наявність законодавства сама по собі не гарантує ефективного переслідування транснаціональної корупції, якщо держава не має спеціалізованих слідчих і прокурорських спроможностей, політичної волі, належних ресурсів та ефективної міжвідомчої координації.

Окремий великий блок документа присвячений результатам оцінювання держав у межах четвертої фази моніторингу. Аналіз Бельгії демонструє наявність проблем навіть у розвинених правових системах. ОЕСР наголошує на хронічному дефіциті людських та фінансових ресурсів у системі розслідування випадків підкупу іноземних посадових осіб, слабкій мотивації компаній впроваджувати антикорупційні програми комплаєнсу, відсутності ефективних механізмів добровільного розкриття інформації та недостатній прозорості механізмів врегулювання справ без судового розгляду. Водночас позитивно оцінюються реформи щодо подовження строків давності, посилення корпоративної відповідальності та впровадження сучасної системи захисту викривачів. ОЕСР рекомендує Бельгії посилити фінансування системи протидії

транснаціональному хабарництву, розробити чіткі методичні документи щодо механізмів врегулювання справ без судового розгляду, забезпечити публічність рішень у справах про підкуп іноземних посадових осіб та посилити відповідальність компаній за незапобігання хабарництву.

Надзвичайно критичною є оцінка Колумбії. OECP прямо зазначає, що країна поступово дистанціюється від виконання своїх зобов'язань за Конвенцією. Документ вказує на низький рівень виявлення випадків підкупу іноземних посадових осіб, практичну відсутність кримінального переслідування фізичних осіб, слабкість системи захисту викривачів та серйозну фрагментованість інституційної структури між органами, які відповідають за виявлення, розслідування та переслідування справ про транснаціональне хабарництво. OECP також наголошує на недостатній незалежності слідства і прокуратури, слабкому використанні механізмів міжнародної правової допомоги та низькій ефективності міжвідомчого обміну інформацією. Водночас позитивно оцінюється розвиток систем комплаєнсу у сфері протидії відмиванню коштів у приватному секторі, які можуть покращити виявлення підозрілих фінансових операцій, пов'язаних із транснаціональною корупцією.

Естонія у звіті представлена як приклад держави, де високий рівень загальної довіри до державних інституцій та сприйняття країни як юрисдикції з низьким рівнем корупції створюють ризик недооцінки ризиків підкупу іноземних посадових осіб. OECP наголошує, що країна фактично не проводила комплексної оцінки ризиків транснаціонального хабарництва, а правоохоронні органи недостатньо використовують різноманітні джерела виявлення корупційних правопорушень. Документ звертає увагу на те, що система захисту викривачів недостатньо чітко охоплює справи про підкуп іноземних посадових осіб, а рівень спеціалізації органів щодо протидії транснаціональній корупції залишається недостатнім. Водночас позитивно оцінюються розвиток механізмів конфіскації активів, міжвідомча співпраця та активна міжнародна взаємодія естонських правоохоронних органів.

Окремий акцент зроблено на Південній Африці, де OECP аналізує боротьбу з транснаціональною корупцією після періоду захоплення державних інституцій приватними інтересами. Документ демонструє, що навіть за умов системного послаблення правоохоронних інституцій окремі міжвідомчі структури та віддані своїй роботі слідчі можуть забезпечувати реальний прогрес у розслідуванні випадків підкупу іноземних посадових осіб. OECP позитивно оцінює використання більш складних методів розслідування, механізмів міжнародної правової допомоги та поступовий розвиток механізмів врегулювання справ без судового розгляду. Водночас наголошується на необхідності гарантувати операційну та фінансову незалежність слідчих і прокурорів, посилити систему захисту викривачів та забезпечити більш прозорі процедури призначення прокурорів і слідчих для мінімізації ризику неналежного впливу.

Документ приділяє дуже значну увагу міжнародній правоохоронній співпраці. OECP детально описує діяльність Global Law Enforcement Network (GLEN), яка функціонує як міжнародна мережа для обміну досвідом, координації транскордонних розслідувань та встановлення прямих оперативних контактів між слідчими і прокурорами різних держав. GLEN позиціонується не просто як платформа для обговорень, а як практичний механізм правозастосування, який уже сприяв запуску паралельних розслідувань, створенню спільних слідчих груп та покращенню обміну доказами. Особливо важливим є наведений у документі кейс співпраці між Україною, Францією та Естонією. OECP описує, як завдяки спільній роботі правоохоронних органів, використанню можливостей GLEN, підтримці Eurojust та Ініціативи StAR вдалося реалізувати скоординоване транскордонне врегулювання справи, у межах якого французька компанія була оштрафована на 18,3 млн євро, а Україна отримала 3,37 млн євро компенсації як потерпіла сторона від корупційного злочину. Документ підкреслює, що скоординовані угоди зі слідством, спільні слідчі групи та постійний неформальний оперативний діалог між правоохоронними

органами стають дедалі важливішими інструментами боротьби з транснаціональною корупцією.

Важливим блоком звіту є тема захисту викривачів та каналів повідомлення про корупцію. ОЕСР наголошує, що ефективне виявлення випадків підкупу іноземних посадових осіб значною мірою залежить від створення безпечних, конфіденційних та функціональних механізмів повідомлення про корупцію. У межах Global Dialogue 2025 учасники обговорювали захищені канали повідомлення, гарантії конфіденційності, ефективні механізми захисту викривачів, стимули для повідомлення про корупційні правопорушення та необхідність формування зміни суспільного ставлення до викривачів. Документ демонструє, що ОЕСР дедалі більше розглядає систему захисту викривачів як один із ключових операційних елементів забезпечення ефективного правозастосування у сфері боротьби з транснаціональним хабарництвом.

Суттєва частина документа присвячена корпоративному комплаєнсу та системам забезпечення доброчесності бізнесу. ОЕСР прямо наголошує, що сучасні антикорупційні програми комплаєнсу не можуть обмежуватися формальним підходом, орієнтованим виключно на формальне виконання вимог. Звіт детально описує нові підходи до оцінки ефективності комплаєнсу, включаючи використання систем ключових показників ефективності, опитувань щодо корпоративної культури, аудитів, аналітики даних, механізмів професійного обміну досвідом та колективних антикорупційних ініціатив. ОЕСР також просуває концепцію активної ролі держав у підтримці колективних антикорупційних заходів, розвитку взаємодії між бізнесом і правоохоронними органами та створенні надійних механізмів повідомлення про корупційні правопорушення для компаній.

Окремий стратегічний блок документа присвячений глобальному розширенню стандартів боротьби з підкупом іноземних посадових осіб. ОЕСР детально описує процеси приєднання України, Індонезії, Таїланду, Маврикію та Саудівської Аравії до Конвенції та Робочої групи з питань хабарництва. У випадку України документ підкреслює, що після проведення попередньої та повної

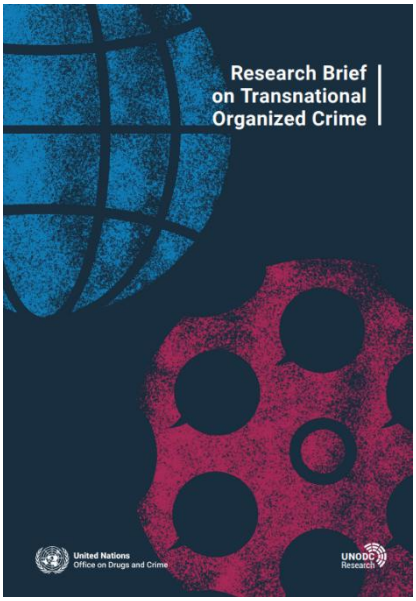
Висновки:

- **Документ демонструє, що глобальна система протидії транснаціональному хабарництву переходить від формального ухвалення законів до моделі активного правозастосування, де ключову роль відіграють реальні розслідування, корпоративна відповідальність, міжнародна співпраця та ефективність санкцій.** Державам необхідно інвестувати насамперед у спеціалізовані правоохоронні спроможності та міжвідомчу координацію.
- **ОЕСР показує, що навіть розвинені держави часто мають слабкі результати у сфері протидії підкупу іноземних посадових осіб через дефіцит ресурсів, недостатню оцінку ризиків та слабкі механізми захисту викривачів.** Ефективна система протидії транснаціональній корупції потребує комплексного поєднання комплаєнсу, ПВК-контролю, міжнародної правової допомоги та міжнародної співпраці правоохоронних органів.
- **Документ підкреслює стрімке зростання ролі міжнародних правоохоронних мереж, спільних слідчих груп та транскордонних розслідувань у боротьбі з транснаціональною корупцією.** Є необхідність у активнішій інтеграції правоохоронних органів у міжнародні антикорупційні механізми.
- **Для України документ має стратегічне значення,** оскільки вступ до Робочої групи ОЕСР з питань хабарництва означає інтеграцію до однієї з найжорсткіших міжнародних систем моніторингу у сфері транснаціональної корупції та відкриває нові можливості для міжнародної правоохоронної співпраці й посилення антикорупційної інфраструктури.

оцінки Робоча група дійшла висновку про відповідність України критеріям приєднання до Конвенції та рекомендувала Раді ОЕСР запросити Україну до Робочої групи. ОЕСР прямо розглядає вступ України як важливий елемент зміцнення глобальної антикорупційної системи та поширення міжнародних стандартів боротьби з підкупом іноземних посадових осіб на нові юрисдикції. Документ також демонструє, що ОЕСР дедалі активніше використовує механізми технічної допомоги, аналіз прогалин у законодавстві та інституційній системі, плани підготовки до приєднання та програми розвитку спроможностей для держав, які прагнуть приєднатися до Конвенції.

Загалом документ демонструє фундаментальну трансформацію сучасної міжнародної антикорупційної архітектури. ОЕСР фактично формує модель інтегрованого транснаціонального антикорупційного врядування, у межах якої кримінальне правозастосування, системи протидії відмиванню коштів, корпоративний комплаєнс, захист викривачів, міжнародна правова допомога, спільні розслідування, механізми забезпечення доброчесності бізнесу та взаємний моніторинг функціонують як єдина взаємопов'язана система. Документ підкреслює, що боротьба з підкупом іноземних посадових осіб дедалі більше інтегрується у ширший контекст міжнародної безпеки, протидії організованій злочинності, незаконним фінансовим потокам та захисту глобальної економічної стабільності. Для України цей звіт має особливе значення, оскільки демонструє інтеграцію держави до однієї з найжорсткіших міжнародних систем взаємного моніторингу у сфері транснаціональної корупції та відкриває нові можливості для міжнародної правоохоронної співпраці, розвитку інституційної спроможності та посилення антикорупційної інфраструктури відповідно до глобальних стандартів ОЕСР.

Глобальна еволюція організованої злочинності: технології, фінансові потоки та захоплення державних інституцій [6]



Документ UNODC, підготовлений до 25-річчя ухвалення Конвенції ООН проти транснаціональної організованої злочинності (UNTOC / Palermo Convention), є комплексним глобальним аналітичним дослідженням сучасної еволюції транснаціональної організованої злочинності, її структурних трансформацій, моделей функціонування, економічних механізмів, форм насильства, використання цифрових технологій та впливу на міжнародну безпеку, державне управління, економічний розвиток і верховенство права. Документ базується на багаторічних дослідженнях UNODC, польових матеріалах, глобальній статистиці, практичних кейсах, аналітичних оцінках та інформації, отриманій від держав-членів ООН. Автори наголошують, що сучасна організована злочинність більше не може розглядатися виключно як діяльність окремих кримінальних угруповань, пов'язаних із наркотрафіком чи контрабандою. Натомість вона трансформувалася у складну транснаціональну екосистему, яка інтегрується у легальну економіку, використовує міжнародні фінансові системи, логістичні ланцюги, цифрові платформи, корупцію, слабкість державних інституцій та глобалізацію для розширення власного впливу й отримання прибутків.

[6] https://www.unodc.org/documents/data-and-analysis/tocta/Brief_2026/Transnational_Organized_Crime_Brief_2026.pdf

У вступній частині документа підкреслюється, що, попри широке міжнародне приєднання до Palermo Convention та розвиток міжнародних механізмів співпраці, транснаціональна організована злочинність залишається одним із ключових глобальних викликів безпеці. Організовані злочинні групи системно використовують відмінності між національними правовими системами, прогалини у міжнародному співробітництві, нерівномірний рівень розвитку державних інституцій, корупцію та швидкий розвиток цифрового середовища для здійснення транскордонної діяльності. Документ наголошує, що сучасна організована злочинність дедалі частіше має гібридний характер, коли одна й та сама кримінальна мережа може бути одночасно залучена до наркотрафіку, торгівлі людьми, незаконного обігу зброї, екологічної злочинності, кіберзлочинності, фінансового шахрайства, незаконного видобутку корисних копалин та відмивання коштів через легальні бізнес-структури. Автори підкреслюють, що сучасні кримінальні екосистеми характеризуються високим рівнем гнучкості, децентралізації та здатності швидко адаптуватися до змін міжнародного середовища, що суттєво ускладнює їх виявлення та традиційні правоохоронні підходи до протидії.

Однією з центральних тем документа є аналіз масштабів шкоди, яку спричиняє організована злочинність. UNODC зазначає, що з моменту ухвалення UNTOC у 2000 році організована злочинність щороку була відповідальною приблизно за 95 тисяч умисних убивств — фактично стільки ж, скільки збройні конфлікти у світі за аналогічний період. Водночас автори наголошують, що насильство є лише найбільш видимою частиною значно ширшої системи негативного впливу організованої злочинності. Документ демонструє, що діяльність організованих злочинних груп підриває державне управління, руйнує верховенство права, дестабілізує фінансові системи, сприяє поширенню корупції, підриває демократичні процеси та створює довгострокові ризики для економічного розвитку. Особлива увага приділяється тому, що значна частина шкоди організованої злочинності залишається статистично невидимою через прихований характер багатьох кримінальних операцій, використання легальних бізнес-структур та складність ідентифікації зв'язків між кримінальними та законними секторами економіки.

Документ детально аналізує проблему класифікації сучасної організованої злочинності. Автори наголошують, що класичні уявлення про мафіозні структури вже не відображають реальну природу сучасних організованих злочинних мереж. У сучасних кримінальних екосистемах можуть одночасно брати участь вуличні банди, кіберзлочинні мережі, терористичні організації, озброєні угруповання, легальні компанії, логістичні оператори, професійні посередники, рекрутингові агентства, фінансові консультанти, корумповані державні службовці та політики. Особливо важливим є висновок документа про поступове стирання межі між легальною та нелегальною економікою. У багатьох секторах організована злочинність функціонує не поза законною економікою, а всередині неї, використовуючи легальні компанії як інструмент інтеграції незаконних доходів у фінансову систему та приховування кримінальної діяльності. У сфері екологічної злочинності законні компанії можуть переходити до незаконної вирубки лісу або нелегального видобутку ресурсів через корупційні механізми чи порушення ліцензійних умов. У сфері торгівлі людьми легальні агентства з працевлаштування можуть використовуватися як прикриття для трудової експлуатації, тоді як у сфері онлайн-гемблінгу формально законні платформи фактично перетворюються на інструменти масштабного відмивання коштів та кіберзлочинної діяльності.

UNODC також пропонує концептуальне розмежування між організованими злочинними групами, орієнтованими на кримінальне врядування, та групами, орієнтованими на здійснення кримінальних транзакцій. Перший тип організованих злочинних груп зосереджується на територіальному контролі, встановленні альтернативних правил, використанні насильства, корупції та системного контролю над локальними ринками й населенням. Такі структури зазвичай мають ієрархічну модель управління, внутрішні правила, репутацію жорстокості та

здатність до проникнення у державні інституції. Натомість групи, орієнтовані на здійснення прибуткових кримінальних операцій, зосереджуються передусім на отриманні доходів від незаконних транзакцій, характеризуються більш гнучкою мережею зв'язків, менш жорсткою організаційною структурою та нижчим рівнем прямого територіального контролю. Документ підкреслює, що сучасні організовані злочинні угруповання можуть поєднувати обидві моделі та еволюціонувати від гнучких кримінальних мереж до квазідержавних структур, здатних здійснювати кримінальне врядування.

Центральне місце у дослідженні займає концепція кримінального врядування, яку автори визначають як здатність організованих злочинних груп встановлювати та забезпечувати виконання альтернативних правил замість державних через насильство, залякування, корупцію, економічний примус, вибіркове надання послуг та маніпулювання ринками. Документ наголошує, що кримінальне врядування є одним із найбільш небезпечних проявів сучасної організованої злочинності, оскільки фактично підміняє функції держави. На територіях, контрольованих організованими злочинними групами (ОЗУ), ОЗУ можуть забезпечувати «безпеку», вирішувати спори, контролювати доступ до економічних ресурсів, регулювати локальні ринки та впливати на повсякденне життя населення. Автори підкреслюють, що кримінальне врядування функціонує не лише через страх, а й через формування певної соціальної легітимності. ОЗУ можуть надавати місцевому населенню економічні можливості, робочі місця, захист від дрібної злочинності або доступ до нелегальних ринків, формуючи тим самим залежність громад від кримінальних структур та підриваючи легітимність державних інституцій.

Документ детально аналізує приклад Гаїті, де ОЗУ фактично контролюють значну частину столиці та ключові логістичні вузли держави. Контроль над портами, транспортними маршрутами та ланцюгами постачання використовується як інструмент політичного й економічного тиску на державні інституції. Водночас дослідження демонструє, що навіть держави з високим рівнем інституційної спроможності не є повністю захищеними від кримінального врядування. Як приклад наводиться Швеція, де організовані злочинні групи формують так звані «паралельні структури», контролюють локальні ринки наркотиків та створюють атмосферу страху, яка руйнує співпрацю населення з правоохоронними органами. Автори наголошують, що кримінальне врядування дедалі частіше стає системною моделлю діяльності організованої злочинності, а не окремим винятком, характерним лише для нестабільних держав.

Велика частина документа присвячена економічному виміру транснаціональної організованої злочинності. Автори наголошують, що наркотрафік залишається фінансовою основою більшості транснаціональних організованих злочинних груп та генерує сотні мільярдів доларів щороку. Прибутки від незаконної торгівлі наркотиками інтегруються у легальну економіку через операції з нерухомістю, міжнародну торгівлю, фінансові системи, логістичні компанії та професійних посередників. Документ підкреслює, що незаконні фінансові потоки не лише підтримують діяльність ОЗУ, а й дозволяють їм здійснювати корупційне захоплення, проникати у державні інституції, фінансувати насильство та контролювати локальні ринки. Значна увага приділяється тому, що організована злочинність системно спотворює функціонування легальних ринків, отримує незаконний доступ до державних контрактів, маніпулює конкуренцією та використовує схеми вимагання для контролю місцевого бізнесу. Автори також наголошують, що незаконні фінансові потоки підривають можливості держав щодо забезпечення сталого розвитку та ефективного використання публічних ресурсів.

Документ детально аналізує явище конвергенції нелегальних ринків, демонструючи, що сучасні організовані злочинні угруповання рідко обмежуються лише одним видом злочинної діяльності. У багатьох регіонах світу наркотрафік, незаконний видобуток корисних копалин, незаконна вирубка лісу, торгівля людьми, злочини проти дикої природи та кібершахрайство

дедалі тісніше переплітаються між собою. У Латинській Америці доходи від кокаїнового бізнесу використовуються для фінансування незаконного видобутку золота, захоплення земель та екологічної злочинності. В окремих країнах Африки озброєні угруповання використовують дитячу працю на золотодобувних об'єктах та інтегрують незаконно видобуті ресурси у міжнародні легальні ринки. Особливу увагу автори приділяють регіону «Золотого трикутника» у Південно-Східній Азії, де слабкі юрисдикції використовуються для створення масштабних шахрайських центрів, у яких жертви торгівлі людьми примушуються здійснювати онлайн-шахрайство в інтересах міжнародних кримінальних мереж.

Окремий великий розділ документа присвячений ролі технологій у трансформації організованої злочинності. Автори наголошують, що цифровізація та глобальна взаємопов'язаність радикально змінили географію злочинності та дозволили організованим злочинним групам масштабувати шахрайство, атаки із застосуванням програм-вимагачів, онлайн-вимагання та кіберзалежне шахрайство на глобальному рівні. Документ підкреслює, що сучасні кіберзлочинні екосистеми функціонують як транснаціональні бізнес-моделі з високим рівнем адаптивності. Значна увага приділяється шахрайським центрам у Південно-Східній Азії, які функціонують як промислові осередки кіберексплуатації та торгівлі людьми. Автори також аналізують використання віртуальних активів для відмивання доходів, отриманих від шахрайства, атак із застосуванням програм-вимагачів та наркотрафіку, а також роль платформ онлайн-гемблінгу та цифрових платіжних систем у формуванні нових каналів незаконних фінансових потоків. Документ наголошує, що розвиток цифрових технологій суттєво ускладнює діяльність правоохоронних органів та потребує нових міжнародних механізмів співробітництва і цифрового регулювання.

Висновки:

- **Документ показує, що транснаціональна організована злочинність перетворилася на систему альтернативного врядування, здатну контролювати території, впливати на державні інституції та проникати у легальну економіку.** Це означає, що протидію ТОЗ необхідно розглядати як питання національної безпеки та інституційної стійкості.
- **UNODC наголошує, що головною силою ОЗУ є фінансові ресурси, які дозволяють їм проникати у легальні ринки, контролювати ланцюги постачання та фінансувати подальшу експансію.** Є необхідність у посиленні фінансових розслідувань, повернення активів та контролю незаконних фінансових потоків.
- **Дослідження підкреслює, що цифрові технології дозволили організованій злочинності діяти через кіберзлочинні екосистеми, віртуальні активи, онлайн-гемблінг та масштабні шахрайські центри.** Це вимагає інтеграції кібербезпеки, механізмів ПВК/ФТ та міжнародної цифрової співпраці.
- **Документ демонструє, що організована злочинність активно використовує конфлікти, слабкі державні інституції та соціальну вразливість населення, поєднуючи торгівлю людьми, контрабанду, незаконний видобуток ресурсів та корупційні мережі.** Це означає, що ефективна протидія ТОЗ потребує не лише силових заходів, а й посилення верховенства права та інституційної спроможності держав.

Суттєва увага приділяється організованій злочинності, що формується та функціонує у пенітенціарному середовищі. Автори демонструють, що пенітенціарні системи дедалі частіше стають не інструментом нейтралізації організованої злочинності, а платформою для її консолідації та координації діяльності. Детально аналізується еволюція Primeiro Comando da Capital (PCC) у Бразилії — від локального тюремного угруповання до однієї з найбільших транснаціональних організацій, залучених до наркотрафіку

у регіоні. Документ підкреслює, що переповненість пенітенціарних установ, корупція, слабке управління пенітенціарною системою та використання цифрових технологій дозволяють організованим злочинним угрупованням координувати міжнародні кримінальні операції навіть із місць позбавлення волі. Аналогічні тенденції фіксуються у країнах Латинської Америки, Східної Європи та Центральної Азії.

У фінальній частині дослідження UNODC переходить до стратегічних наслідків для державної політики та рекомендацій для держав-членів ООН. Автори наголошують, що ефективна протидія транснаціональній організованій злочинності більше не може обмежуватися традиційними правоохоронними підходами. Необхідна комплексна інтегрована модель, яка поєднує кримінальне переслідування, фінансові розслідування, механізми протидії відмиванню коштів та фінансуванню тероризму, антикорупційні інструменти, конфіскацію та повернення активів, кіберстійкість, міжнародний обмін інформацією та посилення державних інституцій. Особливий акцент робиться на необхідності боротьби з кримінальним врядуванням, відновлення державного контролю над територіями, захисту місцевих громад, посилення інституційної стійкості та усунення умов, які дозволяють організованим злочинним угрупованням інтегруватися у соціальну та економічну структуру суспільств. Документ також підкреслює, що Палермська конвенція залишається фундаментальним міжнародним інструментом координації глобальної протидії організованій злочинності, однак сучасні виклики потребують подальшої адаптації міжнародних механізмів співробітництва до цифрової епохи, нових моделей кримінальної економіки та транснаціональних кіберзагроз.

Звіти окремих інституцій та експертів

Ризики ВК/ФТ у готівкових платежах та регулюванні порогових значень [7]

Pinigų plovimo prevencijos kompetencijų centras

Центр компетенцій із протидії відмиванню коштів Литви (AML Centras), що об'єднує представників публічного та приватного секторів, оприлюднив аналітичну позицію щодо ризиків використання готівки в контексті ВК/ФТ і доцільності запровадження порогових значень для готівкових розрахунків у Литві. Документ з'явився у відповідь на активну суспільно-політичну дискусію щодо введення обмежень на готівкові платежі — тему, що набула особливої актуальності у зв'язку з імплементацією нового пакету AML-законодавства ЄС (Регламент (ЄС) 2024/1624, AMLR). AML Centras позиціонує цей документ як первинну аналітику та рекомендаційний документ, що базується на міжнародному досвіді та висновках FATF, одночасно беззастережно визнаючи право фізичних осіб на приватність і свободу вибору платіжного інструменту.

Центральною методологічною основою документа є аналіз специфічних характеристик готівки, що роблять її привабливою для злочинців: анонімність (відсутність аудиторського сліду), висока ліквідність і унікальна здатність служити посередником у транзакціях між правопорушником і жертвою або постачальником послуг. Зокрема зазначається, що предикатні злочини — торгівля наркотиками, торгівля людьми та інша заборонена діяльність — генерують доходи переважно у вигляді готівки, яка стає початковим матеріалом для класичної стадії розміщення (placement) у традиційній схемі відмивання. Операції з готівкою не залишають електронного сліду, що суттєво ускладнює встановлення джерела коштів, реального власника та маршруту їхнього руху — для правоохоронних органів, підрозділів фінансової розвідки та суб'єктів фінансового

[7] https://amlcenter.lt/wp-content/uploads/2026/05/AML-Centro-nuomone-del-grynuju-pinigu.pdf

моніторингу однаково. Як конкретний приклад масштабної схеми AML Centras наводить операцію «Eureka» 2023 року: синдикат 'Ndrangheta відмивав доходи від наркоторгівлі через ресторани у Франції та автомийки у Німеччині, застосовуючи готівкові розрахунки і систему хавала для міжнародних переказів.

У регуляторному контексті AML Centras аналізує вади підходу, закладеного у П'ятій AML-директиві ЄС (2015/849): включення торговців товарами до підзвітних суб'єктів при перевищенні порогу в 10 000 євро за готівкові платежі виявилось неефективним механізмом, оскільки такі суб'єкти — найчастіше торгівці люксовими товарами або будівельними матеріалами — не мали достатніх ресурсів, знань і систем для належного виконання зобов'язань із ВК/ФТ. Ілюстрацією цієї тези є нещодавня угода нідерландського підрозділу Louis Vuitton із правоохоронними органами на суму 500 000 євро за непроведення заходів ПВК/ФТ, унаслідок чого один клієнт витратив близько 2 млн євро нелегального готівкового походження на придбання люксових товарів з їхнім подальшим вивезенням до Китаю (2021–2023 рр.). Новий Регламент (ЄС) 2024/1624 запроваджує загальноєвропейський поріг у 10 000 євро, водночас надаючи державам-членам право встановлювати нижчі обмеження з урахуванням національного профілю ризиків.

AML Centras аналізує литовський контекст через призму Національного оцінювання ризиків (НОР) 2019–2022 рр., яке зафіксувало, що порівняно з середнім показником 27 держав-членів ЄС Литва характеризується значною тіньовою економікою. Загальний рівень ризику ВК/ФТ у контексті використання гоптівки кваліфікується як «великий» (2,8 з 4 за шкалою НОР), що безпосередньо свідчить про необхідність посилених превентивних заходів. AML Centras наголошує, що поріг у 10 000 євро є скоріше компромісом на рівні ЄС, аніж універсальним ризик-орієнтованим стандартом: розмір порогу сам по собі не усуває ризики, а лише виступає одним з елементів системи попередження ВК/ФТ. Відповідно до принципу пропорційності, закладеного у новому AMLR, держави-члени з вищим профілем ризику повинні застосовувати нижчі порогові

Висновки:

- **Позиція AML Centras формує аргументоване підґрунтя для законодавчого пониження порогового значення готівкових операцій нижче загальноєвропейського мінімуму у 10 000 євро**: правове підґрунтя для цього прямо передбачене Регламентом (ЄС) 2024/1624, а литовський НОР з оцінкою ризику 2,8/4 є достатнім обґрунтуванням для прийняття жорсткіших заходів на національному рівні.
- **Гібридні схеми «готівка–криптовалюта» вимагають від СПФМ адаптації систем транзакційного моніторингу для виявлення поведінкових патернів, що свідчать про конвертацію готівкових коштів у криптоактиви** через OTC-посередників або P2P-майданчики; окремі сценарії для cash-to-crypto є необхідним елементом сучасної системи моніторингу.
- **Практичні виклики для суб'єктів із числа торговців дорогими товарами, задокументовані на прикладі кейсу Louis Vuitton у Нідерландах, свідчать про системну неефективність покладення обов'язків з ВК/ФТ на нефінансові суб'єкти без достатнього регуляторного нагляду** та галузевого навчання; підвищена наглядова увага до сектору дорогих товарів і предметів розкоші є закономірним наслідком новел AMLR.
- **Принцип пропорційності між обмежувальними заходами і розвитком альтернативних платіжних інструментів, обстоюваний AML Centras, є методологічно коректним підходом**: виключно заборонні заходи без зниження транзакційних витрат і підвищення доступності легальних каналів ризикують витіснити платежі в неформальний сектор, не зменшивши реального обсягу тіньових операцій.

значення або посилені заходи контролю — що у випадку Литви AML Centras вважає обґрунтованим і необхідним.

Особливої уваги заслуговує аналіз гібридних схем, що поєднують готівкові операції з криптоактивами — явища, яке FATF визначає як наростаючу типологічну загрозу. AML Centras наводить дані аналітичної компанії Crystal Intelligence: постачальники послуг обміну готівки на криптовалюту (cash-to-crypto OTC-платформи) у Гонконзі обробили у 2024 році транзакції на суму понад 2,5 млрд дол. США. FATF у своїй доповіді фіксує, що злочинці — насамперед наркоторговці, учасники схем ФТ і кіберзлочинці — активно застосовують стейблкоїни та інші криптоактиви паралельно із традиційними методами, включаючи готівку. Такий гібридний modus operandi перетворює готівку з ізольованого інструменту на інтегральну ланку складніших багатоетапних схем відмивання, де криптоактиви виконують роль проміжного шару анонімізації між готівковою фазою розміщення та кінцевою фазою інтеграції.

У блоці рекомендацій AML Centras обстоює два взаємодоповнюючі підходи. Перший — фінансова інклюзія: розширення доступу до офіційних фінансових послуг (платіжні рахунки, інструменти електронних платежів) скорочує стимули до використання неформальних розрахункових каналів, підвищує прозорість транзакцій та обмежує можливості для введення нелегальних коштів у законний обіг. Другий — обмеження великих готівкових операцій: пропорційні та таргетовані заходи не зачіпають масиву щоденних дрібних платежів, але суттєво ускладнюють легалізацію значних незаконних сум через систему дорогих товарів тривалого користування, нерухомість і предмети розкоші. AML Centras підкреслює, що поріг у 10 000 євро є прийнятним мінімумом, однак Литва, з огляду на специфіку свого профілю ризику, повинна розглянути встановлення нижчого порогового значення, поєднаного з фінансовою інклюзією та розбудовою альтернативних безпечних платіжних систем.

Когнітивний удар: Як росія руйнує Європу зсередини [8]

Нещодавно оприлюднений масив внутрішніх документів, отриманих журналістами Delfi Estonia та переданих OCCRP, Le Monde, Dossier, Profil та іншим міжнародним медіа, є, без перебільшення, однією з найбільш вичерпних доказових баз російських гібридних операцій за останнє десятиліття. На відміну від попередніх витоків, які часто містили лише фрагменти листувань або непрямі свідчення, цей архів — кілька десятків файлів із внутрішніми звітами, планами операцій, скріншотами робочих чатів і навіть фотографіями підготовки провокацій — дозволяє буквально покроково відстежити логіку, методи та цілі так званих «когнітивних ударів», які росія завдає по країнах Заходу. Головний герой цього розслідування — компанія Social Design Agency (SDA), яка, попри офіційний статус приватної фірми, вже давно діє як структурний підрозділ Адміністрації президента росії під прямим контролем першого заступника керівника адміністрації Сергія Кириєнка. Саме в його кабінеті, як свідчать внутрішні нотатки з нарад, затверджуються найсміливіші та найкривавіші операції.

Найяскравішим і найбільш резонансним епізодом, детально описаним у документах, стала серія нападів на мечеті та ісламські культурні центри в Парижі та його передмістях у вересні 2025 року. Документ під назвою «Звіт про операцію "Свиняча голова"» містить не просто сухі рядки звіту, а справжній оперативний щоденник. Згідно з ним, загін із шести осіб прибув до французької столиці 7 вересня. Наступного дня, 8 вересня, проведено ретельну розвідку

[8] https://www.occrp.org/en/investigation/leaked-documents-reveal-russian-cognitive-strikes-against-the-west-including-islamophobic-pig-head-attacks-in-paris

місцевості біля кожної цілі. Лише в ніч на 9 вересня оперативники вийшли на фінальну фазу: розклали біля дверей дев'яти мечетей свинячі голови, рясно залиті бутафорською кров'ю та помічені прізвищем французького президента Емманюеля Макрона. А потім, як з гордістю зазначає звіт, «успішно залишили країну». Але найціннішим для дослідників є не стільки опис перебігу самої акції, скільки психологічна рамка, в яку її поміщають самі організатори. У звіті додається довжелезний перелік публікацій у французьких, англійських та російських засобах масової інформації, які висвітлили цей інцидент. Це свідчить про парадоксальну, але цілком раціональну логіку: сам злочин — лише засіб, а справжньою метою є медійний резонанс. Чим більше обурення, чим більше публікацій, чим гостріше суспільна дискусія — тим успішнішою вважається операція.

Однак паризькі мечеті стали лише однією з багатьох мішеней. Витік документів містить детальну інформацію про операцію, яку внутрішньо назвали «Зелені синагоги». У травні 2025 року паризький Музей Голокосту та кілька синагог були залиті яскраво-зеленою фарбою, а біля Бранденбурзьких воріт у Берліні, за кількасот метрів від меморіалу Голокосту, зловмисники залишили пластикові скелети. Лише завдяки вироку сербського суду, який засудив тих самих трьох громадян Сербії, що й у справі зі свинячими головами, стало відомо, що ці дві серії нападів є частиною єдиного задуму. Але внутрішнє листування, знайдене в файлах, додає до цієї картини справжню ідеологічну основу. Один із учасників чату, який використовує красномовний псевдонім «Едвард Бернейс» — прямий натяк на австро-американського піонера сучасної пропаганди Едварда Бернейса — в розмові зі старшою співробітницею адміністрації Софією Захаровою (вона ж «Крістін Кілер» у чаті) пише: «Мета акції — дискредитувати французьку владу, яка виявилася неспроможною зупинити хвилю ісламського антисемітизму в Парижі. Удар по іміджу Макрона, який дозволив собі критикувати Ізраїль». Таким чином, провокація працює одразу на кількох рівнях: вона розпалює ворожнечу між мусульманською та єврейською громадами, водночас підриває довіру до французького уряду, а також використовує близькосхідний конфлікт для розхитування єдності західних союзників.

Експерти, опитані журналістами, називають це «шаблоном небезпечної ескалації». Кремль намагається штучно створювати та загострювати конфлікти між різними групами всередині європейських суспільств — між прихильниками правих і лівих, між корінними мешканцями та мігрантами, між релігійними громадами. Особливу тривогу викликає те, що ці операції не обов'язково мають миттєвий ефект. Як зазначає аналітик європейського центру Hybrid, який попросив про анонімність, «можуть минути роки, перш ніж наслідки стануть повністю видимими, а коли це станеться, відповідати ефективно буде вже запізно». Саме тому так важливо, наголошує він, розкривати та нейтралізовувати ці схеми прямо зараз, поки вони не поширилися ще глибше.

Але географія операцій SDA не обмежується Францією та Німеччиною. У документах містяться плани щодо провокацій, які або не були реалізовані, або пройшли непоміченими для широкої публіки. Наприклад, один із внутрішніх файлів детально описує операцію з осквернення пам'ятника генералу Шарлю де Голлю в Парижі. Згідно з планом, вандали мали залишити на монументі символи, які однозначно асоціювалися б з «українськими націоналістами». Але найцинічнішою деталлю цього плану є вимога щодо самих виконавців: у документі підкреслюється, що учасники акції «не повинні були бути задіяними в попередніх операціях», а головне — вони мають бути «абсолютно впевнені, що діють в інтересах України та виконують замовлення Фонду Олени Зеленської». Тобто російська операція передбачала цілеспрямоване введення в оману власних виконавців — аби ті щиро вірили, що працюють на українську сторону, і в разі арешту давали саме такі свідчення.

Хто ж стоїть за цим механізмом? Документи дозволяють зазирнути всередину самої системи управління. У викрадених чатах учасники використовують вигадані імена — «Алекс Еббот», «Сем Спенсер», а також більш екзотичні «Брюс Лі» та «Іммануїл Кант». Однак за допомогою

додаткових даних журналістам вдалося встановити, що під псевдонімом «Крістін Кілер» (посилання на скандально відому англійську танцівницю Крістін Кілер, чиї зв'язки з радянським аташе спричинили політичну кризу в Британії в 1960-х) ховається реальна посадова особа — Софія Захарова, старша співробітниця Адміністрації президента росії. Захарова потрапила під санкції Європейського Союзу ще в 2024 році за її роботу з SDA. В одному з чатів вона пише колегам: «Ми чекаємо на зелене світло від СВК». Розшифровка абревіатури в документі однозначно вказує на Сергія Володимировича Кириєнка — першого заступника керівника Адміністрації президента, людину, яка вважається головним архітектором російської політики впливу всередині країни та за кордоном. Таким чином, ланцюг командування простежується безпосередньо: від виконавців на місці через менеджерів SDA до найвищих рівнів кремлівської адміністрації.

Окремий, надзвичайно важливий пласт документів стосується не Європи, а пострадянського простору — зокрема Вірменії. Тут інструментом впливу виступає медіагрупа SNG Media, яка, згідно з презентацією, знайденою у витоку, насправді контролюється SDA. Офіційно SNG Media володіє портфелем із дванадцяти інтернет-ресурсів, націлених на Вірменію, Казахстан, Узбекистан, Таджикистан, Туркменістан, Киргизстан та Каспійський регіон. У документі метою цієї мережі названо «компенсацію втрачених зв'язків між жителями країн пострадянського простору після розпаду СРСР». Однак справжнє призначення стає зрозумілим із наступних файлів.

Напередодні парламентських виборів у Вірменії, які заплановані на червень 2026 року, SDA підготувала детальний план втручання. Документ під назвою «Вірменські росіяни вирішують» прямо вказує, що значна частка виборців у Вірменії має також російське громадянство, а отже, ця категорія може стати потужним важелем впливу на результати. Завдання ресурсу «Yerevan One» (один із майданчиків SNG Media) полягає в тому, щоб формувати негативне ставлення до чинної вірменської влади та особисто прем'єр-міністра Нікола Пашиняна, який узяв курс на зближення з Європою та Сполученими Штатами. Натомість аудиторії прищеплюватимуть «позитивне ставлення до тих, хто виступає за найтісніший союз з росією». Це відбувається на тлі численних попереджень з боку західних аналітиків про те, що москва активно намагається вплинути на вірменські вибори через кібератаки, пропаганду, інформаційні маніпуляції та нелегальні фінансові потоки.

Але найкраще технологію цих «когнітивних ударів» демонструють кейси з поширення фейкових новин про перших осіб. Один із документів, що має назву «Медіа-кейс Марсель», детально описує кампанію з дезінформації, згідно з якою Нікол Пашинян нібито придбав розкішну віллу в Марселі. У звіті не просто констатується факт запуску цієї брехні, а наводиться детальна аналітика реакції місцевих медіа, підрахунок переглядів (понад 10 мільйонів у всьому світі) та навіть визнання того факту, що згодом з'явилися спростування. Інший проектний файл описує поширення не менш відомої фальшивки про президента України Володимира Зеленського: нібито він придбав для своєї матері квартиру в хмарочосі Бурдж-Халіфа в Дубаї. Ця історія, згідно з внутрішнім звітом, досягла понад 86 мільйонів переглядів по всьому світу, перш ніж була спростована. Що важливо, автори документів з холодним професіоналізмом фіксують навіть публікації фактчекінгів — для них це просто ще один параметр ефективності, адже навіть спростована брехня встигає закріпитися в свідомості частини аудиторії.

Окремої уваги заслуговує ще один напрям роботи SDA — спроби впливати на західну громадську думку через так званих «лідерів думок», зокрема відставних високопосадовців і генералітет. У листуванні Софії Захарової з колегою, який використовує псевдонім «Карен Хорні» (ім'я відомого психоаналітика), обговорюється підготовка заяв для французьких та американських генералів. У квітні 2025 року російське державне інформагентство ТАСС дійсно опублікувало інтерв'ю з колишнім французьким генералом Домініком Делавардом, у якому той передбачив, що війна в Україні завершиться «на російських умовах» до кінця 2025 року. Генерал

помер за місяць після цього інтерв'ю. У тому ж чаті обговорюється фігура Пола Веллі, відставного американського генерал-майора, якого характеризують як людину, близьку до Дональда Трампа. І справді, в березні 2025 року ТАСС процитувало інтерв'ю Веллі, яке вийшло на ізраїльській регіональній радіостанції Galey Israel, де генерал пророкував «швидку зміну влади в Україні та потепління відносин між росією та Заходом».

Висновки:

- **Пряме управління з Кремля.** Операції SDA координувалися безпосередньо Адміністрацією президента рф, зокрема першим заступником керівника адміністрації Сергієм Кириєнком.
- **Метод «подвійного дна» провокацій.** Кремль використовує атаки для одночасного розпалювання конфліктів між різними групами та дискредитації місцевої влади. Виконавців навмисно вводили в оману, змушуючи вірити, що вони працюють на Україну або інші треті сторони.
- **Інструмент для розділення Європи.** Документи містять плани щодо руйнування Вишеградської групи та створення проросійського альянсу Австрії, Угорщини та Словаччини, що свідчить про системну стратегію послаблення ЄС зсередини.
- **Еволюція ШІ.** Росія переходить від ручних «фабрик тролів» до автоматизованих систем: у 2026 році запущено ШІ-бази знань на 200 тис. сторінок для Німеччини та мережі з сотень відео, згенерованих нейромережами, для маніпуляції суспільною думкою.

Один із файлів має назву «Проекти 2026» і перелічує вісім ініціатив, деякі з яких уже частково запущені. Серед них — створення інтернет-ресурсу для впливу на західні аналітичні центри (think tanks), який уже працює англійською та планується німецькою, французькою та іспанською мовами. Скріншот показує сайт World Center for Strategic Studies, зареєстрований 30 березня 2026 року, який публікує аналітичні статті без зазначення авторів — це унеможливлює відстеження справжніх джерел. Інший проект — «самозаповнювана база знань на основі штучного інтелекту», націлена на Німеччину, де вже запущено сервери, а база даних містить понад 200 тисяч сторінок. Також планується «база даних лідерів думок» для моніторингу майже 10 тисяч акаунтів у соціальних мережах, «трекер думок» для 100 найвпливовіших французьких опозиційних лідерів, а також мережа з трьох проектів на шести соціальних платформах, які генеруватимуть сотні відео за допомогою нейромереж. Це вже не просто «фабрика тролів» з написаними вручну коментарями, а повноцінна автоматизована пропагандистська машина, здатна працювати масштабовано й безперервно.

Нарешті, документи містять плани геополітичного переформатування самої Європи. Проект під назвою «Mitteleuropa» (Середня Європа) пропонує встановити тісні політичні та економічні зв'язки між країнами та територіями, які колись входили до Австро-Угорської імперії — насамперед між Австрією, Угорщиною та Словаччиною. Довгострокова мета — створення «єдиного, сильного, незалежного гравця», який зміг би протистояти Брюсселю. При цьому завданням-мінімум є «демонтаж Вишеградської групи (Польща, Чехія, Угорщина, Словаччина)» та заміна її на «Віденську угоду» (Австрія, Угорщина, Словаччина). У документах також згадується про наміри впливати на вибори в Угорщині та Словенії, які відбулися минулого місяця.

Таким чином, «когнітивні удари» SDA є не хаотичною серією акцій, а складовою системної геополітичної стратегії, спрямованої на послаблення Європейського Союзу та руйнування трансатлантичної єдності.

Майбутнє цифрових активів: як токенізація змінює глобальну фінансову систему [9]

Документ є масштабним стратегічним дослідженням, яке аналізує трансформацію глобальної фінансової системи під впливом цифрових активів, токенізації та технологія розподіленого реєстру (DLT). Автори фактично розглядають цифрові активи не як тимчасовий технологічний тренд або окремий сегмент криптовалютного ринку, а як фундаментальну інфраструктурну зміну, здатну перебудувати архітектуру грошей, платежів, ринків капіталу, банківського посередництва та глобальної фінансової інфраструктури. Документ наголошує, що для фінансових установ головним викликом стає не питання «чи брати участь у цифрових активах», а питання того, яким чином зберегти стратегічну релевантність у світі програмованих фінансів, де гроші, активи, розрахунки, управління заставою та корпоративні дії стають токенізованими, автоматизованими та функціонують у режимі безперервних фінансових ринків. Boston Consulting Group (BCG) підкреслює, що банки, регулятори та центральні банки повинні перестати сприймати цифрові активи як сферу виключно інноваційних лабораторій або фінтех-пілотів, оскільки йдеться про довгострокову трансформацію всієї фінансової системи, яка поступово переходить до моделі програмованих фінансових інфраструктур.

Документ формує детальну типологію цифрових активів та поділяє їх на три великі категорії: цифрові гроші, цифрові реальні активи (RWAs) та криптоактиви. Категорія цифрових грошей охоплює стейблкоїни, токенізовані депозити і цифрові валюти центральних банків (CBDCs). Автори наголошують, що хоча ці форми цифрових грошей можуть виглядати подібно з точки зору користувача, вони принципово відрізняються за моделями емісії, структурами управління, механізмами розподілу ризиків та регуляторним режимом. Стейблкоїни описуються як приватні цифрові інструменти, подібні до інструментів на пред'явника, здебільшого прив'язані до фіатних валют, які функціонують як цифрові аналоги готівки та активно використовуються у криптовалютній екосистемі, міжнародних платежах і розрахункових операціях. Наприкінці 2025 року ринок стейблкоїнів досяг приблизно 300 млрд доларів, причому основна частка припадає на стейблкоїни, номіновані у доларах США, таких емітентів як Tether та Circle. Водночас токенізовані депозити розглядаються як цифрові форми банківських депозитів у межах існуючої банківської системи, що дозволяють поєднати програмованість та розрахунки у блокчейн-мережі із пруденційними гарантіями традиційного банкінгу. CBDCs, у свою чергу, визначаються як цифрові зобов'язання центральних банків, покликані модернізувати платіжну інфраструктуру та зберегти державний контроль над грошовою системою. Автори наголошують, що хоча CBDCs перебувають на відносно ранньому етапі розвитку, їхнє стратегічне значення для майбутньої монетарної системи є надзвичайно високим.

Окремий великий блок документа присвячений RWAs, які BCG розглядає як найбільш стратегічно важливий напрямок для майбутньої трансформації банківського сектору та ринків капіталу. Автори пояснюють, що токенізовані RWAs є цифровими представленнями традиційних активів із юридично забезпеченими правами вимоги на базові активи. До цієї категорії належать токенізовані цінні папери, токенізовані товари та токенізовані альтернативні активи, включаючи включаючи прямі інвестиції у приватний капітал, приватне кредитування, інфраструктурні активи та нерухомість. Хоча обсяг токенізованих RWAs наприкінці 2025 року оцінюється лише приблизно у 30 млрд доларів, документ наголошує, що саме цей сегмент має найбільший

[9] https://web-assets.bcg.com/a3/89/c007b26e4eb1b57f6ba70d657f5b/the-future-of-digital-assets-may2026-1.pdf

довгостроковий трансформаційний потенціал для фінансової системи. Автори демонструють, що токенізація здатна радикально змінити процеси емісії активів, розрахунків, зберігання активів, управління заставою, ринки репо, дистрибуцію фондів та обслуговування активів. Особливо підкреслюється значення атомарних розрахунків за принципом «поставка проти платежу», які дозволяють синхронізувати передачу активів і коштів практично миттєво, знижуючи ризик розрахунків, вимоги до маржі та операційну фрагментацію й неефективність. BCG прогнозує, що у сценарії активного розвитку цифрових активів до 2035 року токенізовані RWAs можуть охопити приблизно 16% глобальних інвестиційних активів, що означатиме фундаментальну перебудову інфраструктури ринків капіталу.

У частині, присвяченій криптоактивам, документ підкреслює, що криптоактиви залишаються найбільшою категорією цифрових активів із ринковою капіталізацією близько 3 трлн доларів наприкінці 2025 року. Bitcoin та Ethereum домінують на цьому ринку, формуючи основну частину глобальної капіталізації криптовалютного ринку. Водночас BCG наголошує, що кпиптоактиви мають принципово іншу економічну природу порівняно з цифровими грошима або токенізованими RWAs, оскільки не є правами вимоги на фіатні гроші, зобов'язаннями ідентифікованих емітентів чи цифровими представленнями реальних активів. Вартість криптоактивів визначається дефіцитністю, корисністю протоколу, мережевими ефектами та довірою інвесторів, а не грошовими потоками. Автори зазначають, що криптовалютний сектор уже формує значний пул доходів у сферах трейдингу, деривативів, кастодіальних послуг, стейкінгу та комплексні інвестиційно-брокерські послуги, але водночас підкреслюють, що криптоактиви не є основною трансформаційною історією для банків. На думку BCG, стратегічне значення має не стільки криптовалютний трейдинг, скільки боротьба за контроль над майбутньою інфраструктурою руху коштів, розрахунків, цифрового зберігання активів та програмованих фінансів.

Документ детально аналізує ключові економічні переваги цифрових активів та інфраструктури на базі технології розподіленого реєстру. Серед головних переваг виділяються майже миттєві розрахунки, підвищення ефективності управління балансом і заставою, програмованість, автоматизація, глобальне охоплення та ефективність дистрибуції. Автори наголошують, що токенізація дозволяє інтегрувати бізнес-правила безпосередньо в активи та платежі, автоматизуючи корпоративні дії, умовні платежі, маржинальні вимоги та комплаєнс-перевірки. Значна увага приділяється транскордонному управлінню ліквідністю та казначейськими операціями, програмованій ліквідності та мобільності застави, які можуть суттєво змінити міжнародні платежі, валютні ринки і казначейські операції. Особливо важливо, що BCG підкреслює потенціал цифрових активів у зниженні операційної фрагментації та неефективності, скороченні потреби у посередниках та прискоренні обороту капіталу. Водночас документ наголошує, що цифрові активи створюють не лише нові можливості, але й фундаментальні системні конфлікти щодо майбутньої архітектури фінансової системи.

Одна з центральних частин дослідження присвячена аналізу системних структурних суперечностей, які цифрові активи створюють для сучасної фінансової системи. BCG підкреслює, що ключове питання полягає у тому, чи є технологія розподіленого реєстру (DLT) лише більш ефективним інфраструктурним рівнем для існуючої фінансової системи, чи вона формує основу для принципово нової фінансової архітектури. Документ аналізує конфлікт між демократизацією фінансів на основі програмного коду та інституційною довірою, проблеми сумісності різних систем і регуляторної фрагментації, ризики концентрації залежностей від фінансової інфраструктури, а також потенційні загрози для фінансової стабільності, які виникають через програмовані фінансові ринки, що функціонують у режимі 24/7. Особлива увага приділяється ризику дезінтермедіації для банківської системи у випадку масштабного переходу залишків коштів у стейблкоїни та токенізовані гроші. Автори зазначають, що стейблкоїни фактично відроджують концепцію вузького банкінгу або повністю резервованих

грошей, що може створювати ризики для традиційної моделі банківського кредитування через скорочення депозитної бази та переміщення ліквідності за межі традиційної банківської системи. У цьому контексті документ активно аналізує дискусію між Банком міжнародних розрахунків та прихильниками децентралізованих фінансів (DeFi) щодо майбутньої архітектури грошей, сумісності фінансових систем та ролі державних і приватних інфраструктур у цифровій фінансовій системі.

Важливе місце у документі займає сценарний аналіз розвитку цифрової фінансової системи. BCG пропонує чотири базові сценарії: приватно-орієнтоване цифрове розширення, фрагментована багатотрекова система, інституційна цифрова еволюція та сценарій обмеження і захисного відкату. У сценарії приватно-орієнтованого цифрового розширення домінуючу роль відіграють стейблкоїни та приватні платформи, що можуть призвести до масштабної дезінтермедіації банків (процес зменшення ролі банків як традиційних фінансових посередників у фінансовій системі). Сценарій фрагментованої багатотрекової системи передбачає розвиток цифрових активів у межах несумісних між собою регуляторних і технологічних екосистем. Інституційна цифрова еволюція описує модель, у якій токенізація відбувається під контролем великих банків, інфраструктур центральних банків та регульованих фінансових установ. Нарешті, сценарій обмеження і захисного відкату передбачає регуляторний спротив або системну кризу, які значно сповільнять поширення цифрових активів. Документ наголошує, що банки не повинні робити ставку лише на один сценарій, а мають формувати стратегічну гнучкість і здатність адаптації для функціонування у різних моделях майбутнього фінансового ринку.

Одним із найбільш важливих аспектів дослідження є оцінка потенційного впливу цифрових активів на банківський сектор. Автори прямо попереджають, що у сценарії швидкого масштабування цифрових активів банки можуть зіткнутися із приблизно 10% скороченням балансових показників,

Висновки:

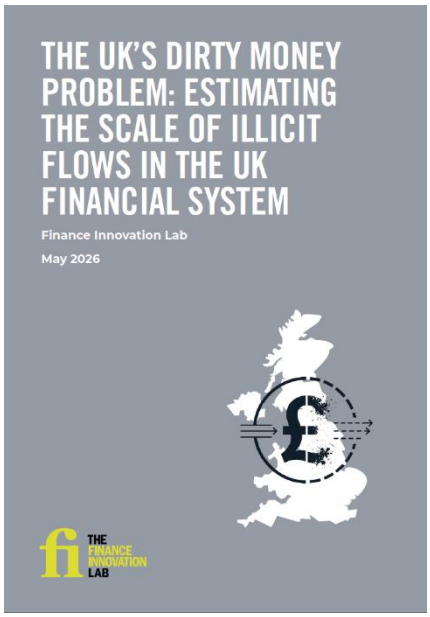
- **Документ демонструє, що цифрові активи більше не є нішевим фінтех-напрямом, а перетворюються на стратегічну трансформацію фінансової системи, здатну змінити моделі платежів, розрахунків, управління заставою та банківського посередництва.** Для банків, центральних банків і регуляторів є необхідність уже зараз формувати довгострокові стратегії у сфері цифрових активів.
- **Дослідження підкреслює, що головна загроза для банків полягає не у криптоактивах як таких, а у втраті контролю над інфраструктурою програмованих грошей, клієнтським інтерфейсом та токенізованими ринками капіталу.** Це означає, що фінансові установи повинні інвестувати у цифрові гаманці, кастодіальні сервіси, токенізовані депозити та інструменти ПВК/санкційного контролю.
- **Автори доводять, що токенізовані реальні активи можуть стати найбільш трансформаційним елементом цифрових фінансів, оскільки токенізація здатна перебудувати процеси емісії, розрахунків, операцій репо, управління заставою та обслуговування активів.** Це вимагає адаптації правових рамок, розрахункової інфраструктури та наглядових моделей до токенізованих ринків капіталу.
- **Документ показує, що програмовані фінансові ринки, які працюють у режимі 24/7, створюють нові системні ризики, включаючи ризики концентрації, вразливості смартконтрактів та залежність від DLT- і хмарної інфраструктури.** Це означає необхідність переходу до нової моделі технологічного та операційного нагляду, де контроль інтегрується безпосередньо у цифрову фінансову інфраструктуру.

14% зниженням доходів та майже 30% падінням прибутків до 2035 року у порівнянні зі сценарієм без широкомасштабної токенізації. Основними драйверами цього процесу називаються зменшення ролі фінансових посередників, перерозподіл вартості та доходів на користь небанківських фінансових установ, скорочення прибутковості традиційного зниження економічної ефективності та прибутковості традиційних післяторговельних процесів та необхідність фінансування паралельного функціонування традиційної і цифрової інфраструктури. Водночас BCG наголошує, що цифрові активи створюють і масштабні можливості для банків, особливо у сферах токенізованих фондів, кастодіальних послуг, цифрового управління ліквідністю та казначейських операцій, транскордонних платежів на базі стейблкоїнів, цифрового управління заставою та криптовалютних сервісів. Документ наводить оцінки, згідно з якими великі глобальні банки можуть отримати сотні мільйонів або навіть мільярди доларів додаткових доходів завдяки новим бізнес-моделям у сфері цифрових активів.

Окремий великий розділ документа присвячений управлінню ризиками та наглядовим наслідкам програмованих фінансів. Автори наголошують, що механізми протидії відмиванню коштів (ПВК), санкційного скринінгу та комплаєнс-моніторингу у сфері цифрових активів поступово переходять від моделі, орієнтованої на банківські рахунки, до підходів, орієнтованих на цифрові гаманці та аналіз фінансових потоків. Це означає, що банки більше не можуть обмежуватися перевіркою лише безпосередніх контрагентів, оскільки ризики виникають через взаємопов’язані екосистеми цифрових гаманців, смартконтракти, міжмережеві блокчейн-мости, пули ліквідності та децентралізовані інфраструктури. Документ підкреслює, що смарт-контракти повинні управлятися як моделі високого ризику із постійним тестуванням, безперервним моніторингом та чітко визначеними повноваженнями для втручання. Значна увага приділяється ризикам концентрації, пов’язаним із постачальниками хмарних сервісів, операторами вузлів блокчейн-мережі, постачальниками аналітичних рішень та механізмам забезпечення сумісності між блокчейн-мережами, які можуть перетворитися на нові системні залежності фінансової інфраструктури. BCG наголошує, що у програмованих фінансових ринках, які функціонують у режимі 24/7, ефективність контрольних механізмів стає важливішою за формальні політики та процедури, а здатність забезпечити операційну стійкість, механізми аварійного зупинення операцій та реагування на інциденти у режимі реального часу визначатиме стійкість майбутньої фінансової системи.

У технологічній частині документа BCG закликає банки сприймати DLT не як набір окремих експериментів, а як довгострокову інфраструктурну платформу. Автори рекомендують із самого початку будувати системи з підтримкою кількох блокчейн-мереж, уникати технологічної залежності від однієї блокчейн-екосистеми та централізувати рівень управління і контролю всередині фінансової установи. Документ також детально аналізує стратегії «створювати самостійно — співпрацювати — купувати», наголошуючи, що банки повинні зберігати контроль над управлінням внутрішніми політиками, управлінням криптографічними ключами, управлінням смартконтрактами та реагуванням на інциденти навіть у випадку використання зовнішніх технологічних партнерів. Для пояснення масштабності майбутньої трансформації BCG проводить аналогію з телекомунікаційною революцією переходу від мереж із комутацією каналів до IP-мереж, демонструючи, що фінансова система також тривалий час функціонуватиме у режимі паралельного співіснування двох інфраструктур, де традиційна фінансова інфраструктура та системи на базі технології розподіленого реєстру співіснуватимуть паралельно.

Від офшорів до криптоактивів: як Велика Британія стала ключовим вузлом глобальних незаконних фінансових потоків [10]



Документ є масштабним аналітичним дослідженням, присвяченим оцінці реальних масштабів незаконних фінансових потоків (IFFs) та ширшого явища «незаконних коштів» у фінансовій системі Великої Британії. Документ формує комплексне бачення того, що Велика Британія, попри статус одного з найбільших глобальних фінансових центрів, водночас виступає одним із ключових вузлів міжнародної інфраструктури незаконних фінансових потоків, які охоплюють відмивання коштів, агресивне податкове планування, приховування активів, офшорні схеми, незаконне переміщення капіталу, корупційні кошти, фінансування злочинної діяльності та інші форми незаконних фінансових потоків. Автори наголошують, що глобальна роль Лондона як одного з провідних міжнародних фінансових центрів, високий рівень відкритості британської фінансової системи, її інтегрованість у міжнародні ринки капіталу, а також історичні зв'язки з офшорними юрисдикціями сформували сприятливі умови для функціонування масштабної системи прихованого капіталу.

У центрі дослідження знаходиться концепція незаконних фінансових потоків у розумінні Організації Об'єднаних Націй. Документ пояснює, що IFFs — це фінансові потоки, які є незаконними за походженням, способом переміщення або використання та перетинають державні кордони. При цьому автори підкреслюють, що поняття незаконних фінансових потоків не обмежується лише класичним відмиванням коштів, одержаних злочинним шляхом, а охоплює також окремі форми агресивного податкового планування та комерційних практик, які можуть формально не порушувати законодавство, але фактично сприяють розмиванню податкової бази, приховуванню доходів та виведенню ресурсів із національних економік. Документ детально описує чотири основні категорії діяльності, що генерують незаконні фінансові потоки: незаконні податкові та комерційні практики, незаконні ринки, корупцію, а також експлуатаційні види діяльності й фінансування злочинності та тероризму. Автори наголошують, що незаконні фінансові потоки можуть виникати як на етапі отримання незаконного доходу, так і на етапі подальшого управління такими коштами через інвестування, переміщення активів або їх інтеграцію у легальну економіку.

Документ наголошує, що оцінка масштабів незаконних фінансових потоків є критично важливою не лише для академічного аналізу, а й для формування ефективної державної політики, належного рівня правозастосування, міжнародної координації та управління ризиками у сфері ПВК/ФТ. Автори прямо зазначають, що незаконні фінансові потоки підривають ринкову доброчесність, спотворюють конкуренцію, послаблюють верховенство права, створюють загрози для макроекономічної стабільності та підривають довіру до британських інституцій. Дослідження також пов'язує проблему незаконних фінансових потоків із питаннями національної безпеки та міжнародної репутації Великої Британії, підкреслюючи, що статус глобального фінансового центру створює не лише економічні переваги, але й значні системні вразливості. Автори розглядають Illicit Finance Summit 2026 як унікальну можливість для радикального перегляду британської політики у сфері економічної злочинності та протидії незаконним фінансовим потокам.

[10] https://financeinnovationlab.org/wp-content/uploads/2026/05/Dirty-Money-report_Final-1.pdf

Ключовим результатом дослідження є кількісна оцінка масштабів незаконних фінансових потоків, пов'язаних із Великою Британією. Автори доходять висновку, що обсяг незаконних фінансових потоків, безпосередньо пов'язаних із британською фінансовою системою, у 2025 році становив приблизно 325 млрд фунтів стерлінгів щорічно. Якщо ж до розрахунків включити коронні володіння та британські заморські території, які автори вважають глибоко інтегрованими з лондонським міжнародним фінансовим центром і ширшою фінансовою екосистемою Великої Британії, то загальний обсяг незаконних фінансових потоків зростає майже до 788 млрд фунтів стерлінгів на рік. Документ спеціально наголошує, що ці цифри є консервативними оцінками, а реальні масштаби проблеми можуть бути суттєво більшими через прихований характер незаконних фінансових потоків, обмеженість доступних даних та методологічні труднощі оцінювання. Автори підкреслюють, що навіть за таких обережних оцінок Велика Британія залишається одним із центральних глобальних вузлів міжнародної системи незаконних фінансових потоків.

Найбільшим компонентом незаконних фінансових потоків автори вважають незаконні податкові та комерційні фінансові потоки. Для оцінки цього сегмента використовується методологія Tax Justice Network, зокрема аналіз прихованого переміщення прибутків транснаціональними корпораціями та офшорних активів заможних фізичних осіб. Документ пояснює, що транснаціональні корпорації активно використовують механізми штучного переміщення прибутків, трансфертного ціноутворення, стратегічного розподілу боргових зобов'язань, зловживання міжнародними податковими угодами та інші інструменти агресивного податкового планування для штучного перенесення прибутків до низькоподаткових або закритих юрисдикцій. При цьому наголошується, що такі фінансові потоки часто не пов'язані з реальною економічною діяльністю та створюються виключно з метою мінімізації податкових зобов'язань. У дослідженні детально описується методологія Tax Justice Network, яка ґрунтується на порівнянні задекларованих прибутків транснаціональних корпорацій із фактичною економічною діяльністю шляхом аналізу даних щодо зайнятості та рівня заробітних плат. Документ прямо називає корпоративні податкові зловживання «глобальною економічною проблемою першочергового значення», підкреслюючи їх системний вплив на міжнародну економіку та державні бюджети.

Окремо дослідження аналізує доходи, пов'язані з офшорними активами заможних фізичних осіб. Автори пояснюють, що юрисдикції фінансової секретності дозволяють приховувати інформацію про власників активів, уникати податкових зобов'язань, відмивати кошти та підтримувати функціонування транснаціональних кримінальних мереж. У документі наголошується, що саме інфраструктура офшорної фінансової секретності забезпечує можливість приховування активів від державних органів та створює умови для глобального переміщення незаконного капіталу. Для оцінки масштабів цієї проблеми Tax Justice Network аналізує незадекларовані офшорні активи, використовуючи Financial Secrecy Index та дані Банку міжнародних розрахунків. Особливо важливим є висновок документа про критичну роль британських заморських територій та коронних володінь у глобальній системі офшорної фінансової секретності. Автори прямо називають ці юрисдикції офшорними податковими юрисдикціями, пов'язаними з Великою Британією, та стверджують, що через них проходить значна частина світових незаконних фінансових потоків. За оцінками дослідження, лише приховане переміщення прибутків, пов'язане з британськими заморськими територіями, становить 282,6 млрд фунтів стерлінгів, що значно перевищує аналогічний показник для самої Великої Британії.

Значний блок дослідження присвячений відмиванню коштів як системному елементу глобальної інфраструктури незаконних фінансових потоків. Через відсутність достатньо деталізованих оцінок щодо незаконних ринків, корупції та діяльності, пов'язаної з експлуатацією і фінансуванням злочинності, автори використовують офіційну оцінку

Національного агентства з боротьби зі злочинністю Великої Британії (NCA) як орієнтовний показник для цих категорій. Згідно з оцінками NCA, щонайменше 124 млрд фунтів стерлінгів щорічно відмиваються через британську фінансову систему або корпоративні структури, зареєстровані у Великій Британії. Документ підкреслює, що ця цифра, ймовірно, також суттєво недооцінює реальний масштаб проблеми, оскільки сама NCA визнає, що обсяги відмивання коштів можуть сягати «сотень мільярдів фунтів». Автори наголошують, що статус Великої Британії як глобального центру фінансових та професійних послуг створює особливі вразливості для відмивання коштів, обходу санкцій та інших форм економічної злочинності.

Документ приділяє значну увагу новим ризикам, пов'язаним із розвитком криптоактивів, установ електронних грошей та використанням штучного інтелекту організованою злочинністю. Автори зазначають, що стрімке впровадження нових фінансових технологій суттєво змінило ризиковий профіль Великої Британії після 2020 року. У дослідженні прямо попереджається, що плани уряду перетворити Лондон на глобальний центр криптофінансів можуть значно посилити ризики ВК/ФТ, незаконного переміщення капіталу та іноземного втручання. У цьому контексті згадується заборона пожертв політичним партіям у криптоактивах через складність відстеження таких транзакцій та ризики незаконного впливу на політичні процеси.

Висновки:

- **Документ демонструє, що Велика Британія та пов'язана з нею офшорна система залишаються одним із ключових глобальних центрів незаконних фінансових потоків, а їх обсяг може сягати 788 млрд фунтів стерлінгів щорічно.** Це свідчить про необхідність розглядати ПВК/ФТ як елемент не лише кримінальної, а й економічної та безпекової політики.
- **Дослідження підкреслює, що основну частину незаконних фінансових потоків формують складні податкові та корпоративні схеми, офшорні структури та механізми переміщення прибутків.** Це вимагає посилення прозорості бенефіціарної власності, міжнародної податкової співпраці та контролю за офшорними юрисдикціями.
- **Автори наголошують, що криптоактиви, електронні гроші та використання штучного інтелекту у фінансовій злочинності швидко змінюють ризиковий профіль Великої Британії.** Тобто є необхідність у посиленні регулювання та нагляду за криптовалютним сектором.
- **Документ також вказує на серйозні проблеми якості даних та недостатньої прозорості офіційних оцінок економічної злочинності.** Автори наголошують, що ефективна протидія незаконним фінансовим потокам неможлива без якісних статистичних моделей, прозорих методологій оцінювання та належного міжвідомчого обміну інформацією.

Окремий розділ дослідження присвячений специфічним типологіям відмивання коштів, зокрема відмиванню коштів через торговельні операції (TBML) та відмиванню коштів через операції з нерухомістю. За оцінками NCA, приблизно 10 млрд фунтів стерлінгів щорічно можуть проходити через британські схеми TBML. Документ пояснює, що TBML базується на маскуванні незаконного переміщення коштів під легальні торговельні операції та становить особливу загрозу для глобальної торговельної системи. Не менш важливою є проблема відмивання коштів через ринок нерухомості. За оцінками NCA, до 10 млрд фунтів стерлінгів щорічно можуть відмиватися через британський ринок нерухомості. Автори наголошують, що нерухомість є надзвичайно привабливим інструментом для злочинців через можливість легалізації великих сум коштів, стабільність такого активу та потенціал подальшого отримання доходу через оренду або перепродаж. Документ також звертає увагу на необхідність подальших досліджень

впливу незаконних інвестицій у нерухомість на доступність житла та житловий фонд у Великій Британії.

У другій частині дослідження аналізується ширше явище внутрішніх «незаконних коштів», яке не обов'язково має транскордонний характер. Автори включають до цієї категорії внутрішні податкові зловживання, шахрайство, корупцію, доходи від злочинної діяльності та незаконне кредитування. Документ демонструє, що масштаби внутрішньої економічної злочинності у Великій Британії також є надзвичайно значними. HMRC оцінює внутрішні податкові втрати приблизно у 26 млрд фунтів стерлінгів, тоді як незалежні оцінки Tax Justice Network підвищують цей показник до 42,3 млрд фунтів стерлінгів. Автори критикують HMRC за ймовірне суттєве недооцінювання масштабів ухилення від сплати податків та недостатню методологічну прозорість. За оцінками уряду, шахрайство завдає британському суспільству збитків приблизно на 6,8 млрд фунтів стерлінгів щорічно, а кількість випадків шахрайства продовжує стрімко зростати. Документ також наголошує на відсутності достовірних оцінок щодо корупції та незаконного кредитування, що свідчить про суттєві прогалини у національному розумінні масштабів економічної злочинності.

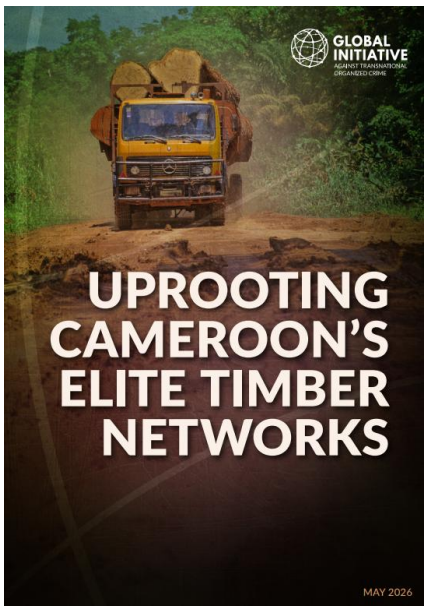
Суттєва увага у дослідженні приділяється проблемам якості даних, прозорості та методології оцінювання. Автори неодноразово підкреслюють, що багато офіційних оцінок базуються на непрозорих методологіях, застарілих даних або неповній аналітичній та розвідувальній інформації. Документ посилається на критику Комітету з державних рахунків Палати громад Великої Британії та Національного аудиторського управління Великої Британії щодо недостатньої оцінки масштабів ухилення від сплати податків, офшорних активів та недотримання податкових вимог заможними фізичними особами. Дослідження фактично формує ширший політичний аргумент щодо необхідності радикального вдосконалення офіційної системи оцінювання незаконних фінансових потоків, міжвідомчого обміну даними, стандартів прозорості та методологічної узгодженості у сфері оцінки незаконних фінансових потоків.

У фінальній частині документа автори формують конкретні рекомендації для уряду Великої Британії напередодні Illicit Finance Summit 2026. Серед ключових пропозицій — посилення прозорості реєстрів прихованих компаній у британських заморських територіях, збільшення ресурсів NCA та Управління з розслідування особливо тяжкого шахрайства Великої Британії (SFO), а також перегляд державної політики щодо розширення сектору криптофінансів. Документ прямо закликає уряд «поставити на паузу» плани перетворення Великої Британії на глобальний центр криптофінансів до моменту створення ефективної системи регулювання та нагляду за криптовалютним сектором. Загалом дослідження формує дуже жорсткий висновок: Велика Брита нія не лише стикається з проблемою незаконних фінансових потоків, а є одним із центральних глобальних вузлів міжнародної системи прихованого капіталу, офшорної фінансової секретності та транснаціональних незаконних фінансових потоків.

Тіньова імперія деревини: політичні зв'язки та незаконна експлуатація лісів Камеруну [11]

Документ, підготовлений Global Initiative Against Transnational Organized Crime (GI-TOC), є масштабним аналітичним розслідуванням, присвяченим системній незаконній вирубці лісів у Камеруні, ролі політичної еліти у захопленні природних ресурсів та функціонуванню транснаціональних корупційно-комерційних мереж у лісовому секторі країни. Дослідження демонструє, що проблема незаконної експлуатації лісів у Камеруні не обмежується окремими

[11] https://globalinitiative.net/wp-content/uploads/2026/05/GI-TOC-Uprooting-Cameroons-elite-timber-networks-May-2026.pdf



випадками корупції чи порушеннями екологічного законодавства, а фактично є частиною глибоко вкоріненої моделі привласнення природних ресурсів політичними елітами, у межах якої державні інституції, політичні еліти, бізнес-групи та міжнародні торговельні мережі функціонують як взаємопов'язана система отримання прибутку від неконтрольованої експлуатації лісових ресурсів. Автори показують, що незаконна вирубка підтримується не лише через хабарництво або слабкість регуляторного контролю, а й завдяки політичному покровительству, непрозорій бенефіціарній власності, маніпуляціям із концесіями, використанню офшорних торговельних структур і міжнародному попиту на деревину. У такій моделі природні ресурси фактично перетворюються на інструмент політичного та економічного збагачення вузьких елітних груп, а формальні механізми державного контролю, екологічного управління та захисту прав місцевих громад стають другорядними або використовуються вибірково. Автори наголошують, що Камерун є однією з ключових держав басейну Конго — другого за величиною тропічного лісового масиву світу після Амазонії та найбільшого глобального природного поглинача вуглецю. На цьому тлі рекордні темпи втрати лісового покриву, зафіксовані у 2023 році, коли країна втратила понад 200 тисяч гектарів лісу, розглядаються не лише як екологічна проблема, а як прояв структурної кризи управління природними ресурсами, державного контролю та верховенства права.

Документ детально описує економічне значення лісового сектору для Камеруну, підкреслюючи, що лісова промисловість є одним із ключових джерел експортних доходів держави після нафти та какао. Водночас автори демонструють, що значна частина галузі функціонує в умовах системної незаконності. У дослідженні наводяться оцінки, згідно з якими понад половина деревини, що реалізується на внутрішньому ринку та експортується з країни, може мати незаконне походження. Особливу увагу приділено ролі корупції у підтриманні цієї системи. Документ посилається на дослідження, які свідчать про мільйонні щорічні втрати бюджету Камеруну через незаконну вирубку, хабарництво та маніпуляції з митною й торговельною статистикою. Автори також аналізують суттєві розбіжності між офіційними даними Камеруну щодо експорту деревини та даними імпорту основних торговельних партнерів, зокрема Китаю та В'єтнаму. Ці розбіжності, на думку авторів, можуть свідчити про приховування реальних обсягів торгівлі, маніпуляції з цінами та існування масштабних непрозорих фінансових потоків, які супроводжують міжнародну торгівлю деревиною.

Центральним елементом дослідження є аналіз мережі компаній, пов'язаних із бізнесменом Абубакаром Аль Фатіхом — впливовим членом правлячої партії Cameroon People's Democratic Movement (CPDM), який має тісні зв'язки з високопосадовцями та оточенням президента Поля Бії. Документ детально досліджує діяльність компаній Sextransbois, SCIEB, Boiscam та Camvert, які, за твердженнями авторів, функціонують як єдина взаємопов'язана бізнес-структура. Автори демонструють, що ці компанії отримали масштабні лісові та аграрні концесії за обставин, які супроводжувалися порушенням законодавства, відсутністю прозорих тендерних процедур, політичним втручанням та ігноруванням прав місцевих громад. Особливо детально документ аналізує ситуацію навколо лісу Ебо — одного з найбільш біорізноманітних і екологічно важливих лісових масивів Центральної Африки. Автори описують, як у 2020 році уряд Камеруну створив дві великі лісові концесії у межах Ебо, однак після масштабного міжнародного резонансу, протестів природоохоронних організацій і корінних громад це рішення було тимчасово скасовано. Попри це, у 2023 році влада повторно створила Forest Management Units

(FMU 07-005 та FMU 07-006) та передала їх компаніям SCIEB і Sextransbois. Дослідження наголошує, що цей процес, за твердженнями громадських організацій, супроводжувався численними порушеннями: відсутністю обов'язкових публічних тендерів, неналежними консультаціями з корінними громадами Banen, непрозорими рішеннями щодо перекласифікації земель та пришвидшеним погодженням документів.

Документ також демонструє, що діяльність компаній починалася ще до завершення необхідних процедур. Автори наводять твердження експертів про те, що деякі компанії отримували дозволи на вирубку раніше, ніж могли бути завершені офіційні лісові інвентаризації та підготовлені плани управління лісовими ресурсами. Це, на думку дослідників, свідчить про те, що рішення про передачу концесій могли бути політично погоджені заздалегідь. Окремо аналізуються твердження про незаконне будівництво доріг у межах лісу Ебо, масштабні вирубки за межами офіційно дозволених територій та відсутність належних екологічних оцінок. Автори підкреслюють, що навіть після початку судових процесів та міжнародної критики компанії продовжували лісозаготівлю практично безперешкодно.

Одним із найважливіших аспектів дослідження є встановлення політичних і сімейних зв'язків між мережею Аль Фатіха та найближчим оточенням президента Камеруну. Автори за допомогою корпоративних реєстрів, інтерв'ю, комерційної документації та інших джерел встановлюють, що компанія Sextransbois спочатку належала родичам Франка Бії — сина президента та одного з найвпливовіших політичних діячів країни. У документі детально описуються зв'язки між власниками компанії та сім'єю Франка Бії, включаючи його родичів по лінії дружини. Після цього формальне володіння компанією було передано Махмуду Муртаді — неповірному брату Аль Фатіха, який на момент отримання контролю над компанією був лише двадцятирічним студентом із мінімальним професійним досвідом. Автори ставлять під сумнів реальну структуру бенефіціарного володіння та припускають можливе використання номінальних власників для приховування політичних інтересів. Дослідження також вказує на роль інших високопосадовців, включаючи представників президентської адміністрації, Міністерства економіки та Міністерства лісового господарства, які, за словами джерел, могли сприяти виділенню концесій і політичному прикриттю діяльності компаній.

Документ детально описує механізми корупції, які підтримують функціонування незаконної вирубки лісів у Камеруні. Автори наводять свідчення нинішніх і колишніх чиновників Міністерства лісового господарства, представників лісозаготівельних компаній та неформальних посередників, які описують хабарництво як системну та майже обов'язкову складову процесу отримання дозволів на вирубку. Дослідження демонструє, що хабарі сплачуються на всіх етапах — від перекласифікації земель і погодження концесій до оформлення транспортних документів та експорту деревини. Автори детально пояснюють роль посередників, які організовують зустрічі між бізнесом та чиновниками, координують передачу коштів і забезпечують політичне погодження документів у президентській адміністрації. Документ також описує практики фальсифікації лісових інвентаризацій, завищення дозволених обсягів вирубки та використання схем «відмивання коштів від незаконної вирубки деревини», коли незаконно заготовлена деревина оформлюється як легальна через маніпуляції з документацією та корумпований контроль з боку державних органів. Автори наголошують, що навіть компанії, які вже були офіційно санкціоновані за незаконну вирубку або інші порушення, продовжують отримувати нові дозволи та масштабні концесії.

Велика частина документа присвячена міжнародному виміру незаконної торгівлі деревиною. Автори демонструють, що компанія SCIEB активно експортувала продукцію до країн Європейського Союзу, включаючи Францію, Іспанію, Італію, Бельгію та Португалію. На думку дослідників, це може свідчити про можливі порушення EU Timber Regulation (EUTR), яка забороняє імпорт деревини, заготовленої з порушенням законодавства країни походження. Документ також аналізує можливі схеми трансфертного ціноутворення, у межах яких деревина

продавалася офшорній компанії United Development (HK) Co Ltd за штучно заниженими цінами, після чого продукція перепродавалася кінцевим покупцям за реальною ринковою вартістю. Автори припускають, що такі схеми могли використовуватися для приховування реального прибутку, мінімізації податкових зобов'язань та виведення коштів за кордон. У дослідженні наголошується, що незаконна вирубка лісів дедалі більше інтегрується у глобальні торговельні та фінансові мережі, де офшорні компанії, міжнародні логістичні ланцюги та слабкий контроль з боку імпортерів дозволяють легалізовувати продукцію сумнівного походження.

Окремий блок документа присвячений діяльності агробізнес-компанії Camvert, яка отримала масштабну концесію для вирощування пальмової олії поблизу Campo Ma'an Key Biodiversity Area. Автори демонструють, що процес надання концесії супроводжувався порушеннями екологічного законодавства, відсутністю належних оцінок впливу на довкілля та неналежними консультаціями з корінними громадами Bagyeli. Документ показує, що вирубка лісу під майбутні плантації почалася ще до офіційного отримання компанією прав на землю, а пов'язані компанії Boiscam та Sextransbois використовувалися для заготівлі деревини у межах проєкту. Автори також наводять численні свідчення місцевих жителів про невиконання Camvert соціальних зобов'язань, включаючи будівництво шкіл, медичних закладів і доріг, а також про втрату доступу до традиційних ресурсів і зростання конфліктів між людьми та дикою природою через масове знищення лісу. Дослідження підкреслює, що корінні громади фактично були усунені від процесу ухвалення рішень щодо використання земель, які мають критичне значення для їхнього способу життя та культурної ідентичності.

У фінальній частині документа автори доходять висновку, що ситуація в Камеруні є прикладом того, як незаконна експлуатація природних ресурсів може підтримуватися через поєднання політичного покровительства, слабкості державних інституцій, непрозорої бенефіціарної власності та міжнародного попиту на ресурси. Дослідження демонструє, що проблема незаконної вирубки лісів має не лише екологічний вимір, а й безпосередньо пов'язана з корупцією, незаконними фінансовими потоками, податковими правопорушеннями, транснаціональною організованою злочинністю та порушенням прав місцевих громад. Автори наголошують, що міжнародні ринки, включаючи Європейський Союз, також несуть частину відповідальності через недостатньо ефективний контроль

Висновки:

- **Документ демонструє, що незаконна вирубка лісів у Камеруні є частиною системи захоплення природних ресурсів елітами, у межах якої політичні еліти, бізнес і корумповані чиновники отримують прибуток від експлуатації лісів.** Це підкреслює необхідність посилення контролю за бенефіціарною власністю, конфліктами інтересів та політичним впливом у сфері природних ресурсів.
- **Дослідження показує, що корупція охоплює весь ланцюг незаконної вирубки — від видачі концесій до міжнародного експорту деревини.** Ефективна протидія незаконній вирубці лісів потребує поєднання антикорупційних механізмів, інструментів у сфері ПВК/ФТ, митного контролю та міжнародного обміну фінансовою інформацією.
- **Автори наголошують, що міжнародні ринки, включаючи ЄС, також сприяють проблемі через слабкий контроль ланцюгів постачання та імпорт деревини сумнівного походження.** Це вимагає посилення перевірок ланцюгів постачання, процедур належної перевірки та контролю за схемами трансфертного ціноутворення.
- **Документ підкреслює, що масштабна вирубка лісів має серйозні соціальні та безпекові наслідки,** оскільки руйнує традиційний спосіб життя місцевих громад, посилює конфлікти та сприяє подальшій криміналізації сектору природних ресурсів.

ланцюгів постачання та імпорт продукції сумнівного походження. Загалом документ формує картину глибоко інтегрованої системи політичного, економічного та транснаціонального контролю над природними ресурсами, у якій незаконна вирубка лісів є не випадковим порушенням, а системною частиною моделі функціонування держави та пов'язаних із нею бізнес-еліт.

Рекомендовані матеріали

Гібридні фінансові загрози та електоральна безпека: Аналітичний огляд механізмів тіньового фінансування [12]

Представлений випуск подкаст «Suspicious Transaction Report», випущений Центром фінансів та безпеки при Королівському об'єднаному інституті оборонних досліджень (RUSI), становить винятковий інтерес для фахівців у сфері фінансового моніторингу, комплаєнсу, розвідки та національної безпеки. Ведучий подкасту, Том Кітінг, веде глибоку та предметну розмову з Веронікою Драгалін, яка донедавна обіймала посаду головного прокурора антикорупційної прокуратури Республіки Молдова. Цей матеріал слугує не просто описом історичних подій, а детальною аналітичною довідкою про те, як саме ворожі держави використовують вразливості фінансових систем для підриву демократичних процесів, і як правоохоронні органи намагаються цьому протидіяти за допомогою інструментів фінансового моніторингу.

Аналіз цієї бесіди дозволяє простежити еволюцію методів незаконного фінансування політичних кампаній, оцінити ефективність традиційних AML-процедур у контексті гібридних загроз та зробити важливі висновки щодо ролі підрозділів фінансової розвідки у захисті виборчих процесів.

У вступній частині розмови формується загальний контекст, без якого неможливо зрозуміти масштаб фінансових загроз, з якими зіткнулася Молдова. Вероніка Драгалін, маючи за плечима досвід роботи федеральним прокурором у Сполучених Штатах Америки, повернулася на батьківщину, щоб очолити боротьбу з корупцією в період критичних політичних трансформацій. Перехід від «препарування тіл до препарування кримінальних справ», як метафорично висловився ведучий, символізує системний, аналітичний підхід, який Драгалін спробувала запровадити в молдовській правоохоронній системі. Вона зазначає, що корупція в Молдові має історичний, ендемічний та системний характер, пронизуючи всі рівні суспільства від найнижчого до найвищого.

Протягом тривалого часу Молдова вважалася так званою «захопленою державою» (captured state), де один олігарх контролював практично всі елементи урядового та приватного секторів, включаючи банківську систему, яка була монополізована невеликою групою впливових осіб. Лише у 2019 році цей олігархічний контроль було частково зруйновано, коли ключові фігуранти втекли з країни, а у 2021 році до влади прийшли нові політичні сили, чиєю головною платформою стала антикорупційна діяльність та реформа правосуддя. Цей період породив величезні надії як всередині країни, так і серед молдовської діаспори, на незворотність

[12] https://www.rusi.org/podcasts/suspicious-transaction-report/episode-20-moldovas-elections-fighting-financial-interference

демократичних змін та успішну європейську інтеграцію. Однак саме ці прагнення зробили країну мішенню для безпрецедентного фінансового втручання.

Для розуміння того, чому фінансова система Молдови виявилася такою вразливою до зовнішнього гібридного впливу під час виборів 2024 року, експерти звертаються до історії двох колосальних фінансових махінацій, які спустошили країну та продемонстрували слабкість її інституцій. Першою такою подією став сумнозвісний «Російський ландромат» (Russian Laundromat), який розпочався приблизно у 2014 році. Ця схема використовувала молдовську правову та банківську системи для відмивання російських грошей. Через механізм фіктивних боргових зобов'язань, які легалізувалися через рішення молдовських судів, колосальна сума у 22 мільярди доларів США була виведена з Росії через один молдовський банк. Звідти ці брудні кошти спрямовувалися до латвійської фінансової системи, а потім інтегрувалися у світову економіку. Для маленької країни з обмеженим ВВП такі обсяги тіньових потоків є не просто фінансовим злочином, а фактором макроекономічної дестабілізації.

Майже одночасно з ландроматом розгорнулася інша катастрофічна схема, відома як «банківське шахрайство» або «крадіжка мільярда». Невелика група осіб захопила контроль над трьома приватними молдовськими банками. Використовуючи складні мережі офшорних компаній, вони кредитували власні підприємства все більшими сумами грошей, аж поки система не зазнала краху, і гроші просто зникли. Наслідком цієї масштабної афери стала необхідність урядового втручання для порятунку банківської системи. Уряд був змушений покрити дефіцит у розмірі одного мільярда доларів США, що на той момент становило близько 12 відсотків валового внутрішнього продукту Республіки Молдова. Ці дві події — гігантська схема відмивання грошей та спустошення приватного банківського сектору — залишили країну у вкрай крихкому стані, наочно продемонструвавши, що за підтримки корумпованих чиновників фінансові інституції легко піддаються маніпуляціям з боку зловмисників.

У цьому історичному контексті формувалися ключові фігури тіньової економіки та політичної корупції, імена яких, за словами Драгалін, відомі в Молдові навіть маленьким дітям. Головним актором, діяльність якого розглядається в подкасті, є Ілан Шор. Будучи бізнесменом із кримінальним ухилом, він відігравав ключову роль у схемі банківського шахрайства, допомагаючи захопити та згодом ліквідувати проблемні банки. За ці злочини його було засуджено до тюремного ув'язнення, але під час апеляційного процесу він був звільнений під заставу, втік з країни і знайшов притулок в Ізраїлі (маючи ізраїльське громадянство), а згодом — у Росії. Шор є класичним прикладом фінансового злочинця, який намагається легалізувати свій статус через політику. Дізнавшись про розслідування щодо своєї ролі у банківському шахрайстві, він заснував власну політичну партію імені себе (партія «Шор»), виграв вибори мера одного з великих міст і використав цей політичний статус як аргумент для пошуку захисту за кордоном, стверджуючи про політичне переслідування. З-за кордону він продовжував відкрито фінансувати антиурядові протести та впливати на політичні процеси в Молдові.

Іншим визначним діячем був Володимир Плахотнюк, який через свою політичну партію фактично встановив контроль над державними інституціями, збагатившись за допомогою різноманітних фінансових схем, включно з вищезгаданим банківським шахрайством. Його незаконні статки дозволяли вести розкішний спосіб життя, що підтверджується відстеженими активами, такими як вілла у Швейцарії за 26 мільйонів євро та приватні літаки. Він також втік з країни у 2019 році, і його поточне місцеперебування залишається невідомим. Третім учасником олігархічного пулу згадується Вячеслав Платон, причетний до захоплення банків та страхових компаній, який згодом знайшов притулок у Великій Британії. Наявність таких могутніх фігурантів, які перебувають у розшуку та керують колосальними тіньовими капіталами з-за кордону, створювала безпрецедентний тиск на антикорупційні органи Молдови. Правоохоронці зіткнулися з дилемою: витрачати обмежені ресурси на відновлення справедливості щодо

історичних злочинів минулого десятиліття, чи сконцентруватися на поточних корупційних загрозах, які можуть зруйнувати країну тут і зараз.

Головна аналітична цінність подкасту полягає у детальному описі еволюції типологій фінансування політичного втручання напередодні вирішальних президентських виборів та референдуму щодо вступу до Європейського Союзу, що відбулися восени 2024 року. Підготовка до цих подій супроводжувалася масованим вливанням брудних грошей з боку угруповання Ілана Шора, яке відкрито платило людям за участь у протестах та здійснювало незаконне фінансування передвиборчих кампаній, як це було зафіксовано, наприклад, під час виборів башкана (губернатора) Гагаузії у 2023 році. Фінансування політичних партій готівкою та використання незадекларованих фондів є прямим порушенням молдовського законодавства. Тому прокуратура ініціювала застосування положення кримінального кодексу, яке забороняє політичним партіям або кандидатам приймати гроші від організованої злочинної групи. Довести такий злочин надзвичайно складно, оскільки правоохоронцям потрібно не лише довести факт існування організованої групи, але й специфічний умисел — що гроші передавалися саме з політичною метою.

Перший етап фінансової інтервенції, виявлений слідчими протягом 2022-2023 років, відзначався досить примітивною типологією, пов'язаною з фізичним переміщенням готівки через державний кордон. У зв'язку з війною в Україні прямі рейси до Москви були неможливі, тому використовувалися транзитні маршрути через Стамбул (Туреччина) та Вірменію. Організовані групи осіб летіли до Росії на дуже короткий термін і поверталися до Кишинева, маючи при собі готівку. Експертам з фінансового моніторингу буде особливо цікаво відзначити суму, яку перевозив кожен такий кур'єр — рівно вісім тисяч доларів США. Як зазначає ведучий Том Кітінг, це класичний приклад техніки «смурфінгу» або структурування, покликаний уникнути порогу обов'язкового декларування згідно з рекомендаціями FATF, який становить десять тисяч доларів. На одному рейсі могло перебувати до п'ятнадцяти таких осіб, що дозволяло за один раз ввозити значні суми без привернення уваги митних органів. Цікаво, що кошти ввозилися в американських доларах, що створювало для злочинців наступну логістичну проблему — необхідність конвертації іноземної валюти в молдовські леї для подальшої роздачі протестувальникам та учасникам політичних кампаній.

На цьому етапі спрацювали базові елементи антилегалізаційної системи на рівні приватного сектору. Валютні кіоски та пункти обміну мали власні зобов'язання щодо звітування та були обладнані камерами відеоспостереження, що дозволяло слідчим фіксувати осіб, які обмінювали великі обсяги готівки. Правоохоронні органи мали певний успіх у перехопленні цих коштів. Організатори схеми діяли дуже шаблонно: вони збиралися вночі у конспіративних квартирах, фасували готівку по сумках, а потім розвозили їх автомобілями по різних регіонах країни для виплат на місцевому рівні. Поліції вдавалося здійснювати перехоплення цих кур'єрів на гарячому, вилучати величезні суми готівки та арештовувати виконавців. Однак, як це часто буває у сфері протидії фінансовим злочинам, правоохоронний тиск лише змусив злочинну групу адаптуватися та ускладнити свої методи. Організатори зрозуміли, що концентрація великих сум готівки в руках кількох осіб створює надто високий ризик втрати коштів через арешти.

Другий етап еволюції схем незаконного фінансування ознаменувався спробою переходу на використання платіжних карток. Замість фізичної готівки організатори спробували використати передплачені дебетові картки, згенеровані в Об'єднаних Арабських Еміратах (Дубай) під назвою, схожою на «People PPL». Ідея полягала в тому, щоб роздати ці картки низовим виконавцям, щоб ті самостійно знімали готівку в банкоматах. Однак завдяки розгалуженій мережі конфіденційних джерел та співпрацюючих свідків правоохоронцям вдалося перехопити велику партію з кількох тисяч таких карток під час їх доставки до Молдови. Злочинці виявилися достатньо обережними, щоб не поповнювати картки до їх фізичного отримання виконавцями,

тому слідчі вилучили «порожній» пластик, але цей превентивний захід зірвав даний вектор фінансування.

Третій, найбільш складний та масштабний етап інновацій у сфері фінансового втручання став справжнім викликом для державної безпеки Молдови. Організатори схеми прийняли стратегічне рішення децентралізувати ризики переміщення та переведення в готівку коштів, переклавши цю відповідальність з вузького кола професійних кур'єрів на десятки тисяч звичайних громадян. Для цього було налагоджено взаємодію з російським «Промсвязьбанком» (ПСБ), фінансовою установою, що має тісні зв'язки з Міністерством оборони Російської Федерації. Такий вибір банку не залишає сумнівів щодо державного сприяння та фінансової підтримки діяльності Ілана Шора з боку Росії.

Механіка схеми полягала в дистанційному відкритті банківських рахунків у ПСБ для громадян Молдови. Їм навіть не були потрібні фізичні картки; достатньо було завантажити спеціальний мобільний додаток, через який вони бачили надходження коштів, наприклад, у розмірі, еквівалентному 500 доларам, але у російських рублях. Головна проблема для правоохоронців полягала в тому, що після отримання віртуальних коштів кожен кінцевий бенефіціар мусив самостійно шукати шляхи переведення їх у готівку. Оскільки офіційні регуляції Молдови жорстко обмежували діяльність російських банків, на території, підконтрольній Кишиневу, не було жодного банкомата чи термінала, де можна було б зняти кошти з рахунків ПСБ. Проте громадяни знаходили обхідні шляхи: використовували фінансову інфраструктуру сепаратистського регіону Придністров'я, який працював з російськими банками, або знімали готівку під час поїздок до Стамбула чи Вірменії.

З точки зору експертів з фінансового моніторингу, ця типологія є надзвичайно небезпечною через її розпорошеність. Слідчі опинилися в ситуації, коли їм доводилося протистояти не десятку централізованих менеджерів, а масовому явищу. Задокументовані дані свідчать про те, що рахунки у вищезгаданому російському банку мали понад 130 000 громадян Молдови. Для правоохоронної системи країни з обмеженими ресурсами фізично неможливо ідентифікувати, допитати та довести злочинний умисел кожного зі ста тридцяти тисяч бенефіціарів. Ба більше, переслідування вразливих верств населення (наприклад, літніх людей, які через бідність погоджувалися прийняти еквівалент ста доларів) не було метою прокуратури; метою було викриття вищої ланки організаторів. Але архітектура схеми надійно ховала керівників на території Російської Федерації, яка припинила будь-яку конструктивну співпрацю з правоохоронними органами Молдови за процедурами взаємної правової допомоги.

Варто також зазначити, що зловмисники експериментували й з іншими методами легалізації. Зафіксовані ознаки використання криптовалют, які згодом конвертувалися в готівку вже на території Молдови, хоча цей вектор не досяг рівня системної загрози порівняно з масовими банківськими рахунками в Росії. Вкрай цинічним виявилося використання релігійних інституцій. Приблизно за півроку до виборів організатори знову спробували повернутися до масового ввезення готівки літаками (під час одного з таких перехоплень на митниці було вилучено понад мільйон доларів з одного рейсу). Щоб мінімізувати ризики обшуків, вони почали використовувати православних священників, які формували групи під виглядом релігійних паломників до Росії. Розрахунок був на те, що митники не наважаться ретельно оглядати духовенство. Хоча наявні докази вказували на їхню причетність до кур'єрської мережі, перехоплені суми готівки у них виявлялися відносно невеликими, що суттєво ускладнювало доведення їхньої ролі в ширшій злочинній змові.

Протистояння такій масштабній та добре фінансованій кампанії вимагало від державних органів Республіки Молдова нестандартних, міжвідомчих рішень. Розгорнулася активна взаємодія між Офісом Прем'єр-міністра, Національним банком, правоохоронними структурами, митницею, прикордонною поліцією та службами безпеки. Застосовувався комбінований підхід, який

об'єднував норми виборчого законодавства та класичне законодавство про банківську таємницю та протидію відмиванню доходів. У певний момент серйозно дискутувалася можливість запровадження жорстких адміністративних обмежень, наприклад, повної заборони готівкових транзакцій на суму понад 5000 доларів. Однак цей захід було відхилено, оскільки економіка Молдови значною мірою залишається готівковою. Через історичну недовіру до банківського сектору (зумовлену втратою мільярда доларів у минулому) багато громадян, особливо тих, хто працює за кордоном, зберігають заощадження вдома у валюті і використовують готівку навіть для великих покупок, таких як нерухомість чи автомобілі. Запровадження таких драконівських обмежень невиправдано вдарило б по законослухняних громадянах.

В контексті пошуку ефективних контрзаходів Вероніка Драгалін підкреслює фундаментальну роль ПФР Молдови та тісної співпраці з банківським сектором. Приватні банки продемонстрували високий рівень кооперації, ретельно виконуючи процедури KYC та своєчасно звітуючи про клієнтів з великими обсягами незрозумілої готівки. Завдяки цьому ПФР мав змогу надзвичайно оперативно отримувати та аналізувати банківську інформацію. Як тільки слідчі виявляли підозрілі індикатори або дати транзакцій, фінансова розвідка в найкоротші терміни надавала необхідні дані без тривалих бюрократичних процедур, пов'язаних з отриманням судових дозволів на доступ до банківської таємниці. Більше того, цей інструмент виявився незамінним у міжнародному масштабі. Наприклад, коли було виявлено, що частина тіньових потоків маскувалася під транзакції з Казахстану (де створювалися компанії-прокладки), комунікація на рівні ПФР між країнами дозволила швидко ідентифікувати та заблокувати ці підозрілі перекази. Том Кітінг погоджується з тим, що обмін даними між ПФР є одним з найефективніших інструментів у глобальній архітектурі AML, дозволяючи обмінюватися критично важливою розвідувальною інформацією з безпрецедентною швидкістю.

Обговорюючи міжнародний вимір проблеми, неможливо оминути тему санкційного тиску. Міжнародна спільнота, включаючи США, ЄС, Канаду та Швейцарію, відносно рано, ще наприкінці 2022 року, включила Ілана Шора, Володимира Плахотнюка та їхнє оточення до санкційних списків. Згодом ці списки розширювалися, охоплюючи ширшу мережу осіб, причетних до підривної діяльності. Драгалін визнає, що санкції мали потужне символічне значення та значно ускладнили життя тим функціонерам схеми, які базувалися у країнах Заходу. Правоохоронці підтверджували це завдяки перехопленням розмов, де фігуранти відверто скаржилися на блокування рахунків та неможливість нормальної життєдіяльності в Європі та США. Однак, щодо кінцевої мети — зупинення потоку нелегальних фінансів з Росії до Молдови — санкції виявилися безсилими. Оскільки основні активи Шора та інфраструктура фінансування знаходилися на території Росії, яка ігнорує західні санкції, «кран» брудних грошей залишався відкритим. Це є яскравою ілюстрацією обмеженості традиційних санкційних механізмів, коли йдеться про суб'єктів, що користуються повним державним захистом ворожої юрисдикції.

Окремим і надзвичайно складним аспектом роботи прокуратури була інформаційна політика та комунікація з громадськістю в умовах гібридної атаки. Правоохоронні органи традиційно прагнуть зберігати конфіденційність під час активної фази розслідування, щоб не зашкодити операції та не розкрити джерела. Проте в умовах, коли ворожі сили буквально купували вибори, а політики нагнітали риторику про екзистенційну загрозу країні, суспільство мало право знати правду. Драгалін розповідає про складний процес балансування між таємницею слідства та суспільним інтересом. Було прийнято безпрецедентне рішення оприлюднити частину аудіозаписів перехоплених розмов, щоб наочно продемонструвати громадянам реальність злочинної схеми. Найважче було пояснити, що незаконна готівка за голоси — це не просто порушення формальних процедур, а пряма загроза суверенітету. Посадовиця публічно артикулювала ключову тезу: політики, які приходять до влади за гроші кримінальних угруповань

та ворожих держав, не будуть діяти в інтересах громадян; вони діятимуть виключно в інтересах тих, хто фінансував їхню кампанію, віддаючи «борги» національними інтересами.

Ще однією підступною політико-фінансовою технологією, розкритою завдяки розслідуванням, була спроба Ілана Шора профінансувати створення фальшивої «проєвропейської» політичної партії. Розрахунок будувався на тому, щоб ця штучна політична сила відтягнула голоси від справжніх демократичних партій під час виборів, а після проходження до парламенту несподівано сформувала б альянс із відверто проросійськими силами Шора, кардинально змінивши геополітичний вектор розвитку країни. Цей приклад яскраво демонструє, наскільки глибоко брудні гроші можуть спотворити демократичний процес, маскуючи справжні наміри політичних гравців.

У підсумку, висока явка виборців під час кампанії 2024 року свідчить про те, що молдовське суспільство, принаймні частково, усвідомило масштаб загрози та мобілізувалося для захисту своїх інституцій. Аналізуючи здобутий досвід, Вероніка Драгалін виділяє найважливіший інструмент у боротьбі з подібними високоорганізованими фінансово-політичними схемами — інститут свідків, що співпрацюють зі слідством. Спираючись на досвід правоохоронної системи США, вона впроваджувала практику вербування учасників злочинних схем. Правоохоронцям вдавалося переконувати інсайдерів, що для них вигідніше почати співпрацювати з урядом, залишитися в злочинному угрупованні під прикриттям, використовувати приховані мікрофони та камери і передавати слідству критично важливу інформацію. Без таких інсайдерів, зазначає Драгалін, правоохоронні органи залишаються «сліпими», адже зрозуміти архітектуру децентралізованих тіньових потоків виключно за рахунок зовнішнього спостереження чи аналізу банківських виписок фактично неможливо. Для майбутніх виборчих циклів у Молдові та інших вразливих країнах регіону (наприклад, у Вірменії) вона настійно рекомендує законодавчо розширювати можливості надання імунітету та інших стимулів для низових учасників злочинних схем в обмін на їхні свідчення проти організаторів вищої ланки.

Висновки, зроблені в цьому випуску подкасту «Suspicious Transaction Report», мають фундаментальне значення не лише для Молдови, а й для всіх відкритих суспільств. Том Кітінг у своєму заключному слові констатує вкрай неприємну реальність: західні демократії залишаються небезпечно слабкими перед обличчям фінансового втручання з боку ворожих держав. Зловмисні суб'єкти активно використовують найслабші ланки у фінансових кордонах демократичних країн для формування їхньої внутрішньої політики. Досвід Молдови з її безпрецедентною спробою децентралізованого підкупу десятків тисяч виборців через рахунки в російських банках доводить, що традиційні AML-парадигми, орієнтовані на пошук великих корупційних транзакцій, повинні адаптуватися до загроз мікрофінансування гібридних кампаній. Роль фінансових установ, ПФР та антикорупційних органів більше не обмежується лише боротьбою з економічними злочинами. Вони стають на передову лінію захисту самої суті демократії, протистоячи процесу, який, може непомітно, але незворотно зруйнувати демократичні інститути, якщо не вибудувати надійну систему фінансової оборони. Цей кейс є суворим попередженням для світової спільноти про те, що інтегрованість у глобальну фінансову систему може бути не лише інструментом економічного розвитку, але й зброєю в руках авторитарних режимів.

Інші новини

Кіберстійкість фінансового сектору в умовах розвитку штучного інтелекту [13]

15 травня 2026 року Банк Англії, Управління з фінансового регулювання і нагляду (FCA) та Казначейство Його Величності (HM Treasury) оприлюднили спільну заяву, в якій акцентують увагу на безпрецедентному виклику для кіберстійкості фінансового сектору, що виникає внаслідок стрімкого розвитку передових моделей штучного інтелекту (frontier AI models). Ключовим тезисом заяви є констатація того, що кібернетичні можливості сучасних моделей AI вже перевищують рівень кваліфікованого спеціаліста — при цьому вони діють значно швидше, у більшому масштабі і за нижчої вартості. Такий асиметричний потенціал, потрапивши до рук зловмисників, суттєво посилює загрозу для фінансової стійкості установ, захисту клієнтів і цілісності ринку. Регулятори особливо наголошують, що установи, які недостатньо інвестували в базову кіберінфраструктуру, опиняються у прогресивно вразливішому становищі зі зростанням потужності нових моделей AI.

Регулятори окреслюють п'ять ключових сфер, в яких від фінансових установ та операторів фінансової ринкової інфраструктури (FMI) очікуються конкретні дії. У сфері управління та стратегії: ради директорів і топ-менеджмент мають забезпечити собі достатнє розуміння ризиків frontier AI, включаючи ризики застарілих систем і систем поза межами вендорської підтримки, а також переглянути належність страхового покриття. У сфері ідентифікації та управління вразливостями: оскільки передові моделі AI здатні швидко виявляти і експлуатувати масштабні масиви вразливостей у технологічній інфраструктурі установи, необхідне пришвидшення і масштабування процесів, пріоритизації і усунення вразливостей, включаючи їх автоматизацію. У сфері управління ризиками третіх сторін — встановлення, моніторинг і управління зовнішніми застосунками, бібліотеками і сервісами, інтегрованими в корпоративні мережі. У сфері захисту — через ефективне управління доступом, сегментацію мереж і захист даних. У сфері реагування та відновлення — з посиланням на ефективні практики, опубліковані Банком Англії, PRA та FCA в жовтні 2025 року.

Регуляторна заява містить важливе методологічне роз'яснення: документ не впроваджує нових вимог, а консолідує та посилює вже існуючі регуляторні очікування у сфері операційної стійкості. Така позиція вписується у загальну стратегію Банку Англії та FCA щодо поступового підвищення регуляторних стандартів без раптових нормативних змін, надаючи установам узагальнений орієнтир в умовах ускладнення операційного середовища. Регулятори підтверджують продовження активного моніторингу розвитку передових AI-моделей та взаємодію з галуззю через Міжгалузеву групу операційної стійкості ринків (CMORG), вебінар якої щодо пом'якшення ризиків frontier AI відбувся 14 травня 2026 року. Національний центр кібербезпеки (NCSC) паралельно продовжує публікацію практичних рекомендацій, зокрема щодо підготовки до «хвилі вразливостей» (vulnerability patch wave) та готовності кіберзахисту до нового покоління AI-загроз.

[13] https://www.bankofengland.co.uk/news/2026/may/boe-fca-and-hm-treasury-joint-statement-on-frontier-ai-models-and-cyber-resilience

Балканські кримінальні мережі в Латинській Америці [14]

Останніми роками організована злочинність у Латинській Америці зазнала суттєвої трансформації, і одним із ключових чинників цих змін стала присутність вихідців з Балкан.

Як свідчить детальний аналіз ситуації, кримінальні актори з Албанії, Сербії, Чорногорії та інших країн регіону вже не є периферійними гравцями — вони інтегрувалися безпосередньо в ядро трансатлантичного наркотрафіку, виконуючи ролі, які раніше належали місцевим угрупованням.

Нещодавнє затримання в Бразилії албанця Ервіна Мати, якого звинувачують у ролі посередника між південноамериканськими постачальниками та європейськими покупцями кокаїну, є лише черговим підтвердженням цього тривожного тренду. Мата, заарештований неподалік Сан-Паулу, нібито координував відправлення кокаїну з Бразилії до портів Іспанії та Німеччини, працюючи в інтересах балканського кримінального синдикату.

Головна відмінність балканських злочинців від традиційних латиноамериканських угруповань, які десятиліттями будували територіальні анклави, полягає в їхній гнучкості та функціональності. Вони не прагнуть захоплювати райони чи міста — натомість вони вбудовуються у фрагментований ланцюг постачання кокаїну, беручи на себе управління маршрутами, логістику та підтримання зв’язків, необхідних для переміщення наркотиків від латиноамериканських виробничих потужностей до зростаючого європейського ринку. Їхня діяльність у Латинській Америці набула системного характеру, а арешти чи ліквідації окремих фігурантів, як-от загибель Ергіса Даші в Гуаякілі або вбивство Адріатіка Треси, не зупиняють загального процесу.

Серед основних ролей, які виконують вихідці з Балкан, можна виокремити три ключові моделі поведінки.

Перша — це так звані емісари. Вони діють від імені децентралізованих злочинних мереж, що базуються на родинних зв’язках та ділових альянсах, а не на жорсткій ієрархії. Їхнє завдання — відправляти довірених осіб безпосередньо до країн-експортерів, таких як Колумбія, Еквадор або Бразилія, де ті ведуть переговори з виробниками та місцевими групами, відповідальними за транспортування і зберігання наркотиків. Таким чином емісари заміняють посередників, збільшуючи прибуток своїх організацій. Яскравим прикладом є Дрітан Рекшепі — албанський злочинець, який організовував перевезення кокаїну з Еквадору, перебуваючи за ґратами, і продовжував координувати дії з колумбійськими та еквадорськими угрупованнями навіть після свого затримання в 2014 році. Інший випадок — клан Фарруку, який координував поставки між Еквадором та Іспанією, а його емісар Даші був убитий у Гуаякілі всього через кілька днів після того, як іспанська поліція вилучила дві тони кокаїну, пов’язані з цим угрупованням.

Друга модель — незалежні спеціалісти з трафіку. Ці особи діють не за дорученням конкретного європейського синдикату, а використовуючи власні ділові навички, особисті зв’язки з виробниками, місцевими мережами та гуртовими покупцями в Європі. Найпоказовішою фігурою тут є Дрітан Гіка — албанець, який отримав громадянство Еквадору. Не маючи підтвердженої афіліації з жодним балканським злочинним угрупованням, він створив власну імперію, уклавши прямі альянси з колумбійськими виробниками та еквадорськими групами, що займалися транспортуванням і контамінацією контейнерів. Для прикриття, Гіка заснував

[14] https://insightcrime.org/news/different-faces-balkan-organized-crime-latin-america/

мережу легальних експортних компаній, які відправляли до Європи банани — один із головних експортних продуктів Еквадору. Його вплив був настільки великим, що він особисто обговорював ціни на кокаїн із покупцями в різних портових містах Європи. Заарештований в Абу-Дабі, він очікує екстрадиції до Еквадору за звинуваченням в організованій злочинності та корупції. За тією ж схемою діяли його співвітчизники Адріатік Треса (ліквідований у 2020 році) та Арбер Цекай (заарештований у Німеччині).

Третя, і особливо небезпечна, роль — експерти з фінансових злочинів. Незалежно від того, чи діють вони у складі групи чи самостійно, багато балканських злочинців спеціалізуються на відмиванні грошей — як від власних операцій, так і на замовлення місцевих чи європейських угруповань. Той самий Дрітан Гіка використовував свої підставні компанії для легалізації понад 31 мільйона доларів через фінансову систему Еквадору в період між 2015 та 2024 роками.

Однак наймасштабніший приклад — це схема, пов'язана з албанським злочинним кланом Хіса. У листопаді 2025 року Міністерство фінансів США запровадило санкції проти 27 осіб та організацій, причетних до мережі відмивання грошей, що діяла в Мексиці в тандемі з картелем Сіналоа. Ця мережа легалізовувала наркодоходи через казино та розкішні ресторани в штатах Сіналоа, Сонора та інших регіонах Мексики. Не менш показовою є історія серба Єздимира Срдана, який, отримавши суперечливе дострокове звільнення з в'язниці в Еквадорі за звинуваченням у наркотрафіку, згодом був засуджений до десяти років ув'язнення саме за відмивання коштів, отриманих злочинним шляхом.

Таким чином, балканська організована злочинність у Латинській Америці постає не як єдиний монолітний блок, а як гнучка, багатошарова система. Її представники виступають і як емісари великих європейських синдикатів, і як незалежні підприємці, і як висококваліфіковані фінансисти, які обслуговують брудні капітали. Їхній успіх полягає в здатності адаптуватися до місцевих умов, використовувати легальний бізнес як прикриття та налагоджувати стратегічні альянси з колумбійськими, еквадорськими та мексиканськими картелями.

Поки європейський попит на кокаїн залишатиметься високим, Балкани продовжуватимуть постачати до Латинської Америки не лише наркотики, а й унікальний злочинний «менеджмент», що робить боротьбу з цим явищем особливо складною для правоохоронних органів обох континентів.

Для загального розвитку

Анатомія боргу: перетворення міграції на підпільну економічну систему [15]

Фам, в'єтнамська підприємиця, розпочала свій шлях, продавши бізнес і взявши гроші в лихварів, аби сплатити $14 000 посереднику (môi giới). Ця сума відкрила їй двері до Шенгену через чеську візу, але насправді купила квиток у систему, з якої майже неможливо вийти, не залишивши себе в боргових зобов'язаннях. Її подорож через Англію до Ірландії, з підробленим паспортом і фальшивим працевлаштуванням у салоні, ілюструє ключову трансформацію: міграція з В'єтнаму більше не є гуманітарною трагедією, а

[15] https://globalinitiative.net/analysis/chasing-irelands-pot-of-gold-how-illicit-brokers-profit-from-vietnamese-migration-routes/

перетворилася на індустрію, де державні програми підтримки замінені тіньовими посередниками.

Історія Фам — це не просто черговий сюжет про нелегальний перетин кордону. Це деталізований портрет сучасної, високоорганізованої та цинічної кримінальної індустрії, де людське бажання кращого життя перетворюється на товар, а маршрут до Європи стає пасткою довічної фінансової залежності.

Сьогодні Ірландія стає несподіваним епіцентром цієї системи. Якщо у 2020 році притулку тут шукали лише 12 в'єтнамців, то до початку жовтня 2025 року ця цифра сягнула приблизно 520. Таке різке зростання не є випадковістю чи наслідком глобальних катастроф — це результат цілеспрямованої роботи маркетингових стратегій у темному сегменті соціальних мереж. Серед самої міграційної спільноти Ірландія позиціонується як «менш переповнена» альтернатива Великій Британії (непередбачуваній і конкурентній) або Німеччині (надто бюрократичній і важкодоступній).

В'єтнамська діаспора в Ірландії, яка виросла з кількох сотень у 1979 році до приблизно 6 000 сьогодні, створила ту саму інфраструктуру, що робить цей маршрут таким привабливим для новачків, але водночас і таким залежним. Тут можна знайти спільне житло, підтримку через буддистські храми чи місцеві бізнеси, а також швидкий вихід на роботу — у салони краси, готельно-ресторанний бізнес або харчову промисловість, де бар'єри для входу мінімальні. На перший погляд, ця система здається напрочуд ефективною: вона вирішує проблеми житла та соціальної ізоляції, з якими стикаються нелегальні мігранти в інших країнах. Але за цією ефективністю ховається справжнє обличчя тіньової економіки, де посередники (môi giới) відіграють роль не просто перевізників, а архітекторів цілісного ланцюга експлуатації.

Вартість їхніх послуг є астрономічною, але справжній тягар полягає не лише в початковій платі. Мігранти, такі як Фам чи 33-річний Хюї, що заплатив $20000 за «пакет» із робочою візою та місцем на фабриці в Монагані, зазвичай заборговують від $10 000 до $30 000. Це не просто позика — це інструмент контролю. Умови кредиту є недискусійними: дефолт призводить до залякувань, прямих погроз або фінансового тиску на родичів, що залишилися у В'єтнамі. Хюї зіткнувся з реальністю, яку обіцянки môi giới приховували за глянцевою картинкою легального працевлаштування: перенаселені каравани замість житла, 17-годинні нічні зміни та зарплата на межі виживання. Його паспорт конфіскував роботодавець, що є класичним методом позбавлення мігранта права на вільне пересування. Історія Хюї демонструє, як початкова угода про працевлаштування перетворюється на форму примусової праці, де борг стає кайданами. Те, що він згодом зміг вирватися, знайти спільноту та стабільну роботу, є швидше винятком, ніж правилом, адже більшість залишаються замкненими в цьому циклі економічного страждання.

За цими окремими долями стоїть системна транскордонна кримінальна індустрія. Шлях сучасного в'єтнамського мігранта — від рекрутингу в північному В'єтнамі, через транзитні хаби в Чехії, Польщі, Франції чи Іспанії, до фінального працевлаштування — є ретельно скоординованою операцією. Môi giới — це не просто контрабандисти в класичному розумінні. Вони є висококваліфікованими координаторами транснаціональної нелегальної сервісної економіки. Вони займаються підробкою документів, організовують транспорт, контролюють житло, а в багатьох випадках самі стають роботодавцями, об'єднуючи міграцію, борг і працю в єдиний ланцюг. Їхній контроль рідко буває відверто насильницьким, але він залишається абсолютним через фінансовий тиск, утримання документів, маніпуляції з житлом та обмеження доступу до альтернативної роботи. Ці мережі демонструють вражаючу адаптивність: вони блискавично змінюють маршрути та цілі залежно від змін у правозастосовній практиці, використовують соціальні медіа (як TikTok) для реклами нових «пакетів» послуг, а також знаходять слабкі місця в легальних візових каналах.

З огляду на це, аналітики GI-TOC роблять принциповий висновок: політична відповідь на проблему не має зосереджуватися на самих мігрантах або явищі міграції як такому. Натомість вона має бути спрямована виключно на організовані кримінальні елементи, що стоять за цією системою.

Ключовими цілями мають стати фінансова модель цих мереж — включно зі схемами поетапних платежів і транскордонними грошовими потоками — а також документування шахрайства та зловживання легальними візовими програмами. Особливу увагу слід приділити зв'язку між працею та посередництвом, особливо в тих випадках, коли роботодавці безпосередньо інтегровані в рекрутингові мережі. Розширення регульованих трудових шляхів міграції може зменшити ризики для окремих людей, але справжній виклик полягає в демонтажі бізнес-моделі, яка перетворила мобільність на контрольований і монетизований ланцюг постачання.

Історично закритий та ізольований характер в'єтнамських мереж ускладнював зовнішнє втручання, однак сучасні дослідження вказують на їхнє перетинання з іншими міграційними коридорами. Наприклад, на півночі Франції вони вже перетинаються з курдськими та багатонаціональними мережами, що, хоч і ускладнює картину, проте відкриває нові можливості.

Подальші аналітичні дослідження є критично важливими для створення доказової бази, необхідної для ефективної боротьби з цією сучасною формою рабства, замаскованою під міграцію.

Ваша думка важлива!

1. Яким чином регулятори повинні поєднати підтримку інновацій у сфері цифрових активів із необхідністю забезпечення ефективного контролю ризиків ВК/ФТ, санкційного обходу та незаконних фінансових потоків?
2. Наскільки ефективними є сучасні корпоративні програми комплаєнсу у запобіганні міжнародній корупції, якщо в багатьох випадках вони залишаються формальним виконанням вимог, а не реальним механізмом формування культури доброчесності?
3. Враховуючи велику кількість громадян України, які стали мігрантами через війну, наскільки існують ризики того, що українська діаспора за кордоном буде використана міжнародними злочинними мережами?
4. Чи повинна держава обмежувати готівкові розрахунки для боротьби з відмиванням коштів — і де проходить межа між захистом фінансової системи та правом людини на приватність?
5. Як мають трансформуватися традиційні інструменти фінансового моніторингу, щоб ефективно протистояти масовому децентралізованому мікрофінансуванню підривних політичних кампаній?

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-2026-22

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].

AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE