Міністерство
фінансів
України

Методологічний бюлетень AML

№46/2026



Зміст

Торговельні санкції ЄС проти Росії: Європейська рахункова палата фіксує нерівномірне застосування та ризик «форум-шопінгу» 3

Онлайн-шахрайство в ЄС: приховані жертви та еволюція європейського законодавства 8

FINMA оновила Постанову про протидію відмиванню коштів напередодні оцінки FATF: прозорість власності, санкційний комплаєнс і кореспондентські відносини 12

EDPB ухвалила остаточну редакцію Настанов щодо законного інтересу: межі обробки персональних даних для запобігання шахрайству та передавання даних правоохоронцям 17

Заходи OFAC проти транснаціональних мереж кібершахрайства 21

Зброя після війни: як незаконний обіг зброї, бойових дронів і вогнепальних засобів випадає з поля зору систем ПВК/ФТ 25

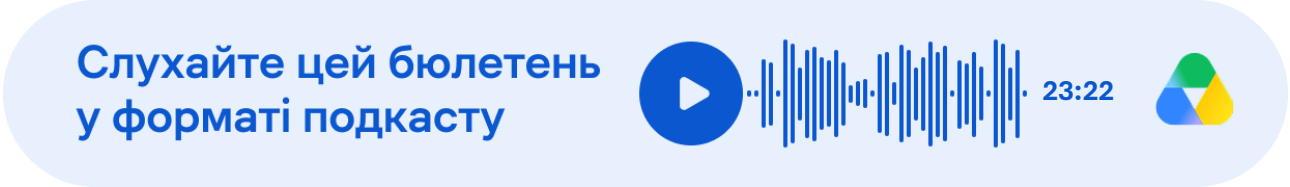
Чому управління даними стає ключовим елементом контролю за фінансовими злочинами 29

Фентаніл і синтетичні наркотики в Північній Америці 32

Конференція європейських наглядових органів 35

Аналіз міжнародних мереж та методів поширення дезінформації у сучасному просторі 37

Трансформація безпекової політики Венесуели 40



Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 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.

Торговельні санкції ЄС проти Росії: Європейська рахункова палата фіксує нерівномірне застосування та ризик «форум-шопінгу» [1]



Європейська рахункова палата оприлюднила спеціальний звіт 30/2026 «EU trade sanctions against the Russian Federation», підзаголовок якого стисло формулює головний висновок: зусилля з координації значні, проте імплементація залишається нерівномірною й обмежує загальний вплив санкцій. Предметом аудиту ефективності було те, наскільки результативно Європейська комісія підтримувала та моніторила застосування торговельних санкцій державами-членами в період з лютого 2022 року до кінця 2025 року. Фінансові санкції, обмеження щодо послуг, транспорту й енергоносіїв, а також рішення Ради ЄС та Європейської служби зовнішніх справ до обсягу аудиту не входили. Доказову базу становлять документи та співбесіди в службах Комісії й ЄСЗД, аналіз торговельних потоків, ознайомчі візити до компетентних органів п'яти держав-членів (Болгарії, Латвії, Нідерландів, Німеччини та Польщі) і консультації з органами Сполученого Королівства.

Аудитори виходять із того, що торговельні санкції мають подвійну природу: вони є інструментом Спільної зовнішньої та безпекової політики, але реалізуються через митний союз, тобто зовнішньополітичних цілей досягають інструментами й системами, створеними для митних органів. Звідси складна архітектура координації. З лютого 2022 року до серпня 2026 року ЄС ухвалив 21 пакет санкцій проти Росії, а строк дії відповідних актів зазвичай становить від шести до дванадцяти місяців, що вимагає їхнього регулярного продовження. Конкретні цілі торговельних санкцій звіт визначає як обмеження доступу Росії до товарів, які використовуються на полі бою та в її військових системах, погіршення промислового потенціалу в середньостроковій перспективі та позбавлення значних джерел доходів через закриття ринків ЄС.

Щодо результатів звіт фіксує глибоке скорочення торгівлі: обсяг торгівлі товарами між ЄС і Росією зменшився з 252,8 млрд євро у 2021 році до 58,3 млрд євро у 2025 році, тобто більш ніж на три чверті, а частка ЄС у товарообігу Росії становила 10,2 %. За оцінками Комісії, вартість експортних обмежень і заборон досягла 49 млрд євро (56 % довоєнного рівня експорту), імпортних – близько 110 млрд євро (75 % довоєнного імпорту). Прямий експорт товарів спільного високого пріоритету

[1] https://www.eca.europa.eu/ECAPublications/SR-2026-30/SR-2026-30_EN.pdf

(CHP) та економічно критичних товарів (ECG) з ЄС до Росії з 2023 року майже припинився. Показовим є аналіз Комісією компонентів, виявлених у нещодавно виготовлених російських ракетах і дронах: лише 8 з 202 ідентифікованих компонентів (близько 4 %) походили безпосередньо з ЄС, тоді як на ширший західний ланцюг постачання припадало близько 72 %. Аудитори трактують це як свідчення ефективності санкцій щодо прямого експорту і водночас як ознаку того, що обхід триває. Росія частково заміщує торгівлю з ЄС: товарообіг Китаю з Росією у 2024 році був на 82 % вищим, ніж у 2021 році, торгівля з Індією зросла більш ніж ушестеро, а ціни, які Росія сплачує за імпорт товарів подвійного використання, зросли на 39 % більше, ніж ціни на ті самі товари для решти світу.

Окремий розділ присвячено обходу санкцій. Аналіз даних Спільного дослідницького центру щодо вибірки товарів CHP у торгівлі з Туреччиною, Вірменією та Казахстаном показує різке зростання імпорту з ЄС і реекспорту до Росії та Білорусі після 2022 року, яке здебільшого повернулося до довоєнного рівня до 2025 року. Водночас аудитори застерігають, що повної та надійної статистики торгівлі Росії з третіми країнами немає, а частина обходу взагалі не відображається в торговельних даних. Як приклад наведено «хибне заміщення» (false backfilling): за даними Київської школи економіки, 44 % товарів, експортованих до Росії з країн, що не застосовують санкцій, виготовлено дочірніми компаніями західних, зокрема європейських, виробників; формально такі операції законні, але по суті є формою обходу. Серед антиобхідних інструментів звіт аналізує механізм заборони експорту до третіх країн, запроваджений 11-м пакетом (2023) і вперше застосований щодо Киргизстану в межах 20-го пакета у 2026 році, переліки CHP і ECG, загальне застереження (catch-all) 18-го пакета (липень 2025), діяльність Спеціального посланця ЄС з питань санкцій (45 місій до 17 країн до кінця 2025 року) та платформу для викривачів, яка до серпня 2026 року отримала понад 2 600 повідомлень; 10 % з них передано національним органам або ЄСЗД, однак оцінити результативність неможливо, бо держави-члени не зобов'язані звітувати про подальші дії. Аудитори фіксують зміщення маршрутів обходу до нових хабів у Південно-Східній Азії.

Юридичний аналіз звіту стосується якості нормативного тексту. Термін «strictly necessary» (суворо необхідний) вживається в Регламенті (ЄС) № 833/2014 63 рази, переважно в контексті дерогацій, що зумовлює різне тлумачення підстав для видачі дозволів; поняття «best efforts» (максимальних зусиль) щодо відповідальності материнських компаній за дочірні структури в третіх країнах не має визначеного мінімального змісту, хоча Комісія первісно пропонувала конкретніший стандарт; невизначеним є й обов'язок вживати «appropriate steps and policies» під час продажу товарів CHP. Розбіжності між санкційною та митною термінологією стосуються, зокрема, поняття «країна походження» та терміна «transfer», що не є митним; відсутність кодів Комбінованої номенклатури в частині A додатка VII та перетин додатків VII і XXIII (окремі позиції, як-от електронні схеми, є в обох) ускладнюють митний контроль. Аудитори прямо пов'язують нечіткість формулювань із потребою досягати одностайності в Раді: гнучкість полегшує ухвалення пакетів, але відкриває простір для нерівномірного застосування. Щодо кримінально-правового виміру звіт констатує, що Директиву (ЄС) 2024/1226 про визначення кримінальних правопорушень і санкцій за порушення обмежувальних заходів ЄС мали транспонувати до 20 травня 2025 року, однак до

серпня 2026 року про повне транспонування повідомили лише 19 держав-членів, а правильність транспонування Комісія ще не оцінювала.

Ключовим ризиком аудитори називають «форум-шопінг» – свідомий вибір юрисдикцій, органів видачі дозволів або митних пунктів із менш суворим контролем. Під час візитів виявлено суттєві відмінності: митниці країн Балтії за певних умов вимагають декларації виробника на санкційні товари, тоді як інші держави – ні. Дерогаційні дозволи не централізовані: за автомобільного перевезення кожна держава, через територію якої рухаються товари, видає окремий дозвіл. Звіт описує випадок, коли товари, зупинені митницями виходу в Литві та Польщі, було повернуто до Італії, де їх знову прийняли до експорту і відправили до Росії через італійський порт, а Комісія заявила, що не має підстав втручатися. Показовою є статистика порушень щодо товарів, що походять з інших держав-членів: Болгарія з 2022 року не зафіксувала жодного такого випадку, тоді як Латвія лише у 2024 році зафіксувала близько 2 100 експортних відправлень, що становили три чверті всіх виявлених нею порушень. Як позитивні практики звіт наводить центральний орган ліцензування в структурі митниці Нідерландів, Балтійську митну ініціативу (Естонія, Латвія, Литва, Польща, Фінляндія, Хорватія) та ризик-орієнтовані постмитні аудити, а реформа митного союзу зі створенням Митного органу ЄС і Митного хабу даних дасть ефект лише в середньостроковій перспективі, оскільки повне впровадження заплановано на 2034 рік.

Інформаційна інфраструктура, за висновком аудиторів, використовується не повною мірою. З 2022 року державами-членами видано понад 12 000 форм ризикової інформації (RIF) у Системі управління митними ризиками (CRMS2), пов'язаних із санкціями, причому половина таких форм щодо Росії та Білорусі стосується випадків, коли митниця виходу відмовила у вивезенні товарів, уже випущених для експорту митницею іншої держави-члена. Держави, що межують з Росією та Білоруссю, використовують систему значно активніше, механізму зворотного зв'язку немає, а Комісія аналізує ці форми лише з 2024 року. У Репозитарії обміну санкційною інформацією (SIER) держави самостійно визначають обсяг даних про дозволи, тож часто бракує класифікації товарів, кількості, сторін і строку дії; обмін інформацією про структури власності та контролю є недостатнім, попри наявність окремого модуля, а доступ до SIER мають не всі митні органи, що здійснюють санкційний контроль. Настанови Комісії (одинадцять загальних настанов і тематичні FAQ, останнє оновлення – травень 2026 року, торговельні сповіщення, Санкційна служба підтримки для бізнесу з 2025 року) держави оцінюють як вичерпні, але вони не мають обов'язкової сили й не охоплюють, зокрема, взаємне визнання дозволів та визначення компетентної держави в багатосторонніх операціях.

Моніторинг ефективності розпорошено між генеральними директоратами Комісії (FISMA, TRADE, TAXUD, ECFIN, JUST), Спільним дослідницьким центром та OLAF без центрального сховища даних і формалізованої політики їх збирання; OLAF з лютого 2022 року відкрив 20 справ щодо імпорту та 8 щодо експорту, зокрема розслідування експорту понад 760 транспортних засобів, задекларованих до третіх країн, але фактично доставлених до Росії. Комісія не має критеріїв оцінки загальної ефективності санкцій, а її оцінки економічного впливу ґрунтуються переважно на торговельних потоках і не охоплюють вплив на окремі компанії, держави-члени та адміністративні ресурси. Палата сформулювала чотири рекомендації: підвищити правову визначеність,

уникаючи неоднозначних термінів і пом'якшуючи розбіжності між митним і санкційним законодавством (2027); провести поглиблений аналіз застосування санкцій державами-членами, зокрема митного контролю, постмитних аудитів і поводження з дозволами (2027); стимулювати повне використання RIF, SIER і надання доступу митним органам до центральних систем (2028); інтегрувати збирання даних і запропонувати критерії оцінки ефективності санкцій із регулярним її проведенням (2028).

Для систем ПВК/ФТ і санкційного комплаєнсу звіт має значення, що виходить за межі митного адміністрування. Він підтверджує, що найбільші вразливості санкційного режиму лежать не в змісті заборон, а в розривах між юрисдикціями, органами та інформаційними системами: у неоднаковому тлумаченні винятків, відсутності взаємного визнання рішень і неповному обміні даними про власність і контроль. Україна входить до Форуму санкційних координаторів, через який Комісія координує застосування санкцій з міжнародними партнерами, тож описані типології – реекспорт через «платформні» країни, зміщення маршрутів до Південно-Східної Азії, «хибне заміщення» через дочірні компанії та використання розбіжностей між митними пунктами – безпосередньо релевантні для оцінки ризиків українськими банками, митними й правоохоронними органами.

Висновки

«Форум-шопінг» є системною типологією обходу, а не сукупністю поодиноких порушень: розбіжність між нулем зафіксованих порушень у Болгарії та близько 2 100 відправленнями в Латвії, відсутність взаємного визнання дозволів і випадок повторного експорту через італійський порт свідчать, що маршрут, місце митного оформлення та попередні відмови у вивезенні мають розглядатися фінансовими установами як самостійні фактори ризику під час торговельного фінансування.

Дані про власність і контроль залишаються найслабшою ланкою: недостатній обмін такими даними в SIER і частка 44 % «хибного заміщення» через дочірні компанії західних виробників означають, що належна перевірка в санкційному контексті не може обмежуватися країною походження товару, а має охоплювати структуру корпоративної групи постачальника й покупця.

Неоднозначна термінологія переходить у національне правозастосування: терміни на кшталт «strictly necessary» (63 вживання в Регламенті № 833/2014) та «best efforts», а також неповне транспонування Директиви (ЄС) 2024/1226 (19 держав-членів станом на серпень 2026 року) показують, наскільки важливими є точні визначення складів порушень і узгодження санкційних понять із митними під час розроблення національного законодавства про відповідальність за порушення санкцій.

Ефективність санкцій потребує вимірюваних критеріїв і зворотного зв'язку: відсутність критеріїв оцінки, понад 2 600 повідомлень викривачів без даних про подальші дії та понад 12 000 RIF без механізму зворотного зв'язку відображають ширшу проблему, знайому і системам фінансового моніторингу: без систематичного зворотного зв'язку від органів, що отримують інформацію, неможливо оцінити якість повідомлень і скоригувати підходи до виявлення ризиків.

Онлайн-шахрайство в ЄС: приховані жертви та еволюція європейського законодавства [2]



Онлайн-шахрайство перетворилося на одну з найдинамічніших та найприбутковіших сфер організованої злочинності, що стрімко зростає як за обсягами, так і за рівнем складності. Технологічний прогрес, зокрема автоматизація, використання штучного інтелекту та модель "злочинність як послуга" (crime-as-a-service), значно полегшили діяльність зловмисників.

Сучасні схеми шахрайства розробляються з ретельно продуманими стратегіями маніпуляції, спрямованими на те, щоб змусити жертв надсилати гроші або розкривати конфіденційну інформацію. Масштаби проблеми вражають: за даними Europol, шахрайські схеми є найшвидше зростаючим напрямком організованої злочинності. У Сполучених Штатах, за даними ФБР, збитки від інтернет-шахрайства у 2024 році перевищили 16 мільярдів доларів, що на 33% більше, ніж у 2023 році, а за оцінками Global Anti-Scam Alliance, глобальні втрати від шахрайства у 2025 році сягнули 442 мільярдів доларів. В Європейському Союзі ситуація також є критичною: згідно зі звітом Агентства з фундаментальних прав (FRA) за 2026 рік, кожен четвертий житель ЄС став жертвою онлайн-шахрайства протягом свого життя, причому понад третина з них постраждали від більш ніж однієї схеми.

Найпоширенішим типом є фальшиві інтернет-магазини, за ними йдуть шахрайство з імітацією особи (impersonation scams) та інвестиційні афери. Романтичне шахрайство також є досить поширеним, вражаючи 11% жертв. Молоді дорослі віком 25-39 років є найбільш уразливою групою (майже кожен третій ставав жертвою), що, ймовірно, зумовлено їхньою більшою залученістю до інтернету, хоча вік не впливає на тип шахрайства, від якого страждають люди. Масштаби проблеми варіюються між країнами-членами: якщо в Греції та Румунії лише 11% людей заявляють, що стали жертвами онлайн-шахрайства, то в Естонії та Люксембурзі цей показник сягає 39%.

Привабливість онлайн-шахрайства для організованих злочинних угруповань зумовлена низкою факторів. Початкові витрати на запуск кібершахрайства є мінімальними завдяки доступності сервісу "злочинності як послуги", який пропонує програмне забезпечення, створення веб-сайтів та IT-підтримку. Крім того, в даркнеті доступні персональні дані, банківські реквізити, імена користувачів та паролі, а також існують готові скрипти для певних типів шахрайства. Штучний інтелект зробив онлайн-шахрайство набагато простішим у виконанні, а охоплення зловмисників стало глобальним.

[2] https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/797012/EPRS_BRI(2026)797012_EN.pdf

Одним із найтривожніших аспектів сучасного онлайн-шахрайства є існування так званих "шахрайських центрів" (scam centres) керованих міжнародними злочинними організаціями, які працюють у промислових масштабах. Ці центри, що налічують від кількох сотень до кількох тисяч працівників, здебільшого розташовані в Південно-Східній Азії, хоча з часом поширилися на Близький Схід, Північну Африку, Центральну Америку та Західну Африку. Більшість працівників цих центрів є жертвами примусової праці та торгівлі людьми. За оцінками Міжнародної організації з міграції, щонайменше 300 000 осіб були перевезені з метою експлуатації в Південно-Східній Азії, а в 2023 році ООН повідомила про щонайменше 120 000 осіб у М'янмі та близько 100 000 у Камбоджі, які працюють виключно в онлайн-шахрайстві. Людей заманюють фальшивими оголошеннями про роботу з високими зарплатами, після чого утримують у закритих комплексах, переобладнаних готелях або багатоповерхівках, де вони працюють по 12-20 годин на добу в небезпечних умовах під охороною, за колючим дротом та під наглядом камер. Тих, хто намагається втекти або не виконує норми шахрайства, піддають погрозам або застосуванню насильства.

Проблема жертв онлайн-шахрайства полягає не лише в фінансових втратах, а й у стигматизації та недостатній підтримці. Існує тенденція визначати жертв як наївних або жадібних людей, які зробили нерозумні рішення, що посилює звинувачення жертв і перешкоджає повідомленню про злочини. Згідно зі звітом FRA, 56% жертв онлайн-шахрайства не повідомили про це поліції чи будь-якій іншій службі. Рівень повідомлень зростає з віком: 11% людей віком 15-24 років повідомляють про шахрайство поліції, тоді як серед осіб 55 років і старше цей показник становить 18%. Існують значні відмінності між країнами-членами: 28% повідомляють поліції у Швеції, 6% – у Румунії та Словенії, а в Угорщині та Польщі жертви частіше звертаються до інших організацій, а не до поліції. Крім того, жертви часто стають об'єктом повторної віктимізації, коли їхні дані продаються іншим злочинцям, які видають себе за правоохоронців або юристів, пропонуючи допомогу в поверненні вкрадених коштів за попередню оплату. Транснаціональний характер онлайн-шахрайства ускладнює отримання жертвами достатньої підтримки від правоохоронних органів, банків та соціальних служб, оскільки розслідування часто зосереджуються на злочинцях, залишаючи жертв осторонь.

Міжнародна відповідь на цю загрозу отримала новий імпульс завдяки Конвенції ООН проти кіберзлочинності (Ханойська конвенція), глобальному договору, спрямованому на створення міжнародної рамки співпраці для запобігання та подолання кіберзлочинності та онлайн-шахрайства. Конвенція, значною мірою заснована на Будапештській конвенції Ради Європи, вводить спільне розуміння правопорушень та визначає процедури міжнародних розслідувань, збору, збереження та обміну електронними доказами. ЄС дав згоду на укладення угоди через Рішення Ради (ЄС) 2026/1347 у червні 2026 року. Конвенція набуде чинності після приєднання 40 держав; наразі її підписали 95 країн, але лише три стали сторонами.

На рівні ЄС діє комплексна система інструментів, що охоплює багато аспектів цього виду шахрайства. Регламент про цифрові послуги (DSA) є одним із головних інструментів боротьби з онлайн-шахрайством на великих платформах, вимагаючи від них спрощення процедур звітування про шахрайський контент та швидкого реагування на повідомлення про фальшиві

інтернет-магазини, шахрайські оголошення та фінансові афери. Європейська комісія вже надіслала офіційні запити Apple, Google та Microsoft щодо фальшивих банківських додатків, шахрайських результатів пошуку та фальшивих оголошень.

Директива NIS 2 встановлює оновлену структуру кібербезпеки ЄС, вимагаючи від організацій впровадження суворого управління ризиками, обов'язкового навчання працівників та контролю за безпекою ланцюгів поставок для запобігання фішингу та компрометації ділової електронної пошти. Регламент про миттєві платежі (ЄС) 2024/886 вимагає від постачальників платіжних послуг здійснювати миттєві кредитні перекази в євро протягом 10 секунд та пропонувати платнику безкоштовну послугу перевірки отримувача. Директива (ЄС) 2019/713 про безготівкові платежі забезпечує ефективне правозастосування щодо шахрайства з безготівковими засобами платежу. Європейський кодекс електронних комунікацій (EECC) встановлює правила функціонування електронних комунікаційних мереж та послуг, включаючи захист споживачів. Регламент про Europol надає агентству мандат підтримувати держави-члени у розслідуваннях транскордонного шахрайства. Директива про права жертв (ЄС) 2026/1472 опосередковано захищає жертв онлайн-шахрайства. Крім того, існує низка законодавчих актів про захист прав споживачів, включаючи Директиву про недобросовісну комерційну практику, Директиву про права споживачів та Регламент про загальну безпеку продуктів.

Майбутні політичні ініціативи ЄС зосереджені на подальшому вдосконаленні законодавства. Після завершення огляду EECC у січні 2026 року Комісія запропонувала Регламент про Закон про цифрові мережі (DNA), який має замінити EECC та забезпечити уніфіковане застосування телекомунікаційних правил, а також переглянути Регламент BEREC, Регламент про відкритий інтернет, Директиву про електронну конфіденційність та програму радіочастотної політики. Того ж місяця Комісія розпочала збір доказів для майбутнього плану дій проти онлайн- та телефонного шахрайства, спрямованого на покращення транскордонної співпраці між регуляторами, правоохоронними органами та приватними компаніями, краще виявлення шахрайства, полегшення повернення вкрадених коштів та посилення підтримки жертв.

Комісія також виявила недоліки в Директиві про платіжні послуги (PSD2) і запропонувала її перегляд – Директиву PSD3 та Регламент про платіжні послуги на внутрішньому ринку, які містять заходи боротьби з платіжним шахрайством, включаючи обмін інформацією про шахрайство між постачальниками платіжних послуг, підвищення обізнаності споживачів, посилення правил автентифікації клієнтів та розширення прав на відшкодування для жертв. Ці пропозиції планується ухвалити на пленарному засіданні в грудні 2026 року. Крім того, 26 травня 2026 року Група співробітництва NIS2 ухвалила спільні шаблони для звітування про інциденти, що забезпечить чіткий та уніфікований формат, зменшуючи адміністративне навантаження на компанії, хоча Комісія ще має ухвалити імплементаційний акт, щоб зробити ці шаблони обов'язковими в усіх державах-членах.

Таким чином, онлайн-шахрайство в ЄС є складною, багатогранною проблемою, яка вимагає скоординованих дій на національному, європейському та міжнародному рівнях. Незважаючи на

значний прогрес у розробці законодавчих інструментів, боротьба з цим явищем ускладнюється його швидкою еволюцією, транснаціональним характером та використанням новітніх технологій.

Ключовими викликами залишаються підвищення обізнаності громадян, покращення системи звітування та підтримки жертв, а також посилення міжнародної співпраці для ефективного переслідування злочинних організацій, які стоять за цими схемами.

Висновки

Онлайн-шахрайство є найшвидше зростаючим напрямком організованої злочинності в ЄС: кожен четвертий житель Союзу ставав жертвою, а понад третина постраждалих зазнали повторних атак, причому найпоширенішими є фальшиві інтернет-магазини, шахрайство з імітацією особи та інвестиційні афери.

Значна частина шахрайських схем походить із «скам-центрів» у Південно-Східній Азії та інших регіонах, де працюють сотні тисяч людей, які самі є жертвами торгівлі людьми та примусової праці, що робить цю проблему не лише фінансовою, а й гуманітарною.

Понад половина жертв (56%) не повідомляють про шахрайство поліції чи іншим організаціям, що значно ускладнює розслідування, а стигматизація постраждалих та транснаціональний характер злочинів перешкоджають наданню їм належної підтримки.

ЄС реагує на загрозу комплексно, а міжнародна співпраця посилюється завдяки Ханойській конвенції ООН, хоча її практичне застосування ще попереду.

FINMA оновила Постанову про протидію відмиванню коштів напередодні оцінки FATF: прозорість власності, санкційний комплаєнс і кореспондентські відносини [3]



10 листопада 2026 року Швейцарський орган нагляду за фінансовими ринками (FINMA) оприлюднив часткову ревізію Постанови FINMA про протидію відмиванню коштів (GwV-FINMA). Одночасно Рада директорів FINMA визнала мінімальними стандартами переглянуту Угоду про кодекс поведінки швейцарських банків щодо належної перевірки (VSB 27) та регламент саморегулівної організації Швейцарської асоціації страховиків (SRO-SVV). Постанова й обидва набори правил саморегулювання набирають чинності 1 січня 2027 року, причому для правил саморегулювання передбачено чотиримісячний перехідний період. Пакет документів містить попередню редакцію акта про зміни (остаточну буде опубліковано у Fedlex), пояснювальний звіт від 29 жовтня 2026 року, звіт про консультації, позиції учасників і окреме наглядове повідомлення FINMA 06/2026 щодо Циркуляра FINMA 2011/1.

Ревізія впроваджує зміни до Закону про протидію відмиванню коштів (GwG), ухвалені парламентом паралельно з Федеральним законом про прозорість юридичних осіб та ідентифікацію бенефіціарних власників (TJPG) від 26 вересня 2025 року, яким запроваджено федеральний реєстр прозорості; обидва закони набрали чинності 1 жовтня 2026 року, а Федеральна рада відповідно змінила свою постанову (GwV) і 12 червня 2026 року ухвалила імплементаційну постанову до TJPG. Головним рушієм FINMA прямо називає зауваження FATF за результатами четвертого раунду взаємної оцінки (звіт грудня 2016 року) та звіту про прогрес (жовтень 2023 року), а також критику Глобального форуму OECP (оцінка 2020 року) щодо підходу до сумнівів у контролі над компаніями. Виїзну місію FATF п'ятого раунду очікують у травні–липні 2027 року; оскільки для оцінки враховуються лише норми, чинні до завершення виїзної місії, FINMA відмовилася від попередніх консультацій і скоротила публічні консультації до одного місяця (12 травня – 9 червня 2026 року).

Центральною новелою є нова стаття 9b: фінансовий посередник зобов'язаний розуміти структуру власності та контролю контрагента. Пояснювальний звіт розкриває цю вимогу через поняття «простежуваності» відносин власності та контролю: посередник має бачити, які фізичні особи в

[3] https://www.finma.ch/en/news/2026/11/20261110-mm-gwv-finma/

кінцевому підсумку контролюють компанію, об'єднання осіб, траст, інше відокремлене майно чи операційну компанію і в який спосіб цей контроль здійснюється, щоб правильно ідентифікувати й верифікувати контролерів і бенефіціарних власників. Норма є відповіддю на висновок FATF 2023 року за критерієм 10.8 про відсутність явної вимоги розуміти структуру власності для всіх типів компаній. Глибина з'ясування визначається ризиком ділових відносин – чим складніша й ризикованіша структура, тим ґрунтовніше дослідження; як приклад наведено доміциліарну компанію, що є базовою компанією трасту. Для складних структур рекомендовано схематичне зображення, а результати з'ясування мають документуватися відповідно до ст. 7 GwG і ст. 22 GwV-FINMA. Стаття 9b доповнює чинні норми про з'ясування причин використання доміциліарних компаній (ст. 9a) та про складні структури як ознаку підвищеного ризику (ст. 13 ч. 2 п. h); FINMA підкреслює, що нового матеріального обов'язку не створено, а кодифіковано наявну наглядову практику.

Стаття 9b стала найбільш дискусійною під час консультацій. Швейцарська асоціація банкірів, economiesuisse та SRO Асоціації лізингу ставили під сумнів її необхідність і достатність правової підстави, вимагали розмежувати операційні компанії, де встановлюються контролери, і доміциліарні структури, а також визначити, що саме означає «простежуваність» у змістовному і формальному вимірах; низка учасників просила закріпити ризик-орієнтований обсяг вимоги безпосередньо в тексті. Пропонувалося також створити центральний реєстр бенефіціарних власників із суворішими порогами участі та відображенням усіх ланцюгів володіння, а також визнати як доказ верифіковані облікові дані за Законом про електронну ідентифікацію. FINMA відхилила ці пропозиції по суті: правовою підставою визначено повноваження конкретизувати обов'язки з належної перевірки (ст. 17 ч. 1 п. a GwG) та обов'язок з належною ретельністю встановлювати бенефіціарних власників (ст. 4 ч. 1 GwG); розмежування контролерів і бенефіціарних власників суперечило б пояснювальній записці до Рекомендації 10 FATF (критерії 10.10–10.11); реєстр прозорості вже створено на підставі TJPG, а чинні пороги відповідають вимогам FATF. Ризик-орієнтований підхід, приклад, взаємодію норм і вимоги до документування відображено лише в пояснювальному звіті; текст статті не змінено.

Ту саму логіку посилення прозорості власності продовжують зміни до положень про встановлення контролюючих осіб. Відповідно до нової редакції ч. 2 ст. 56, якщо компанія не контролюється особами, визначеними на першому рівні каскаду, або існують сумніви щодо цього, посередник повинен отримати від контрагента письмове повідомлення про те, хто контролює компанію. Зміна відповідає на критику Глобального форуму OECP і FATF (критерій 10.10) щодо «другого рівня каскаду» та формалізує обов'язок повторної ідентифікації в разі сумнівів, уже закріплений у ст. 5 GwG і правилах банківського кодексу; саме тому її, за поясненням FINMA, можна було внести після консультацій. Новий п. d ч. 2 ст. 65 вимагає завжди отримувати повідомлення про бенефіціарного власника, якщо контрагент веде субрахунки для окремих клієнтів, оскільки такі рахунки несуть ризики, які інакше важко контролювати. Водночас скасовано ч. 3 ст. 10, яка дозволяла розглядати платежі до Ліхтенштейну та з нього як внутрішні й не передавати повний набір даних: норма втратила практичне значення після запровадження QR-рахунку з 1 липня 2020 року, а FATF вважала її несумісною зі своїми стандартами.

Другим масштабним блоком є новий розділ 5 «Заходи із запобігання порушенням примусових заходів відповідно до Закону про ембарго (EmbG)» з новою ст. 30, а мету постанови (ст. 1) розширено на запобігання таким порушенням. Правовою підставою є оновлена ст. 8 у поєднанні зі ст. 1 GwG, що, за поясненням FINMA, імплементує Рекомендації 1 і 2 FATF у частині фінансування розповсюдження зброї масового знищення. Стаття 30 передбачає відповідне застосування положень про платежі (ст. 10), моніторинг (ст. 20), нові продукти й технології (ст. 23), комплаєнс-функцію (ст. 24, 25), внутрішні директиви (ст. 26), персонал (ст. 27) і залучення третіх осіб (ст. 28–29). Пояснювальний звіт конкретизує, що санкції завжди становлять підвищений ризик, тож ділові відносини й операції мають перевірятися до їх здійснення; регулярний автоматизований санкційний скринінг є частиною обов'язку моніторингу для банків і торговців цінними паперами; скринінг охоплює вхідні та вихідні платежі й усіх учасників – платників, отримувачів та інших посередників. Нагляд розподілено: дотримання самого Закону про ембарго контролює Державний секретаріат з економічних питань (SECO), тоді як FINMA наглядає за організаційними вимогами, управлінням ризиками та внутрішнім контролем.

Учасники консультацій наголошували на принциповій відмінності між моніторингом операцій у сфері ПВК/ФТ, що здійснюється переважно постфактум, і санкційним скринінгом, який має превентивний характер, застерігали від поширення відповідальності за законодавством про ПВК/ФТ на сфери, урегульовані спеціальними законами, і пропонували диференціювати вимоги залежно від типу й розміру установи або вилучити посилання на ст. 20. FINMA погодилася з відмінністю природи цих механізмів, але наголосила, що обов'язок дотримуватися санкцій діє незалежно від виду діяльності, розміру чи ризику посередника, а градація заходів уже закладена в чинних нормах (обов'язкова IT-система моніторингу для банків і торговців цінними паперами, полегшення для окремих посередників за ст. 75 і 75a); пояснення щодо відповідного застосування ст. 20 розширено, текст норми не змінено. У сфері кореспондентських відносин (ст. 37) із ч. 3 вилучено слова «залежно від обставин»: посередник завжди має з'ясовувати, які заходи з ПВК/ФТ здійснює банк-респондент, а обсяг перевірки залежить від того, чи підлягає респондент належному регулюванню й нагляду. Норма поширюється й на банки однієї групи, оскільки Рекомендація 13 FATF не передбачає винятку для груп. Нова ч. 5 дозволяє виконувати платежі клієнтів респондента, які мають прямий доступ до наскрізних рахунків (payable-through accounts), лише якщо посередник переконався, що респондент виконав обов'язки з належної перевірки й надасть відповідні документи на запит (у широкому розумінні – від деталей операцій до KYC-профілів). Після консультацій сферу дії ч. 5 звужено саме до клієнтів із прямим доступом, щоб не охопити звичайні востро-рахунки, що узгоджується з Рекомендацією 13 FATF; посилання в ст. 35, 40, 41 і 42 оновлено відповідно до VSB 27 та регламенту SRO-SVV від 23 жовтня 2026 року.

Звіт про консультації (публікацію позицій погодили одинадцять учасників – від Швейцарської асоціації банкірів і Raiffeisen до Wise та IT-постачальників) окреслює межі повноважень FINMA. Відхилено пропозиції поширити організаційні вимоги на Закон про заморожування та повернення незаконних активів іноземних ПЕП, оскільки законодавець обмежив мандат FINMA Законом про ембарго; врегулювати розбіжності між висновками посередника та даними реєстру прозорості, оскільки FINMA не має повноважень ухвалювати норми щодо цього реєстру;

запровадити обов'язковий скринінг негативних публікацій, оскільки правила моніторингу операцій свідомо залишаються принциповими, а очікування FINMA (виявлення операцій, пов'язаних із країнами високого ризику, і відхилень від звичайної поведінки клієнта та порівнянних відносин) було сформульовано ще у 2017 році. Окремо врегульовано наслідки розширення сфери дії GwG на окремі консультаційні послуги, зокрема щодо операцій з нерухомістю та створення й структурування юридичних осіб. Згідно з наглядовим повідомленням 06/2026, Циркуляр 2011/1 застосовується лише до діяльності фінансових посередників за ч. 2 і 3 ст. 2 GwG і не поширюється на консультантів, а його положення щодо страхових посередників, адвокатів і нотаріусів, сектору нерухомості та державної діяльності не застосовуються, якщо суперечать закону, і будуть переглянуті. Нагляд за консультаційною діяльністю банків та інших посередників, що перебувають під прямим наглядом FINMA, здійснює FINMA (ст. 12a ч. 1 GwG), за діяльністю інших посередників – відповідні наглядові та саморегулівні організації, тоді як щодо «чистих» консультантів FINMA некомпетентна.

Висновки

Розуміння структури власності та контролю стає окремим документованим обов'язком: поєднання ст. 9b (простежуваність ланцюга до фізичних осіб, схеми для складних структур, документування) з письмовою декларацією в разі сумнівів щодо контролера (ч. 2 ст. 56) показує, як оцінювачі FATF тлумачать критерії 10.8 і 10.10: недостатньо зафіксувати бенефіціарного власника, потрібно продемонструвати, як і через які ланки він здійснює контроль.

Санкційний комплаєнс вбудовується в архітектуру ПВК/ФТ без змішування функцій: санкції завжди вважаються підвищеним ризиком, перевірка здійснюється до виконання операції й охоплює всіх учасників платежу, а нагляд розподілено між SECO і FINMA; такий підхід дозволяє використати наявні комплаєнс-процеси, водночас чітко відокремлюючи превентивний скринінг від подальшого моніторингу операцій.

Кореспондентські відносини не мають групового винятку: обов'язкова оцінка контролів респондента навіть у межах однієї групи та умовність payable-through accounts (виконання обов'язків з належної перевірки й надання документів на запит) відображають підхід Рекомендації 13 FATF, де ризик визначається наявністю кореспондентських відносин, а не корпоративною близькістю сторін.

Графік підготовки до взаємної оцінки визначає регуляторні рішення: скорочення консультацій до одного місяця через вимогу, щоб норми набрали чинності до завершення виїзної місії FATF, і кодифікація наявної наглядової практики для правової визначеності демонструють, що технічна відповідність потребує явних норм у нормативних актах, а не лише усталеної практики нагляду.

EDPB ухвалила остаточну редакцію Настанов щодо законного інтересу: межі обробки персональних даних для запобігання шахрайству та передавання даних правоохоронцям [4]

Європейська рада із захисту даних (EDPB) ухвалила версію 2.0 Настанов щодо обробки персональних даних на підставі пункту (f) частини 1 статті 6 GDPR (законний інтерес). Першу версію документа було ухвалено 8 жовтня 2024 року для публічних консультацій, які тривали до 20 листопада 2024 року. Остаточна редакція інтегрує новішу практику Суду ЄС, зокрема рішення у справах Mousse (січень 2025 року) і NTH Haustechnik (червень 2026 року), а також узгоджується з іншими документами EDPB – Висновком 28/2024 щодо моделей штучного інтелекту, настановами щодо псевдонімізації, наукових досліджень і анонімізації. Для сфери ПВК/ФТ документ важливий тим, що визначає правову підставу обробки даних у ситуаціях, де комплаєнс-функції діють поза межами прямих законодавчих обов'язків: під час запобігання шахрайству, забезпечення інформаційної безпеки, повідомлення правоохоронних органів про можливі злочини та реагування на запити органів третіх країн.

Настанови виходять із того, що законний інтерес є однією з шести рівноцінних правових підстав і не може слугувати «останнім засобом» чи «відчиненими дверима» для обробки, не охопленої іншими підставами; оскільки Суд ЄС вимагає обмежувального тлумачення підстав статті 6, EDPB наполягає на вузькому застосуванні пункту (f). Обробка допустима лише за трьох умов: наявності законного інтересу контролера або третьої особи, необхідності обробки для його досягнення та відсутності переваги інтересів, прав і свобод суб'єкта даних. Оцінку необхідно провести й задокументувати до початку обробки відповідно до принципу підзвітності, окремо для кожної мети. Органи публічної влади не можуть покладатися на законний інтерес під час виконання своїх завдань; виняток можливий лише для діяльності, не пов'язаної з публічними повноваженнями, якщо це дозволяє національне право, і з обов'язковим внутрішнім документуванням.

Принципово важливим для фінансового сектору є розмежування законного інтересу та юридичного обов'язку. Інтерес має бути правомірним, чітко сформульованим, реальним і наявним, а не гіпотетичним. Ширші суспільні інтереси EDPB не ототожнює з інтересами третіх осіб: якщо закон зобов'язує приватного оператора сприяти протидії незаконній діяльності, первинною підставою є пункти (c) або (e) частини 1 статті 6; якщо ж контролер виходить за межі таких обов'язків, він має довести власний законний інтерес або інтерес конкретної третьої особи, а законний інтерес не може використовуватися для обходу законодавчих вимог чи обмежень. З посиланням на рішення Суду ЄС у справі Meta v Bundeskartellamt (C-252/21) Настанови

[4] https://www.edpb.europa.eu/system/files/2026-11/edpb_guidelines_202401_legitimateinterest_v2_en.pdf

нагадують, що передавання даних правоохоронним органам для запобігання злочинам або їх переслідування саме по собі є законним інтересом, проте за загальним правилом не є законним інтересом контролера, діяльність якого має переважно економічний і комерційний характер. Рішення у справі NTH Haustechnik додатково встановлює, що контролер-одержувач не може посилатися на законний інтерес щодо даних, про незаконне збирання яких передавальною стороною він знав або мав знати.

Критерій необхідності трактується суворо: обробка має бути не просто корисною, а «суворо необхідною», і контролер повинен перевірити, чи можна досягти мети так само ефективно менш обтяжливими засобами, з урахуванням принципу мінімізації даних. На етапі зважування інтересів враховуються характер даних (зокрема особливі категорії, дані про кримінальні правопорушення та фінансові дані), контекст (масштаб, поєднання з іншими масивами, доступність, відносини сторін, уразливість суб'єктів) і наслідки (правові наслідки, дискримінація, репутаційна чи фінансова шкода, стримувальний ефект). Розумні очікування суб'єктів оцінюються об'єктивно: усталена галузева практика й інформаційні повідомлення самі по собі їх не формують. За високого ризику обов'язковою є оцінка впливу на захист даних, а пом'якшувальні заходи – додаткова прозорість, безумовна можливість відмовитися від обробки, видалення даних понад вимоги закону, часовий розрив між збиранням і використанням – мають бути задокументовані так, щоб було видно, як вони змінюють результат зважування інтересів.

Розділ 4.3 присвячено запобіганню шахрайству. Хоча преамбула 47 GDPR визнає законним інтересом обробку, «суворо необхідну» для запобігання шахрайству, EDPB підкреслює, що це не автоматична підстава: тести необхідності та балансування застосовуються повною мірою, а обробка проти шахрайства часто зачіпає й невинних осіб. Шахрайство визначено як навмисну оманливу дію чи бездіяльність з метою отримання неналежної переваги, а запобігання – як сукупність заходів проти такої поведінки. У цій сфері, крім інтересу постачальника послуг, можуть існувати інтереси клієнтів і третіх осіб, які іноді збігаються із ширшим суспільним інтересом і додають ваги під час зважування інтересів. Контролер повинен конкретно визначити, на запобігання яким видам шахрайства спрямована обробка і які дані для цього справді потрібні, а політика зберігання має враховувати принцип обмеження строку зберігання. Загальне посилання на «протидію шахрайству» в повідомленні про конфіденційність визнано недостатнім. Повідомлення правоохоронних органів може переважати права суб'єкта лише тоді, коли дані точні й доказово релевантні для оцінки ризику віктимізації чи причетності. Якщо обробку для запобігання шахрайству вимагає закон, належною підставою є пункт (c), а дані, зібрані з іншою метою, які випадково виявили ознаки шахрайства, можуть оброблятися далі лише з дотриманням правил щодо подальшої обробки.

Розділ 4.7 врегульовує передавання даних компетентним органам. Відповідно до преамбули 50 GDPR повідомлення про можливі злочини чи загрози громадській безпеці та передавання відповідних даних в окремих випадках є законним інтересом, однак узагальнене, превентивне й систематичне звітування приватних операторів цим положенням не передбачено, а передавання заборонено, якщо воно суперечить обов'язку зберігати таємницю. Дані, правомірно зібрані з іншою метою, зазвичай можна передати правоохоронцям. Водночас, з посиланням на справу

Meta, приватний економічний оператор за загальним правилом не може спиратися на законний інтерес для збирання та передавання даних з метою правоохоронної діяльності – для цього потрібен конкретний юридичний обов'язок; законний інтерес можна розглядати, якщо оператор не збирає дані превентивно й систематично для такої мети, а лише повідомляє про злочини, про які дізнався випадково. Приклад 8 ілюструє цю логіку: повідомлення наглядовому органу про витік даних після кібератаки ґрунтується на юридичному обов'язку, тоді як передавання органам з кіберзлочинності додаткових даних, як-от IP-адрес, може спиратися на законний інтерес за умови необхідності.

Окремо розглянуто запити органів третіх країн. Контролер має спершу проаналізувати контекст і правову основу запиту: якщо він обов'язковий і виконуваний на підставі міжнародної угоди, застосовується пункт (c), якщо співпраця дозволена, але не обов'язкова, – пункт (e), у виняткових випадках (наприклад, щодо викрадених дітей) – життєво важливі інтереси. Контролер може мати законний інтерес у виконанні запиту, зокрема коли невиконання тягне санкції за іноземним правом, але тести необхідності й балансування зберігаються; EDPB нагадує, що у спільній відповіді 2019 року щодо американського CLOUD Act інтереси суб'єктів даних переважили інтерес уникнути санкцій. Розкриття даних органу за межами ЄЕЗ є міжнародним передаванням і потребує дотримання глави V GDPR. Щодо інформаційної безпеки (розділ 4.6) Настанови визнають можливість спиратися на законний інтерес з урахуванням рішення у справі Breyer, преамбули 49 GDPR і преамбули 121 Директиви NIS2, але застерігають від надмірної обробки, як-от глибокої інспекції пакетів; щодо передавання даних у межах групи підприємств для внутрішніх адміністративних цілей (розділ 4.5) – така обробка також не є автоматично виправданою й підлягає повній оцінці.

Завершальний блок стосується прав суб'єктів даних. Особу необхідно повідомити, що підставою обробки є законний інтерес, і розкрити, у чому він полягає; EDPB рекомендує оприлюднювати результати балансування заздалегідь або надавати їх на запит. Право на заперечення за частиною 1 статті 21 GDPR встановлює вищий поріг, ніж первинне балансування: контролер має довести «переконливі законні підстави», що переважають інтереси особи з огляду на її конкретну ситуацію, і тягар доказування лежить на ньому. У сукупності Настанови чітко розмежовують обробку, яку вимагає законодавство (належна перевірка клієнтів, звітування до підрозділу фінансової розвідки), і добровільні заходи – внутрішні антишахрайські бази, обмін сигналами шахрайства, ініціативне повідомлення правоохоронців, для яких законний інтерес можливий лише за суворої, наперед задокументованої оцінки.

Висновки

Межа між юридичним обов'язком і законним інтересом визначає правову підставу комплаєнс-обробки: належна перевірка клієнтів і звітування, що вимагаються законом, ґрунтуються на пункті (c) частини 1 статті 6 GDPR, тоді як добровільні антишахрайські заходи понад законодавчі вимоги потребують окремої, задокументованої до початку обробки оцінки за трьома кроками; законний інтерес не може використовуватися для обходу законодавчих обмежень.

Антишахрайська обробка має бути конкретизованою, а не загальною: контролер повинен визначити види шахрайства, на які спрямовано заходи, необхідні категорії даних і строки їх зберігання, враховувати вплив на непричетних осіб і повідомляти суб'єктів про конкретні цілі, оскільки загальне посилання на «протидію шахрайству» Настанови визнають недостатнім.

Ініціативне передавання даних правоохоронцям допустиме лише в окремих випадках: з огляду на справу Meta комерційні оператори не можуть превентивно й систематично збирати дані для правоохоронних цілей без юридичного обов'язку, тому моделі обміну інформацією між приватним сектором і державними органами потребують чіткого законодавчого підґрунтя, а не лише посилання на суспільно корисну мету.

Запити іноземних органів потребують окремого правового аналізу: обов'язковість запиту, наявність міжнародної угоди та вимоги до міжнародного передавання даних визначають, чи може фінансова установа розкрити інформацію, а загроза санкцій за іноземним правом сама по собі не є вирішальною.

Заходи OFAC проти транснаціональних мереж кібершахрайства [5]

5 листопада 2026 року Управління з контролю за іноземними активами (OFAC) Міністерства фінансів США оголосило про черговий етап боротьби з глобальною кіберзлочинністю.

Санкції були запроваджені проти чотирьох фізичних осіб та сорока однієї компанії, які утворюють складну, розгалужену корпоративну та фінансову інфраструктуру, що забезпечує функціонування так званої Транснаціональної злочинної організації Prince Group. Цей крок є логічним продовженням попередніх хвиль тиску, розпочатих у жовтні 2025 та червні 2026 років, і демонструє стратегічний зсув у політиці Вашингтона: від переслідування окремих лідерів до системного знищення самої екосистеми, що дозволяє злочинцям почуватися безкарно. Окремою мішенню став малайзієць Чуї Кок Ва (Chui Kok Wa), який керував мережею шахраїв, що ошукали американців на понад 400 тисяч доларів у цифрових активах, що підкреслює глобальний характер загрози та рішучість США застосовувати безпекові інструменти для захисту своїх громадян.

За офіційною заявою Міністра фінансів Скотта Бессента, кібершахрайські синдикати продовжують викрадати мільярди доларів у американських платників податків, покладаючись при цьому на складні міжнародні бізнес-мережі для відмивання незаконних доходів. Нові санкції, запроваджені на виконання Указу Президента США Дональда Трампа від 6 березня 2026 року (E.O. 14390) щодо боротьби з кіберзлочинністю та шахрайством, спрямовані на те, щоб позбавити ці організації будь-яких шансів на виживання. Аналіз документа свідчить, що Prince Group не є простою бандою, а виступає як складна транснаціональна корпорація, що використовує легальні бізнес-структури, офшорні юрисдикції та професійних фінансових посередників для відмивання коштів, отриманих від цифрових інвестиційних афер, романтичних шахрайств та інших видів онлайн-обману.

Ключовим елементом цієї злочинної екосистеми, як наголошується в документі, є використання масштабних шахрайських таборів у Південно-Східній Азії, де торгівля людьми та примусова праця є основою «виробничого процесу». Жертви цих таборів, часто викрадені або завербовані обманом, змушені цілодобово працювати над ошукуванням людей по всьому світу, що додає до фінансових злочинів ще й вимір грубого порушення прав людини. Отримані кошти потім проходять через складні ланцюги підставних компаній, офшорних холдингів та транзакцій з

[5] https://home.treasury.gov/news/press-releases/sb0683

криптовалютою, що дозволяє організації приховувати походження грошей та інтегрувати їх у легальну фінансову систему.

Центральною фігурою нової хвилі санкцій став Кю Юн (Qiu Yong), який, за даними OFAC, є ключовим членом Prince Group. Він контролює численні компанії на Британських Віргінських Островах (BVI) та в Гонконзі, діючи від імені та в інтересах лідера організації Чена Чжі. Цікаво, що Кю Юн є громадянином одразу кількох юрисдикцій, включаючи Камбоджу, Сент-Люсію та Туреччину, що свідчить про глибоке розуміння злочинцями принципів функціонування світової фінансової системи. Він є бенефіціарним власником низки компаній, зареєстрованих на BVI, які, в свою чергу, контролюють мережу гонконгських фірм, задіяних у кредитуванні та інших бізнес-операціях. Серед них виділяються Premium Financial Limited та Solar Scape Financial Limited, що спеціалізуються на видачі позик, а також компанії, пов'язані з виноробничою індустрією, такі як Glad Vast Limited та Glad Sparkle Limited. Це ілюструє, як злочинні доходи маскуються під прибуток від цілком легальних, на перший погляд, видів діяльності.

Важливим елементом корпоративної структури є особисті асистенти та довірені особи. Зокрема, Чжао Мен'яо (Zhao Mengyao), відома як Емі Чжао, є особистою помічницею Кю Юна і обіймає посади корпоративного секретаря та директора у багатьох підконтрольних йому гонконгських компаніях. Вона разом з Кю Юном є акціонером Mighty Divine Trust Hong Kong Limited – компанії, якою керує Чжоу Юнь, раніше визначена OFAC як фінансовий менеджер Prince Group. Це демонструє, наскільки тісно переплетені особисті та бізнесові зв'язки в цій організації, де довірені особи виконують роль «номінальних» директорів та власників, приховуючи справжніх бенефіціарів.

Окремий блок санкцій стосується оточення іншого високопосадовця Prince Group – Чена Бо, який був внесений до санкційних списків у червні 2026 року. OFAC наклало санкції на його дружину, громадянку Камбоджі Хе Юйцзін (He Yujing), та його камбоджійського партнера Вісала Панга (Visal Pang). Після жовтневих санкцій 2025 року Чен Бо переписав право власності на свій будинок у Токіо на дружину, яка також володіє камбоджійською компанією Super Light Speed Kh Technology Co., Ltd. Це яскравий приклад спроби уникнення санкцій шляхом перереєстрації активів на членів родини. Вісал Панг, у свою чергу, контролює одинадцять камбоджійських компаній, кілька з яких він очолює разом з Ченом Бо. Серед них – будівельні, логістичні, девелоперські компанії, а також фірми, що працюють у сфері розваг та технологій, що свідчить про диверсифікацію злочинного бізнесу в легальні сектори економіки Камбоджі.

Сам Чен Бо, незважаючи на санкції, зберігає контроль над ще одинадцятьма камбоджійськими компаніями, включаючи Asian Welfare Lotteries Co., Ltd., CB General Insurance PLC., Prince International Airlines Co., Ltd. та інші. Це підкреслює складність боротьби з подібними структурами, адже навіть після потрапляння до санкційних списків, особи продовжують керувати активами через підставних осіб та складні корпоративні ланцюжки. Санкції також торкнулися компаній, пов'язаних з іншими високопосадовцями, зокрема Dai An, який володіє сінгапурською Chen Hua Holdings Pte Ltd та очолює компанії на Маврикії та в Малайзії, а також Thet Li, якому належить сінгапурська Greenbay Multi Media Pte Ltd. Ці факти свідчать про те, що Prince Group

побудувала розгалужену мережу в різних юрисдикціях Південно-Східної Азії та Океанії, використовуючи місцеві закони для прикриття своєї діяльності.

Окремо варто зупинитися на справі Чуї Кок Ва, який став єдиною особою, проти якої були застосовані санкції на підставі Указу Е.О. 13694 щодо значної кібердіяльності. Він керував великою мережею шахраїв на Мадагаскарі, які використовували криптовалюти та цифрові технології для ошукування американців. Використовуючи методи соціальної інженерії та викликаючи співчуття у вразливих верств населення, мережа Чуї виманила понад 400 тисяч доларів, завдаючи шкоди національній безпеці та економічному здоров'ю США.

Підсумовуючи, варто зазначити, що нові санкції OFAC є ретельно спланованою операцією з демонтажу фінансової та корпоративної архітектури транснаціональної злочинності. Вони демонструють розуміння того, що сучасні кібершахрайські мережі діють як складні бізнес-корпорації, використовуючи офшорні зони, номінальних директорів, професійних консультантів та цифрові активи для відмивання грошей.

Координація зусиль між OFAC, ФБР, Міністерством юстиції США, а також міжнародними партнерами, зокрема Агентством фінансових розслідувань Британських Віргінських Островів та Міністерством закордонних справ Великої Британії, підкреслює важливість міжнародного співробітництва у боротьбі з цим явищем.

Санкції покликані не лише покарати винних, а й створити нестерпні умови для функціонування злочинного бізнесу, позбавивши його доступу до світової фінансової системи та можливості легалізувати злочинні доходи. Успіх цієї кампанії залежатиме від того, наскільки швидко та ефективно міжнародна спільнота зможе адаптуватися до нових методів роботи злочинців, адже, як показує практика, вони здатні швидко перебудовувати свої мережі, використовуючи прогалини в законодавстві різних країн.

Висновки

Стратегічний зсув від персональних до структурних санкцій. Міністерство фінансів США перейшло від точкового переслідування лідерів злочинних угруповань до системного демонтажу всієї корпоративної та фінансової екосистеми, яка забезпечує їхнє функціонування.

Злочинність як бізнес-модель. Транснаціональні шахрайські мережі, зокрема Prince Group, діють за принципами складних корпорацій: вони диверсифікують діяльність у легальні сектори, використовують офшорні юрисдикції та покладаються на професійних фінансових посередників.

Поєднання фінансових злочинів із порушенням прав людини. Ключовим «активом» є масштабні шахрайські табори в Південно-Східній Азії, де примусово працюють жертви торгівлі людьми, що робить боротьбу з такими мережами питанням не лише фінансової, а й гуманітарної безпеки.

Ефективність лише за умови міжнародної координації. Успіх санкцій залежить від синхронізації зусиль США з партнерами, а також від здатності адаптуватися до спроб уникнення санкцій через перереєстрацію активів на родичів та підставних осіб.

Зброя після війни: як незаконний обіг зброї, бойових дронів і вогнепальних засобів випадає з поля зору систем ПВК/ФТ [6]



Шістнадцятий випуск аналітичного бюлетеня Dirty Money під назвою «Underworld Arsenal» розглядає не гуманітарні наслідки збройних конфліктів, а паралельну тенденцію – еволюцію торгівлі зброєю та зв'язок між новими видами озброєнь у зонах конфліктів і новими маршрутами незаконного обігу. Відправною точкою є заява Генерального секретаря ООН від 26 травня 2026 року про найбільшу кількість конфліктів з часу заснування Організації: кількість держав, що переживають збройні конфлікти, зросла з 56 у 2020 році до 61 у 2024 році, Міжнародний рух Червоного Хреста і Червоного Півмісяця зареєстрував 284 тис. зниклих безвісти (на 70 % більше за рік), а понад 204 млн людей живуть на територіях, повністю або частково контрольованих збройними угрупованнями.

Центральна теза першого розділу винесена в заголовок «Follow the Money – If You Can»: незаконна торгівля зброєю функціонує як повністю інтегрована кримінальна економіка, у якій зброю закуповують, транспортують, продають через брокерів і монетизують мережами, що відтворюють складність легальних ланцюгів постачання, але без жодних комплаєнс-обов'язків. Великі партії, вимірювані сотнями тонн, пов'язані з постачанням учасникам збройних конфліктів чи до країн під ембарго й проходять через численні юрисдикції. Автор підкреслює, що на американському континенті половина вбивств пов'язана з організованою злочинністю, причому майже 70 % з них скоєно з використанням вогнепальної зброї, тоді як у світі цей показник становить близько 40 %. Найменш дослідженим каналом він називає «післявоєнний ринок»: зброя, поставлена в зони бойових дій з мінімальними вимогами до відстежуваності, після завершення активної фази повертається до незаконного обігу. Відповідь ЄС автор оцінює як недостатню: більшість положень Регламенту (ЄС) 2025/41, що переглядає Регламент (ЄС) № 258/2012 про експорт, імпорт і транзит вогнепальної зброї, почнуть застосовуватися лише з лютого 2029 року, а запропонована Комісією у 2026 році директива щодо незаконного обігу вогнепальної зброї встановлює мінімальні критерії криміналізації, проте, на думку автора, не охоплює окремо організовані злочинні угруповання мафіозного типу, не передбачає механізму відстеження зброї, проданої в зони конфліктів чи поблизу них, і не запроваджує обов'язку повідомляти про підозрілі фінансові потоки, пов'язані з

[6] https://www.canva.com/design/DAGzhr5OlOQ/v0tK-2ay8CTtxAU0rnK9MA/view

брокерською діяльністю. Чинне законодавство у сфері ПВК/ФТ, за оцінкою автора, лише відносить торгівлю вогнепальною зброєю до сектору підвищеного ризику.

Другий розділ простежує спадщину балканських воєн. У березні 2026 року Фінансова гвардія Італії та прокуратура Реджо-Калабрії викрили «супермаркет зброї», пов'язаний із кланом Моле з Джоя-Тауро: 17 автоматів Калашникова серед 25 одиниць бойової зброї, нелегальну вогнепальну зброю, ручні гранати та 600 г тротилу з колишньої Югославії, закопані в сільській місцевості, а домовленості щодо них велися в зашифрованих чатах Sky ECC. За даними слідства, клан переозброювався для протистояння з кланом Піромаллі, а походження зброї з балканських конфліктів свідчить, на думку слідчих, про «інтегровану злочинну систему» калабрійських угруповань з балканськими та східноєвропейськими організаціями. Щодо України автор формулює ризик ширше: йдеться не лише про витік вогнепальної зброї, а й про складніші системи та знання щодо їх використання. Він посилається на дані українських органів влади про 780 465 одиниць зброї, втрачених або викрадених з 2022 року, і водночас сам застерігає, що ця цифра не означає, що вся зброя потрапила до злочинців. Прокурор Палермо Мауріціо Де Лучія попереджає про інтерес мафії до якісніших арсеналів, зокрема бойових дронів; згадано також підготовку українською оборонною промисловістю контрольованого експорту. Найглибшим ризиком автор вважає поширення знань: з посиланням на аналіз Королівського коледжу Лондона він зазначає, що кількість атак із застосуванням дронів у Колумбії у 2025 році зросла на 445 %, а бразильське угруповання Comando Vermelho, за цими даними, направляло своїх членів в Україну.

Третій розділ присвячено використанню дронів картелями. У Мексиці їх понад десятиліття застосовують для спостереження за силовими структурами й контрабанди, а згодом – для атак на конкурентів, силові структури та залякування громад; Новий картель Халіско (CJNG) у Мічоакані використовував їх для витіснення мешканців зі спірних територій. Дослідження центру NCITE Університету Небраски в Омасі 2026 року ідентифікувало 221 інцидент із застосуванням бойових дронів у Мексиці у 2021–2025 роках; 27 з них призвели до загибелі 77 осіб. У Колумбії, за даними Diálogo Américas, кількість збройних угруповань, що використовують бойові дрони, зросла з п'яти у 2024 році до 19 у 2026 році, а у вересні 2026 року атака кількох дронів з вибухівкою, яку приписують Армії національного визволення (ELN), забрала життя трьох військових у департаменті Норте-де-Сантандер. Автор підкреслює асиметрію витрат: дешеві комерційні апарати змушують держави інвестувати у складні системи протидії, а для фінансових розслідувачів дрон є лише видимим кінцем ланцюга – ключові питання стосуються того, хто фінансує закупівлі, постачає компоненти, надає технічні послуги й переміщує доходи, включно з легальними постачальниками, якими зловживають кримінальні покупці.

Четвертий розділ аналізує «примарну зброю» (ghost guns). Традиційний незаконний ринок спирався на викрадену зброю, корумпованих посередників і транскордонну контрабанду; натомість дедалі частіше виробництво наближається до покупця завдяки цифровим кресленням, споживчим технологіям і компонентам, що оминають звичайні ланцюги постачання вогнепальної зброї. На прикладі Коста-Рики, де Diálogo Américas фіксує поєднання викраденої зброї, імпортованих деталей, локального складання та надрукованих на 3D-принтері компонентів, автор

показує, що готова зброя може жодного разу не перетнути кордон як цілісний виріб. Дослідження 186 зареєстрованих випадків засвідчило помітне зростання таких інцидентів з 2021 року з переважанням гібридної зброї та окремих компонентів, а слідчі стикаються з невизначеним походженням, відсутніми чи зміненими серійними номерами й браком традиційних слідів. Матеріали, що рекламують обладнання для виготовлення такої зброї, доступні на звичайних вебсайтах, а не лише в даркнеті. Штучний інтелект, за оцінкою автора, поки не дає змогу «одним натиском» створити надійну зброю, проте знижує потрібний рівень спеціальних знань і витрати; у 2026 році повідомлялося про прототип пістолета, надрукованого з допомогою ШІ, хоча й з обмеженими характеристиками. Запропоноване Комісією законодавство передбачає криміналізацію незаконного створення, придбання, зберігання та поширення креслень для 3D-друку зброї.

Заключний розділ пропонує підхід професора Нікасо «Follow the flow»: класичне відстеження грошей залишається необхідним, але слідчі мають простежувати також цифрову інформацію, онлайн-маркетплейси, криптовалюти, соціальні мережі, технічну експертизу та вплив, оскільки розслідування, обмежені банківськими рахунками, оминають інфраструктуру, що поєднує злочинні мережі. Автор пропонує забезпечувати для кожної поставки зброї в зону конфлікту відстежуваний ланцюг передавання – від донора й виробника до отримувача, місця зберігання та остаточного розпорядження, а після завершення конфлікту систематично збирати, реєструвати та відстежувати зброю, не чекаючи її появи на чорному ринку; щодо України він окремо зазначає, що поставлена зброя підлягає системам відстеження, хоча ризик зберігається. Серед інших пропозицій – обов'язок електронних торговельних і спеціалізованих майданчиків, що продають дрони з високими можливостями, ідентифікувати покупців понад визначені пороги ризику, зберігати відомості про них і надавати компетентним органам на законний запит (з гарантіями приватності), обов'язки платформ, що розміщують креслення зброї, виявляти заборонений контент і зберігати докази, інтеграція фінансової розвідки, митниці, поліції, оборонних органів і технічних фахівців, а також посилення нагляду за виробниками й дистриб'юторами з посиланням на позицію Міжамериканського суду з прав людини щодо обов'язку держав оцінювати ризики виробництва зброї й торгівлі нею. Мета, за формулюванням автора, полягає не лише в тому, щоб вилучати більше зброї, а в тому, щоб зробити всю екосистему складнішою для зловживань.

Висновки

Торгівля зброєю є фінансовою типологією з власними точками контролю: закупівля, брокерська діяльність, логістика, постачання компонентів і технічні послуги генерують платежі, які проходять через фінансову систему, тому віднесення сектору торгівлі зброєю до підвищеного ризику доцільно доповнювати індикаторами, пов'язаними з брокерськими схемами, компонентами подвійного використання та платежами за деталі для дронів.

Децентралізоване виробництво змінює точку контролю: гібридна та надрукована на 3D-принтері зброя, яка може ніколи не перетнути кордон як цілісний виріб, переносить ризик у сферу купівлі компонентів, обладнання, цифрових креслень і послуг онлайн-маркетплейсів, де фінансові установи та платіжні сервіси бачать відповідні операції раніше, ніж правоохоронні органи бачать зброю.

Простежуваність поставок у зони конфліктів має і безпекове, і доказове значення: автор сам застерігає, що 780 465 одиниць втраченої чи викраденої зброї не дорівнюють обсягу, що потрапив до злочинців; документований ланцюг передавання від донора до остаточного розпорядження та післявоєнна реєстрація дозволяють відокремлювати фактичні випадки відволікання зброї до злочинних мереж від інших випадків її втрати.

Ефективна протидія потребує міжвідомчої інтеграції даних: запропонована модель «Follow the flow» поєднує фінансову розвідку з митними, поліцейськими, оборонними та технічними даними, а також з інформацією від маркетплейсів і платформ; роз'єднані бази даних створюють сліпі зони, у яких легальні закупівлі не пов'язуються з подальшою кримінальною діяльністю.

Чому управління даними стає ключовим елементом контролю за фінансовими злочинами [7]

Історія з безпрецедентними штрафами проти Bank of America, оголошеними Міністерством фінансів США 13 жовтня 2026 року, стала потужним сигналом для всієї індустрії.

Загальна сума санкцій вражає: FinCEN наклав штраф у розмірі 1,2 мільярда доларів, а Управління контролера грошового обігу (OCC) – рекордні 750 мільйонів доларів, які були зараховані в рахунок сплати першого штрафу. Окремо OFAC оголосив про врегулювання на суму 11,6 мільйона доларів у зв'язку з 475 ймовірними порушеннями санкцій. Однак для професіоналів у сфері протидії фінансовим злочинам набагато важливішим є не розмір покарання, а першопричини, які до нього призвели. Корінь проблем лежить у площині управління даними (data governance), а не лише в технічній несправності окремих систем.

Згідно з наказом FinCEN, середовище моніторингу транзакцій у банку функціонувало вкрай неефективно. Протягом кількох років понад третина розслідувань підозрілої активності ініціювалася не автоматизованими системами банку, а правоохоронними органами, іншими фінансовими установами або внутрішніми ручними зверненнями. Це свідчить про те, що власні контрольні механізми установи не були здатні самостійно виявляти загрози. FinCEN наголосив, що ці недоліки спричинили пропуск або затримку звітування про підозрілу діяльність на суму понад 5 мільярдів доларів. Зокрема, йдеться про транзакції на суму понад 600 мільйонів доларів з ознаками потенційного відмивання грошей через торгівлю (TBML), пов'язаного з вживаними автомобілями, а також про сотні мільйонів доларів, що відповідали типології китайської мережі з відмивання коштів.

Цей випадок ілюструє важливий принцип: зовнішні сигнали, такі як повістки до суду, запити від партнерів чи правоохоронців, є цінним джерелом розвідувальної інформації, але вони повинні доповнювати внутрішні системи контролю, а не бути основним механізмом виявлення. Якщо банк покладається на зовнішні стимули для ідентифікації підозрілих операцій, це означає, що його власні системи моніторингу зазнали краху.

Схожа ситуація спостерігалася і в сфері санкційного скринінгу. Хоча врегулювання з OFAC стосувалося інших правових вимог, воно порушило аналогічне питання щодо контролю. OFAC зазначив, що ймовірні порушення включали обробку платежів за участю заблокованих банків, неспроможність належним чином пріоритезувати оповіщення для клієнтів, чиї імена та дати народження точно збігалися з заблокованими особами, несвоєчасне оновлення списків спостереження та помилки в роботі з бізнес-рахунками, пов'язаними з заблокованими особами.

[7] https://www.acams.org/en/opinion/bank-america-case-makes-data-governance-financial-crime-control

Це підкреслює, що простого генерування інформації недостатньо – вона повинна бути належним чином пріоритезована, оновлена та негайно використана для прийняття рішень.

У сучасному світі, коли фінансові установи все більше покладаються на автоматизовані інструменти скринінгу та моніторингу, ця різниця стає критичною. Технічно справна система може генерувати високий рівень ризику, якщо відповідні дані надходять із запізненням, порогові значення погано відкалібровані, оповіщення про високий ризик не мають належного пріоритету, або виявлені проблеми не доходять до слідчих достатньо швидко. Таким чином, ефективність контролю залежить не від наявності програмного забезпечення, а від якості та швидкості обробки даних.

Найважливішим висновком зі справи Bank of America є те, що управління даними перестало бути виключно сферою відповідальності IT-відділів. FinCEN вимагає від банку проведення незалежної перевірки не лише програм моніторингу підозрілої активності, належної перевірки клієнтів (CDD) та комплексної перевірки іноземних кореспондентських рахунків, а й системи управління даними, які використовуються в програмі AML. Це означає, що для програм боротьби з фінансовими злочинами управління даними визначає, чи надходить інформація про клієнтів, дані про транзакції, санкційні списки та індикатори ризику до правильного контрольного рішення в потрібний час.

Фінансовим установам слід перевіряти не лише те, чи технічно генерують їхні системи моніторингу та скринінгу оповіщення. Вони повинні розуміти, чи є базові дані повними, точними та своєчасними, чи відображають порогові значення та правила пріоритезації поточний ризик, і чи дозволяють процеси ескалації слідчим діяти швидко. Зовнішня розвідка може посилити програму комплаєнсу, але вона не повинна бути тим, що змушує програму працювати.

Контроль за фінансовими злочинами ефективний настільки, наскільки ефективні дані, які він отримує, правила, які він застосовує, та швидкість, з якою хтось реагує на ці сигнали. Там, де рухаються товари, рухаються гроші, а за грошима слідує ризик – і саме належне управління даними є тим запобіжником, який дозволяє тримати цей ризик під контролем.

Висновки

Ефективність контролю залежить від якості даних, а не від кількості оповіщень. Технічно справна система моніторингу не гарантує виявлення ризиків, якщо базові дані про клієнтів і транзакції є неповними, застарілими або надходять із запізненням.

Зовнішні сигнали мають доповнювати, а не замінювати внутрішній контроль. Якщо більшість підозрілих операцій виявляється лише завдяки правоохоронцям чи партнерам, це свідчить про системну слабкість власних механізмів фінансового моніторингу.

Санкційний скринінг вимагає не лише генерації, а й пріоритезації та швидкої дії. Наявність точних збігів у списках не має сенсу, якщо оповіщення не оновлюються вчасно, не мають належного пріоритету та не доходять до слідчих оперативно.

Управління даними є комплаєнс-функцією, а не суто IT-завданням. Регулятори дедалі частіше вимагають незалежного аудиту систем управління даними в межах програм AML, визнаючи їхній прямий вплив на якість контрольних рішень.

Фентаніл і синтетичні наркотики в Північній Америці [8]

Дослідження GI-TOC аналізує ринок синтетичних речовин у Канаді, США та Мексиці та спирається на польові дослідження, офіційні дані, лабораторний аналіз вуличних наркотиків і понад тридцятирічну статистику мексиканської армії. Головна теза: ринок зазнав фундаментальної трансформації, а стандартні підходи до контролю дедалі частіше виявляються неефективними.

Фентаніл присутній у всіх трьох країнах, однак його склад, домішки та географія поширення суттєво різняться. Особливу тривогу викликають речовини «бромазолам» і «медетомідин», які дедалі частіше змішують із фентанілом, щоб продовжити дію та «розтягнути» запас. Вони становлять серйозну загрозу, оскільки їхня дія не піддається зворотному впливу налоксону. Попри зниження офіційних показників смертності від передозувань у Канаді та США й кількості вбивств у Мексиці, смертність залишається високою, а позитивні зрушення розподілені нерівномірно: різниця між расовими та етнічними групами зростає. У 2024 році в США корінні американці мали вдвічі вищий рівень смертності від опіоїдів, ніж білі, а в Канаді представники Перших націй у Британській Колумбії помирали в 5,4 раза частіше за інших жителів.

Автори відходять від спрощеного ототожнення фентанілу з усіма синтетичними опіоїдами. Лише 5% зразків фентанілу в Торонто відповідали очікуванням споживачів, а опіоїди мають найвищий рівень фальсифікації серед усіх класів речовин. Служба перевірки наркотиків Торонто пропонує розглядати фентаніл як речовину, яку фальсифікують, а не як домішку. За даними CDC, 65,1% смертей від передозування в США пов'язані з нелегально виготовленим фентанілом; у Канаді – 56% із фентанілом і 60% з аналогами.

Всупереч поширеній думці, операції мексиканської армії за Лопеса Обрадора (2018–2024) були зосереджені переважно в Сіналоа. Гасло «Обійми, а не кулі» надмірно спрощене: дані показують, що контрнаркотичні операції в Сіналоа супроводжувалися розподілом соціальних програм вище середнього – 30,5% жителів штату отримували федеральну підтримку проти 15,4% по країні, тоді як у Чіапасі – лише 4%. Точніше характеризувати підхід як «гроші та кулі». Незважаючи на цілеспрямовані дії, виробництво фентанілу триває: адміністрація Шейнбаум вилучила 5,5 млн таблеток і 0,7 тонни порошку фентанілу.

Пріоритети вилучень в Мексиці ігнорують попит на лікування. Канабіс становив 85,1% вилучень у 1999 році проти 41,8% у 2024-му, а з 2010 року скорочення вилучень канабісу супроводжувалося зростанням вилучень метамфетаміну. Попри відносно низький ризик канабісу, влада концентрує ресурси на ньому, тоді як більше мексиканців звертаються за лікуванням від метамфетамінової

[8] https://globalinitiative.net/analysis/fentanyl-monitor-north-america/

залежності. Вживання метамфетаміну зросло на 400% між 2013 і 2023 роками; ціна дози в регіоні Бахіо стабільна з 2020 року (75–100 песо), а в північних містах сягає 50 песо. Організація Barbies Testeadoras повідомляє, що лише 4 з 10 зразків відповідали очікуванням, 25% були фальсифіковані, а половина доз MDMA містила метамфетамін.

За 34 роки вилучення розширилися географічно, хоча сім штатів становлять половину всіх вилучень, а 66% припадає на тихоокеанські штати. Вилучення фентанілу відхиляються від тенденції: Баха-Каліфорнія (30%), Сонора (28%) і Сіналоа (15%) становлять більшість, а 83,8% фентанілу вилучається в північних штатах. 97,5% вилучених лабораторій розташовані в Сіналоа, Мічоакані та Халіско; Сіналоа має 2 448 лабораторій, а Куліакан – 1 361. У березні 2025 року вилучення лабораторії в Сакатекасі запобігло виробництву понад 27 тонн метамфетаміну, однак ціна дози не зросла, що свідчить про стабільність постачання.

Франшизна модель CJNG дозволяє місцевим групам використовувати назву картелю в обмін на збори та відсотки, зберігаючи територіальний контроль за місцевими угрупованнями. Після зникнення «Лицарів Тамплієрів» десятки дрібних осередків зайняли обмежені території, а згодом почали з'являтися у відео під прапором CJNG. Це не включення до картелю, а модель експансії: закриття однієї лабораторії не має істотного впливу на CJNG і майже не зменшує постачання.

Злочинні групи підтримують себе примусовою вербовкою молоді. У 2021 році близько 4 мільйонів дітей і підлітків віком від 5 до 17 років працювали на злочинні групи. Рекрутів заманюють фальшивими вакансіями в TikTok, Facebook та Instagram, вербують у підпільних реабілітаційних центрах або викрадають під час поїздок, іноді масово й у змові з поліцією. Після потрапляння до CJNG втечі немає: новобранців утримують у «тренувальних» центрах, відомих як «ескусітас». У березні 2025 року колектив Guerreros Buscadores de Jalisco виявив такий об'єкт на ранчо Ісагірре в Теучітлані, де знайшли 1 800 особистих речей. Між 2011 і 2025 роками ідентифіковано щонайменше 12 тренувальних і 17 інших таборів у 21 муніципалітеті Халіско, Агуаскальєнтесу, Сакатекасу та Мічоакану. Після «випуску» учасники отримують зарплату від 2 500 до 3 000 песо на тиждень (138–165 доларів США), а їхнє життя стає витратним матеріалом.

Документ відзначає, що попри напружену політичну риторику країни продовжують співпрацювати в Комісії ООН з наркотичних засобів. На 69-й сесії в березні 2026 року Мексика представила резолюцію щодо відстеження спеціалізованого обладнання та контрольованих матеріалів для запобігання їх використанню у виробництві синтетичних наркотиків; резолюцію ухвалили, проти проголосувала лише Індія. 70-та сесія в березні 2027 року покаже, чи країни поза Північною Америкою впровадили її в національну політику. Крім того, арешт Раяна Веддінга в Мексиці в січні 2026 року та його передача США можуть дати цінну інформацію про те, як транснаціональні суб'єкти діють у регіоні, які завдання виконували члени організації, а які – підрядники без формального зв'язку з організованою злочинністю, а також які агенції трьох юрисдикцій були головними цілями для хабарів.

Висновки

Фальсифікат, а не лише фентаніл, є головним чинником ризику. Інші речовини дедалі частіше домішують до опіоїдів; ці речовини не мають медичного застосування для людини і не піддаються дії налоксону, що ускладнює порятунок при передозуванні.

Ринок фрагментований географічно, тому універсальні підходи неефективні. Регіони США й провінції Канади відрізняються за складом домішок і шляхами синтезу; політика має враховувати локальну специфіку, а не орієнтуватися на усереднені національні показники.

Показники вилучень не відображають потреб у лікуванні. Мексика концентрує ресурси на канабісі за обсягом, тоді як найбільший попит на лікування пов'язаний із метамфетаміном; орієнтація на «витрати» замість «результатів для здоров'я» викривляє пріоритети.

Організаційна стійкість злочинних мереж знижує ефект правоохоронних операцій. Франшизна модель CJNG означає, що закриття окремих лабораторій майже не впливає на постачання, а примусова вербовка молоді відтворює кадровий ресурс угруповань.

РЕКОМЕНДОВАНІ ПОДІЇ



Конференція європейських наглядових органів [9]

Європейські наглядові органи – Європейський банківський орган (EBA), Європейський орган зі страхування та професійного пенсійного забезпечення (EIOPA) та Європейський орган з цінних паперів і ринків (ESMA) – проводять спільну конференцію «The first two years of DORA Oversight». Захід відбудеться 2 грудня 2026 року з 9:00 до 12:30 за центральноєвропейським часом. Мета – підбити підсумки перших двох років нагляду відповідно до Регламенту про цифрову операційну стійкість (DORA), зокрема досягнень, отриманих уроків і нових викликів у нагляді за критично важливими сторонніми постачальниками ІКТ-послуг (CTPP). Цільова аудиторія – представники наглядових органів, фінансових установ, галузевих асоціацій, CTPP, академічної спільноти та медіа. Очна участь можлива лише за запрошенням, водночас конференцію транслюватимуть онлайн; окремої форми реєстрації на сторінці заходу немає, а посилання на трансляцію поки не оприлюднено, тож його варто відстежувати на сторінці події.

Згідно з проєктом програми, конференцію відкриє керівниця комунікацій EBA і модераторка заходу Франка Роза Конджу, з вітальним словом виступить Голова EBA Франсуа-Луї Мішо. Перша панель «Призначення, залежності та цифровий суверенітет» під модеруванням Виконавчої директорки ESMA Наташі Казнав охопить порядок визнання постачальників критично важливими, еволюцію залежності фінансового сектору від ІКТ-послуг, стратегічну автономію й цифровий суверенітет. Друга панель «Майбутні тенденції нагляду: інновації, стійкість і штучний інтелект» під модеруванням Виконавчого директора EIOPA Даміана Яворського присвячена впливу нових технологій на фінансові послуги, взаємозв'язку штучного інтелекту й операційної

[9] https://www.eba.europa.eu/publications-and-media/events/first-two-years-dora-oversight-key-european-response-context-rising-global-cyber-challenges

стійкості та міжнародним підходам до нагляду за ІКТ і технологіями. Кожна панель завершується запитаннями аудиторії, а підсумкове слово належить Голові EBA.

Серед учасників панелей – Фредді Дезере (заступник директора з інформаційної безпеки Microsoft у Європі), Метью Елдерфілд (член наглядової ради Rabobank), професорка Лаура Грассі (Міланська політехніка), Ян Лешель, Светослав Манолов (SAP), Франческо Маццаферро (керівник Секретаріату Європейської ради із системних ризиків), Джузеппе Сіані (Банк Італії) та Аннелі Туомінен (член Наглядової ради Банківського нагляду ЄЦБ); організатори анонсують додаткових доповідачів. Для підготовки до заходу корисні тематичні сторінки EBA та спільна сторінка ESAs про нагляд за DORA, де розміщено посібник з наглядової діяльності, відомості про Форум з нагляду та спільні екзаменаційні команди. Регламент DORA застосовується з 17 січня 2025 року; перелік 19 постачальників, визнаних критично важливими, ESAs оприлюднили 18 листопада 2025 року, призначивши EBA провідним наглядачем щодо кожного з них, тож конференція стане першим публічним підсумком повного наглядового циклу.



Аналіз міжнародних мереж та методів поширення дезінформації у сучасному просторі [10]

Розслідування, проведене OCCRP у партнерстві з Delfi Estonia, Jan Kuciak Investigative Center та The Nerve, проливає світло на безпрецедентні масштаби та методи роботи однієї з найбільш відомих російських дезінформаційних кампаній під назвою «Допельгангер» (Doppelgänger). Журналістське розслідування базується на унікальному масиві даних: після того, як один із головних сайтів кампанії, Recent Reliable News (RRN), був зламаний, він перетворився на своєрідну базу даних, яка каталогізувала понад 500 інтерв'ю, опублікованих на пов'язаних ресурсах. Аналіз цих матеріалів дозволив дослідникам та журналістам розкрити складну мережу вербування, фінансування та поширення пропаганди, яка охопила понад 50 країн світу.

Кампанія «Допельгангер» набула широкого розголосу ще у 2022 році, коли почала створювати точні клони справжніх новинних сайтів для поширення проросійських наративів, спрямованих на підрив підтримки України на Заході. З того часу операція значно еволюціонувала, створивши десятки нових сайтів, які видають себе за легітимні новинні організації та публікують пропагандистський контент англійською, французькою, німецькою та іншими мовами. Масштаб цих зусиль вражає: серед сотень людей, які дали інтерв'ю для цих ресурсів, виявилися колишні офіцери розвідки США, Франції та Іспанії, майже десяток ультраправих німецьких політиків, а

[10] https://www.occrp.org/en/investigation/from-politicians-to-academics-hundreds-around-the-globe-interviewed-and-featured-in-notorious-russian-disinformation-campaign

також академіки з усього світу. Географія респондентів охоплює понад 50 країн, а їхній профіль варіюється від французьких фермерів і фінських теоретиків змови до високопосадовців і колишніх військових НАТО. Усі вони, часто не усвідомлюючи цього, стали обличчям нового типу російської пропаганди, яка, за словами експертів, відрізняється від традиційних державних медіа або розвідувальних операцій і функціонує як багатомільйонна індустрія, що шукає фінансування від російської держави.

Ключовим гравцем у цій схемі, за даними розслідування, є структура під назвою SDA (ймовірно, пов'язана з російськими державними структурами), яка, згідно з витоками, ставила за мету «поглиблення внутрішніх суперечностей між правлячими елітами» західних країн та «стимулювання протестної активності серед опозиційних сил». Внутрішні документи, на які посилається ФБР, свідчать про плани використання «широкого спектру інформаційних інструментів» для впливу на реальні конфлікти та штучного створення конфліктних ситуацій у країнах-союзниках США. SDA також відома тим, що відстежувала тисячі «лідерів думок» по всьому світу. Це пояснює, чому інтерв'ю часто виглядають як цілком легітимні розмови з експертами, які потім нарізаються на короткі відео з яскравими заголовками, що просувають вигідні кремлю тези.

Особливу увагу в розслідуванні приділено Німеччині, яка, схоже, є однією з головних цілей кампанії. Найбільша частка опитаних політиків походить з ультраправої партії «Альтернатива для Німеччини» (AfD).

Виявилося, що не всі причетні до «Допельгангера» були росіянами. Кілька респондентів розповіли, що їх контактували бразильські послідовники ультранаціоналістичного російського ідеолога Олександра Дугіна. Зокрема, п'ятеро опитаних зазначили, що їхні розмови організував або провів Рафаель Мачадо – лідер бразильського відділення «Нового Опору», транснаціонального неофашистського руху, натхненного ідеологією Дугіна. Державний департамент США зазначає, що «Новий Опір» має глибокі зв'язки з російською екосистемою дезінформації та пропаганди. Серед інтерв'ю, які провів Мачадо, було й інтерв'ю з Сімоною Манджанте Пападопулос, дружиною колишнього помічника передвиборчої кампанії Дональда Трампа 2016 року. У цій розмові, частини якої цитуються у статті на французькому пропагандистському сайті Phrygien, вона зневажливо висловлюється про економічні перспективи Європи. Коли журналісти зв'язалися з нею, пані Пападопулос заявила, що не знала про французький сайт і не співпрацювала свідомо з кампанією «Допельгангер», але після перегляду відео згадала, що співрозмовником був саме Мачадо. Цей випадок яскраво демонструє, як операція використовує міжнародні мережі однодумців, часто не пов'язаних безпосередньо з кремлем, для створення ілюзії незалежної експертної думки.

Інший канал вербування, виявлений журналістами, – це соціальні мережі. Кілька відомих фігур отримували повідомлення від молодого чоловіка, який представлявся журналістом на ім'я Ніколай Маслов. Він описував себе як «журналіста та продюсера», який розвиває «молоду німецьку медіакомпанію з російським бекграундом», і пропонував інтерв'ю через Zoom, Skype або WhatsApp. Посилання, яке він надсилав, вело на сайт Meisterurian – німецькомовний новинний ресурс, який пізніше був викритий ФБР у зв'язках з «Допельгангером», а домен згодом вилучено.

Журналісти не знайшли жодних доказів того, що Маслов колись працював журналістом; у 2022 році він подавав резюме на посаду аналітика KYC у банківському секторі. Один із його співрозмовників, колишній британський парламентар Метью Гордон-Бенкс, розповів, що спілкувався з Масловим тричі й вважав його «фінансовим аналітиком з москви».

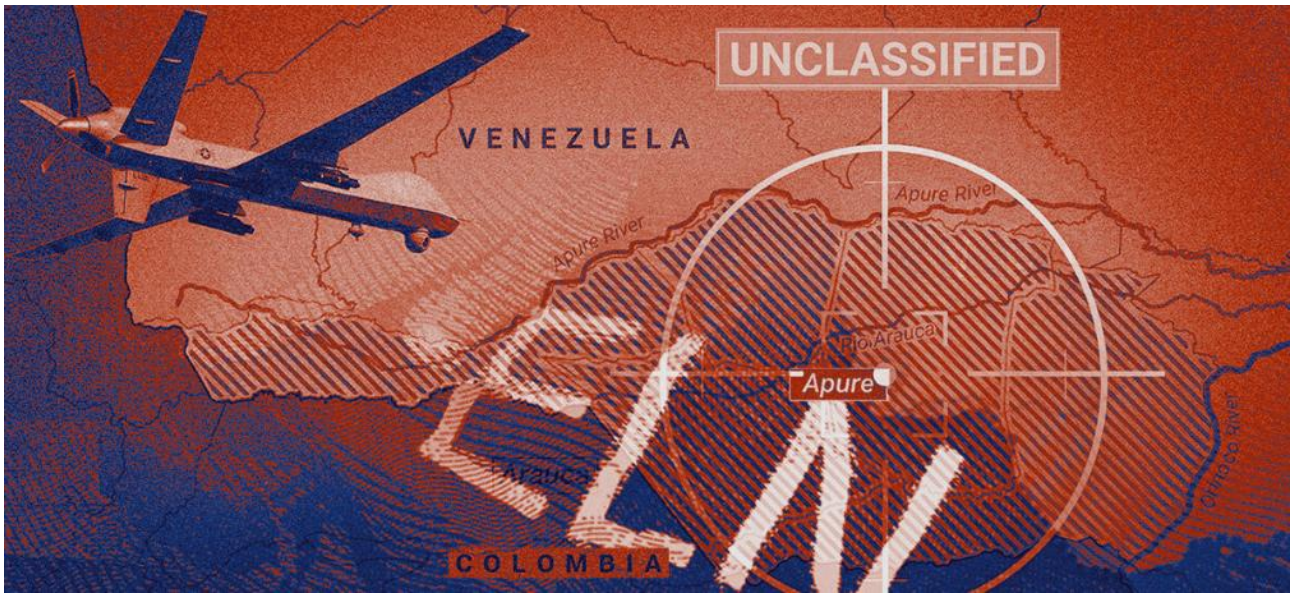
Ще один канал – це Telegram-канали, присвячені Дугіну. Норвезький правий політик Крістен Крогвіг розповів, що його контактував користувач на ім'я Антоніо Андреас, який надіслав список письмових запитань на теми німецької допомоги Україні та громадської думки щодо купівлі російського газу, попросивши Крогвіга самостійно записати відеовідповіді. OCCRP ідентифікувала Telegram-акаунт «Антоніо Андреас», який регулярно публікував контент у каналі, присвяченому Дугіну, а також виявила бразильця на ім'я Антоніо Андреас Пірес, який є адміністратором кількох інших каналів. На LinkedIn профіль Андреаса Піреса з відповідним фото вказує на посаду соціального менеджера державного медіагрупи що керує Sputnik та іншими ресурсами, орієнтованими на міжнародну аудиторію.

Експерти, опитані в рамках розслідування, наголошують, що ефективність «Допельгангера» не обов'язково вимірюється прямим впливом на думку читачів. Джеймс Паммент, директор Інституту досліджень психологічної оборони Лундського університету та співавтор звіту 2025 року про «Допельгангер», зазначає, що мета кампанії – не стільки просування конкретного наративу, скільки «проникнення в західне інформаційне середовище». Кір Джайлз, експерт з російської армії, додає, що компанії, подібні до SDA, повинні «доводити кремлю цінність своєї роботи, щоб продовжувати отримувати гранти», і що велика кількість інтерв'ю може відображати саме цей стимул.

Цікаво, що до червня 2026 року багато сайтів «Допельгангера» припинили роботу. Однак, за даними розслідування, принаймні два з них залишаються активними, зареєстрованими на турецьких доменах. Один із них, туркомовний сайт Kıtalararası, очолює Мехмет Перінчек – член проросійської партії Vatan, який називав себе близьким до родини Дугіна і раніше співпрацював з «Новим Опором» Мачадо. Після злому RRN бренд також почав працювати під турецьким доменом, змінив назву на Researchers & Reporters Network і тепер рекламує штат турецьких журналістів, які обіймали офіційні посади в партії Vatan.

Таким чином, розслідування OCCRP малює картину надзвичайно складної, гнучкої та добре схованої мережі, яка використовує широкий арсенал засобів – від прямих контактів через соцмережі до використання ідеологічно близьких посередників у Бразилії, Німеччині та Туреччині. Вона не просто поширює фейки, а конструює паралельну реальність, в якій голоси поважних західних експертів та політиків звучать на підтримку кремлівських наративів.

Масштаб операції свідчить про те, що російська дезінформація стала індустрією, яка використовує відкритість західних суспільств, їхню медійну культуру та прагнення багатьох публічних осіб до уваги. І хоча ефективність цієї кампанії ще належить оцінити, сам факт її існування та розмах є тривожним сигналом для демократичних країн, які змушені шукати нові способи захисту свого інформаційного простору від подібних гібридних загроз.



Трансформація безпекової політики Венесуели [11]

Протягом майже двох десятиліть Венесуела за часів Уго Чавеса та Ніколаса Мадуро слугувала надійним тилом та безпечним прихистком для лівих колумбійських повстанських угруповань. Однак події кінця жовтня 2026 року можуть свідчити про тектонічний зсув у безпековій політиці Каракаса. Перший в історії масштабний авіаудар венесуельських сил по табору Армії національного визволення (ELN) у штаті Апуре не лише порушив багаторічний негласний пакт про недоторканність, але й оголив складний вузол геополітичних інтересів, корупційних схем та боротьби за владу в регіоні.

Згідно з наявною інформацією, операція, що відбулася 30 жовтня, була проведена із застосуванням дронів та, за даними The New York Times, здійснювалася за безпосередньої підтримки Сполучених Штатів. Удар по табору, який, судячи з відео та фотографій у соціальних мережах, виконував функції лабораторії з переробки наркотиків, призвів до загибелі щонайменше 19 осіб. Серед загиблих – громадяни Венесуели, Колумбії та Мексики, що підкреслює транснаціональний характер діяльності угруповання. Ця атака стала безпрецедентним кроком для уряду Дельсі Родрігес, яка очолила країну як тимчасова президентка після захоплення Ніколаса Мадуро американськими силами в січні 2026 року. Цей політичний транзит, що супроводжувався безпрецедентним тиском з боку Вашингтона, очевидно, змусив нове керівництво Венесуели переглянути свої стосунки з угрупованнями, які раніше користувалися заступництвом держави.

Історичний контекст цієї події є надзвичайно важливим для розуміння масштабу змін. Зв'язки між венесуельським урядом та колумбійськими партизанами сягають часів президентства Уго

[11] https://insightcrime.org/news/venezuelas-airstrike-the-eln-tests-decades-chavista-tolerance/

Чавеса, який фактично відкрив кордони для Революційних збройних сил Колумбії (FARC). Після підписання мирної угоди 2016 року та часткової демобілізації FARC, саме ELN швидко заповнила кримінальний вакуум. Угруповання не просто закріпилося на важкодоступній лінії кордону, але й розширило свою присутність всередині держави, сягнувши навіть східних кордонів з Гаяною. Ця експансія стала можливою завдяки системним альянсам з численними венесуельськими чиновниками та військовослужбовцями. Такі домовленості дозволили ELN встановити систему «кримінального управління» на підконтрольних територіях, вербувати тисячі венесуельців до своїх лав та контролювати ключові зони незаконного видобутку золота і кокаїну. Штат Апуре, що межує з колумбійським департаментом Араука, історично був одним із головних операційних хабів ELN, звідки здійснювалося постачання наркотиків до багатьох країн світу.

Однак нинішня ситуація кардинально відрізняється від попередніх років. Попри те, що Національні боліваріанські збройні сили (FANB) під час перебування Мадуро при владі час від часу звітували про вилучення нарукавних пов'язок ELN або знищення «підпільних таборів», жодних рішучих операцій проти цього угруповання насправді не проводилося. Більше того, протягом поточного року венесуельські силовики переважно утримувалися від втручання у територіальні суперечки між ELN та дисидентами FARC за контроль над районами видобутку корисних копалин на півдні країни, обмежуючись лише розгортанням сил для запобігання ескалації насильства.

Наразі венесуельські силові структури, ймовірно, перебувають у невигідному становищі для ведення затяжного конфлікту з ELN. Роки «чавістського» правління призвели до втрати професійних навичок і тактичної підготовки армії, а корупція глибоко проникла в усі ланки військового та поліцейського апарату. На противагу їм, бійці ELN вирізняються високим рівнем дисципліни та підготовки. Це дозволило їм, наприклад, у 2021 році успішно протистояти 10-му фронту дисидентів FARC – завдання, яке виявилося не під силу регулярній венесуельській армії. Таким чином, нинішній авіаудар, хоч і демонструє рішучість нового уряду, ставить перед ним складне питання: чи вистачить у Каракаса ресурсів та волі довести справу до кінця, адже ELN навряд чи відмовиться від свого територіального контролю без запеклої боротьби.

Ключовим фактором, що змінив правила гри, є безпрецедентна роль Сполучених Штатів та новий політичний альянс у регіоні. Адміністрація Дельсі Родрігес опинилася під колосальним тиском Вашингтона. Держсекретар США Марко Рубіо ще у вересні під час візиту до Колумбії відкрито заявляв, що Вашингтон обговорював з урядом Родрігес можливі операції проти ELN на венесуельській території. Хоча офіційний Каракас поки що не опублікував жодної заяви щодо результатів удару, а міністр внутрішніх справ Діосдадо Кабельйо лише обмежився коментарем про «вжиття запобіжних заходів у відповідь на спалахи насильства в Колумбії», сам факт операції свідчить про те, що Венесуела діє в координації з зовнішніми партнерами.

Особливу роль у цій конфігурації відіграє Колумбія. Президент Абелардо де ла Еспрієлья, який став одним із головних союзників США у боротьбі з організованою злочинністю в регіоні, запропонував свою країну як операційну базу для ініціативи «Щит Америк». Однією з перших безпекових операцій його уряду став авіаудар по позиціях ELN у регіоні Кататумбо, де угруповання

з 2025 року веде боротьбу за контроль над зонами вирощування коки з 33-м фронтом дисидентів FARC. Ситуація загострилася після атак у департаменті Норте-де-Сантандер, що призвело до часткової мілітаризації кордону. Враховуючи, що ELN ще з 1997 року має статус іноземної терористичної організації в США, зараз складаються сприятливі умови для проведення скоординованої кампанії проти угруповання на території обох країн.

Водночас, попри активізацію співпраці, взаємодія між США та венесуельськими силовиками залишається доволі обмеженою. Головною спільною операцією досі залишається червневий удар, в результаті якого було ліквідовано Ектора Рустенфорда Герреро Флореса, відомого як «Ніньйо Герреро», – лідера угруповання «Трен де Арагуа». Хоча Вашингтон тоді назвав цю операцію перемогою, вона не поширилася на інші кримінальні структури, залучені до незаконного видобутку золота в штаті Болівар, незважаючи на очевидну зацікавленість США у контролі над виробництвом золота в цьому регіоні.

Підсумовуючи, можна констатувати, що авіаудар по табору ELN є не просто черговою військовою операцією, а важливим сигналом про зміну правил гри в регіоні. Він знаменує собою спробу Венесуели дистанціюватися від свого минулого як «спонсора» партизанських рухів під тиском зовнішніх обставин та нового політичного керівництва.

Однак, чи зможе уряд Дельсі Родрігес трансформувати цей поодинокий удар у послідовну стратегію подолання впливу ELN, враховуючи глибоку корупцію в силових структурах та високий бойовий потенціал угруповання, залишається відкритим питанням. Подальший розвиток подій залежатиме від того, наскільки ефективною виявиться координація дій між Каракасом, Боготою та Вашингтоном, і чи готові вони будуть до довготривалої та виснажливої боротьби з тіньовими структурами, які десятиліттями вкорінювалися в прикордонних регіонах.

Ваша думка важлива!

Які елементи Директиви (ЄС) 2024/1226 найважливіше врахувати в українському законодавстві про відповідальність за порушення санкцій з огляду на виявлену Рахунковою палатою ЄС неоднорідність правозастосування?

Які процедури дозволили б суб'єктам первинного фінансового моніторингу документально підтверджувати розуміння структури власності та контролю клієнта, не дублюючи відомостей реєстру КБВ?

За яких умов банки й платіжні установи в Україні можуть обмінюватися між собою даними про шахрайські операції без порушення вимог законодавства про захист персональних даних?

Які з європейських інструментів боротьби з онлайн-шахрайством є найбільш пріоритетними для імплементації в Україні в умовах обмежених ресурсів правоохоронної системи?

Які фінансові індикатори дозволили б суб'єктам моніторингу в Україні виявляти операції, пов'язані з незаконним обігом зброї, компонентів дронів чи цифрових креслень для 3D-друку зброї?

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-2026-46

Архів

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.

Міністерство фінансів України

AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE