

“У житті немає нічого, чого варто було б боятися, є тільки те, що потрібно розуміти”

Марія Складовська-Кюрі

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

FATF про фінансування розповсюдження: типології, вразливості, глобальні виклики для фінансових систем¹



АУДІОПЕРЕКАЗ



Документ FATF є найбільш ґрунтовним і всебічним дослідженням сучасних загроз, пов'язаних зі схемами фінансування розповсюдження (ФР) та обходу санкцій, яке було підготовлено в межах Глобальної мережі FATF. У вступній частині документа наголошується, що ФР і пов'язані з цим схеми обходу санкцій є серйозною загрозою як для міжнародної безпеки, так і для цілісності глобальної фінансової системи. Якщо держави та приватний сектор не зміцнять свої системи технічної відповідності та ефективності контролю за фінансуванням розповсюдження, то як державні, так і недержавні учасники й надалі будуть активно використовувати слабкі місця у фінансових і регуляторних системах для досягнення своїх цілей. Особливо

¹ <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf>

наголошується, що з огляду на потенційно катастрофічні наслідки від використання зброї масового знищення (ЗМЗ), забезпечення ефективної протидії фінансуванню їх розповсюдження є пріоритетним для глобальної спільноти.

Звіт надає всебічний аналіз методів і тенденцій, які використовують суб'єкти, що ухиляються від застосування цільових фінансових санкцій (TFS), передбачених Рекомендацією 7 FATF, а також обходу інших санкційних режимів — як національних, так і наднаціональних — які виходять за межі прямого мандату FATF. Важливим аспектом є те, що охоплення ширших аспектів ухилення від санкцій не змінює нормативні зобов'язання відповідно до Рекомендації 7, але дозволяє забезпечити більш актуальне розуміння загроз, вразливостей і типологій для побудови ефективних систем національної протидії.

Основною загрозою FATF визнає Кореїську Народно-Демократичну Республіку (КНДР), яка вже понад два десятиліття перебуває під санкціями ООН і FATF, проте продовжує нарощувати свій ракетно-ядерний потенціал. Протягом останніх років КНДР значно диверсифікувала способи отримання доступу до міжнародної фінансової системи та генерації доходів для фінансування своєї програми ЗМЗ. Окремо виділено приклад — у лютому 2025 року КНДР здійснила кібератаку на криптовалютну біржу ByBit, внаслідок чого було викрадено 1,5 мільярда доларів США. Крім того, Пхеньян активно використовує мережі IT-працівників за кордоном, які, діючи під виглядом громадян інших країн, офіційно отримують дохід у валюті. Цей дохід потім спрямовується на фінансування програм розробки ЗМЗ, обходячи міжнародні фінансові обмеження. Паралельно триває використання традиційних незаконних джерел фінансування — торгівля наркотиками, зброєю, підробленими документами та навіть незаконна торгівля об'єктами дикої природи.

У звіті відзначається, що хоча формально під дію Рекомендації 7 підпадає лише КНДР, у практичному вимірі численні країни також розглядають як актуальні загрози схеми, що використовуються Іраном та рф. Іран широко застосовує складні фінансові та логістичні механізми для обходу національних санкцій, зокрема за допомогою проксі-груп, таких як Хезболла, та кримінальних організацій. Вказується, що Іран використовує банки, біржі дорогоцінних металів, валютні обмінники та нелегальні грошові перекази (hawala) для фінансування своїх програм. Більше того, Іран активно використовує світову мережу компаній, зокрема легальні компанії IT-сектору, що контролюються іранськими висококваліфікованими мігрантами, для маскування незаконної діяльності.

Щодо російської федерації, після повномасштабного вторгнення в Україну в 2022 році та запровадження широких міжнародних санкцій, рф значно активізувала використання механізмів ухилення від санкцій. Особливо небезпечним є укладання договору про всебічне стратегічне партнерство з КНДР у 2024 році, який передбачає не лише економічну координацію, але й військову співпрацю, включаючи розгортання північнокорейських військових на території росії у контексті війни проти України. Водночас рф використовує транзит через треті країни для забезпечення поставок товарів подвійного призначення, обходу фінансових обмежень і залучення валютних ресурсів.

Документ детально аналізує ключові національні та секторальні вразливості, які використовуються для реалізації схем фінансування розповсюдження та ухилення від санкцій. На національному рівні найбільш суттєвими факторами є слабкість механізмів прозорості бенефіціарної власності, відсутність ефективних систем контролю за експортом товарів подвійного призначення, недосконалість законодавчих норм у сфері фінансового моніторингу, а також географічне розташування країн поруч із підсанкційними державами. На секторальному рівні найвищий ризик спостерігається в банківському секторі, серед постачальників віртуальних активів (VASP), у секторі морських перевезень, логістичних компаніях, операторах вільних

економічних зон (FTZ), а також у сфері дорогоцінних металів, інформаційних технологій і суднобудування.

Типологічно FATF ідентифікує чотири основні схеми ухилення від санкцій, що використовуються в контексті ФР. Перша — це залучення посередників, зокрема використання фіктивних і підставних компаній, банківських рахунків у третіх країнах і транзитних торговельних маршрутів для маскування походження і призначення товарів і фінансових потоків. Друга типологія пов'язана з приховуванням кінцевих бенефіціарних власників через складні корпоративні структури, використання номінальних директорів, нелегальних фінансових посередників і фінансових інструментів, таких як кредитні та дебетові картки. Третя — це активне використання віртуальних активів і технологій DeFi для переміщення коштів і генерації доходів, у тому числі шляхом створення фальшивих IT-компаній, що офіційно обслуговують клієнтів, але фактично генерують прибуток для програм ЗМЗ. Четверта — зловживання морськими перевезеннями, включно з підrobкою суднових документів, вимкненням системи AIS, зміною прапорів суден і перевалкою товарів у нейтральних водах.

Звіт також приділяє значну увагу системним викликам у сфері виявлення, розслідування й переслідування злочинів, пов'язаних із ФР і санкційним ухиленням. Основними проблемами залишаються слабка міжвідомча координація, обмеженість у доступі до даних про кінцевих бенефіціарів, низька якість національних оцінок ризиків, а також нерівномірність у підходах до регулювання ФР у різних юрисдикціях. Окремо підкреслюється, що значна частина розслідувань ініціюється саме через підозрілі транзакції (SAR/STR), що свідчить про необхідність поглиблення співпраці між державним і приватним секторами.

Документ завершується рекомендаціями для подальших дій FATF і країн-членів. Основними серед них є необхідність регулярного оновлення аналізу загроз і типологій, посилення обміну інформацією між державним і приватним секторами, проведення горизонтального огляду підходів до оцінки ризиків ФР у межах Глобальної мережі FATF і введення упродовж п'яти років офіційного визначення терміну «фінансування розповсюдження» у Глосарій FATF для уніфікації глобальних стандартів і подолання юрисдикційних розбіжностей, які ускладнюють міжнародну співпрацю та ефективне правозастосування у сфері протидії ФР і ухиленню від санкцій.

Висновки:

- **Проблема масового невиконання Рекомендації 7 FATF:** Більшість країн не забезпечують належного рівня технічної відповідності та ефективності TFS щодо фінансування розповсюдження.
- **Основні загрози походять від КНДР, а також Ірану та РФ:** КНДР використовує кібератаки, фіктивні компанії, IT-фахівців за кордоном та нелегальну торгівлю (включно з торгівлею дикими тваринами) для фінансування програми ЗМЗ.
- **Криптовалюти, DeFi і морська логістика — ключові сектори ризику:** Відсутність або слабка імплементація регуляторних вимог для VASP, а також складність контролю за судноплавством дозволяють обходити санкції.
- **Необхідність глобальної уніфікації підходів і стандартів:** Відсутність єдиного визначення ФР заважає ефективній міжнародній співпраці. FATF рекомендує впровадження формалізованого терміну «фінансування розповсюдження» у глобальний Глосарій.

Як ЄС планує контролювати AI: суперечності навколо визначень, заборон і захисту прав²

Документ є результатом комплексного дослідження, проведеного Центром європейських політичних досліджень (CEPS) за замовленням Європейської Комісії, і присвячений аналізу результатів консультацій із зацікавленими сторонами щодо двох ключових аспектів регулювання штучного інтелекту в ЄС — визначення поняття «система AI» та заборонених практик, передбачених статтею 5 Акта ЄС про штучний інтелект (AI Act). У рамках дослідження було опрацьовано відповіді на 88 запитань, які охоплюють спектр правових, технічних та етичних питань, пов'язаних із впровадженням і застосуванням AI у різних сферах суспільного життя та економіки. Демографічна структура респондентів показала домінування представників приватного сектора — понад 47% респондентів складають індустріальні організації, розробники та користувачі AI. Це формує суттєвий перекис у бік комерційних інтересів, тоді як частка громадян, які потенційно найбільше зазнають впливу AI, становить лише близько 5%. Географічно консультація охопила більшість країн ЄС, але найактивнішими були респонденти з Німеччини, Бельгії та Франції, що також створює певне географічне викривлення представництва.



Analysis of EU AI Office stakeholder consultations: defining AI systems and prohibited applications

Final study report

Written by
CEPS - Centre for European Policy Studies
Place du Congrès 1, B-1000 Brussels
Tel. +32 2 229 10 11



Одним із найгостріших питань стала проблема визначення терміну «система AI». Більшість респондентів наголошують, що чинне визначення є занадто широким і ризикує охопити навіть традиційне програмне забезпечення, яке не має властивостей машинного навчання або самостійного прийняття рішень. Особливу увагу викликають поняття «адаптивність», «автономність» та «інференція», які виявилися надто розмитими для чіткої юридичної інтерпретації. Учасники консультацій вимагають розробки деталізованих технічних критеріїв, які дозволять відокремити системи AI від звичайного програмного забезпечення — наприклад, калькуляторів податків, статистичних моделей, баз даних або систем на основі жорстких правил. Крім того, значна кількість респондентів висловила занепокоєння, що поточне визначення створює ризик як надмірного регулювання, так і навпаки — уникнення відповідальності шляхом юридичних маніпуляцій з класифікацією систем.

Не менш серйозним викликом стала інтерпретація заборонених практик, визначених у статті 5 AI Act. Стейкхолдери масово звернули увагу на те, що поняття «шкідливий сублімінальний вплив», «маніпуляція», «значна шкода» та «матеріальне спотворення поведінки» є недостатньо чіткими для правозастосування. Відсутність конкретних меж між допустимими комерційними практиками, такими як персоналізований маркетинг, і недопустимими маніпулятивними технологіями створює серйозний ризик як для бізнесу, так і для захисту споживачів. Наприклад, залишається невизначеним, де закінчується м'яке підштовхування до вибору як легітимна форма впливу і починається маніпуляція, що підпадає під заборону. Подібна ситуація спостерігається у сфері використання емоційного розпізнавання — респонденти вимагають повної заборони таких систем принаймні в критичних сферах, включаючи трудові відносини, освіту та громадський простір.

Особливий резонанс викликає заборона соціального скорингу. Стейкхолдери навели низку реальних кейсів, зокрема нідерландський скандал із системою оцінки добробуту, яка призвела до дискримінації та системних порушень прав людини. Консультація показала, що межа між законними інструментами оцінки кредитоспроможності або виявлення шахрайства і

² <https://digital-strategy.ec.europa.eu/en/library/european-commission-releases-analysis-stakeholder-feedback-ai-definitions-and-prohibited-practices>

забороненим соціальним скорингом є надзвичайно тонкою і потребує чіткої регуляторної деталізації. Без цього існує високий ризик як необґрунтованого переслідування добросовісних учасників ринку, так і потрапляння громадян під дискримінаційні алгоритми.

Не менш спірним виявилось використання систем прогнозування злочинної поведінки і систем оцінки індивідуального ризику скоєння злочинів. Окремі країни вже мають досвід їх використання — ProKid у Нідерландах, RisCanvi в Іспанії, COMPAS у США. Консультація показала глибоку стурбованість тим, що такі системи часто ґрунтуються на історичних даних, які відображають расові, соціальні або економічні упередження. Це створює реальні ризики для фундаментальних прав, включно з презумпцією невинуватості та правом на недискримінацію. Водночас частина респондентів наголошує, що інструменти для боротьби з шахрайством у фінансових установах, які також використовують оцінку ризиків, не повинні автоматично підпадати під дію цієї заборони.

Ще одним центральним питанням стала заборона нецільового скрапінгу зображень облич з відкритих джерел для створення біометричних баз даних. Консультації підтвердили, що приклади таких практик, як діяльність Clearview AI або PimEyes, широко розглядаються як порушення принципів GDPR і є вкрай небезпечними з точки зору масового стеження та втручання в приватне життя. Проте багато респондентів звертають увагу, що відсутність чіткої межі між цільовим і нецільовим збором даних може створити серйозні проблеми для легітимних дослідницьких або безпекових ініціатив.

Дуже важливим аспектом, який чітко простежується у всіх секціях консультації, є потреба в гармонізації AI Act із чинним правом ЄС, насамперед із Загальним регламентом про захист даних (GDPR), а також із законодавством про захист прав споживачів, цифровими послугами та цифровими ринками. Відсутність інтегрованого підходу призводить до перекресних суперечностей, що створює регуляторну невизначеність для бізнесу та ризики для прав громадян. Учасники консультацій наполягають на необхідності розробки керівних документів, які б чітко роз'яснювали взаємодію між цими законодавчими актами.

Висновки:

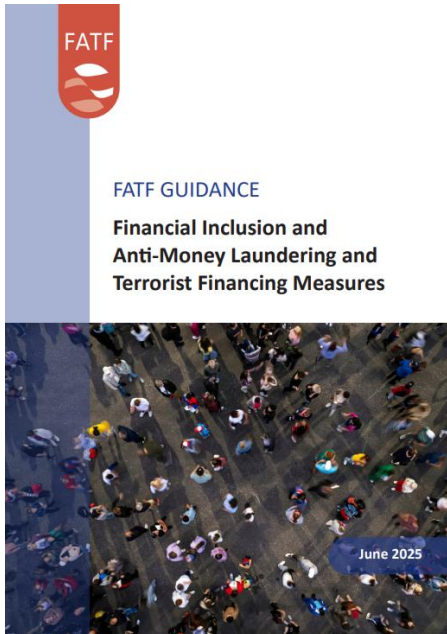
- **Необхідна термінологічна ясність.** Визначення «системи AI» має бути чітко відокремленим від традиційного програмного забезпечення, особливо з точки зору «адаптивності», «інференції» та «автономності».
- **Посилення захисту прав людини.** Потрібні конкретні приклади та чіткі межі для заборонених практик: маніпуляція, експлуатація вразливостей, соціальний збір даних, біометричний моніторинг.
- **Гармонізація з чинними законами.** AI Act має бути чітко інтегрований із GDPR та іншими регуляторними рамками ЄС для уникнення дублювання або суперечностей.
- **Необхідність спеціальних заходів для МСП.** Впровадження спрощених механізмів відповідності, шаблонів оцінки ризиків і підтримки для малого бізнесу.

Окремий акцент зроблений на проблемах малих і середніх підприємств (МСП), які, на думку багатьох респондентів, опиняються у вкрай складній ситуації. Вони не мають ані достатніх ресурсів, ані компетенцій для повноцінного забезпечення відповідності всім вимогам AI Act. Без розробки адаптивних механізмів підтримки, включно зі спрощеними процедурами оцінки ризиків, типовими шаблонами політик і процесів, а також доступними навчальними ресурсами, існує високий ризик витіснення МСП із ринку інновацій.

Документ підсумовує, що основним пріоритетом для Європейського офісу AI є якнайшвидше створення детальних роз'яснень, включно з технічними глосаріями, прикладними сценаріями використання, межами допустимих і недопустимих практик. Тільки за цієї

умови можливо досягти балансу між захистом фундаментальних прав людини та стимулюванням інноваційної економіки в умовах розвитку AI.

Як FATF інтегрує фінансову інклюзію у глобальні стандарти ПВК/ФТ: оновлене керівництво 2025 року³



Документ є комплексним керівництвом, яке визначає, як держави, наглядові органи, фінансові установи та інші підзвітні суб'єкти мають впроваджувати заходи протидії відмиванню коштів і фінансуванню тероризму таким чином, щоб вони не створювали бар'єрів для фінансової інклюзії. Основна ідея документа полягає у тому, що надмірно суворе або надто формалізоване застосування стандартів ПВК/ФТ не лише шкодить соціально-економічній стабільності, але й, що більш критично, підриває саму ефективність системи фінансового моніторингу, оскільки штовхає фінансову активність у тіньовий сектор, де вона стає невидимою для державних органів і значно підвищує ризики ВК/ФТ.

У вступній частині підкреслюється, що FATF ще з 2011 року послідовно інтегрує цілі фінансової інклюзії у свою нормативну та методологічну базу. Зміни, внесені у 2025 році до Рекомендації 1 та її пояснювальної записки, а також

до Рекомендацій 10 і 15, формалізували обов'язок держав не лише дозволяти, а й активно заохочувати застосування спрощених заходів належної перевірки клієнтів у ситуаціях із низьким рівнем ризику ВК/ФТ. Це стало відповіддю на негативні наслідки попередніх підходів, які нерідко призводили до де-рискінг та фінансового виключення.

Документ докладно розкриває концепцію фінансової інклюзії, яка вже давно вийшла за межі просто фізичного доступу до фінансових послуг. Сьогодні під фінансовою інклюзією мається на увазі не лише доступ, але і реальне використання якісних, безпечних, доступних і зручних фінансових продуктів, які відповідають потребам клієнтів, включаючи найуразливіші категорії населення — малозабезпечених, мешканців сільських та віддалених територій, осіб без документів, біженців, внутрішньо переміщених осіб, жінок, людей з обмеженими можливостями та інші соціально вразливі групи. Недостатнє охоплення фінансовими послугами таких категорій громадян не лише підвищує ризики ВК/ФТ, а й позбавляє країну можливості забезпечити фінансову прозорість, контроль за потоками коштів і знижує ефективність фінансового моніторингу.

Далі документ наводить масштабний огляд глобальних тенденцій у сфері фінансової інклюзії, використовуючи статистику Світового банку, МВФ та GSMA. Вказується, що хоча кількість власників фінансових рахунків зросла на 50% між 2011 і 2021 роками, все ще понад 1,4 мільярда дорослих у світі залишаються без доступу до формальних фінансових послуг. Особливо критичними є показники для жінок у країнах Африки та Близького Сходу, де гендерний розрив сягає 12-13%, що суттєво перевищує світовий середній рівень. Звертається увага на те, що навіть серед власників рахунків велика частина користується ними дуже обмежено, або ж рахунки залишаються неактивними, що свідчить про наявність бар'єрів не тільки на етапі відкриття, а й під час використання фінансових послуг.

³ <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf>

Особливий акцент у документі зроблено на аналізі причин фінансового виключення, які включають як фактори з боку клієнтів (відсутність ідентифікаційних документів, віддаленість, недовіра, висока вартість послуг, відсутність цифрових навичок), так і бар'єри, що створюються самими фінансовими установами та державними регуляторами. Серед найнебезпечніших практик FATF виділяє де-рискінг — систематичне припинення співпраці або відмова у відкритті рахунків окремим категоріям клієнтів не через реальну оцінку ризиків, а через страх перед регуляторними санкціями або через занадто вузьке тлумачення вимог ПВК/ФТ. При цьому FATF чітко зазначає, що де-рискінг не лише суперечить принципам ризик-орієнтованого підходу, але й прямо порушує Стандарти FATF, підриваючи їх ефективність.

Документ детально розкриває правові, операційні та інституційні передумови впровадження спрощених процедур належної перевірки клієнтів. Описується механізм створення поетапної ідентифікації, коли клієнт отримує доступ до базових фінансових продуктів за спрощеними процедурами, а з часом, в залежності від історії транзакцій, обсягу операцій і накопиченої інформації, вимоги до перевірки можуть поступово зростати. FATF рекомендує країнам розробити спеціальні законодавчі та нормативні рамки для використання цифрових ідентичностей, які є критично важливими для забезпечення доступу до фінансових послуг для осіб без традиційних документів, таких як внутрішньо переміщені особи, біженці, трудові мігранти та інші.

Дуже важливий блок документа присвячено рекомендаціям державам щодо інтеграції політики фінансової інклюзії у національні стратегії ПВК/ФТ. Зокрема, країни мають враховувати ризики фінансового виключення у своїх національних оцінках ризиків (НОР) і розробляти відповідні компенсаторні механізми. Це може включати спрощення процедур для певних типів фінансових продуктів, цифровізацію урядових виплат (пенсій, соціальної допомоги, субсидій), впровадження масового відкриття базових рахунків, що використовуються виключно для отримання соціальних виплат, із застосуванням спрощених процедур належної перевірки клієнта.

Документ також надає безліч практичних прикладів із досвіду різних юрисдикцій. Наприклад, в Австралії наглядовий орган AUSTRAC оприлюднив офіційну позицію щодо недопустимості де-рискінг та зобов'язав банки переглядати внутрішні політики, щоб уникати надмірних відмов у відкритті рахунків для вразливих груп. У США Міністерство фінансів розробило національну стратегію протидії де-рискінгу, яка включає перегляд підходів до нагляду за банками, модернізацію санкційної політики, спрощення процедур для гуманітарних організацій та зниження адміністративного навантаження на фінансові установи.

Висновки:

- **FATF офіційно вимагає від країн дозволяти та заохочувати спрощені заходи у ситуаціях з низьким ризиком.** Це є обов'язковим елементом впровадження НОР після змін до Рекомендації 1 у 2025 році.
- **Де-рискінг суперечить стандартам FATF і прямо підриває ефективність систем ПВК/ФТ.** Країни повинні активно боротися з де-рискінг через уточнення регуляторних очікувань і заохочення фінансових установ застосовувати пропорційний підхід.
- **Ідентифікація є ключовим бар'єром для фінансової інклюзії.** FATF рекомендує країнам впроваджувати цифрові ідентичності, системи поетапної перевірки клієнтів та спрощення документальних вимог для низькоризикових груп.
- **Фінансова інклюзія є критично важливим інструментом підвищення ефективності ПВК/ФТ.** Включення широких верств населення у формальний фінансовий сектор знижує загальний рівень ризику ВК/ФТ і посилює фінансову прозорість.

Особливий акцент робиться на важливості міжнародної співпраці, зокрема в контексті подолання бар'єрів для транскордонних платежів, зниження вартості грошових переказів і забезпечення доступу до глобальної фінансової системи для країн із обмеженими можливостями. FATF нагадує, що відмова у відкритті рахунків для фінансових установ з окремих країн через їхнє перебування у списках підвищеного моніторингу (сірий список) не є виправданою, якщо вона не ґрунтується на конкретній оцінці ризиків і можливостей їхнього управління.

У заключній частині FATF підкреслює, що без ефективної фінансової інклюзії жодна система ПВК/ФТ не може бути стійкою, оскільки залишення значної частини населення за межами формальної фінансової системи автоматично підвищує ризики використання нелегальних або тінювих фінансових каналів. Таким чином, забезпечення фінансової інклюзії стає не лише соціальною або економічною метою, але й прямим інструментом захисту фінансової системи від зловживань, пов'язаних із ВК/ФТ.

Санкції

Морські санкції проти тінювого флоту росії: роль страхових компаній і держав прапора у глобальній боротьбі з обходом санкцій ⁴

Документ є комплексним аналітичним дослідженням, підготовленим Королівським об'єднаним інститутом оборонних досліджень (RUSI), який детально розглядає механізми, що забезпечують функціонування російського тінювого флоту, а також аналізує критичні вразливості міжнародної системи санкційного контролю в морському секторі. Основна увага зосереджена на двох ключових елементах — страховому секторі та юрисдикціях держав прапора, які у разі недостатнього контролю або свідомої співучасті стають критичними ланками у забезпеченні обходу міжнародних санкцій, спрямованих на обмеження експорту російської нафти та інших товарів, що фінансують військову машину рф. Документ ґрунтується на роботі експертної групи, що включає представників урядів країн G7, страхової індустрії, банківського сектору, юридичних фірм, брокерських компаній та постачальників морських даних.



У контексті страхового сектору автори акцентують увагу на тому, що хоча страхування відповідальності (P&I) традиційно перебуває під найсуворішим наглядом регуляторів через його критичну роль у забезпеченні доступу суден до портів і покриття відповідальності за аварії, забруднення або шкоду третім сторонам, інші види страхування — такі як корпусне страхування і вантажне страхування — значною мірою залишаються поза належним контролем. Це створює серйозні лазівки, які активно використовуються операторами тінювого флоту. Особливо проблемними є довгострокові договори страхування, які забезпечують страхування одразу для серії вантажів і рейсів без необхідності надання деталізованої інформації щодо кожного конкретного перевезення. Це призводить до того, що навіть у разі коли товари або країни підлягають санкціям, страхові компанії можуть несвідомо покривати такі ризики, не маючи достатньої інформації для верифікації законності операції.

Важливим аспектом, який підкреслюється у звіті, є обмеженість можливостей страхових компаній здійснювати глибоку перевірку клієнтів своїх клієнтів — так звану практику Know Your

⁴<https://static.rusi.org/maritime-sanctions-taskforce-insurance-flag-states-jun-25.pdf>

Customer's Customer (KYCC). У складних ланцюгах судноплавства без доступу до інформації митних органів, підрозділів фінансової розвідки, судових реєстрів або портових інспекцій навіть великі міжнародні страховики не мають можливості ефективно виявляти кінцевих бенефіціарів або фактичних операторів суден. Таким чином, система наразі побудована переважно на добровільних заявах клієнтів, що робить її вкрай вразливою до зловживань.

Особливої уваги заслуговує опис ситуації, коли, реагуючи на ризики санкційних порушень, деякі страхові компанії взагалі виходять з високоризикових ринків. Це не усуває проблему, а навпаки, відкриває шлях для менш прозорих, слабо регульованих або навмисно недобросовісних страховиків, включно з тими, що діють під патронатом Центрального банку рф. Таким чином формується паралельна система страхування, яка задовольняє формальні вимоги для отримання документів про покриття відповідальності (наприклад, Blue Card відповідно до вимог IMO), але фактично не гарантує реальної спроможності виконати фінансові зобов'язання у разі страхового випадку, зокрема, великомасштабного розливу нафти.

Значна частина дослідження присвячена аналізу ефективності держав прапора, які за Конвенцією ООН з морського права (UNCLOS) зобов'язані забезпечувати нагляд за суднами, що плавають під їхніми прапорами, включаючи контроль за технічним станом, дотриманням екологічних норм і наявністю дійсного страхового покриття. Проте відсутність механізмів міжнародного примусу робить ці зобов'язання фактично декларативними. У звіті наведені приклади країн, де реєстри держав прапора, де-факто, перетворилися на комерційні підприємства, що існують виключно для отримання доходу за реєстрацію суден без будь-якого належного контролю. Серед таких держав називаються Гамбія, Сьєрра-Леоне, Монголія, Сан-Томе і Принсіпі, Танзанія. Судна в рамках кількох тижнів можуть змінювати прапори, переходячи від одного слабо регульованого реєстру до іншого, що ускладнює їхнє відстеження і контроль.

Водночас наголошується, що у разі послідовного дипломатичного тиску окремі держави прапору здатні коригувати свою політику. Позитивними прикладами є Панама, Ліберія, Габон і Барбадос, які під впливом Сполученого Королівства, Європейського Союзу та інших партнерів почали знімати з реєстрації судна, що беруть участь в обхідних схемах, або мають зв'язки з підсанкційними структурами.

Ще одним суттєвим питанням є відсутність єдиного міжнародного механізму оцінки якості флагових реєстрів. Taskforce пропонує створити відкритий глобальний список високоризикових реєстрів держав прапора, аналогічний до біло-сіро-чорних списків Паризького та Токійського меморандумів взаєморозуміння з портового контролю. Такий інструмент дозволить страховим компаніям, фінансовим установам і портовим органам коректно оцінювати ризики та уникати співпраці з недобросовісними юрисдикціями.

Особливу увагу приділено інфраструктурі, яка забезпечує діяльність тіньового флоту. Центральне місце в цих мережах займають брокери, судновласники, фінансові посередники, юристи, які допомагають структурувати угоди, приховувати справжніх бенефіціарів та забезпечувати формальну законність операцій. Як ілюстрацію цієї проблеми наведено випадок британського фінансиста Джона Ормерода, який допоміг поставити до тіньового флоту рф 25 танкерів через складні схеми власності та використання офшорних компаній. Водночас покарання було застосоване лише до нього як продавця, а брокери, посередники і фінансисти, які допомагали організовувати ці угоди, залишилися поза увагою правоохоронних органів.

Дослідження також наголошує на ролі країн, які залишаються умовно нейтральними або відкрито ігнорують санкційні режими. Серед них виокремлюються Китай, Індія, Малайзія, Індонезія і частково Об'єднані Арабські Емірати. Порти цих країн активно приймають судна тіньового флоту, забезпечують бункерування, ремонт, зміну екіпажів, зберігання нафти у плавучих сховищах або організацію перевалок з судна на судно у відкритому морі. Особливо кричущими є приклади Малайзії та Індонезії, де систематично відбуваються маніпуляції із

системами автоматичної ідентифікації суден (AIS), що дозволяє приховувати маршрути та справжнє походження вантажів.

Звіт наголошує на критичній необхідності для ЄС, Великої Британії та партнерів по G7 переглянути власні санкційні інструменти і адаптувати їх до реалій, в яких США успішно застосовують вторинні санкції проти третіх юрисдикцій, які допомагають обхідним схемам. ЄС і Велика Британія наразі позбавлені такої можливості, що створює нерівні умови і значно знижує ефективність їхніх обмежувальних заходів.

У підсумку автори дійшли висновку, що без системної трансформації підходів до контролю над реєстрами держав прапора, без радикального підвищення прозорості страхового сектору та без перенесення санкційного тиску з окремих суден на всю інфраструктуру обходу санкцій — включно з брокерами, портами, логістичними компаніями, реєстраторами та страховиками — морський компонент санкцій залишатиметься значною мірою неефективним. Вирішення цієї проблеми потребує не лише правових змін, але й посилення міждержавної координації, політичної волі, глибокого залучення фінансових розвідок, митних органів і галузевих асоціацій до спільної роботи над виявленням та руйнуванням мереж обходу санкцій.

Висновки:

- **Необхідно підвищити прозорість страхового сектору**, запровадивши обов'язкове розкриття фінансових даних страхових компаній для підвищення якості контролю державами прапора та портовими органами.
- **Інтеграція нагляду за реєстрами суден до процедур FATF** може стати ефективним інструментом боротьби з використанням реєстрів держав прапора зручності для обходу санкцій і стандартів безпеки.
- **Необхідно запровадити публічний список високоризикових реєстрів держав прапора**, який використовуватиметься страховиками, банками та портовими державами для посилення перевірок і відмови у співпраці з такими реєстрами.
- **Санкційна політика повинна розширити фокус з окремих суден на всю інфраструктуру ухилення**, включно з брокерами, портами, реєстрами, фінансовими посередниками та логістичними компаніями, з акцентом на застосування вторинних санкцій проти третіх країн.

Таємні маршрути: Як санкційні вантажівки потрапляють до росії⁵



Документ опублікований виданням iFact, є ґрунтовним розслідуванням, яке викриває складні механізми обходу західних санкцій, запроваджених проти росії після її повномасштабного вторгнення в Україну у

2022 році. Розслідування детально описує, як європейські вантажівки Volvo, MAN, Mercedes і Scania, попри офіційну заборону їхнього експорту до росії, продовжують з'являтися на російських дорогах і навіть у продажу на популярних торговельних платформах, таких як Avito. Основна увага приділена ролі Грузії як ключового транзитного хабу в цих схемах, а також участі сусідніх країн, зокрема Туреччини, Вірменії, Азербайджану, Казахстану, Киргизстану, Узбекистану та Таджикистану, які використовуються як посередники для прихованого реекспорту санкційних товарів до росії.

⁵ <https://ifact.ge/en/how-sanctioned-trailers-enter-russia/>

Для збору даних журналісти iFact використовували міжнародні торговельні бази, такі як Volza, ImportGenius, ExportGenius, Comtrade, Sayari і Trademo, а також офіційні статистичні звіти з Грузії, Вірменії, Узбекистану, Казахстану, Таджикистану та Киргизстану. Аналіз проводився шляхом зіставлення VIN-кодів (унікальних ідентифікаторів транспортних засобів), митних декларацій і торговельних записів, що дозволило виявити розбіжності між задекларованими маршрутами вантажівок і їхніми фактичними кінцевими пунктами призначення. Наприклад, вантажівки, експортовані з Грузії під митним кодом 8704 (вантажні автомобілі), у деяких випадках реєструвалися в країнах-одержувачах, таких як росія чи Казахстан, під кодом 8701 (важка техніка), що свідчить про навмисні маніпуляції з класифікацією товарів для приховування їхнього справжнього призначення.

Розслідування викриває кілька ключових схем обходу санкцій. Перша схема передбачає продаж вантажівок із Грузії до Туреччини або інших країн, звідки вони згодом переправляються до росії. Яскравим прикладом є діяльність грузинської компанії LLC «Enterprise», яка у 2023 році поставила 33 німецькі вантажівки MAN вартістю понад 4 мільйони доларів до росії через Азербайджан і Дагестан, використовуючи турецькі компанії-посередники, такі як «LYSCHOR GUNEE ELEKTRIK TICARET LIMITED SIRKETI» та «EXIM TURKEY EV TEKSTIL URUNLER TICARET LIMITED SIRKETI». Ці турецькі компанії, засновані російськими чи ізраїльськими громадянами, офіційно займаються торгівлею електронікою чи текстилем, але на практиці виступають ланками в ланцюгу постачання санкційних вантажівок. У росії кінцевим отримувачем виступала компанія ООО «ЛАКОР», зареєстрована в Санкт-Петербурзі як брокерська та логістична фірма.

Друга схема полягає в експорті вантажівок із Грузії до країн Центральної Азії, таких як Киргизстан, Казахстан чи Узбекистан, із подальшим їхнім «зникненням» у росії. З 2022 року експорт вантажівок до Киргизстану зріс у дев'ять разів: якщо з 2013 по 2021 рік Грузія відправила туди лише 31 вантажівку, то за три роки після початку війни цей показник сягнув 295. Однак аналіз даних показав, що з 230 вантажівок, відправлених до Киргизстану в 2023–2024 роках, лише 43 досягли пункту призначення, тоді як решта залишилися в росії. Ця схема використовує той факт, що транзитні маршрути до Центральної Азії проходять через російську територію, що дозволяє «втрачати» вантаж на шляху. Наприклад, грузинська компанія «Palfinger Georgia», пов'язана з російськими та австралійськими власниками, у 2024 році продала чотири вантажівки Mercedes-Benz вартістю 560,000 доларів, які нібито прямували до Киргизстану, але опинилися в росії у власності компаній Logisport і ZT Sever.

Третя схема, описана в розслідуванні, передбачає приховування санкційних автозапчастин під виглядом сільськогосподарської продукції. Грузинська компанія LLC «Union Export 2024», зареєстрована в Сігнаху в травні 2024 року, декларує експорт фруктів і овочів до росії, але в 23 випадках у 2024 році її вантажі містили автозапчастини вартістю 380,370 доларів, заборонені до експорту з 2023 року. За даними російської митниці, ці запчастини отримували компанії MAXIMA LLC, LAZUR LLC і SPETSSNAB LLC, які спеціалізуються на торгівлі автозапчастинами. Власник компанії, Бесік Сікмашвілі, у розмові з журналістами припустив, що порушення могли статися через дії водіїв у «нейтральній зоні», але не надав доказів, які б спростовували інформацію з міжнародних баз даних.

Статистичні дані підтверджують масштаби проблеми. Імпорт вантажівок до Грузії з Європи значно зріс після 2022 року, а експорт до «третіх країн» збільшився в рази. Наприклад, експорт до Казахстану зріс із 14 вантажівок у 2019–2021 роках до 322 у 2022–2025 роках. Вірменія стала ще одним важливим транзитним хабом: якщо у 2021 році вона експортувала до росії лише 10 вантажівок, то у 2022 році цей показник сягнув 9256, що становить зростання на 92,460%. На російському сайті Avito.ru у січні–березні 2025 року було розміщено понад 1000 оголошень про продаж європейських вантажівок, виготовлених у 2023–2025 роках, що вказує на безперервне постачання санкційної техніки.

Журналісти звернулися до виробників вантажівок, щоб з'ясувати їхню позицію. Volvo заявили, що дотримуються санкцій і впровадили заходи для їх забезпечення, включаючи перевірку контрактів і партнерів. Після надання VIN-кодів трьох вантажівок, які потрапили до росії, компанія повідомила, що ці транспортні засоби були продані партнерам у Європі та Центральній Азії, а не в росії чи білорусі.

Mercedes-Benz (Daimler Truck) підтвердили припинення діяльності в росії та впровадження заходів для запобігання нелегальному експорту, регулярно перевіряючи своїх партнерів. MAN і Scania не відповіли на запити, попри неодноразові спроби зв'язатися через електронну пошту та соціальні мережі.

Грузія формально не порушує санкції, оскільки вантажівки експортуються до «третіх країн», а не безпосередньо до росії. Грузинська митна служба стверджує, що не може відстежувати подальший рух товарів після перетину кордону, що створює юридичну лазівку для обходу санкцій. Відсутність міжнародного механізму для відстеження кінцевих пунктів призначення санкційних товарів ускладнює боротьбу з такими схемами. Розслідування також вказує на зв'язки грузинських компаній із російськими власниками, як у випадку з «Palfinger Georgia», чії власники одночасно володіють російськими компаніями, що отримують санкційні товари.

На основі досвіду Литви журналісти пропонують низку заходів для протидії схемам обходу санкцій. По-перше, Грузія має розслідувати компанії, залучені до таких схем, і запровадити суворіші вимоги до експортерів, зокрема зобов'язати їх надавати інформацію про кінцевих власників вантажу. По-друге, необхідно обмежити експортні права компаній, які постачають санкційні товари до росії через треті країни, до завершення розслідувань. По-третє, експорт до країн Центральної Азії має супроводжуватися додатковою документацією, яка забороняє перепродаж санкційних товарів до росії. Нарешті, Грузія та західні країни повинні регулярно аналізувати міжнародні торговельні бази даних, щоб виявляти розбіжності між задекларованими та фактичними маршрутами вантажів.

Розслідування підкреслює, що Грузія стала центральним вузлом у глобальній мережі обходу санкцій, що дозволяє росії отримувати європейські вантажівки та автозапчастини, підтримуючи її економіку та військову логістику. Попри заяви європейських виробників про дотримання санкцій, їхня продукція продовжує потрапляти до росії через складні ланцюги посередників, що вимагає негайного посилення міжнародного контролю та координації.

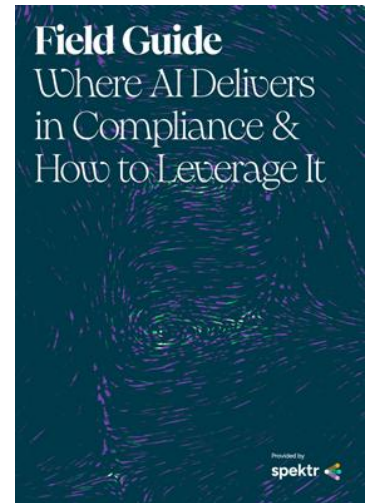
Висновки:

- **Посилення митного нагляду в Грузії:** Грузинська митна служба повинна запровадити обов'язкову перевірку кінцевих отримувачів вантажівок, що експортуються до «третіх країн», і вимагати від експортерів документи, які унеможливають їхній подальший рух до росії.
- **Міжнародна система відстеження VIN-кодів:** Європейські країни та виробники (Volvo, MAN, Mercedes, Scania) мають створити єдину базу даних VIN-кодів для моніторингу маршрутів вантажівок, співпрацюючи з митними органами Грузії, Туреччини та Центральної Азії.
- **Санкції проти посередників:** Компанії, такі як LLC «Enterprise», «Palfinger Georgia» та «Union Export 2024», які беруть участь у схемах обходу санкцій, повинні бути внесені до міжнародних санкційних списків, а їхні експортні права обмежені до завершення розслідувань.
- **Моніторинг торговельних баз даних:** Грузія та західні країни мають регулярно аналізувати дані з баз ImportGenius, ExportGenius і Sayari для виявлення розбіжностей у маршрутах санкційних товарів, використовуючи досвід Литви.

Звіти окремих інституцій та експертів

Штучний інтелект у комплаєнсі: як перейти від теорії до реальних результатів⁶

Документ є ґрунтовним практичним дослідженням того, як штучний інтелект вже сьогодні приносить відчутну користь у сфері комплаєнсу, зокрема у напрямках протидії відмиванню коштів (ПВК), фінансуванню тероризму (ФТ) та належної перевірки клієнтів і контрагентів. Автори переконливо підкреслюють необхідність зміни дискурсу навколо застосування AI у комплаєнсі — від абстрактних обіцянок і хайпових заяв до конкретних результатів, що мають реальний операційний вплив на роботу комплаєнс-підрозділів. Центральна ідея документа полягає в тому, що AI не є магічним інструментом, який повністю вирішує проблему комплаєнсу або замінює людей, але він виступає потужним акселератором, здатним зняти навантаження з аналітиків, зменшити кількість рутинних задач, покращити якість скринінгу та перевірок, а також забезпечити масштабованість процесів у середовищі, де обсяги даних і швидкість змін є критичними факторами.



Особливої уваги в документі приділено сфері протидії відмиванню коштів за допомогою AI, де окреслюються три ключові напрямки застосування: обробка негативних згадок у ЗМІ, скринінг по санкційних списках і виявлення політично значущих осіб (PEP). Під час роботи з негативними згадками AI здатний не лише знаходити прості збіги імен, але й інтерпретувати контекст повідомлень, відокремлювати релевантні ризики від інформаційного шуму, автоматично структурувати отримані дані, а також зменшувати кількість хибнопозитивних спрацювань, які є великою проблемою для традиційних рішень. Це не лише підвищує ефективність моніторингу, але й дозволяє командам зосередитись на аналізі дійсно значущих кейсів.

У контексті санкційного моніторингу AI застосовує методи розширеного зіставлення даних, аналізуючи альтернативні імена, псевдоніми, локації та зв'язки для ідентифікації реальних ризиків. Це дозволяє значно знизити ризики як недовиявлення, так і надмірної кількості хибних спрацювань, які виникають при використанні традиційних систем скринінгу. При цьому кожне спрацювання супроводжується чітким джерелом інформації, яке можна миттєво верифікувати, що критично важливо для якості прийняття рішень у комплаєнсі.

Перевірка політично значущих осіб за допомогою AI виходить за межі простого зіставлення зі списками — вона включає глибокий контекстуальний аналіз: відстеження кар'єрних шляхів, аналіз публічних декларацій, виявлення пов'язаних осіб та історичних зв'язків, що дозволяє формувати більш точні ризик-профілі та уникати як пропуску ризиків, так і необґрунтованих підозр.

Дуже важливим і водночас новаторським напрямом є застосування AI для перевірки легітимності вебсайтів компаній-контрагентів. Інструмент здатний в автоматичному режимі зіставляти інформацію із сайтів (контактні дані, опис бізнесу, наявність регуляторних ліцензій) з офіційними реєстрами та іншими джерелами. Виявлення невідповідностей, відсутність активних доменів або розбіжності в адресах і номерах реєстрації є важливими індикаторами потенційних ризиків, пов'язаних із фіктивними або шахрайськими структурами.

Ще одним важливим застосуванням AI є автоматизація аналізу документів. Штучний інтелект дозволяє оперативно витягувати необхідну інформацію з установчих документів, договорів,

⁶ https://www.spektr.com/api/guides?name=aifieldguide_ba54176d6d.pdf

банківських формулярів та інших джерел. Отримані дані автоматично зіставляються з відкритими джерелами, базами регуляторних органів і корпоративними реєстрами. Це дає можливість миттєво виявляти розбіжності у таких критичних параметрах, як адреса, структура власності, реєстраційні дані, що, в свою чергу, знижує ризики роботи з ненадійними контрагентами.

Особливо вагоме місце в документі займає опис застосування AI для автоматизованого KYB (Know Your Business) процесу, а саме ідентифікації кінцевих бенефіціарних власників (КБВ). В умовах, коли структура власності є навмисно заплутаною або інформація про власників розкидана по різних юрисдикціях і джерелах, AI здатний відновлювати відсутні фрагменти, автоматично будувати структуру власності компанії і виявляти реальних бенефіціарів. Це особливо актуально для юрисдикцій, які є традиційними офшорними зонами або використовуються для фінансового маскування.

Окрема частина документа присвячена аналізу системних проблем сучасного ринку AI-рішень для комплаєнсу, основною з яких є фрагментованість. Переважна більшість рішень зосереджуються на окремих функціях — наприклад, окремо санкційний моніторинг, окремо медіа-аналітика, окремо перевірка PEP — і не забезпечують наскрізної інтеграції. Такий підхід призводить до утворення інформаційних «шлюзів», коли дані і результати аналізу не передаються між різними модулями, що ускладнює формування комплексної картини ризику по клієнту або контрагенту.

Пропоноване рішення — це платформенний підхід, який дозволяє об'єднати всі ці функції у єдину екосистему з наскрізною логікою обробки даних, можливістю аудиту, пояснюваністю кожного кроку і повною відтворюваністю прийнятих рішень. На прикладі платформи «Spektr»

Висновки:

- AI вже ефективно вирішує ключові завдання комплаєнсу, зокрема санкційний моніторинг, перевірку PEP, аналіз негативних згадок і виявлення бенефіціарів, значно скорочуючи кількість хибних спрацювань і прискорюючи обробку кейсів.
- Основна проблема сучасних рішень — фрагментарність, відсутність інтеграції між окремими інструментами для комплаєнсу, що знижує ефективність і ускладнює забезпечення прозорості процесів.
- Платформенний підхід є найбільш ефективним шляхом впровадження AI в комплаєнс, оскільки забезпечує цілісний, контрольований та прозорий робочий процес з можливістю аудиту та гнучкого масштабування.
- AI має працювати як інструмент підтримки рішень, а не як повний заміник людини — ефективність досягається при правильному балансі між автоматизацією рутинних задач і збереженням критичного мислення та досвіду комплаєнс-фахівців.

показано, як можна автоматизувати весь робочий процес — від первинної обробки документів, скринінгу і класифікації ризиків до формування фінального звіту або рішення по кейсу. Такий підхід дозволяє одночасно підвищити ефективність, забезпечити відповідність регуляторним вимогам і зберегти повний контроль над процесами.

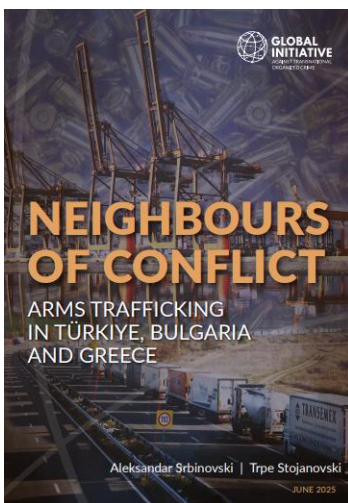
Ключовим принципом є концепція «AI You Control», що означає — AI не замінює людину, а підсилює її можливості. Система працює як асистент, який бере на себе обробку великих обсягів даних, виконує первинний скринінг, ідентифікацію ризиків і формування проміжних

висновків. При цьому критичні рішення завжди залишаються за людиною, яка може в будь-який момент перевірити, скоригувати або відхилити рекомендації AI. Гнучкість системи дозволяє самостійно визначати рівень автоматизації: наприклад, для низькоризикових контрагентів

процес може бути повністю автоматизованим, тоді як для складних випадків — AI працює як інструмент підтримки прийняття рішень.

Фінальна частина документа підкреслює, що майбутнє комплаєнсу — це не конкуренція між людьми і машинами, а їх симбіоз. Найбільш ефективні команди комплаєнсу будуть ті, які поєднують людський досвід, аналітичне мислення та професійну інтуїцію із можливостями AI обробляти великі масиви даних, знаходити закономірності, які недоступні для людини через обмеження пам'яті або швидкості обробки інформації, і при цьому забезпечувати прозорість, відтворюваність і повну підзвітність прийнятих рішень. Саме такий підхід дозволяє відповідати зростаючим регуляторним вимогам, ефективно боротися з фінансовими злочинами і забезпечувати стійкість фінансових установ у світі, де ризики стають дедалі складнішими, а обсяги даних — дедалі більшими.

Торгівля зброєю на південно-східному фланзі Європи: Динаміка, виклики та стратегії протидії в Туреччині, Греції та Болгарії⁷



Документ, підготовлений Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC, є всебічним аналізом динаміки незаконного обігу вогнепальної зброї в трьох країнах Південно-Східної Європи, які відіграють ключову роль як транзитні вузли, джерела та споживчі ринки для нелегальної зброї, що надходить до Європейського Союзу та за його межі. Звіт ґрунтується на польових дослідженнях, проведених із вересня по грудень 2024 року, які включали напівструктуровані інтерв'ю з представниками державних структур, правоохоронних органів, громадянського суспільства, журналістами, академіками та навіть учасниками кримінального світу. Дослідження доповнене аналізом відкритих джерел, включаючи звіти поліції, профільні дослідження, дані міжнародних організацій, таких як Europol, SELEC, SEESAC, а

також матеріали міністерств торгівлі та медіа.

Звіт розпочинається з висвітлення глобального контексту, наголошуючи на занепокоєнні щодо потенційного зростання нелегального обігу зброї внаслідок російського вторгнення в Україну в 2022 році, яке може повторити сценарій витоку зброї після балканських конфліктів 1990-х років. Однак автори застерігають, що фокус виключно на Україні може призвести до звуженого розуміння проблеми, адже європейський ринок нелегальної зброї є багатограним і включає різноманітні джерела, такі як старі радянські арсенали, перероблені газові пістолети, саморобну зброю та навіть сучасні 3D-друковані моделі. Туреччина, Греція та Болгарія розглядаються як країни, що утворюють складний регіональний кластер на так званому «Балканському маршруті», який використовується для транзиту наркотиків, мігрантів і зброї. Ці країни є не лише транзитними пунктами, але й активними учасниками торгівлі зброєю через свою близькість до зон конфлікту на Близькому Сході, історичні зв'язки з Балканами та потенційні канали постачання зброї з України та Росії через Чорне море.

У Туреччині ринок нелегальної зброї є одним із найбільших у регіоні, з оцінкою в 36 мільйонів одиниць неліцензованої зброї, що становить приблизно 90% від загальної кількості. Цей феномен частково пояснюється історичними традиціями Османської імперії, коли володіння зброєю було нормою, а також сучасними культурними практиками, такими як святкові стрільби під час весіль, свят чи спортивних подій. Зброя в Туреччині сприймається як невіддільна частина

⁷ <https://globalinitiative.net/wp-content/uploads/2025/06/Aleksandar-Srbinovski-and-Trpe-Stojanovski-Neighbours-of-conflict-Arms-trafficking-in-Tu%CC%88rkiye-Bulgaria-and-Greece-GI-TOC-June-2025.v2.pdf>

побуту, подібна до володіння автомобілем, причому 70% власників, за оцінками, носять її для самозахисту.

Статистика демонструє серйозність проблеми: за період 2014–2024 років у Туреччині зафіксовано 34 197 інцидентів збройного насильства, що призвели до 21 647 смертей і 31 207 поранень, причому 75% злочинів у 2023–2024 роках скоєно з використанням неліцензованої зброї. Ринок включає широкий спектр зброї: від саморобних пістолетів, виготовлених у регіоні Чорного моря з традиційних технологій, до газових пістолетів, які легко переробляються в летальну зброю, та промислових зразків, таких як пістолети Glock чи SIG Sauer, що є символами престижу серед кримінальних еліт.

Транскордонні коаліції постачають більш сучасну та прибуткову зброю, тоді як особи, пов'язані з державними структурами, беруть участь у незаконних поставках до Сирії, Лівії та внутрішніх парамілітарних груп. Іноземні терористичні організації, такі як PKK (розпущена у травні 2025 року) та ІДІЛ, також сприяли контрабанді в південно-східних прикордонних регіонах. Туреччина є ключовим транзитним хабом для зброї, що надходить із Сирії, Іраку та Ірану через гірські райони Тавр і Загрос, а також для експорту газових пістолетів до Європи через кордон Капікуле-Капітан Андреево. Морська контрабанда, зокрема до Лівії та Нігерії, дозволяє перевозити великі партії, іноді порушуючи ембарго ООН.

Турецькі правоохоронці посилили боротьбу з нелегальним обігом, вилучивши 90 000 одиниць зброї у 2017–2021 роках і ще стільки ж за перші 10 місяців 2024 року, а також запровадивши суворіші покарання (до 12 років за переробку газової зброї). Проте брак послідовного правозастосування та глибоко вкорінена культура володіння зброєю ускладнюють прогрес. Міжнародна співпраця з Europol, SELEC та іншими організаціями є активною, але специфічної кооперації щодо торгівлі зброєю бракує через невідповідність турецького законодавства про захист даних стандартам ЄС.

Греція має власну складну динаміку нелегального обігу зброї, з оцінкою в 800 000–1 000 000 одиниць неліцензованої зброї, що становить 57% від загальної кількості. Культура володіння зброєю різниться залежно від регіону: на Криті, Пелопоннесі та в гірських селах Центральної Греції вона пов'язана з історичним опором Османській імперії та німецькій окупації, а також сімейними традиціями, тоді як в Афінах і Салоніках попит зумовлений організованою злочинністю. Кожен десятий грек володіє приватною колекцією зброї, часто успадкованою, а дрібні злочинці зазвичай мають хоча б одну одиницю з чорного ринку.

Основними джерелами нелегальної зброї є залишки з балканських конфліктів 1990-х, викрадені албанські склади 1997 року, а також імпорту з Туреччини та Близького Сходу. Російські та грузинські кримінальні групи контролюють високоякісний сегмент ринку, тоді як албанці постачають дешевшу, застарілу зброю, таку як пістолети Tokarev. З'являються також 3D-друковані моделі, що створюють нові виклики. Греція слугує транзитною країною для зброї з Близького Сходу, Туреччини та Балкан, з експортом до Туреччини, Іраку та Сирії, використовуючи морські маршрути (порт Пірей) та наземні канали через Албанію.

У 2024 році грецька поліція вилучила близько 10 000 одиниць нелегальної зброї та значні обсяги вибухівки, зокрема під час рейдів проти турецької мафії. У жовтні 2024 року створено Директорат із боротьби з організованою злочинністю («грецьке ФБР»), а також електронну базу даних для відстеження легальної зброї, що полегшує обмін інформацією з міжнародними партнерами. Греція дотримується директив ЄС і міжнародних угод, таких як Протокол ООН про вогнепальну зброю, і активно співпрацює через Europol (зокрема в рамках EMPACT 2022–2025, що призвело до 566 арештів, 69 з яких пов'язані з торгівлею зброєю) та SELEC. Проте національної стратегії щодо легкої стрілецької зброї (SALW) бракує, що обмежує системний підхід до проблеми.

Болгарія вирізняється найнижчим рівнем володіння зброєю в регіоні, з 244 267 одиницями неліцензованої зброї, що становить 41% від загальної кількості. Відсутність культури володіння зброєю пояснюється репресивною політикою комуністичного режиму (1945–1990), яка змушувала громадян і злочинців уникати збройної діяльності, віддаючи перевагу «м'яким» злочинам, таким як підробка та шахрайство. Навіть після падіння комунізму болгарська організована злочинність зосередилася на торгівлі наркотиками та людьми, уникаючи насильства. Зброя використовується переважно для залякування в суперечках, а вбивства є рідкістю (останнє гучне вбивство – бізнесмена Олексія Петрова в Софії у 2023 році).

Болгарія є транзитною зоною для турецьких газових пістолетів, які перевозяться через кордон Капітан Андреево-Капікуле до Румунії, Хорватії, Сербії чи Косова, де конвертуються в летальну зброю, приносячи до 500% прибутку. Джерелами також є викрадена зброя з військових складів, саморобні моделі та контрафактні бренди, такі як Winchester чи Taurus, що навіть потрапляли до Латинської Америки. Після 2022 року Болгарія значно наростила виробництво зброї для експорту до Польщі (для України), але витоків із цих поставок не зафіксовано. У 1990-х роках болгарська збройна промисловість була замішана в незаконному експорті до країн під санкціями, використовуючи фальшиві сертифікати кінцевого користувача, але після вступу до ЄС у 2004 році такі потоки припинилися. Проте сучасні конфлікти в Сирії та Іраку знову відкрили ринки для болгарських виробників, таких як VMZ Sorot, які експортували зброю на суму понад 1,2 мільярда євро.

Болгарія не має національної стратегії SALW, але регулює газові пістолети через внутрішні директиви МВС, а покарання за торгівлю зброєю є суворими (до 8 років ув'язнення, до довічного за зв'язок із організованою злочинністю). Співпраця через SELEC та Europol посилюється, зокрема через операцію «Conversus» у 2023 році, яка призвела до арешту 22 торговців зброєю по всій Європі.

Звіт підкреслює транскордонний характер торгівлі зброєю, що пов'язує ці країни з нестабільними регіонами, такими як Близький Схід, Балкани та потенційно Україною. Культурні фактори, зокрема глибоко вкорінена традиція володіння зброєю в Туреччині та Греції, ускладнюють боротьбу з нелегальним обігом, тоді як Болгарія є винятком через історичну відсутність такої культури. Нові загрози, такі як зростання 3D-друкованої зброї в Туреччині та Греції та потенційний витік зброї з України, вимагають негайної уваги.

Геополітичні відмінності, з Грецією та Болгарією в ЄС і Туреччиною поза ним, створюють

Висновки:

- **Розробка національних стратегій SALW:** Туреччина, Греція та Болгарія повинні терміново розробити та впровадити національні плани дій щодо легкої стрілецької зброї, що відповідають міжнародним стандартам, зокрема Протоколу ООН про вогнепальну зброю, для системного контролю над нелегальним обігом, враховуючи відсутність таких стратегій у всіх трьох країнах.
- **Посилення транскордонної співпраці:** Необхідно розширити спільні патрулі та впровадити передові технології, такі як рентген-сканери, на ключових прикордонних пунктах для ефективного перехоплення контрабанди зброї, а також активізувати обмін розвідданими через SELEC і Europol.
- **Регулювання 3D-друкованої зброї:** Для протидії зростанню «зброї-привидів» необхідно запровадити регулювання 3D-друку зброї, обмежити онлайн-доступ до креслень і розширити співпрацю з Europol для аналізу кримінального використання цієї технології та навчання правоохоронців.
- **Зміна культурних норм:** У Туреччині та Греції слід запустити кампанії громадської обізнаності, спрямовані на зміну ставлення до володіння зброєю, зокрема шляхом просування альтернатив святковим стрільбам, що може зменшити попит на нелегальну зброю та рівень збройного насильства.

перешкоди для спільного законодавства та обміну розвідданими, хоча співпраця в багатосторонніх форумах, таких як SELEC і Eurropol, демонструє прогрес.

Для ефективної протидії автори пропонують низку рекомендацій: розробку національних стратегій SALW, що відповідають міжнародним стандартам, залучення приватного сектору, академій і громадянського суспільства, посилення транскордонної співпраці через спільні патрулі та передові технології (наприклад, рентген-сканери) на ключових кордонах, боротьбу з корупцією в правоохоронних органах, створення спеціалізованих підрозділів для розгрому мереж торгівлі зброєю, регулювання 3D-друкованої зброї та обмеження доступу до креслень, а також кампанії з підвищення обізнаності для зміни культурних норм щодо володіння зброєю, особливо в регіонах із міцними традиціями, таких як Крит чи турецькі провінції.

Корупція та відмивання коштів у Латинській Америці й Карибському басейні⁸



Стаття, опублікована Global Financial Integrity (GFI) за авторством Леона Доусона, пропонує глибокий аналіз взаємозв'язку між корупцією та відмиванням грошей у регіоні Латинської Америки та Карибського басейну (ЛАК). Використовуючи дані Індексу сприйняття корупції (CPI) від Transparency International та Індексу протидії відмиванню грошей (AML) від Базельського інституту, звіт розкриває, як високий рівень корупції створює сприятливе середовище для фінансових злочинів,

зокрема відмивання злочинних доходів. Документ підкреслює, що корупція послаблює інституційні структури, правоохоронні органи та регуляторні механізми, сприяючи проникненню незаконних фінансових потоків у фінансові системи, що, своєю чергою, погіршує економічні сектори та створює ідеальні умови для відмивання грошей.

Аналіз розпочинається з опису методологій двох ключових індексів. Індекс сприйняття корупції (CPI) базується на 13 джерелах даних від різних установ, які оцінюють сприйняття корупції за останні два роки. Ці дані стандартизуються шляхом віднімання середнього значення кожного джерела за базовий рік від оцінки країни та ділення на стандартне відхилення, що забезпечує можливість порівняння між роками. У 2024 році 15 країн ЛАК, включаючи Нікарагуа, Гаїті, Венесуелу, Гватемалу, Ель-Сальвадор, Парагвай, Болівію, Перу, Еквадор, Ямаїку, Тринідад і Тобаго, були визнані висококорумпованими. Індекс AML, у свою чергу, оцінює ризики відмивання грошей, спираючись на звіти Financial Action Task Force (FATF), рамки боротьби з корупцією та шахрайством, дані про фінансову та публічну прозорість від Tax Justice Network і World Bank, а також оцінки політичних і правових ризиків від World Justice Project і Freedom House. Ці індекси разом демонструють чіткий зв'язок: країни з високим рівнем корупції зазвичай мають значні вразливості до відмивання грошей.

Документ наводить порівняльну таблицю, яка ілюструє кореляцію між показниками CPI та AML для країн ЛАК. Наприклад, Венесуела (CPI: 10, AML: 5), Гаїті (CPI: 16, AML: 2) і Нікарагуа (CPI: 14, AML: 34) мають одні з найгірших показників корупції в регіоні, що супроводжується високими ризиками відмивання грошей через слабкі фінансові системи. Аналогічно, Гватемала, Ель-Сальвадор і Мексика демонструють схожий зв'язок між слабкими структурами управління та підвищеними AML-ризиками. Водночас країни, такі як Аргентина та Бразилія, мають відносно кращі показники CPI, але все ще стикаються з високими ризиками відмивання через регуляторні та інституційні недоліки. У Карибському регіоні, зокрема в Панамі (CPI: 33, AML: 47), Ямаїці,

⁸ <https://gfintegrity.org/corruption-and-money-laundering-in-latin-america-and-the-caribbean-a-tale-of-two-indices/>

Тринідаді і Тобаго, проблеми посилюються через офшорні юрисдикції, торгівлю наркотиками та відсутність прозорості у реєстрах бенефіціарних власників. Навіть країни з помірними рівнями корупції, такі як Парагвай (CPI: 24, AML: 90), Еквадор (CPI: 32, AML: 87) і Перу (CPI: 31, AML: 105), мають високі AML-ризики через регуляторні прогалини, слабкі фінансові установи та низькоподаткові юрисдикції.

Документ виділяє кілька ключових тенденцій. По-перше, країни зі слабкими демократичними інститутами та верховенством права мають вищі ризики як корупції, так і відмивання грошей. Корупція підриває ефективність правоохоронних органів, судової системи та регуляторних агентств, дозволяючи незаконним фінансовим потокам залишатися непоміченими. По-друге, вплив організованої злочинності та політичних еліт на фінансове регулювання підвищує AML-ризики. По-третє, навіть за наявності AML-рамоч їхня ефективність обмежена через слабе правозастосування. У Карибському регіоні ситуація ускладнюється юрисдикціями з низькими податками та проблемами, пов'язаними з наркотрафіком, що робить такі країни, як Багами та Кайманові острови, вразливими до відмивання грошей, навіть якщо вони не входять до основного набору даних звіту.

Важливою частиною аналізу є роль Конвенції ООН проти корупції (UNCAC), яку ратифікували всі країни ЛАК. UNCAC пропонує стандартизовані превентивні заходи, залучає громадянське суспільство до підвищення обізнаності про корупцію та підтримує процес повернення активів до державних адміністрацій. Проте впровадження UNCAC стикається з викликами, такими як брак незалежності правоохоронних органів, недостатня міжнародна координація та складність розслідувань, особливо коли активи відмиваються через криптовалюти або традиційні фінансові системи. Лише Чилі, Перу, Гватемала та Гондурас впровадили "обіцянку прозорості" UNCAC, що вказує на обмежене виконання конвенції в регіоні.

Документ завершується низкою практичних рекомендацій для боротьби з корупцією та відмиванням грошей. Для державного сектору пропонується розвивати міжсекторальну співпрацю на національному та міжнародному рівнях для обміну інформацією та впровадження стратегій протидії фінансовим злочинам. Приватний сектор закликають проводити програми підвищення обізнаності працівників про негативний вплив корупції на бізнес, що сприятиме корпоративній прозорості. У розслідуваннях корупційних справ рекомендується залучати незалежних слідчих для уникнення конфлікту інтересів. Громадянське суспільство, відповідно до принципів UNCAC, має відігравати ключову роль у забезпеченні прозорості та підзвітності через механізми участі в розробці політик та антикорупційних рамок.

Висновки:

- **Посилення міжсекторальної співпраці:** Країни ЛАК повинні розвивати координацію між національними та міжнародними агентствами для обміну інформацією, що дозволить ефективніше виявляти та запобігати відмиванню грошей, пов'язаному з корупцією.
- **Залучення незалежних слідчих:** Для уникнення конфлікту інтересів у розслідуваннях корупції необхідно використовувати незалежних експертів, що підвищить довіру до результатів та ефективність повернення активів.
- **Підвищення обізнаності приватного сектору:** Впровадження програм навчання для працівників компаній щодо впливу корупції на бізнес сприятиме корпоративній прозорості та зменшенню ризиків відмивання грошей.
- **Активізація громадянського суспільства:** Уряди повинні створювати механізми участі громадськості в розробці антикорупційних політик, як це передбачено UNCAC, для забезпечення прозорості та підзвітності.

Інші новини

Від пабу в Бішкеку до офшорної імперії: Як Дуглас Едельман створив глобальну схему ухилення від податків⁹

Стаття Міжнародного консорціуму журналістів-розслідувачів (ICIJ), детально розкриває історію американського бізнесмена Дугласа Едельмана, який, використовуючи контракти Пентагону на суму понад 7 мільярдів доларів, створив складну офшорну мережу для ухилення від сплати податків у США. Ця справа, визнана Міністерством юстиції США однією з найбільших в історії розслідувань щодо ухилення від податків, завершилася 22 травня 2025 року визнанням Едельманом провини у вашингтонському суді за звинуваченнями у змові, наданні неправдивих свідчень та інших кримінальних діях.



Дуглас Едельман, 73-річний уродженець Каліфорнії, розпочав свою кар'єру в середині 1990-х у Киргизстані, куди переїхав із росії, де він заробляв як посередник у торгівлі паливом після розпаду СРСР. У росії він налагодив зв'язки з нафтопереробними заводами, що дало йому глибоке розуміння паливного ринку. У Бішкеку, столиці Киргизстану, у 1998 році він відкрив американський паб, який пропонував німецьке пиво, американські бургери та ікру, ставши популярним серед експатів, зокрема колишніх американських військових. Серед них був Чак Свайрс, экс-підполковник армії США, який працював оборонним аташе в посольстві США в Бішкеку і згодом став генеральним директором однієї з компаній Едельмана. Ці зв'язки стали ключовими для входження Едельмана у світ контрактів Пентагону.

Після терактів 11 вересня 2001 року аеропорт Манас у Бішкеку перетворився на стратегічний хаб для військової операції США в Афганістані. Едельман і його киргизський партнер отримали контракти на постачання авіаційного палива, забезпечуючи до 500 тисяч галонів щодня. Їхні компанії, Mina Corp. та Red Star Enterprises, продемонстрували вражаючу логістичну спроможність: щодня створювався документ, який відстежував рух кожного залізничного вагона з паливом із росії до Киргизстану. Компанії найняли до 1200 співробітників, щоб задовольнити потреби Пентагону. Внутрішні документи свідчать, що вони "розгадали код" експорту російського палива, обійшовши офіційну заборону росії на постачання палива для військових цілей, завдяки зв'язкам із російськими виробниками, залізничними органами та урядовими чиновниками.

Використовуючи величезні прибутки, Едельман створив складну схему ухилення від податків, організувавши мережу офшорних компаній у Британських Віргінських Островах, Белізі, Великій Британії та Панамі. Він приховав свою 50% частку в Mina Corp. і Red Star Enterprises, оформивши її на свою французьку дружину Дельфіну Ле Дейн, яка, не будучи громадянкою США і не проживаючи в країні, була звільнена від сплати американських податків. За оцінками звинувачення, Едельман уникав сплати податків із доходу в розмірі 350 мільйонів доларів. Панаманська юридична фірма Alemán, Cordero, Galindo & Lee (Alcogal) відіграла ключову роль у приховуванні його власності, надсилаючи в 2010 році листи іншим юридичним фірмам, коли конгресове розслідування посилювало увагу до бізнесу Едельмана, із зазначенням, що Ле Дейн та її діти є бенефіціарами трасту, який контролював його інвестиції. Фірма наголошувала, що ця інформація є "строго конфіденційною" і не повинна включатися до корпоративних записів. Після

⁹ <https://www.icij.org/inside-icij/2025/05/how-a-pentagon-contractor-built-a-global-empire-and-a-massive-tax-evasion-scheme/>

публікації звіту Конгресу в грудні 2010 року, який широко висвітлювався в The Washington Post, Alcotag припинила співпрацю з офшорною мережею Едельмана. Один із його представників у відповідь висловив обурення, звинувачуючи журналістів у відсутності доказів, але це не зупинило розслідування.

Едельман використовував прибутки для розкішного життя. Він придбав особняк у Лондоні за 43 мільйони доларів, лижний шале в Австрії, записав його на безробітного брата своєї дружини, а також дві яхти, названі Divinity та Princess Juliet. Його інвестиції охоплювали різноманітні сфери: він фінансував компанію, яка забезпечувала інтернет для американських військ в Афганістані, проекти нерухомості в Тулумі (Мексика), рекламний бізнес у Південному Судані, паливну інфраструктуру в Мексиці та важку техніку для нафтовидобутку, продану Міністерству енергетики США. Його корпоративна структура включала десятки компаній із химерними назвами, як-от Joseph Schmo Investment Ltd., що ускладнювало відстеження активів. Єдине місце, де його ім'я з'являлось, було в окремому внутрішньому документі, який надавав йому повноваження управляти панамським фондом на користь його дружини та дітей.

Розслідування, назване "Operation Jetsetter", проводилося міжнародною групою J5", до якої входять податкові органи США, Австралії, Канади, Великобританії та Нідерландів. Воно стало першим значним успіхом цієї організації, створеної після витоків Panama Papers та Paradise Papers, які виявили необхідність глобальної координації для боротьби з ухиленням від податків. У процесі розслідування було вилучено близько 2,5 мільйона документів із різних юрисдикцій. У 2020 році британська поліція обшукала особняк Едельмана в лондонському районі Кенсінгтон, а в 2023 році кіпрська поліція вимагала документи, пов'язані з його бізнесами, включно з компанією, якою він раніше володів разом із хрещеником короля Чарльза, від юридичної фірми в Нікосії. Шестеро колишніх співробітників Едельмана, включно з Чаком Свайрсом, визнали свою провину в ухиленні від сплати податків, уклавши угоди з прокурорами, що зобов'язували їх надавати свідчення проти Едельмана. Його киргизький партнер і багаторічний бухгалтер, Грем Коллетт, також підтвердили ключові аспекти справи, що прискорило переговори про визнання провини.

Ключовим фактором, який дозволив Едельману так довго уникати відповідальності, була відсутність належного аудиту в Пентагоні. Пентагон ніколи не проходив комплексного аудиту, протягом семи років не надаючи повного звіту про свої трильйони доларів активів і зобов'язань. Закон 2021 року, який вимагав від підрядників розкривати бенефіціарну власність, не був виконаний, що полегшило Едельману приховування його частки в Mina Corp. та Red Star Enterprises. Навіть адреси, вказані компаніями в листуванні з Пентагоном, були віртуальними офісами або спільними робочими просторами, а в Киргизстані опозиційні політики звинувачували компанії в перекачуванні коштів корумпованому президентові, що сприяло політичній нестабільності та революції.

Едельман був заарештований на Ібіці в липні 2024 року, екстрадований до США та перебував під домашнім арештом із заставою 12,9 мільйона доларів. Проте незабаром він порушив умови арешту, зв'язавшись із одним із співучасників, Робертом Дунером, пропонуючи йому доступ до мільйонів доларів у акціях із банківського рахунку на Багамах, що належав одній із компаній Едельмана. Ця "надзвичайно дурна" дія, як назвав її його власний адвокат, призвела до ув'язнення Едельмана в грудні 2024 року. Під час судового слухання в грудні він пояснив свої дії самотністю, а коли суддя зазначив, що Едельман, як розумна людина, мав би знати про порушення умов, він відповів: "Я не впевнений".

Його визнання провини в травні 2025 року стало кульмінацією розслідування, але він ще може зіткнутися з додатковими звинуваченнями за ухилення від податків у період із 2013 по 2020 роки. Суд пізніше 2025 року визначить точний розмір доходу, з якого Едельман ухилявся від податків, що безпосередньо вплине на тривалість його ув'язнення.

Справа Едельмана висвітлює системні проблеми в США: Пентагон не забезпечує належного контролю за контрактами, а Податкова служба США (IRS) зіткнулася зі скороченням ресурсів. З 2010 року кількість спеціальних агентів IRS зменшилася на 16%, а кількість кримінальних справ щодо ухилення від податків із законних доходів впала на 40% до 2023 року. За оцінками IRS, щороку не збирається понад 600 мільярдів доларів податків. Плани адміністрації Трампа щодо скорочення до 25% штату IRS, а також призначення на посаду директора IRS екс-конгресмена, який виступав за ліквідацію агентства, можуть ще більше погіршити ситуацію.

Соціально-політичні наслідки справи Едельмана також значні. У Киргизстані його компанії звинувачували в корупційних зв'язках із президентом, що підживлювало суспільне невдоволення, яке зрештою переросло в революцію. У США справа підкреслює необхідність реформ у системі оборонних контрактів і посилення податкового нагляду, щоб запобігти подібним схемам у майбутньому.

Ваша думка важлива!

1. Як можна забезпечити баланс між вимогами ПВК/ФТ і доступом до фінансових послуг для вразливих груп населення? Чи є у вашій установі практика поетапної КУС? Чи допомогла вона зменшити виключення певних категорій клієнтів?
2. Які переваги та ризики ви бачите у впровадженні AI для автоматизованого КУВ або скринінгу санкційних списків? Чи використовує ваша організація інструменти AI для аналізу негативних згадок у ЗМІ або структурованих перевірок контрагентів?
3. Як поточний конфлікт в Україні може вплинути на зростання нелегального обігу зброї через Туреччину, Грецію та Болгарію, враховуючи їхню географічну близькість до України та роль транзитних хабів на Балканському маршруті?
4. Які механізми може запровадити Україна для моніторингу та блокування постачання європейських вантажівок і автозапчастин до росії через треті країни, щоб послабити російську військову логістику?
5. Які кроки, на вашу думку, є найбільш важливими для кращого впровадження Конвенції ООН проти корупції (UNCAC) в Україні, зокрема щодо забезпечення прозорості бенефіціарної власності, ефективного повернення активів та залучення громадянського суспільства до формування антикорупційної політики?
6. Як Україні побудувати власну систему регулювання штучного інтелекту, яка б ефективно балансувала між захистом прав людини, запобіганням зловживанням та стимулюванням інновацій, з урахуванням стандартів ЄС і глобальних тенденцій?
7. Які законодавчі, регуляторні та технологічні зміни необхідно запровадити в Україні для впровадження механізмів цифрової ідентифікації та поетапної ідентифікації клієнтів відповідно до оновлених стандартів FATF?

Контакуйте щодо цього документу з Міністерством фінансів України:

- Email: aml_bulletin@minfin.gov.ua
- Поштова адреса: Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- Ідентифікація контакту: стосовно Методологічного Бюлетеня № МінФін-AML-2025-26

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

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