

“Маленькі справи, зроблені наполегливо, сильніші за великі задуми без дій”

Пітер Маршалл

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

Ключові червоні прапорці у фінансовій звітності та іншій нефінансовій інформації: аналітика ПФР Мальти ¹



Цей аналітичний документ, підготовлений ПФР Мальти (FIAU), містить узагальнені практичні рекомендації для підзвітних суб'єктів щодо виявлення ключових індикаторів відмивання коштів і фінансування тероризму на основі аналізу фінансової та нефінансової звітності компаній. Документ побудований на підставі реальних прикладів та аналізу звітів, поданих до FIAU, і не має на меті бути вичерпним або нормативно зобов'язуючим, проте є потужним орієнтиром для аналізу підозрілої фінансової поведінки.

У центрі уваги — аналіз окремих статей фінансової звітності (звіт про прибутки та збитки, баланс, звіт про рух грошових коштів), а також

¹ <https://fiaumalta.org/app/uploads/2025/05/SA25-01-Key-Red-Flags-in-Financial-Statements-and-other-Non-Financial-Information-Insights-from-the-FIAU.pdf>

нефінансових документів, які разом можуть виявляти ознаки фінансових злочинів.

У розділі про дохід зазначено, що раптові стрибки у виручці без видимих причин, а також значна частка готівкових продажів порівняно з аналогічними бізнесами галузі, можуть свідчити про інфляцію доходу з метою легалізації коштів. Підозру може викликати також продаж товарів або послуг на віддалені або нехарактерні географічні ринки без відповідної маркетингової стратегії.

Закупівлі та товарно-матеріальні запаси часто використовуються для створення фіктивних витрат. Сюди входить завищення залишків товарів, створення фальшивих рахунків-фактур, підозрілі контрагенти, розбіжності між обліковими залишками і фактичними запасами.

Витрати на оплату праці також підлягають аналізу: нетипово велика кількість працівників для малого бізнесу, витрати на заробітну плату, які не відповідають масштабам діяльності, або виплати працівникам без чітко визначених посад — усе це може свідчити про використання компанії для трудової експлуатації або як каналу переведення коштів.

Консультаційні послуги і маркетингові витрати можуть приховувати платежі пов'язаним або фіктивним особам, особливо у випадках, коли контрагенти не мають чітко визначеного предмету діяльності чи присутності в публічному просторі.

Витрати на оренду, відсотки за кредитами, а також незвичні структури позик від акціонерів або пов'язаних осіб розглядаються як типові канали виведення коштів. Зокрема, увагу варто звертати на неринкові умови позик, відсутність джерел фінансування, кредити без відсотків або з надвисокими ставками, а також взаєморозрахунки з офшорними або невідомими контрагентами.

Аналіз балансу повинен враховувати:

- завищені чи занижені значення активів (у т.ч. нематеріальних),
- надмірну дебіторську заборгованість,
- великий залишок готівки без обґрунтованого джерела,
- інвестиції у високоризикові інструменти,
- часті або нелогічні транзакції з афілійованими особами.

В окремому розділі розглянуто структурні та нефінансові червоні прапорці, зокрема:

- розбіжність між заявленим видом діяльності в установчих документах і фактичними операціями компанії (наприклад, будівельна компанія, що торгує мобільними телефонами);
- відсутність досвіду чи професійної кваліфікації у директорів або власників;

Висновки:

- **Раптові або непропорційні зміни у фінансових показниках** - виручці, зарплаті, витратах на консультації чи рекламу - повинні оцінюватися в сукупності з бізнес-моделлю та галузевими нормами, як можливі індикатори ВК.
- **Фіктивні або завуальовані операції з пов'язаними особами**, у т.ч. через позики, консалтингові послуги, оренду чи рахунки-фактури, є типовими механізмами легалізації доходів і мають бути об'єктом підвищеної уваги.
- **Нефінансова інформація** (установчі документи, структура власності, ділова репутація керівників, дата інкорпорації, зміни акціонерів) **є важливим джерелом індикаторів можливих злочинів** і має оцінюватися нарівні з фінансовими звітами.
- **Звіти аудитора** (особливо з застереженнями, негативним висновком або без висновку) та незвичні події, як-от зміна аудитора, можуть вказувати на спроби приховати суттєві викривлення і мають ініціювати додаткову перевірку.

- нехарактерно швидке зростання активності після реєстрації компанії;
- часті зміни власників або ускладнена корпоративна структура;
- наявність кваліфікованих або негативних висновків у звітах аудитора.

Також підкреслюється, що аудиторські висновки можуть бути важливими індикаторами — зокрема, відмова аудитора, наявність зауважень, або звільнення/заміна аудитора повинні привертати увагу.

Документ завершується застереженням, що жоден окремих індикатор не є беззаперечним доказом злочину, і кожна ознака повинна розглядатися в контексті з іншими обставинами, з урахуванням характеру бізнесу.

Типологічний звіт ПФР Швейцарії ²

Цей документ є першою частиною типологічного звіту, опублікованого Швейцарським підрозділом фінансової розвідки (MROS) під егідою Федерального департаменту юстиції та поліції. Його мета — представити реальні приклади виявлених схем відмивання коштів, фінансування тероризму, ухилення від санкцій, шахрайства та зловживань у фінансовому секторі з метою навчання та підвищення обізнаності працівників комплаєнс-підрозділів, керівництва та осіб, які безпосередньо взаємодіють із клієнтами.

Документ охоплює 20 типових справ, класифікованих за видами злочинної діяльності, типом учасників, каналами переміщення коштів і характером фінансових інструментів. Описані випадки охоплюють широкий спектр галузей — від торгівлі золотом, обігу криптовалют і ринку творів мистецтва до операцій із нерухомістю, страхування життя, транзитних рахунків, послуг юристів та обробки платежів через віртуальні IBAN.

Кожен кейс детально розкриває як механізми, якими зловмисники намагаються замаскувати походження коштів, так і дії, які вживав фінансовий посередник — з акцентом на найкращі практики: перевірки відповідності KYC, аналіз транзакцій, оцінка ділової мети, використання OSINT, виявлення невідповідностей у документах або поведінці клієнтів. Зокрема, у справі №1 клієнт намагався приховати свою участь у транзакції, перерахувавши готівку на *postro*-рахунок банку; у справі №5 описано поділ платежу на 13 частин через офшорні рахунки карибської галереї мистецтва; у справі №12 — аналіз ризику обігу коштів, які могли бути пов'язані з поваленим режимом у Сирії.

Окрему увагу у звіті приділено секторам, які традиційно вважаються вразливими до відмивання коштів, однак у наведених прикладах розкривається їх новітнє, нестандартне або ускладнене використання:

- у справі №11 показано, як адвокатський рахунок використовується для посередництва в угоді купівлі розкішного авто, а фактичний власник і структура транзакції залишаються непрозорими через посилання на адвокатську таємницю;



² <https://www.bj.admin.ch/dam/fedpol/en/data/kriminalitaet/geldwaescherei/mros-typologiebericht-2025-e.pdf.download.pdf/mros-typologiebericht-2025-e.pdf>

- справа №19 демонструє нетипову ситуацію для аптечного ритейлу: клієнт вносить понад 100 000 CHF готівкою за фармацевтичну продукцію через посередника, уникаючи прямої ідентифікації — така схема потенційно використовується для прикриття джерел

Висновки:

- **Фінансові посередники зобов'язані реагувати на найменші ознаки невідповідності між KYC-профілем та фінансовими операціями**, навіть у випадках, коли формально відсутнє підтвердження конкретного злочину. Незрозумілі або маскувальні схеми (через трасти, субрахунки, адвокатські рахунки) мають одразу викликати підозру.
- **Використання криптовалют та віртуальних IBAN створює реальні можливості для обходу фінансового контролю**, що вимагає негайного реагування з боку CASP та банків шляхом аналізу хешів, гаманців, верифікації КБВ і застосування автоматичних тригерів блокування.
- **Сектор мистецтва, нерухомості, предметів розкоші та страхування життя й надалі становить підвищений ризик з точки зору ВК/ФТ**, особливо коли фінансові операції здійснюються через маловідомих оцінювачів, оформлюються у готівковій формі або супроводжуються сумнівними або необґрунтованими ринковими оцінками.
- **Усі фінансові установи мають формалізувати механізми реагування на червоні прапорці** — у тому числі на основі OSINT, перевірок у ЗМІ, публічних баз даних та постійного моніторингу клієнтських дій — з метою подальшого подання SAR/STR до MROS навіть без чітко ідентифікованого предикатного злочину.

походження готівки;

- у справі №16 описано складну багаторівневу схему, коли під прикриттям інвестування у твори мистецтва через довірчі компанії та трасти проводиться виведення готівки, а надані клієнтом документи містять розбіжності, непрозорі умови та ознаки введення в оману інвесторів;
- справи №18 і 20 ілюструють використання фальсифікованих ідентифікаційних документів (маніпульовані ID-картки, підроблені підписи) у спробах відкрити рахунки для здійснення шахрайських транзакцій — типова, але водночас складна для виявлення практика, коли злочинці маскують себе за викраденими або зміненими особистими даними.

Особлива увага приділяється віртуальним активам: у справах №8, 10, 17 MROS розкриває як через брокерів криптовалют, псевдо-гаманці та віртуальні IBAN клієнти намагались приховати незаконне походження активів або уникнути контролю. Водночас демонструється важливість оперативного блокування профілю,

збереження слідів транзакції (хешів, адрес), перевірки реального кінцевого отримувача та звітності до MROS згідно з AMLA.

Значущим є розгляд справи №13, у якій через закупівлі обладнання здійснювались операції з контрагентом, підозрюваним у торгівлі російським золотом. Звіт наголошує на необхідності врахування обмежень згідно санкційних норм при встановленні ділових відносин у сфері торгівлі товарами.

У справі №14 яскраво демонструється зв'язок нерухомості, офшорних компаній, PER із країн Перської затоки та швейцарських нотаріальних структур. MROS фіксує перекази понад 10 млн CHF через рахунок нотаріуса з відсутністю інформації про продавця, що підсилює підозри щодо відмивання активів, пов'язаних із корупційними практиками.

У кожному випадку відображається правове підґрунтя подання SAR або STR згідно зі статтями AMLA або Швейцарського кримінального кодексу (SCC), а також описується співпраця з іноземними фінансовими розвідками, включаючи обмін інформацією через FIU-to-FIU канали.

Глобальний спротив корупції: виклики, досягнення і стратегія Transparency International у 2024 році³



Річний звіт Transparency International за 2024 рік є стратегічним оглядом глобальних викликів у сфері протидії корупції, досягнень міжнародного антикорупційного руху та ключових напрямів діяльності самої організації. Документ окреслює зростання авторитарних тенденцій у світі, які дедалі більше ускладнюють боротьбу з корупцією, зменшують прозорість державного управління і звужують простір для громадянського суспільства. Центральним фокусом звіту є занепокоєння з приводу послаблення верховенства права в багатьох юрисдикціях, що створює системні перешкоди для ефективного розслідування корупційних злочинів і притягнення винних до відповідальності.

У документі підкреслюється важливість підтримки активістів, викривачів і журналістів-розслідувачів, які часто працюють під тиском або в умовах ризику для життя. Transparency International

наводить приклади конкретної підтримки цих груп у рамках національних осередків і через глобальні адвокаційні ініціативи. Значна увага приділена моніторингу Індексу сприйняття корупції (Corruption Perceptions Index – CPI), результати якого у 2024 році засвідчили негативну динаміку у понад двох третинах країн світу. Це слугує вагомим сигналом про погіршення інституційної спроможності держав у стримуванні корупції, а також про необхідність невідкладних реформ у судовій, правоохоронній та публічній сферах.

Організація у звіті також акцентує увагу на проблемах фінансової прозорості, зокрема щодо глобальних потоків капіталу, які часто використовуються для відмивання коштів, уникнення сплати податків та фінансування корупційних режимів. Вона надає приклади того, як офшорні схеми, а також складні корпоративні структури використовуються для маскування бенефіціарних власників та виведення активів з-під контролю юрисдикцій. Ті просуває впровадження обов'язкових відкритих реєстрів кінцевих бенефіціарних власників, посилення контролю за публічними закупівлями, а також вимагає більшої відповідальності від міжнародного банківського сектору у виявленні та запобіганні корупційним фінансовим потокам.

В аналітичній частині звіту організація робить акцент на тому, що глобальні виклики, такі як кліматична криза, пандемії, воєнні конфлікти та економічна нестабільність, використовуються корумпованими елітами для подальшого посилення свого

Висновки:

- **Необхідність посилення незалежності судових органів:** Для ефективного боротьби з корупцією країнам слід забезпечити незалежність суддів та захист їх від політичного тиску.
- **Підтримка громадянського суспільства:** Уряди та міжнародні організації повинні створювати сприятливі умови для діяльності НУО та журналістів, які займаються антикорупційною діяльністю.
- **Впровадження механізмів прозорості в державному секторі:** Рекомендується впроваджувати електронні системи закупівель, відкриті реєстри бенефіціарних власників та інші інструменти для підвищення прозорості.
- **Міжнародне співробітництво у боротьбі з корупцією:** Країни повинні активізувати співпрацю у сфері обміну інформацією, екстрадиції та спільних розслідувань для ефективно протидії транснаціональній корупції.

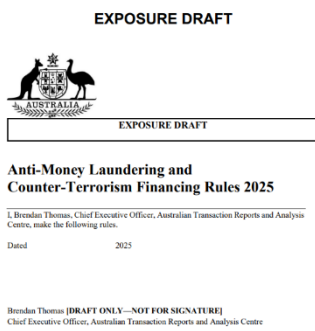
³ https://issuu.com/transparencyinternational/docs/transparency_international_annual_report_2024

впливу через зловживання бюджетними коштами, маніпуляції з гуманітарною допомогою або надзвичайними повноваженнями. На цьому тлі Transparency International виступає за посилення міжнародної співпраці у сфері антикорупційних розслідувань, екстрадиції, обміну інформацією про активи та розбудову більш стійких і підзвітних інституцій.

Окремий розділ звіту присвячено фінансовій звітності самої Transparency International, що демонструє її відданість стандартам підзвітності, ефективному управлінню донорськими коштами та прозорості у витрачанні ресурсів. У звіті відображено структуру фінансування, основні донорські програми, а також реалізовані проєкти у понад 100 країнах. Загалом, документ є не лише оглядом діяльності за рік, а й аналітичним дороговказом для урядів, міжнародних організацій та громадянського суспільства, спрямованим на актуалізацію порядку денного у сфері боротьби з корупцією на глобальному рівні.

Регулювання

Правила AUSTRAC з ПВК/ФТ 2025 ⁴



Документ є другим проєктом комплексного оновлення правил з ПВК/ФТ в Австралії. Його підготовлено Австралійським ПФР (AUSTRAC) відповідно до Закону про ПВК/ФТ 2006 року, з урахуванням зобов'язань Австралії в межах міжнародних стандартів FATF та потреб цифрової трансформації фінансового сектору. Цей документ не просто оновлює чинні правила — він формує нову архітектуру управління ризиками, нагляду та взаємодії між державою й підзвітними установами в епоху цифрових активів, складних фінансових продуктів і транскордонної фінансової взаємозалежності.

Один із центральних напрямів змін — перегляд структури Програми ПВК/ФТ, яку мають розробити, впровадити та підтримувати всі підзвітні організації. Програма має базуватися на системній оцінці ризиків і включати обов'язкові елементи: політики, процедури та системи з управління ризиками; постійне навчання персоналу; внутрішній контроль; і регулярну (не рідше одного разу на два роки) незалежну оцінку ефективності програми. У разі виявлення недоліків правила вимагають вжиття коригувальних заходів протягом 14 днів.

Окремий блок документа присвячено різним формам звітності, включаючи порогові транзакції, підозрілі операції (SMRs), міжнародні перекази, використання готівки, і щорічну звітність про дотримання вимог ПВК/ФТ (Compliance Reports). Зазначено, що подання річного звіту є обов'язковим і має супроводжуватися підписом уповноваженої особи. Для пов'язаних осіб (reporting group members) передбачено можливість централізованої подачі, якщо це дозволено угодою між ними.

У частині ідентифікації та перевірки клієнтів (KYC/CDD) документ встановлює гнучкий, але суворий підхід. Зокрема, вводиться можливість тимчасової відстрочки верифікації особи клієнта до моменту здійснення транзакції (наприклад, при відкритті рахунку), але виключно за умов наявності механізмів управління ризиками. Також передбачено посилені вимоги до виявлення та перевірки бенефіціарних власників, а також до ідентифікації політично значущих осіб (PEPs) — як місцевих, так і іноземних.

⁴ <https://www.austrac.gov.au/sites/default/files/2025-05/Second%20Exposure%20Draft%20AMLCTF%20Rules.pdf>

Особлива увага в документі приділена регулюванню постачальників послуг, пов'язаних із віртуальними активами (VASPs). Передбачено вимоги до обов'язкової реєстрації VASPs, подання структурованої інформації щодо організації, ключового персоналу, процедур ПВК/ФТ, заходів безпеки, перевірки доброчесності керівників. Також передбачається механізм анулювання реєстрації в разі недотримання вимог, зміни істотних обставин або недостовірності поданих відомостей. Окремо визначено вимоги до обігу стейблкоїнів, криптогаманців і транскордонних переказів віртуальних активів.

У розділі про перекази коштів (Funds Transfers) документ детально описує зобов'язання ініціаторів, посередників і отримувачів транзакцій. Зокрема, встановлено, що інформація про відправника та одержувача має супроводжувати кожну переказану суму незалежно від того, чи здійснюється транзакція через традиційний банківський канал, платіжну систему чи віртуальний актив. Якщо постачальник послуг не може передати супровідні дані, він має зберігати обґрунтування дій.

Упроваджено також правила для об'єднань підзвітних організацій (наприклад, банківських холдингів або фінансових груп), які можуть делегувати між собою виконання частини обов'язків, зокрема щодо навчання персоналу, звітності чи управління ризиками. Така система дозволяє уникнути дублювання ресурсів, водночас зберігаючи повну відповідальність кожного члена групи за відповідність вимогам.

Окремо деталізовано положення щодо "fit and proper person tests" — перевірок ділової репутації, відсутності судимостей, професійної компетентності комплаєнс-офіцерів та керівного персоналу. Для осіб, які в минулому були засуджені, але їхні вироки вважаються погашеними відповідно до законодавства, передбачено можливість не повідомляти про ці судимості під час проходження перевірки доброчесності. Водночас така можливість застосовується не автоматично: кожен випадок оцінюється індивідуально на підставі чітко визначених критеріїв — наприклад, характер правопорушення, час, що минув після вироку, і чи має особа ризик для системи ПВК/ФТ.

Значний наголос у документі зроблено на забезпеченні функціональної прозорості обов'язків і відповідальності між суб'єктами, які здійснюють спільну діяльність у межах однієї фінансової екосистеми. Так, у випадках, коли кілька підзвітних осіб одночасно беруть участь у виконанні транзакції (наприклад, платіжний посередник, банк, постачальник криптогаманця), правила чітко визначають, хто з них несе відповідальність за виконання вимог AML/CTF у частині верифікації особи клієнта, збереження записів, передавання супровідної інформації або подання звітності. Таке розмежування спрямоване на уникнення прогалин у контролі та забезпечення підзвітності кожного суб'єкта.

У частині ведення документації та зберігання записів новий проект правил уточнює часові рамки зберігання даних: мінімум п'ять років з дати завершення транзакції або припинення ділових відносин. Зазначено, що записи мають бути доступні в електронному вигляді та готові до надання AUSTRAC протягом чітко визначених термінів. Для суб'єктів, які використовують сторонні або хмарні системи зберігання, встановлено вимоги до доступності, захищеності та здатності миттєвого відновлення інформації.

Окрему увагу приділено механізмам запобігання "tipping off", тобто незаконного повідомлення клієнта про подання звіту про підозрілу діяльність. Передбачено спеціальні вимоги до підготовки персоналу, а також механізми внутрішнього документування ситуацій, коли таке розголошення могло мати місце. Установлено також вимоги до захисту даних клієнтів у контексті AML/CTF-звітності, включно з обмеженням доступу до відповідних інформаційних систем та забезпеченням аудитного сліду.

Суттєво оновлено вимоги щодо впровадження системи навчання персоналу, яка має бути адаптована до ризиків, характерних для конкретного бізнесу. Зокрема, працівники, які безпосередньо взаємодіють із клієнтами, повинні отримувати спеціалізоване навчання щонайменше раз на рік, а нові працівники — до початку виконання своїх функцій. Програми мають документуватись, оцінюватись на ефективність і оновлюватись відповідно до змін у законодавстві або ризик-профілі установи.

Документ також закріплює важливі новації щодо гнучкості системи управління ризиками, даючи змогу підзвітним установам, з одного боку, адаптувати політики до особливостей свого бізнесу, а з іншого — вимагати чіткої формалізації підходів до оцінювання та класифікації клієнтів, транзакцій, продуктів та каналів обслуговування. Уведено обов'язок періодичного перегляду ризикового профілю не лише клієнтів, а й самої установи — принаймні раз на два роки або раніше, якщо змінюються ринкові умови, продукти або юрисдикції обслуговування.

Висновки:

- **Впроваджено чіткі вимоги до реєстрації постачальників послуг з віртуальними активами (VASPs)** — зокрема щодо ризиків ВК/ФТ, належної перевірки персоналу, політик ПВК/ФТ та фінансової звітності, що посилить контроль над цифровими активами та попередить зловживання ними.
- **Визначено зобов'язання щодо регулярного перегляду оцінки ризиків та незалежної оцінки програм з ПВК/ФТ** — включаючи вимогу здійснювати коригування політик упродовж 14 днів після виявлення недоліків, що посилює гнучкість та актуальність системи внутрішнього контролю.
- **Посилено вимоги до звітності про підозрілі операції та порогові транзакції**, у тому числі в межах груп пов'язаних осіб, із уточненням ролей учасників групи, що дозволяє забезпечити централізовану відповідальність за звітність.
- **Закріплено вимоги до підготовки та оцінки фаховості комплаєнс-офіцерів** на підставі як професійної придатності, так і доброчесності, що сприяє підвищенню ефективності функцій нагляду та контролю в межах підзвітних установ.

Юридична класифікація DeFi у Швейцарії: нова законодавча рамка для розмежування децентралізованих і централізованих фінансових протоколів⁵

Циркуляр, підготовлений Робочою групою з цифрових активів Швейцарської федерації блокчейну (версія 1.0, березень 2025), пропонує системний підхід до правової кваліфікації DeFi-протоколів та пов'язаних з ними активностей у межах швейцарського фінансового законодавства. У документі наголошено, що попри швидке зростання DeFi-сектору, значна частина правових аспектів залишається неврегульованою або неоднозначною, що створює правову невизначеність для учасників ринку. Водночас визначається потреба у створенні зрозумілих правових критеріїв для розмежування між справжніми децентралізованими протоколами та централізованими структурами, які лише використовують блокчейн-технології.

Циркуляр починається з окреслення поняття DeFi як надання фінансових послуг через публічні блокчейни і смарт-контракти без участі централізованих операторів. Зазначено, що термін «децентралізація» використовується не завжди коректно, і велика кількість так званих DeFi-



⁵ https://blockchainfederation.ch/wp-content/uploads/2025/05/20250318-SBF-Circular-DeFi-final_EN.pdf

проєктів є де-факто централізованими (on-chain CeFi). У цьому контексті основна мета документа полягає в розробці правової рамки, яка дозволяє визначити, чи підпадає конкретний протокол або активність під сферу дії швейцарського фінансового ринку. Документ послідовно розвиває підхід у кілька етапів. Насамперед він опирається на технічну модель, запропоновану дослідниками Schuler, Cloots і Schär, яка враховує три рівні оцінки децентралізації: рівень блокчейну, рівень смарт-контрактів та рівень користувацького інтерфейсу. На кожному з рівнів вивчаються вектори централізації — ознаки, що вказують на можливість контролю або впливу з боку конкретної особи чи групи.

Окремий акцент зроблено на розмежуванні між технічною і юридичною децентралізацією. Технічна децентралізація пов'язана із захищеністю інфраструктури від централізованого втручання, тоді як юридична — з наявністю суб'єкта або групи, що фактично здійснює контроль і може бути ідентифікована як оператор. Юридично значущим є не лише факт централізації як такий, а здатність особи здійснювати вирішальний вплив на функціонування протоколу, наприклад через адмін-ключі, адміністрування токенами управління або вплив на зовнішні залежності (наприклад, оракули чи обіцянки підтримки вартості стейблкоїна).

Для визначення, чи існує персональна точка прив'язки, автори використовують також концепцію «регуляторної групи» з практики швейцарського права — ситуацій, коли низка

Висновки:

- **Законодавча рамка дозволяє точно ідентифікувати операторів DeFi-протоколів для цілей регулювання:** якщо особа або група має контроль над критичними функціями (смарт-контракти, оракули, токени), вони підпадають під фінансове регулювання (напр., ПВК/ФТ або ліцензування).
- **Справжні DeFi-протоколи не підпадають під фінансове законодавство Швейцарії,** якщо немає контролюючого оператора. Це відкриває можливості для інновацій, але вимагає від проєктів прозорості у структурі управління.
- **Псевдо-децентралізовані проєкти (on-chain CeFi) повинні готуватись до правових наслідків,** оскільки юридична відповідальність може бути встановлена навіть за наявності формальної децентралізації, якщо зберігається реальний контроль.
- **Звичайна діяльність (написання коду, надання оракула, інтерфейсу або ліцензії) не є підставою для регуляторного статусу оператора,** однак за певних умов може набувати такого значення, якщо супроводжується фактичним контролем або генерацією доходу у межах фінансової діяльності.

суб'єктів організовують діяльність так, аби уникнути регуляції індивідуально, але при колективному розгляді мають економічний або організаційний зв'язок, що дозволяє їх кваліфікувати як єдину регульовану групу. Це дозволяє врахувати сценарії, коли формально розпорошена структура все одно зберігає централізовану логіку управління.

У документі також детально описано супутні активності, які можуть бути пов'язані з DeFi, але самі по собі не є його «операцією» в юридичному сенсі. Серед таких активностей — розробка та публікація коду, розгортання протоколу, участь в управлінні, робота оракулів, підтримка інтерфейсів, ліцензування програмного забезпечення, маркетинг, а також

участь у валідації блокчейнів. Окремо наголошується, що надання інтерфейсів, навіть платних, не вважається автоматично ознакою контролю над протоколом, якщо сам протокол функціонує незалежно і без можливості втручання з боку розробника інтерфейсу.

У висновках циркуляру зафіксовано консенсус серед швейцарського регулятора FINMA, законодавчих і наукових кіл щодо того, що справжні децентралізовані протоколи не підпадають під чинне фінансове законодавство, а on-chain CeFi структури — підпадають. У відповідь на потребу правової визначеності для учасників ринку автори пропонують практичну і гнучку

законодавчу рамку для оцінки DeFi-протоколів на основі конкретних векторів централізації і юридичної прив'язки до суб'єктів, які можуть нести відповідальність відповідно до принципів «однакові ризики — однакові правила». Таким чином, документ є не лише аналітичним оглядом, а й прикладом методологічного підходу до регулювання DeFi.

Санкції

Санкції Міністерства фінансів США за контрабанду палива ⁶



Пресреліз, опублікований Міністерством фінансів США 1 травня 2025 року, описує санкційні заходи Управління з контролю за іноземними активами (OFAC) проти трьох мексиканських громадян та двох

мексиканських компаній, пов'язаних із наркокартелем Халіско Нуева Хенерасьйон (CJNG), який також визнаний у США як іноземна терористична організація.

Ці суб'єкти залучені до мережі, що займається торгівлею фентанілом, крадіжками палива та контрабандою сирої нафти через південно-західний кордон США, генеруючи сотні мільйонів доларів щорічного прибутку для CJNG. Документ підкреслює, що крадіжка палива, зокрема сирої нафти (відомої в Мексиці як "гуачиколь"), стала основним джерелом доходу (окрім наркоторгівлі) для мексиканських картелів, що призводить до мільярдних втрат для мексиканського уряду через крадіжки з державних нафтових компаній, таких як Pemex.

Злочинна мережа використовує різноманітні методи, включаючи підкуп працівників Pemex, незаконне буріння нафтопроводів, викрадення бензовозів та погрози працівникам. Викрадену нафту переправляють до США, часто маркуючи як "відпрацьовану олію" для ухилення від податків і регуляцій, після чого продають за зниженими цінами на американському та глобальному ринках, повертаючи прибутки картелям.

Санкції спрямовані проти Сезара Морфіна (відомого як Пріміто), лідера осередку CJNG у штаті Тамауліпас, який раніше очолював фракцію картелю дель Гольфо, а також його братів Альваро Ное та Реміхіо Морфіна, які беруть участь у торгівлі наркотиками та крадіжках нафти. Крім того, OFAC запровадив санкції проти двох компаній — SLA Servicios Logísticos Ambientales та Grupo Jala Logística, — які контролюються Пріміто та використовуються для продажу викраденого палива.

Документ також зазначає, що CJNG відповідає за значну частку фентанілу, що потрапляє до США, та імпортує прекурсори для наркотиків із Китаю. Фінансова мережа з протидії фінансовим злочинам (FinCEN) видала попередження, яке описує типології та ознаки схем контрабанди сирої нафти, пов'язаних із CJNG та іншими транснаціональними злочинними організаціями.

Ця все є частиною ширшої стратегії Міністерства фінансів США, спрямованої на ліквідацію картелів, включаючи попередні санкції проти CJNG та інших організацій, таких як картель Сіналоа та Ла Нуева Фамілія Мічоакана. Санкції блокують активи зазначених осіб і компаній у США, забороняють транзакції з американськими особами та передбачають ризик вторинних санкцій для іноземних фінансових установ, які співпрацюють із підсанкційними суб'єктами. Міністерство підкреслює координацію між OFAC, FinCEN, правоохоронними органами США (DEA, HSI, FBI, CBP) та мексиканським урядом, зокрема фінансовою розвідкою Мексики (UIF), для боротьби з фінансовими потоками картелів.

⁶<https://home.treasury.gov/news/press-releases/sb0125>

Звіти окремих інституцій та експертів

Новий пакет ЄС з ПВК: що змінюється та чому це важливо ⁷



Стаття Анни Стиліану, опублікована на платформі AML Cube, надає стислий, але змістовний огляд ключових елементів нового пакета ЄС з протидії відмиванню коштів, який набув чинності у 2024 році та передбачає значні зміни в регуляторному ландшафті Європейського Союзу.

Основною метою цього пакета є уніфікація та централізація підходів до боротьби з відмиванням коштів і фінансуванням тероризму шляхом запровадження єдиного нормативного

акту, створення нової наглядової структури та посилення вимог до суб'єктів фінансового моніторингу.

Ключовим компонентом є Регламент про ПВК (AMLR), який встановлює єдині правила для всіх держав-членів ЄС, включаючи вимоги до ідентифікації клієнтів, виявлення політично значущих осіб (PEPs), розкриття бенефіціарної власності, внутрішнього контролю та звітності. Важливою зміною є зниження порогу для застосування процедур належної перевірки клієнтів до транзакцій від €10,000 (раніше €15,000) та заборона готівкових операцій, що перевищують €10,000. Також введено обов'язкову ідентифікацію для транзакцій у діапазоні від €3,000 до €10,000.

Шоста Директива про ПВК зосереджується на структурі нагляду та забезпеченні виконання вимог, вимагаючи чіткого розмежування функцій між пруденційним та ПВК-наглядом у державах-членах. Вона також посилює повноваження підрозділів фінансової розвідки (ПФР), надаючи їм інструменти для призупинення транзакцій, моніторингу та накладення адміністративних санкцій. Крім того, директива передбачає створення централізованих реєстрів бенефіціарної власності, банківських рахунків та інформації про нерухомість, доступних для наглядових органів, суб'єктів фінансового моніторингу та представників громадянського суспільства з легітимним інтересом.

Створення нового центрального органу — Європейського органу з питань ПВК (AMLA) — є ще одним важливим кроком у цьому пакеті. AMLA матиме повноваження здійснювати прямий нагляд за високоризиковими суб'єктами, особливо тими, що ведуть діяльність у кількох

Висновки:

- Введення єдиного регламенту AMLR забезпечує пряме застосування правил з ПВК у всіх державах-членах ЄС, усуваючи необхідність національної імплементації та зменшуючи регуляторні розбіжності.
- Розширення кола суб'єктів фінансового моніторингу включає нові сектори, такі як платформи краудфандингу, оператори інвестиційної міграції, посередники іпотечного кредитування та футбольні клуби/агенти, що вимагає від них впровадження відповідних ПВК-процедур.
- Створення AMLA як центрального наглядового органу з прямими повноваженнями над високоризиковими суб'єктами покликане забезпечити узгоджене та ефективне застосування ПВК-правил на рівні ЄС.
- Посилення вимог до прозорості бенефіціарної власності та створення централізованих реєстрів сприятиме кращому виявленню та запобіганню схем відмивання коштів.

⁷ <https://www.amlcube.com/post/the-eu-s-new-aml-package-what-s-changing-and-why-it-matters>

державо-членах, а також координуватиме дії національних наглядових органів, забезпечуючи узгодженість та ефективність у боротьбі з відмиванням коштів на рівні ЄС.

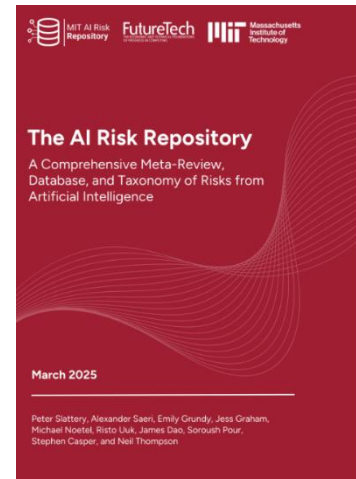
Ці реформи мають на меті усунути фрагментацію та неоднорідність у застосуванні ПВК-правил у різних країнах ЄС, забезпечити більшу прозорість та посилити ефективність заходів з протидії фінансовим злочинам. Для суб'єктів фінансового моніторингу це означає необхідність перегляду та оновлення своїх політик і процедур, впровадження нових механізмів внутрішнього контролю та забезпечення відповідності новим вимогам.

AI Risk Repository: нова основа для системного регулювання ризиків штучного інтелекту⁸

Документ представляє собою найповніше на сьогодні системне дослідження ризиків, пов'язаних з використанням штучного інтелекту (AI), яке поєднує систематичний огляд літератури, базу даних реальних і теоретичних загроз, а також нову двокомпонентну таксономію ризиків. Головна мета проекту — створити спільну і загальнодоступну рамку для ідентифікації, класифікації та моніторингу потенційних та фактичних загроз, які AI може спричинити для людини, суспільства, економіки, довкілля і безпеки.

Відправною точкою дослідження стала проблема фрагментації попередніх підходів до класифікації ризиків, які або дублювалися,

або



Висновки:

- **Необхідність уніфікації термінології та підходів до ризиків AI:** Відсутність єдиного понятійного апарату суттєво ускладнює міждисциплінарне регулювання та оцінку ризиків. AI Risk Repository усуває цю прогалину через єдину каузальну і доменну структуру.
- **Переважають ризики після розгортання систем AI, що виникають ненавмисно:** 62% ризиків виникають на етапі після розгортання, 35% — як ненавмисні. Це вимагає посилення контролю за поведінкою AI у реальних умовах, зокрема через аудит та етичну оцінку.
- **Недостатнє охоплення окремих доменів (екологія, права AI, мультиагентні ризики):** Наприклад, менше 1% ризиків стосується прав потенційно розумних систем AI або екологічної шкоди, що свідчить про прогалини у дослідженнях і практиці.
- **Практична цінність для політики, аудиторів, дослідників і компаній:** Repository уже застосовується для формування регуляторних рамок, аудиту моделей, розробки стандартів та виявлення прогалин у дослідженнях. Може слугувати основою для побудови української моделі оцінки ризиків AI.

суттєво відрізнялися в термінології, сфері охоплення, точності визначень і методології, що призводило до плутанини, неповноти аналізу та неможливості створення узгоджених стандартів для управління ризиками. Автори реалізували методологію «синтезу на основі найвідповіднішої рамкової моделі», тобто об'єднання найвідповідніших існуючих класифікаційних підходів з подальшим їх емпіричним доповненням і адаптацією на основі аналізу 65 першоджерел (наукових статей, звітів тощо), в результаті чого було виділено 1612 унікальних ризиків, кожен з яких класифіковано згідно з двома таксономіями.

Перша — каузальна — описує походження ризику через три

⁸ <https://arxiv.org/pdf/2408.12622>

параметри: джерело (людина, AI, інше), намір (навмисний, ненавмисний, невизначений) і час виникнення (до або після розгортання AI). Друга — доменна — включає сім доменів ризику та 24 піддомени, які деталізують сфери впливу: дискримінація й токсичність; конфіденційність і кібербезпека; дезінформація; зловживання і шкода від злочинного використання AI; взаємодія людини з AI; соціально-економічні та екологічні ризики; технічна несправність і етичні дилеми, пов'язані із самими системами AI. Згідно з аналізом, найбільше ризиків стосуються сфери безпеки і функціональних обмежень AI, а також соціально-економічного впливу, дискримінаційних ефектів і токсичного контенту. Натомість ризики, пов'язані з правами «розумного AI», екологічним навантаженням та інформаційною екосистемою, є суттєво недооціненими в академічному і практичному полі. Статистичний аналіз також виявив, що основна маса ризиків (62%) реалізується після розгортання AI, причому в майже рівній пропорції як результат навмисних дій (34%), так і ненавмисних збоїв чи прорахунків (35%).

Значна частина проблем також виникає внаслідок того, що відповідальність часто розмивається між людьми й системами. Автори не лише описують структуру бази даних і дві таксономії, а й надають рекомендації для різних цільових аудиторій: для політиків — як використовувати репозиторій для формування регуляторної політики і стандартів; для аудиторів — як застосовувати таксономії для розробки аудитних процедур; для дослідників — як виявляти «білі плями» у поточному знанні і вибудовувати подальші напрямки наукового аналізу.

База даних оновлюється постійно й доступна онлайн, дозволяючи здійснювати фільтрацію ризиків за каузальними та доменними параметрами. Таким чином, запропонований підхід закладає фундамент для міждисциплінарного, прозорого та порівнюваного аналізу ризиків AI, що особливо актуально в умовах стрімкого розвитку технологій і дефіциту узгоджених норм у сфері AI -регулювання.

Глобальні тренди боротьби з фінансовими злочинами у 2024–2025 роках: санкції, цифрові ризики та нові виклики комплаєнсу⁹



Звіт від компанії Sanction Scanner є масштабним аналітичним документом, який відображає глобальні трансформації у сфері боротьби з фінансовими злочинами, а також динаміку нормативних змін у ключових юрисдикціях світу. Звіт охоплює геополітичні, регуляторні, технологічні й секторальні фактори, що формують сучасний ландшафт протидії відмиванню коштів, фінансуванню тероризму та іншим видам фінансових зловживань, і є джерелом стратегічних орієнтирів для фінансових установ, регуляторів та аналітиків у сфері ПВК/ФТ.

Звіт починається з аналізу обсягів нелегальних фінансових потоків у 2023 році: понад 3,1 трлн доларів США пройшли через глобальну фінансову систему у вигляді незаконних коштів. З цієї суми 782,9 млрд припадали на наркотрафік, 346,7 млрд — на торгівлю людьми, а 11,5 млрд були використані на фінансування тероризму. Ці цифри

демонструють не лише масштаби проблеми, але й пряму загрозу для фінансової стабільності держав. Геополітичні конфлікти, зокрема на Близькому Сході, а також посилення тиску на гуманітарні канали в умовах конфлікту, ускладнюють моніторинг і потребують гнучких регіонально орієнтованих підходів. У цьому контексті особливу увагу приділено складності

⁹ <https://www.sanctionsanner.com/content/report/2023-2024-financial-crime-and-compliance-report.pdf>

імплементції санкцій — за результатами опитування, саме «складність санкцій» назвали головним викликом 2024 року 38% комплаєнс-офіцерів.

На прикладі США розглядаються структурні та законодавчі нововведення, спрямовані на підвищення прозорості та протидію фінансовим злочинам. Ухвалення Закону про корпоративну прозорість (Corporate Transparency Act, CTA), який набрав чинності 1 січня 2024 року, знаменувало обов'язкове розкриття інформації про кінцевих бенефіціарів для понад 32 млн компаній. Крім цього, у США посилено вимоги до інвестрадників, які відтепер зобов'язані впроваджувати повноцінні програми ПБК/ФТ, а також вжито заходів з регулювання криптовалют через ухвалення закону FIT21 та публікацію першої національної оцінки ризиків DeFi-платформ. Регулятори, такі як FinCEN і FINRA, активізували контроль за ринком цифрових активів, зокрема у відповідь на резонансне падіння біржі FTX і засудження її экс-СЕО Сема Бенкмана-Фріда.

Велика Британія також зробила серйозні кроки в напрямі модернізації антикорупційної політики — запроваджено Economic Crime Plan 2 з бюджетом £400 млн, а також новий Закон про економічні злочини та корпоративну прозорість (ECCTA), який зобов'язує верифікацію КБВ, розширює повноваження Companies House, запроваджує санкції за невиявлення шахрайства компаніями, і вперше вводить механізми вилучення криптовалютних активів, отриманих злочинним шляхом. Поряд із цим UK Gambling Commission та FCA продовжують активно штрафувати порушників ПБК-регулювання та посилювати обмеження для криптобізнесу. У 2024 році понад 88% заявок на реєстрацію криптофірм були відхилені через недостатність заходів контролю. Крім того, у Великій Британії оновлено підходи до визначення PER, зменшено регуляторний тиск на внутрішніх PER, а також гармонізовано список високоризикових третіх країн відповідно до стандартів FATF.

У Європейському Союзі ключовими змінами стали імплементція шостої Директиви з ПБК (6AMLD), створення єдиного гармонізованого набору обов'язкових правил, стандартів і процедур для всієї зони, запуск Європейського AMLA до 2029 року та посилення регулювання CASPs у межах регламенту MiCA. 6AMLD розширює визначення ВК, гармонізує санкції за порушення, зобов'язує до обов'язкового навчання працівників, вимагає чіткої ідентифікації КБВ і посилює обмін інформацією між країнами ЄС. ЄС також впроваджує регламенти щодо штучного інтелекту (AI Act) та цифрової ідентичності (eID), які мають інтегрувати цифрові інструменти у ПБК-системи. Проте частина країн, зокрема Франція, Ірландія та Латвія, отримали зауваження за неповну імплементцію попередніх директив.

Серед країн Близького Сходу та Африки детально розглядається приклад ОАЕ, які вийшли з «сірого списку» FATF завдяки реформам, спрямованим на посилення

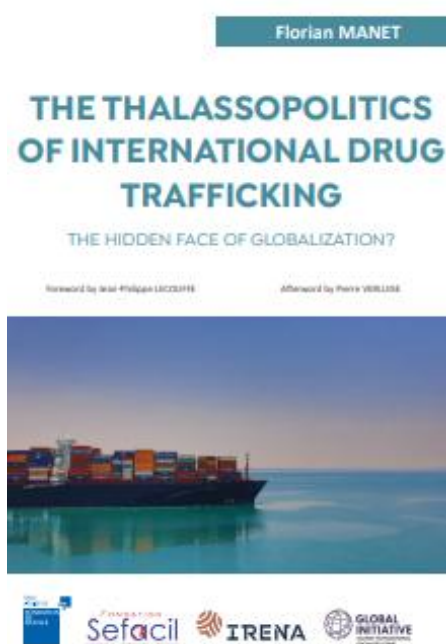
Висновки:

- **Регуляторний тиск і цифрова прозорість зростають:** впровадження обов'язкової звітності щодо КБВ (США, ЄС, Велика Британія) та ПБК-програм для інвестрадників і CASPs свідчить про посилення глобального нагляду за ризик-секторами.
- **DeFi і криптовалюти – головні виклики на 2025 рік:** на тлі стрімкого зростання використання криптоактивів, країни переходять від фрагментарного регулювання до комплексних підходів – MiCA в ЄС, FIT21 та DeFi Risk Assessment в США.
- **Санкції та геополітична турбулентність диктують нові ризики:** ситуації на Близькому Сході, у Східній Європі та Африці ускладнюють моніторинг транзакцій і вимагають адаптивних, регіонально чутливих підходів до ПБК/ФТ.
- **Потреба у спільних стандартах та міждержавній координації:** створення AMLA, перегляд 6AMLD, гармонізація визначень КБВ і підходів до ризиків — це ключ до ефективної глобальної відповіді на ВК/ФТ.

регуляторної бази, впровадження нових стандартів бухгалтерського обліку, цифрову верифікацію транзакцій і створення стабільного середовища для контролю криптовалют. Туреччина також вийшла з «сірого списку» завдяки ухваленню закону про ліцензування криптопослуг. У контрасті, Іран залишається під глобальними санкціями, особливо в енергетичному секторі, у зв'язку з його політикою та регіональною дестабілізацією. В Африці ключовими загрозами залишаються торгівля людьми, незаконний видобуток корисних копалин, торгівля дикою природою та тероризм, що призводять до щорічних втрат у \$60 млрд. Поряд із цим наводяться позитивні приклади зусиль ПАР і Нігерії щодо розбудови спроможностей у боротьбі з фінансовими злочинами, зокрема в частині цифрового шахрайства та природоохоронних злочинів.

Звіт завершується стратегічною картою дій на 2025 рік, де рекомендується поглиблення міжнародної координації, впровадження цифрових платформ обміну інформацією, розширення регуляторних зон відповідальності на крипторинки і посилення контролю за новими технологіями, включно з DeFi і штучним інтелектом. Автори підкреслюють, що майбутнє боротьби з фінансовими злочинами лежить на перетині регуляторної чіткості, технологічної адаптивності та міжнародного співробітництва.

Політика міжнародного наркотрафіку: розкриття прихованого обличчя глобалізації¹⁰



Книга Флоріана Мане є комплексним дослідженням, яке розглядає міжнародний наркотрафік через призму «таласополітики» — новаторського підходу, що об'єднує геополітику, кримінологію, право та логістику морських і портових операцій. Автор, спираючись на свій багаторічний досвід старшого офіцера французької жандармерії та керівника Національної служби розслідувань морської жандармерії, а також як міжнародний експерт з морських ризиків, аналізує, як море стало центральним каналом для транспортування наркотиків від зон виробництва до ринків споживання. Мане розкриває, як кримінальні організації використовують переваги глобалізації — вільний рух товарів, даних і людей — для створення складної, ефективної та прихованої логістичної системи, що пронизує глобальні торговельні мережі. Книга підкреслює не лише кримінальну природу наркотрафіку, але й його глибокий вплив на геополітичну стабільність, економіку та суспільний порядок, пропонуючи міждисциплінарний підхід до розуміння та протидії цьому явищу.

Книга розпочинається з передмови Жан-Філіпа Лекуффа, заступника виконавчого директора з операцій Європолу, який підкреслює, що боротьба з наркотрафіком залишається пріоритетом для європейських правоохоронних органів. Лекуфф зазначає, що розкриття зашифрованих комунікаційних мереж, таких як ENCROCHAT і SKY ECC, дозволило отримати ключову інформацію про масштаби та глобальну природу наркотрафіку, зокрема про важливість морського вектора. Післямова П'єра Верлюїза, засновника DIPLOWEB.COM, акцентує на геополітичних наслідках наркотрафіку, підкреслюючи, як він послаблює держави, сприяє корупції та дестабілізує

¹⁰ https://globalinitiative.net/wp-content/uploads/2025/04/Florian-Manet-The-thalassopolitics-of-international-drug-trafficking.-The-hidden-face-of-globalization_.pdf

міжнародні відносини. Верлюїз закликає до стратегічних і структурних рішень, особливо для Франції як другої за величиною морської держави, щоб протистояти цій загрозі.

У вступі, Мане ділиться особистими спостереженнями, спираючись на досвід розслідування гучної справи 2017 року, коли три французькі яхти, що перевозили дві тонни кокаїну з Панами до Австралії через Полінезію, були перехоплені французькою владою. Цей випадок ілюструє складність міжнародного наркотрафіку: від закупівлі та переобладнання суден до вербування екіпажів, співпраці з колумбійськими картелями та відмивання грошей. Автор вводить концепцію «таласополітики», яка розглядає море як ключовий простір для злочинної діяльності, що поєднує логістичну ефективність із можливістю приховати незаконні вантажі серед легальних потоків. Він наголошує, що наркотрафік є не лише кримінальною проблемою, але й викликом для держав, які змагаються з гнучкими та фінансово потужними кримінальними організаціями.

Перший розділ книги присвячений визначенню наркотрафіку як «матричного злочину», що породжує широкий спектр інших правопорушень, включаючи насильство, викрадення, корупцію, відмивання грошей і екологічні злочини. Мане пояснює, що наркотрафік — це міжнародна торгівля психотропними речовинами, яка охоплює вирощування сировини (кока, опій, коноплі), її обробку, транспортування та продаж. Він підкреслює складність оцінки масштабів цього явища через «темну цифру» — приховану природу злочинів, які не фіксуються через відсутність скарг від жертв, оскільки споживачі наркотиків добровільно беруть участь у процесі. Автор також аналізує зростання глобального ринку наркотиків, спричинене збільшенням попиту, вдосконаленням методів виробництва та розширенням культивацийних зон, зокрема в Колумбії, Перу та Болівії. Окрема увага приділяється морському транспорту як безпечному та економічно вигідному способу доставки великих обсягів наркотиків.

Другий розділ зосереджується на «маритимізації» наркотрафіку, тобто використанні моря як основного логістичного каналу. Мане описує, як злочинці використовують різні типи суден — від рибальських човнів і яхт до спеціально сконструйованих «підводних човнів» — для транспортування наркотиків. Він детально аналізує технологічні інновації, які підтримують цю діяльність, такі як підводні дрони, кібератаки на портову інфраструктуру та використання криптовалют для фінансових транзакцій. Автор також звертає увагу на методи зараження легальних вантажів, наприклад, приховування наркотиків у контейнерах із фруктами, та на виклики, пов'язані з відстеженням суден через зміну прапорів (flag shopping) і складність міжнародного морського права.

Третій розділ описує маршрути наркотрафіку, підкреслюючи роль Південної Америки (Колумбія, Перу, Болівія) як основного центру виробництва кокаїну та Західної Африки й європейських портів (Антверпен, Роттердам, Альхесірас) як перевалочних пунктів. Мане аналізує, як кримінальні мережі використовують порти як логістичні хаби, а також як корупція в портових структурах сприяє їхній діяльності. Він розглядає регіональні особливості, такі як роль Макронезії та Мозамбіцької протоки як гарячих точок для наркотрафіку, і підкреслює, що маршрути часто визначаються не лише географічними умовами, але й кримінальними мережами підтримки.

Четвертий розділ присвячений новим тенденціям у наркотрафіку, включаючи зростання торгівлі синтетичними наркотиками, такими як каптагон, і бартер між кокаїном і каннабісом між Африкою та Південною Америкою. Мане описує феномен «нафтового розливу» — розширення наркотрафіку в нові регіони, такі як Індійський океан. Автор наголошує на адаптивності кримінальних організацій до нових викликів і їхній здатності використовувати цифрові інструменти для оптимізації логістики.

П'ятий розділ вводить концепцію «кримінальної таласократії» — організованої злочинної системи, яка використовує море як стратегічний простір для досягнення своїх цілей. Мане

описує, як ці організації інфільтрують порти, корумпують посадовців і відмивають гроші через легальні сектори економіки, такі як нерухомість, ресторани та онлайн-ігри. Він аналізує історичні та сучасні приклади, такі як італійська мафія та албанські кримінальні групи, які стають дедалі впливовішими в Європі. Автор також розглядає вплив наркотрафіку на портові міста, де створюються сегреговані простори, але спільна доля змушує місцеві громади боротися з цією проблемою.

Шостий розділ досліджує роль портів, суден і контейнерів (TEU) у глобальній торгівлі та їхню уразливість до наркотрафіку. Мане підкреслює, що порти, такі як Танжер Мед, Альхесірас і Марсашлокк, є ключовими хабами, які використовуються як легальними, так і нелегальними операторами. Він аналізує логістичні стратегії, такі як «hub and spokes», і підкреслює важливість розуміння зв'язків між портами для оцінки кримінальних ризиків. Автор також звертає увагу на використання старих суден і другосортних флотів для незаконних перевезень, що ускладнює їх відстеження.

У висновках Мане наголошує, що наркотрафік є не лише кримінальною, але й геополітичною проблемою, яка дестабілізує держави, сприяє корупції та послаблює міжнародні відносини. Він пропонує низку практичних рекомендацій, включаючи створення регіональних центрів моніторингу, таких як МАОС-N, для Середземномор'я та Індійсько-Тихоокеанського регіону, посилення розвідки щодо логістичних потоків, створення спеціалізованого судового органу для морських злочинів і розвиток міждисциплінарного прогнозування для передбачення еволюції організованої злочинності. Автор закликає до інтеграції таласополітичного підходу в стратегії боротьби з наркотрафіком, підкреслюючи важливість морської перспективи для розуміння глобальних викликів безпеки.

Висновки:

- **Маритимізація економіки та злочинності:** Книга підкреслює, що море є основним каналом для 90% глобальних торговельних потоків, що робить його ідеальним для наркотрафіку. Злочинні організації використовують переваги глобалізації, такі як вільний рух товарів і даних, для створення складних логістичних мереж.
- **Технологічна адаптивність:** Злочинці активно використовують інновації, такі як підводні дрони, криптовалюти та кібератаки, що ускладнює виявлення та протидію їхнім операціям.
- **Геополітичні наслідки:** Наркотрафік не лише є кримінальною проблемою, але й впливає на стабільність держав, сприяючи корупції, послабленню інститутів і навіть появі «нарко-держав». Це створює загрозу для міжнародних відносин.
- **Порти як осередки ризику:** Порти є ключовими вузлами, де легальна та нелегальна діяльність переплітаються. Корупція в портових структурах і слабка безпека сприяють проникненню наркотрафіку в легальні логістичні ланцюги.
- **Міждисциплінарний підхід:** Автор пропонує поєднувати кримінологічні, геополітичні, правові та логістичні підходи для боротьби з наркотрафіком, наголошуючи на важливості міжнародної співпраці та обміну розвідданими.

Книга завершується бібліографією та таблицею ілюстрацій, які включають карти, графіки та статистичні дані про обсяги вилучених наркотиків, маршрути перевезень і вплив наркотрафіку на портові міста. Вона є цінним ресурсом для правоохоронців, дослідників і політиків, які прагнуть зрозуміти складність міжнародного наркотрафіку та розробити ефективні стратегії протидії.

Як забезпечити прозорість у земельному управлінні для боротьби з великомасштабною корупцією¹¹

Документ від Transparency International, є детальним аналізом проблеми великомасштабної корупції в земельному секторі та практичним керівництвом для її подолання через прозорість, співпрацю та використання спеціалізованих інструментів. Його мета – надати чіткий план дій для громадян, громадських організацій, урядів та інших зацікавлених сторін, для зменшення корупції, захисту права громад і збереження природних ресурсів.



Великомасштабна корупція в земельному управлінні, як зазначається, має руйнівний вплив не лише на економіку, а й на права людини, довкілля та соціальну справедливість. Вона процвітає через секретність, слабкий нагляд і правові прогалини, що дозволяють потужним гравцям незаконно привласнювати землю, витісняючи громади та сприяючи деградації екосистем. У таких країнах, як Бразилія, Камбоджа та Гана, корупційні схеми включають маніпуляції із земельними реєстрами, продаж судових рішень і обмежений доступ до інформації, що ускладнює громадський контроль. Наприклад, у Бразилії маніпуляції із земельними даними сприяють незаконній вирубці лісів Амазонії, що погіршує екологічну ситуацію та довіру до влади.

Для боротьби з цією проблемою документ пропонує комплексний підхід, який починається з розуміння того, що корупція залежить від браку прозорості та слабкого нагляду. Для ефективної протидії необхідні міцні правові рамки, незалежний нагляд і активне громадянське суспільство. Ключовим інструментом є Індекс стану земельної інформації (SOLI), розроблений Land Portal Foundation, який оцінює доступність і повноту земельних даних у країнах Африки та Латинської Америки за двома критеріями: повнотою (чи збираються дані про власність, використання, оцінку землі) та відкритістю (чи доступні ці дані безкоштовно онлайн у зручному форматі). Згідно з SOLI, у 70% із 42 досліджених країн спостерігається високий рівень корупції та низька прозорість земельних даних, що створює ідеальні умови для корупційних схем.

Документ наголошує, що часткова прозорість, коли публікуються лише деякі дані, є недостатньою, оскільки корупціонери можуть використовувати її для прикриття своїх дій. Для справжньої боротьби з корупцією потрібне повне розкриття інформації про власність землі (включаючи бенефіціарну власність), земельні транзакції, концесії, зонування, оцінку, записи про права корінних народів, жінок та інших вразливих груп, а також дані про лобіювання бізнесу, фінансування політичних партій і декларації активів. Рекомендується створювати сумісні, машинні бази даних, які будуть доступними для широкого загалу, замість громіздких технічних звітів на урядових сайтах.

Співпраця з такими платформами, як Land Portal Foundation, відіграє ключову роль у просуванні відкритих земельних даних через SOLI Index, відкриті набори даних, дослідження та інструменти для моніторингу. Документ закликає громадянське суспільство співпрацювати з такими організаціями для аудиту прозорості, створення публічних інформаційних панелей і участі в коаліціях за краще земельне управління. Особлива увага приділяється інклюзивності: земельні дані часто недоступні для вразливих груп, таких як сільські громади, корінні народи, жінки чи люди з обмеженими можливостями, через брак інтернету, неграмотність або складні формати.

¹¹ <https://www.transparency.org/en/blog/ensure-transparency-land-governance-counter-grand-corruption-practical-guide>

Для вирішення цього пропонується перекладати дані на місцеві мови, поширювати їх через офлайн-канали, як-от радіо, та створювати мобільні платформи для доступу до інформації.

Прозорість розглядається як стратегічний інструмент боротьби з корупцією, але вона ефективна

Висновки:

- **Використовуйте SOLI Index для виявлення прогалин у прозорості:** Громадяни та організації повинні застосовувати Індекс стану земельної інформації для оцінки доступності даних у своїй країні та вимагати від урядів публікації повних і відкритих земельних реєстрів, зокрема даних про власність, транзакції та права вразливих груп.
- **Вимагайте повної прозорості та сумісності даних:** Уряди повинні забезпечити читабельність баз даних про землю, включаючи інформацію про бенефіціарну власність, зонування та фінансування, щоб унеможливити приховані корупційні схеми.
- **Забезпечте інклюзивність земельних даних:** Для ефективної боротьби з корупцією дані про землю потрібно перекладати місцевими мовами, поширювати через офлайн-канали та адаптувати для мобільних платформ, щоб вони були доступні для вразливих груп, таких як сільські громади та корінні народи.
- **Співпрацюйте з платформами та беріть участь у глобальних ініціативах:** Партнерство з організаціями, як Land Portal Foundation, та участь у заходах, таких як Всесвітня земельна конференція 2025 року, допоможуть посилити тиск на уряди для впровадження реформ і підвищення прозорості в земельному управлінні.

лише в поєднанні з сильними законами, незалежними наглядовими органами, вільною пресою та активним громадянським суспільством. Уряди повинні закрити правові прогалини, чітко визначити ролі земельних агенцій, забезпечити їх ресурсами та залучити до прийняття рішень. Корупція в земельному секторі також має екологічні наслідки, сприяючи знищенню лісів і ускладнюючи боротьбу зі зміною клімату. У контексті урбанізації документ підкреслює, що корупція в міському плануванні погіршує нерівність і якість життя, тому потрібні спеціальні заходи для захисту міського земельного управління.

Заклучна частина документу закликає до активної участі в таких заходах, як Всесвітня земельна конференція Світового банку 2025 року, яка фокусується на безпеці земельних прав, кліматичних ініціативах і моніторингу прозорості. Боротьба з корупцією не потребує ідеальних умов –

достатньо використовувати наявні інструменти, як SOLI Index, і співпрацювати з організаціями, як Land Portal Foundation. Прозорість є потужною зброєю, яка може захистити землю, права громад і довкілля, якщо вона буде доступною та інклюзивною.

Рекомендовані матеріали та події

Оновлена конвергенція ЄС-США? ¹²

Третій епізод подкасту This Month in EU Sanctions став глибоким зануренням у трансформацію санкційної політики Європейського Союзу, зокрема в контексті подій квітня 2025 року. Починаючи з огляду останніх рішень щодо Ірану, Лівії, М'янми та Молдови, ведучий Ян Дунін-Васович фіксує ключову зміну в динаміці санкційної архітектури ЄС — поступову інституціоналізацію центральної ролі Європейської Комісії у розробці санкцій. Це, за словами запрошеного експерта Яна Лепо, знаменує собою нову еру, в якій санкції більше не є лише

¹² https://www.youtube.com/watch?v=DtqLELooDW8&t=182s&ab_channel=ThisMonthinEUSanctions

інструментом зовнішньої політики, а трансформуються у важіль захисту безпекових інтересів ЄС.



У центрі уваги обговорення — історичний розвиток санкційної політики ЄС. Ретроспектива, яка охоплює перші санкції проти Ірану 1980 року, висвітлює, наскільки складними були внутрішньоєвропейські дебати щодо автономних санкцій поза рамками ООН. У ті часи багато держав-членів вважали односторонні обмеження контрпродуктивними, а Комісія ще не відігравала провідної ролі. Розрив між зовнішньополітичним (міжурядовим) та

економічним (наднаціональним) вимірами ЄС призвів до інституційних суперечок про те, хто саме має право ініціювати та впроваджувати санкції. Саме приклад збройного конфлікту в Аргентині у 1982 році започаткував модель подвійного акту — рішення Ради як політичний крок та регламент як правовий інструмент для імплементації, що й стало основою сучасної санкційної практики ЄС.

Цей випуск також зосереджується на зміні балансу влади між державами-членами та інституціями ЄС у санкційній процедурі після 2022 року. З початком повномасштабного вторгнення Росії в Україну роль Європейської Комісії в підготовці санкційних пакетів зростає кардинально. Перші три пакети, прийняті до і відразу після вторгнення, були розроблені практично повністю в Комісії — без звичного кола погоджень з державами-членами. Такий підхід був продиктований потребою в секретності та оперативності. Це призвело до появи так званих "конфесійних процедур", коли замість багатосторонніх обговорень держави-члени окремо або в малих групах зустрічалися з представниками Комісії для висловлення "червоних ліній", але без повного доступу до текстів.

На тлі загальної еволюції санкцій, Лепо акцентує увагу на розширенні санкційної методології від точкових обмежень до секторальних заходів, що зачіпають функціонування єдиного ринку ЄС. Це породжує нові виклики, зокрема у сфері впровадження та контролю. ЄС, який раніше покладався на домінування США в реалізації санкцій, наразі зіткнувся з перспективою, коли Вашингтон може змінити курс щодо Росії, а ЄС — залишитися на жорсткіших позиціях. Вперше саме ЄС може виявитися стороною, яка чинить більший тиск у збереженні санкцій, що створює нову парадигму трансатлантичної динаміки.

Важливим лейтмотивом дискусії є концепція стратегічної автономії ЄС: чи зможе Союз розвинути незалежну спроможність не лише готувати та приймати санкції, а й забезпечувати їх ефективне впровадження без залежності від США? Цей процес неминуче супроводжуватиметься дебатами про скасування вимоги одностайності у санкційній політиці, створення спільного санкційного органу впровадження, а також переглядом ролі національних урядів у цьому процесі.

Зрештою, подкаст наголошує, що санкції ЄС уже давно вийшли за межі інструменту "реакції на порушення", ставши наріжним каменем європейської геополітики, засобом проєкції норм, цінностей та безпекових пріоритетів. У нових умовах ЄС дедалі частіше використовує не лише тематичні санкційні режими, як-от глобальний режим щодо прав людини, а й цілісні обмежувальні пакети, спрямовані на виснаження військово-промислового потенціалу держав-противників, як це відбувається у випадку з Росією.

Основоположні принципи Директиви 2015/849¹³

Аудіофайл, який ліг в основу цього аналітичного допису, є детальним, доступним і структурованим поясненням 4-ї Директиви ЄС 2015/849 (AMLD IV) про запобігання використанню фінансової системи Євросоюзу для цілей відмивання коштів і фінансування тероризму. Це практичний аудіогід у форматі діалогу, який знайомить слухача з основами директиви, її логікою, ключовими вимогами та інституційною структурою. Особливою цінністю аудіоматеріалу є його освітній підхід — пояснення не лише юридичних вимог, але й мотивації, чому ці норми були запроваджені.



Першим питанням, яке підіймається в аудіофайлі, є коло суб'єктів, яких охоплює AMLD IV. Автори пояснюють, що директива застосовується не лише до банків та фінансових установ, а й до нотаріусів, податкових консультантів, агентів з нерухомості, бухгалтерів, а також постачальників послуг, пов'язаних з віртуальними активами — категорію, яка на час прийняття AMLD IV лише починала формуватися. І вже пізніше, у Директиві AMLD V (2018/843) було прямо визначено обов'язковість включення криптовалютних бірж і кастодіальних гаманців до переліку зобов'язаних суб'єктів.

Першим питанням, яке підіймається в аудіофайлі, є коло суб'єктів, яких охоплює AMLD IV. Автори пояснюють, що директива застосовується не лише до банків та фінансових установ, а й до нотаріусів, податкових консультантів, агентів з нерухомості, бухгалтерів, а також постачальників послуг, пов'язаних з віртуальними активами — категорію, яка на час прийняття AMLD IV лише починала формуватися. І вже пізніше, у Директиві AMLD V (2018/843) було прямо визначено обов'язковість включення криптовалютних бірж і кастодіальних гаманців до переліку зобов'язаних суб'єктів.

В аудіофайлі значну частину займає пояснення ризик-орієнтованого підходу (РОП) — системи, за якої не встановлюються однакові вимоги для всіх суб'єктів, а заходи обираються залежно від оціненого ризику. Це означає, що кожна установа повинна розробити власну внутрішню модель оцінки ризиків — клієнтів, продуктів, географії, каналів доставки послуг. Важливо, що AMLD IV вимагала документування такої оцінки, її періодичного оновлення та надання на вимогу регулятору. Проте лише з ухваленням Регламенту з ПВК/ФТ 2024/1624 (AMLR) ці положення стали безпосередньо обов'язковими у всіх державах-членах. Регламент деталізує критерії застосування посиленних або спрощених перевірок і створює єдине поле вимог.

Змістовним блоком є розгляд концепції Customer Due Diligence (CDD) — процесу перевірки клієнта, який складається з чотирьох етапів: ідентифікація клієнта, встановлення бенефіціарного власника, розуміння мети ділових відносин і постійний моніторинг. Акцент робиться на понятті бенефіціарного власника як ключового чинника прозорості — фізичної особи, яка реально контролює юридичну особу. У AMLD IV запроваджено вимогу створення національних реєстрів бенефіціарних власників, проте лише у AMLD V було визначено, що частина інформації має бути доступною не лише для ПФР і банків, але й для громадськості — журналістів, громадських організацій, осіб з «легітимним інтересом».

Окрема частина присвячена Politically Exposed Persons (PEPs). Пояснюється, що ці особи — державні діячі, парламентарі, судді вищих судів, керівники держпідприємств — становлять підвищений ризик з точки зору корупції. У зв'язку з цим AMLD IV вимагає посиленних заходів: встановлення джерел коштів, постійний моніторинг, залучення керівництва при встановленні або продовженні ділових відносин. У AMLR ця вимога стала частиною єдиного наглядного підходу, а новий орган ЄС - AMLA - отримала мандат на розробку уніфікованої методології оцінки ризиків, включаючи роботу з PEPs.

Файл містить ґрунтовне пояснення ролі ПФР. Наголошується, що повідомлення про підозрілі транзакції має здійснюватися не після встановлення правопорушення, а в момент виникнення

¹³ https://drive.google.com/file/d/1PIBYVBldiig_MkJEeCorxuf8ONPGTyre/view?usp=drive_link

обґрунтованої підозри. Це основоположний принцип — проактивність, а не реактивність. Саме для підвищення ефективності ПФР було створено в 2024 році Європейську агенцію AMLA (Регламент 2024/1620) — яка координує та підтримує ПФР, забезпечує IT-інфраструктуру для безпечного обміну інформацією (FIU.net), розробляє стандарти, проводить спільний аналіз та сприяє гармонізації підходів.

Аудіофайл завершується роздумами про виклики, які постають перед регулюванням у зв'язку з цифровими технологіями, глобалізацією і появою нових інструментів. Постає питання, наскільки ефективним може бути регулювання, яке завжди йде позаду інновацій. Відповіддю стало ухвалення AMLD VI (2024/1640), яка розширює повноваження держав у частині визначення додаткових секторів ризику, охоплює ризики, пов'язані з іноземними структурами, та посилює вимоги до інституційного управління ризиками.

Ще один важливий блок, не присутній у самому аудіо, але логічно пов'язаний з положеннями AMLD IV, — це нова Директива щодо доступу до реєстрів банківських рахунків (2024/1654), яка встановлює транскордонний доступ до банківських реєстрів через систему BARIS. Це суттєво зміцнює оперативні можливості фінансової розвідки та слідчих органів у межах ЄС. Таким чином, підхід, запропонований у AMLD IV — тобто створення реєстрів — розвинуто до рівня їх повноцінної інтеграції в інфраструктуру безпеки ЄС.

Європейська система захисту викривачів: аналіз Директиви ЄС 2019/1937 та її імплементаційний потенціал ¹⁴

Даний матеріал — це пояснення у формі усного змісту Директиви Європейського Союзу 2019/1937 про захист викривачів. У простій і доступній манері викладаються ключові положення директиви, її мета, сфери застосування, коло осіб, які підпадають під захист, механізми повідомлення про порушення та гарантії захисту від репресій. Текст має популяризаторський характер і спрямований на покращення розуміння цього нормативного акту серед широкої аудиторії.



Директива Європейського Союзу 2019/1937 про захист осіб, які повідомляють про порушення права Союзу, становить фундаментальний нормативний акт у сфері забезпечення прозорості, підзвітності та верховенства права на рівні всіх держав-членів ЄС. Її ухвалення було зумовлено необхідністю усунути правовий вакуум і фрагментарність національних систем захисту викривачів, що в багатьох країнах ЄС залишалися нерозвиненими або неефективними. Основною метою директиви є створення

мінімальних і водночас обов'язкових стандартів захисту для осіб, які добросовісно повідомляють про порушення законодавства ЄС у пріоритетних сферах, що мають суспільну значущість. До таких сфер належать державні закупівлі, фінансові послуги, боротьба з відмиванням коштів та фінансуванням тероризму, безпека продукції і транспорту, охорона довкілля, ядерна безпека, безпека харчових продуктів, захист прав споживачів, персональних даних, кібербезпека, а також будь-які дії, що загрожують фінансовим інтересам Європейського Союзу або підривають правила функціонування внутрішнього ринку.

¹⁴ https://drive.google.com/file/d/123UNTcfQFlpXKpwePsr2dilcFZkq1yJN/view?usp=drive_link

Директива закріплює надзвичайно широке тлумачення поняття викривача — це не лише наймані працівники або держслужбовці, а й самозайняті особи, акціонери, члени наглядових та управлінських органів, постачальники, підрядники, волонтери, стажери (як оплачувані, так і ні), а також будь-які особи, які ще не вступили або вже припинили трудові чи ділові відносини. Під захист підпадають і посередники, які допомагають у повідомленні, а також родичі, колеги та інші треті особи, що можуть зазнати тиску через зв'язок із викривачем. Інноваційною особливістю директиви є її поширення на період до офіційного початку співпраці, наприклад, під час проходження співбесіди, і на час після її припинення, що фактично розширює поняття «професійний контекст».

Процедурна частина директиви передбачає три канали повідомлення про порушення: внутрішній, зовнішній і публічний. Внутрішній канал стосується звернення до структур або осіб усередині компанії або установи, причому юридичні особи приватного сектору з кількістю працівників від 50 осіб і всі державні установи зобов'язані створити безпечні й конфіденційні канали повідомлення. Обов'язковими є фіксація факту отримання повідомлення впродовж семи днів, неупереджене розслідування, а також надання відповіді протягом трьох місяців. Якщо такий механізм не працює або викривач має підстави вважати, що його використання є ризикованим, дозволяється звернення до уповноважених державних органів — зовнішній канал. Держави-члени ЄС зобов'язані визначити такі органи і забезпечити повноцінне функціонування відповідних процедур. У разі серйозної загрози публічним інтересам або якщо інші способи повідомлення виявились неефективними, директива допускає публічне розкриття інформації, у тому числі через ЗМІ або соціальні мережі.

Надання захисту викривачу вимагає наявності обґрунтованих підстав вважати, що повідомлена інформація є достовірною на момент її розкриття, і що вона стосується порушень, які охоплюються положеннями директиви. Важливо, що мотив викривача не впливає на надання захисту, і навіть у разі анонімного викриття, якщо особу буде пізніше встановлено і вона зазнає тиску, застосовуються всі передбачені механізми захисту. Директива також встановлює широкий і невичерпний перелік можливих форм репресій, включаючи не лише звільнення чи догани, але й непрямі дії, такі як погіршення умов праці, блокування кар'єрного зростання, фінансовий тиск, залякування, дискримінація або внесення в «чорні списки». Забороняється будь-яка форма негативного впливу, яка прямо або опосередковано пов'язана з фактом повідомлення.

Одним із ключових механізмів захисту, передбачених директивою, є перекладання обов'язку доведення: якщо після повідомлення про порушення викривач зазнає негативних наслідків, вважається, що це пов'язано з фактом викриття, і саме роботодавець має довести, що вжиті дії були обґрунтованими та не пов'язані з помстою. Окрім того, директива гарантує викривачам доступ до інформації, консультацій щодо їхніх прав, а в окремих випадках — і до безоплатної правової допомоги або фінансової підтримки. Особа, яка розкриває порушення, не несе юридичної відповідальності, якщо при цьому була змушена розкрити конфіденційну або службову інформацію, за умови дотримання критеріїв, визначених директивою.

Таким чином, директива 2019/1937 закладає системну модель захисту викривачів, орієнтовану на запобігання серйозним порушенням, стимулювання добросовісного повідомлення та створення довіри до механізмів правозастосування в межах ЄС. Водночас, зважаючи на те, що державам-членам надано можливість адаптувати ці стандарти відповідно до національного контексту, залишається ризик нерівномірної реалізації директиви, що потенційно може впливати на ефективність її впровадження. Це ставить додаткові виклики перед країнами, зокрема Україною як потенційним кандидатом на вступ до ЄС, у розробці гармонізованої, справедливої та дієвої системи захисту викривачів на національному рівні.

Директива ЄС 2019/153: Баланс між боротьбою зі злочинністю та захистом приватності¹⁵

Директива ЄС 2019/153, що присвячена використанню фінансової інформації для запобігання, розслідування та переслідування серйозних злочинів, є ключовим інструментом для посилення боротьби з транскордонною злочинністю в Європейському Союзі. Основна мета директиви полягає у встановленні чітких правил, які спрощують доступ компетентних органів до фінансової інформації, зокрема даних про банківські рахунки, для запобігання, розслідування та переслідування серйозних злочинів, таких як відмивання грошей і фінансування тероризму. Ця директива замінила застарілий механізм, що діяв з 2000 року, і спрямована на підвищення ефективності співпраці між підрозділами фінансової розвідки (ПФР) країн-членів ЄС, а також на вдосконалення доступу до фінансових даних.



Компетентні органи, до яких зазвичай належать поліція, прокуратура та спеціалізовані офіси з повернення активів (ARO), визначаються кожною країною-членом ЄС індивідуально. Вони отримують прямий і негайний доступ до централізованих реєстрів банківських рахунків у своїй країні, а також до реєстрів інших країн ЄС через захищену мережу BARIS (Bank Account Registers Interconnection System), яка діє як єдиний шлюз для швидкого обміну інформацією. Директива також охоплює доступ до аналітичних фінансових даних, наявних у ПФР, що дозволяє проводити глибший аналіз, зокрема у справах, пов'язаних із криптоактивами.

Порівняно з попереднім механізмом, ключовою інновацією є прямий і негайний доступ до інформації, який дозволяє обробляти запити майже миттєво, часто автоматично, без участі посередників, що зменшує бюрократію та прискорює розслідування як на національному, так і на транскордонному рівнях.

Значну увагу в директиві приділено захисту персональних даних і приватності. Доступ до фінансової інформації надається лише за наявності обґрунтованої підстави, пов'язаної з конкретним розслідуванням, і тільки спеціально уповноваженим співробітникам. Високі стандарти конфіденційності та безпеки даних відповідають Загальному регламенту захисту даних (GDPR). Кожен запит і пошук у реєстрах протоколюється, журнали зберігаються протягом п'яти років і регулярно перевіряються спеціально уповноваженими із захисту даних.

Обмін інформацією між органами країн-членів ЄС або з Європолом відбувається через захищені канали, такі як мережі SIENA чи FIU.net, а для особливо чутливих даних діють додаткові обмеження. Таким чином, директива прагне знайти баланс між необхідністю швидкого та ефективного розслідування серйозних злочинів і захистом фундаментальних прав людини, зокрема права на приватність і захист даних, закріплених у Хартії основних прав ЄС.

Документ також підкреслює виклики, пов'язані зі швидким розвитком фінансових технологій, зокрема криптоактивів. Директива намагається адаптуватися до цих змін, забезпечуючи інструменти для аналізу криптоактивів у транскордонних розслідуваннях. Однак для збереження ефективності необхідно постійно оновлювати законодавство, вдосконалювати технологічні рішення для нагляду та поглиблювати міжнародну співпрацю, щоб регуляторні рамки залишалися актуальними в умовах стрімкого розвитку цифрового фінансового світу.

¹⁵ https://drive.google.com/file/d/19wFhsLw3CFmCgZONXFaZmzOxfPcbbKnZ/view?usp=drive_link

Інші новини

Власник Cash App Block сплатив штраф у розмірі 40 мільйонів доларів штату Нью-Йорк за порушення комплаєнсу¹⁶



У квітні 2025 року компанія Block Inc., власник платіжного сервісу Cash App, погодилася сплатити 40 мільйонів доларів США штрафу та призначити незалежного аудитора для врегулювання претензій Департаменту фінансових послуг штату Нью-Йорк (NYDFS) щодо суттєвих недоліків у системах протидії відмиванню коштів та ідентифікації клієнтів (KYC). Це рішення стало наслідком виявлення критичних прогалин у дотриманні вимог Закону про банківську таємницю (BSA), включаючи недостатню перевірку клієнтів та слабкі контролю щодо запобігання відмиванню коштів і фінансуванню тероризму.

Особливу увагу регулятор звернув на недостатній нагляд за транзакціями з біткоїнами, які стали доступними через Cash App з 2018 року. Швидке зростання компанії без належного посилення комплаєнс-функцій створило сприятливі умови для зловживань. Зокрема, внутрішнє розслідування у 2022 році виявило понад 8 000 акаунтів, пов'язаних з російською злочинною мережею.

Цей штраф доповнює попереднє врегулювання у січні 2025 року, коли Block погодилася сплатити 80 мільйонів доларів США для врегулювання подібних звинувачень з боку 48 фінансових регуляторів штатів США. Хоча компанія не визнала провину, вона заявила, що ці врегулювання завершують всі попередні питання щодо ліцензій на переказ коштів на рівні штатів.

Цей випадок підкреслює важливість адаптації комплаєнс-функцій до масштабів та складності операцій компанії, особливо в умовах швидкого зростання та впровадження нових фінансових продуктів, таких як криптовалюти. Для фахівців у сфері ПВК/ФТ/ФР це є нагадуванням про необхідність постійного перегляду та вдосконалення систем внутрішнього контролю та управління ризиками.

Литва оштрафувала Revolut на 3,5 мільйона євро за провали у запобіганні відмиванню грошей¹⁷

У квітні 2025 року Центральний банк Литви наклав на фінтех-компанію Revolut рекордний штраф у розмірі 3,5 мільйона євро за порушення у сфері запобігання відмиванню коштів. Це рішення стало результатом планової перевірки, яка виявила суттєві недоліки в моніторингу бізнес-відносин та операцій, що призвело до неналежної ідентифікації підозрілих транзакцій. Хоча підтверджених випадків відмивання коштів не було виявлено, регулятор



¹⁶ <https://www.reuters.com/business/finance/payments-company-block-pay-40-million-fine-new-york-over-compliance-failures-2025-04-10/>

¹⁷ <https://www.reuters.com/technology/lithuania-fines-revolut-35-million-euros-money-laundering-prevention-failures-2025-04-08/>

наголосив на необхідності покращення існуючих контролів.

Revolut, що працює в Європейському Союзі за ліцензією, виданою в Литві, та під наглядом європейських і литовських центральних банків, співпрацював з регулятором і вжив негайних заходів для усунення процедурних недоліків. Компанія підписала угоду з центральним банком і вжила заходів для вирішення виявлених проблем. Штраф був встановлений з урахуванням серйозності порушення та доходів Revolut Holdings Europe, холдингової компанії для регульованих операцій Revolut у Європейській економічній зоні.

Цей випадок підкреслює важливість ефективного моніторингу та контролю в системах ПВК, особливо для фінансових установ, що швидко розвиваються. Для фахівців у сфері ПВК/ФТ/ФР це є нагадуванням про необхідність постійного перегляду та вдосконалення систем внутрішнього контролю та управління ризиками.

Золоті паспорти: боротьба ЄС із корупційними схемами громадянства¹⁸



Документ від Transparency International, опублікований 25 квітня 2025 року, детально розглядає проблему програм "золотих паспортів" у Європейському Союзі, зосереджуючись на судовому процесі між Європейською Комісією та

Мальтою, єдиною країною-членом ЄС, яка на той момент продовжувала надавати громадянство за інвестиції. Стаття висвітлює корупційні ризики, пов'язані з такими схемами, їхній вплив на безпеку та цілісність громадянства ЄС, а також аналізує потенційні наслідки рішення Суду ЄС (CJEU), яке поклало край шкідливим програмам громадянства за інвестиції.

Програми "золотих паспортів" дозволяють іноземним громадянам отримувати громадянство країн ЄС, таких як Мальта, в обмін на значні фінансові внески, часто без необхідності фізичного проживання в країні. Це створює серйозні ризики, оскільки такі схеми використовуються для відмивання грошей, уникнення санкцій та приховування корупційних статків. Документ наводить приклад молодого росіянина, засудженого у Великій Британії за відмивання грошей, який отримав мальтійське громадянство у 2022 році через інвестиційну програму. Після його засудження Мальта розпочала процес позбавлення його громадянства, що стало єдиним підтвердженням випадком такого рішення. Transparency International, спираючись на свій звіт 2018 року "European Getaway", підготовлений спільно з Global Witness, зазначає, що подібні програми часто залучають осіб із високим корупційним ризиком, які отримують доступ до привілеїв громадянства ЄС, таких як вільне пересування, спрощене відкриття банківських рахунків чи компаній, а також можливість інвестувати в елітну нерухомість, обходячи обмеження для громадян третіх країн. Аналіз 2023 року, проведений спільно з Anti-Corruption Data Collective, виявив щонайменше 20 випадків, коли власники мальтійських "золотих паспортів", переважно вихідці з Росії, відкривали компанії у Франції, декларуючи лише мальтійське громадянство, хоча деякі з них перебували під санкціями або були пов'язані з політично значущими особами в Росії.

Зростаюче занепокоєння щодо цих схем спонукало Європейську Комісію та Європейський Парламент визнати їх несумісними з принципами громадянства ЄС через відсутність "справжнього зв'язку" між заявниками та країною, що видає паспорт. Кіпр і Болгарія припинили свої програми у 2020 та 2022 роках відповідно, тоді як Мальта відмовилася це зробити, що призвело до позову Європейської Комісії до CJEU. У червні 2024 року Суд заслухав аргументи

¹⁸ <https://www.transparency.org/en/news/eu-golden-passports-on-trial-malta-court-of-justice-citizenship>

сторін: Комісія стверджувала, що Мальта порушує принцип щирої співпраці між країнами-членами ЄС, надаючи громадянство без належного зв'язку, тоді як Мальта наполягала, що питання громадянства є виключно національною компетенцією. У жовтні 2024 року Генеральний адвокат Суду висловив неформальну думку, відхиливши позов Комісії та підтримавши Мальту, що викликало занепокоєння Transparency International. Організація попередила, що рішення на користь Мальти може спровокувати "гонку", коли інші країни ЄС почнуть створювати подібні програми, залучаючи корупційні капітали. Натомість рішення на користь Комісії могло б зупинити такі схеми або запровадити суворіші критерії для надання громадянства. Зрештою, рішення CJEU оголосило про припинення шкідливих схем громадянства за інвестиції, що стало значним кроком до вирішення проблеми.

Transparency International наголошує, що "золоті паспорти" суперечать чотирьом основним свободам ЄС — вільному пересуванню людей, товарів, послуг і капіталу, — оскільки вони фактично продають ці привілеї, створюючи безпечний притулок для міжнародних злочинців. Організація закликає до гармонізації правил у межах ЄС, посилення нагляду за програмами інвестиційної міграції та ретельних перевірок походження коштів заявників.

Для загального розвитку

Як Global RADAR революціонізує скринінг санкцій за допомогою AI та машинного навчання ¹⁹



Публікація, опублікована на платформі AML Intelligence, демонструє трансформаційний підхід компанії Global RADAR до процесу санкційного скринінгу шляхом інтеграції передових технологій штучного інтелекту, машинного навчання (ML) та обробки природної мови (NLP). У сучасному середовищі, де санкційні режими стрімко змінюються, а обхідні тактики стають дедалі витонченішими, застосування традиційних, переважно ручних або правилозалежних підходів виявляється неефективним і витратним.

Особливої уваги заслуговує перетворення неструктурованих даних у структуровану аналітичну інформацію для цілей скринінгу. За допомогою NLP-моделей система Global RADAR здатна витягувати ключові елементи — імена, реєстраційні номери, географічну інформацію — з документів у форматах PDF, Word, Excel, TIFF, контрактів або електронних листів. Це суттєво знижує обсяг ручної підготовки даних і мінімізує ризик втрати релевантної інформації через її нестандартну форму.

Другий етап — це очищення та збагачення даних. Використовуючи AI, система проводить нормалізацію (видалення шумів, спеціальних символів, HTML-кодів), фільтрацію «зайвих» слів залежно від типу об'єкта, а також лінгвістичне збагачення (ідентифікація варіацій імен через псевдоніми, фонетичні варіанти тощо). Це підвищує точність і релевантність відповідних збігів.

Ключовою перевагою платформи Global RADAR є інтелектуальне зіставлення даних — поєднання декількох метрик подібності (Jaro-Winkler, Levenshtein, Metaphone 3), що дозволяє ефективно виявляти помилки введення, варіативність правопису, транслітерацію та регіональні відмінності. Це критично важливо для ідентифікації осіб, що навмисно змінюють написання своїх імен з метою ухилення від санкцій.

Окрема увага приділена скороченню хибнопозитивних результатів — однієї з головних проблем у санкційному скринінгу. Завдяки алгоритмам контекстної релевантності, машинному аналізу

історії попередніх перевірок, системи здатні автоматично знижувати пріоритет або фільтрувати повторювані несправжні збіги. Це дає змогу суттєво скоротити навантаження на комплаєнс-команди і зосередити їхню увагу на дійсно ризикових кейсах. Заявлений рівень зменшення ескалацій — до 0,2% (тобто лише 20 з 10 000 спрацьовувань) — вказує на надзвичайно високий рівень точності системи.

Таким чином, впровадження AI-інструментів у процес санкційного скринінгу забезпечує не лише зниження вартості операцій, пришвидшення ухвалення рішень і підвищення задоволеності клієнтів, а й відповідність вимогам регуляторів та готовність до нових режимів санкцій у режимі реального часу.

Ваша думка важлива!

1. Які приклади з практики MROS доцільно використати як орієнтири для розробки національних методичних матеріалів з протидії відмиванню коштів у таких вразливих сферах, як ринок мистецтва, юридичні послуги та операції з криптоактивами?
2. Наскільки існуючі підходи в Україні до ризик-орієнтованого регулювання — зокрема щодо CASPs, внутрішнього навчання персоналу та незалежної оцінки ПБК/ФТ-програм — відповідають сучасним моделям на кшталт оновлених правил AUSTRAC, і в яких напрямках вони потребують уточнення або розвитку?
3. Які уроки для НКЦПФР, НБУ та інших регуляторів містить нова правова модель кваліфікації DeFi-протоколів у Швейцарії, і як її можна адаптувати для українського законодавства?
4. Які елементи нового регуляторного пакета ЄС з ПБК/ФТ — зокрема AMLR та 6AMLD — доцільно адаптувати в українське законодавство, аби забезпечити ефективне функціонування системи фінансового моніторингу в умовах цифровізації, розширення кола підзвітних суб'єктів та зростання транскордонних ризиків?
5. Які кроки може зробити Україна для посилення фінансової розвідки та координації з міжнародними партнерами, щоб виявляти компанії-посередники, які можуть бути залучені до відмивання грошей через паливний сектор?
6. Якою має бути стратегія України щодо відновлення після війни з точки зору запобігання корупції у сферах державних закупівель, міжнародної допомоги та відбудови інфраструктури?
7. Якою має бути роль підрозділів фінансової, кібер- та антикорупційної розвідки в системі попередження та реагування на високорівневі AI-ризики (зокрема, дезінформацію, автоматизовані фінансові шахрайства, порушення приватності)?
8. Чи можлива ефективна імплементація європейських стандартів захисту викривачів в Україні за умов низької довіри до державних інституцій та судової системи?

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-2025-21

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

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