Методологічний бюлетень

Серійний номер: МінФін-AML-2026-24

Червень 2026

“Той, хто пересуває гори, починає з того, що відносить маленькі камінці!”

давньокитайська мудрість

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

Фінансування тероризму через неприбутковий сектор: сучасні загрози, вразливості та механізми протидії [1]

Документ, підготовлений AUSTRAC у травні 2026 року, є оновленою секторальною оцінкою ризиків фінансування тероризму у сфері неприбуткових організацій (НПО) Австралії. Дослідження було розроблено у співпраці з Австралійською комісією з питань благодійності та неприбуткових організацій (ACNC), Австралійським податковим управлінням (ATO), правоохоронними органами та іншими державними партнерами з метою уточнення актуального профілю загроз, вразливостей і наслідків, пов’язаних із можливим використанням НПО для цілей фінансування тероризму. Документ не є повноцінною національною оцінкою ризиків, а виступає спеціалізованим тематичним дослідженням, яке оновлює та деталізує висновки попередньої Національної оцінки ризиків у секторі неприбуткових організацій Австралії (2017) та пов’язується із ширшою Національною оцінкою ризиків фінансування тероризму в Австралії (2024). Основною ідеєю документа є те, що сектор неприбуткових організацій загалом не становить високого ризику фінансування тероризму, однак існує дуже вузька категорія організацій, для яких через специфіку діяльності, географію операцій, організаційну структуру або транзакційні моделі ризик суттєво підвищується.

[1] https://www.austrac.gov.au/sites/default/files/2026-05/Risk%20assessment_Terrorism%20financing-NPO%20sector-%20May%202026.pdf

Методологія оцінки побудована відповідно до ризик-орієнтованого підходу FATF та базується на аналізі повідомлень про підозрілі операції (SMRs), міжнародних переказів коштів, фінансової розвідки AUSTRAC, даних правоохоронних органів, відкритих джерел, академічних досліджень та міжнародних типологій фінансування тероризму. Аналіз охоплює період 2017–2025 років і спрямований на виявлення типових поведінкових, структурних та операційних ознак, які можуть бути пов'язані з ризиками фінансування тероризму у секторі неприбуткових організацій. Важливо, що міжнародні приклади використовуються не як прямий доказ існування ризику в Австралії, а як інструмент для перевірки релевантності глобальних тенденцій та типологій для австралійського контексту. Окрему увагу приділено змінам у системі регуляторної видимості сектору після запровадження нових вимог до щорічної звітності для неприбуткових організацій, які самостійно декларують статус звільнення від оподаткування.

Документ детально описує структуру австралійського сектору неприбуткових організацій, який характеризується значними масштабами, високою різноманітністю та фрагментованою системою нагляду. За оцінками AUSTRAC, в Австралії функціонує приблизно 222 400 неприбуткових організацій, зареєстрованих із чинним Австралійським бізнес-номером (ABN) – унікальним ідентифікаційним номером суб'єкта господарювання в Австралії. Близько 29 % із них є благодійними організаціями, зареєстрованими в ACNC та такими, що користуються податковими пільгами, 68 % – це неприбуткові організації, які самостійно декларують звільнення від податку на прибуток, а близько 3 % залишаються оподатковуваними структурами. Водночас офіційна статистика не охоплює значну кількість неформальних, незареєстрованих або таких, що не виконують вимоги щодо звітності, організацій. Це створює суттєві обмеження для державної видимості сектору та означає, що реальний масштаб потенційних ризиків не може бути точно оцінений. Документ наголошує, що система регулювання сектору розподілена між різними федеральними, штатними та територіальними органами влади, через що жоден державний орган не має повного комплексного контролю над усією екосистемою неприбуткових організацій.

Одним із центральних елементів дослідження є оновлення характеристик організацій, які можуть належати до категорії підвищеного ризику. AUSTRAC порівнює профіль ризиків, визначений у 2017 році, з новими даними фінансової розвідки та відзначає, що більшість базових індикаторів залишаються актуальними, хоча окремі характеристики були уточнені. До ключових ознак підвищеного ризику належать наявність повідомлень про підозрілі операції, сервісно-орієнтований характер діяльності, статус юридичної особи, концентрація діяльності у штаті Новий Південний Уельс, проведення великих готівкових операцій та міжнародні перекази коштів до високоризикових юрисдикцій. Водночас аналіз показав, що ризиковий профіль змістився від переважно малих організацій до поєднання малих і середніх структур, а також відзначено зростання ролі зареєстрованих асоціацій та австралійських публічних компаній серед організацій, які потрапляють у поле зору фінансової розвідки. Особливу увагу приділено вихідним міжнародним переказам коштів (IFTIs) до високоризикових країн, тоді як вхідні міжнародні перекази більше не розглядаються як вагомий індикатор ризику. Водночас було виключено критерій «новостворена організація», оскільки більшість виявлених випадків пов'язані з організаціями, які тривалий час здійснювали легальну діяльність.

Важливий розділ документа присвячений трансформації глобального середовища фінансування тероризму. AUSTRAC зазначає, що після ослаблення централізованих міжнародних мереж, пов'язаних із такими організаціями, як Аль-Каїда та ІДІЛ, моделі фінансування тероризму стали значно більш децентралізованими та фрагментованими. Якщо раніше терористичні структури активно використовували складні міжнародні мережі збору та переміщення коштів через благодійні організації, то сучасні схеми дедалі більше базуються на невеликих індивідуальних пожертвах, самофінансуванні або локальних зборах коштів. Це призводить до того, що обсяги операцій часто є невеликими, але водночас значно ускладнюється їх виявлення. Документ підкреслює, що навіть незначні фінансові ресурси

можуть використовуватися для забезпечення поїздок, логістики, вербування, придбання обладнання або підтримки операційної діяльності екстремістських структур.

AUSTRAC окремо акцентує увагу на ролі міжнародних переказів та діяльності у конфліктних регіонах. Значна частина виявлених випадків пов'язана із переказами коштів до зон конфліктів або юрисдикцій із підвищеним ризиком, де діють терористичні організації або насильницькі екстремістські групи. Такі перекази часто маскуються під гуманітарну допомогу, релігійні пожертви, медичну підтримку чи фінансування соціальних програм. Саме ця схожість із законною благодійною діяльністю створює серйозні труднощі для виявлення підозрілих операцій. Документ наголошує, що після переміщення коштів за кордон рівень видимості суттєво знижується, особливо якщо організації використовують місцевих партнерів, посередників або працюють у середовищах із низьким рівнем державного контролю. У таких умовах суттєво зростає ризик відволікання коштів або матеріальної допомоги на користь терористичних структур.

Окремий блок дослідження присвячений цифровим технологіям та збір благодійних коштів через цифрові платформи. AUSTRAC відзначає, що цифрові платіжні системи, краудфандингові платформи, месенджери та соціальні мережі дедалі активніше використовуються для збору коштів, зокрема у межах кампаній, пов'язаних із гуманітарними кризами або конфліктами. Такі кампанії часто орієнтовані на невеликі пожертви, але завдяки швидкому поширенню інформації можуть охоплювати дуже широку аудиторію. Хоча більшість коштів усе ще проходить через формальні банківські канали або ліцензованих операторів грошових переказів, AUSTRAC підкреслює, що визначення намірів донорів та перевірка кінцевого використання коштів залишаються складними завданнями. Особливі ризики виникають тоді, коли кампанії запускаються дуже швидко, використовують особисті рахунки або рахунки посередників, а також коли подальший рух коштів за межами Австралії неможливо відстежити. Документ також звертає увагу на те, що значна частина збоу благодійних коштів через цифрові платформи здійснюється поза межами офіційного сектору неприбуткових організацій через тимчасові, неформальні або шахрайські кампанії, що створює додаткові репутаційні ризики для легітимного благодійного сектору.

У розділі, присвяченому загрозам, AUSTRAC визначає нецільове використання коштів як найбільш поширену модель зловживання неприбутковими організаціями у контексті фінансування тероризму. Нецільове використання коштів може відбуватися на етапі збору пожертв, зберігання ресурсів або реалізації програм допомоги. У багатьох випадках гроші, офіційно зібрані для благодійних або гуманітарних цілей, перенаправляються особам чи групам, пов'язаним із насильницьким екстремізмом. Ризики суттєво зростають, коли доступ до фінансових ресурсів мають посадові особи, працівники або волонтери, здатні впливати на прийняття фінансових рішень. Окремо аналізуються випадки, коли терористичні структури або їхні прихильники використовують особисті, сімейні, релігійні чи громадські зв'язки для встановлення контактів із неприбутковими організаціями, а також випадки проникнення до організацій під виглядом волонтерів, донорів або організаторів збору коштів.

Документ також детально описує ризики зловживання легітимною гуманітарною діяльністю. Навіть у ситуаціях, коли організація діє добросовісно, програми допомоги можуть використовуватися терористичними структурами через контроль над логістикою, розподілом ресурсів або доступом до населення у зонах конфлікту. Допомога може бути перенаправлена через місцевих партнерів, транспортні компанії, склади або інші елементи інфраструктури. AUSTRAC підкреслює, що у багатьох випадках такі зловживання відбуваються без відома самої організації, що відображає практичні труднощі роботи в нестабільних регіонах із низьким рівнем контролю та обмеженими можливостями перевірки кінцевих отримувачів допомоги.

Суттєва частина дослідження присвячена структурним та регуляторним вразливостям сектору. Документ наголошує, що більшість неприбуткових організацій не підпадає під вимоги законодавства про ПВК/ФТ і не має обов'язків щодо проведення належної перевірки

клієнта, моніторингу транзакцій чи подання повідомлень про підозрілі операції. У результаті значна частина виявлення ризиків залежить від банків, платіжних сервісів та операторів грошових переказів, які перебувають під наглядом AUSTRAC. Додатковою проблемою є різний рівень вимог до звітності та нагляду для різних категорій організацій, а також наявність окремих винятків із вимог щодо системи управління та фінансової звітності для деяких релігійних структур. Водночас такі винятки не стосуються вимог законодавства у сфері ПВК/ФТ, однак вони можуть зменшувати прозорість діяльності організацій і ускладнювати виявлення та оцінку ризиків.

У фінальній частині документа AUSTRAC аналізує наслідки фінансування тероризму через сектор неприбуткових організацій. Підкреслюється, що навіть поодинокі або невеликі випадки можуть мати серйозний вплив на національну та міжнародну безпеку, оскільки навіть обмежені суми здатні підтримувати діяльність терористичних структур. Крім безпекових ризиків, значну увагу приділено негативному впливу на гуманітарні результати, оскільки відволікання коштів або неможливість перевірити кінцеве використання ресурсів означає, що допомога може не доходити до людей, які її реально потребують. Також документ наголошує на ризиках для суспільної довіри до благодійного сектору, міжнародної репутації організацій та фінансової інклюзії. AUSTRAC зазначає, що надмірний де-ріскінг з боку банків та інших фінансових установ може призводити до закриття рахунків або обмеження доступу організацій до фінансових послуг, що, у свою чергу, штовхає частину сектору до використання готівки, особистих рахунків або неформальних каналів переказу коштів. Це створює додаткові ризики непрозорості та ускладнює ефективний фінансовий моніторинг. У підсумку документ робить висновок, що ефективна система протидії фінансуванню тероризму у секторі НПО повинна базуватися на пропорційному ризик-орієнтованому підході, який одночасно забезпечує захист національної безпеки, підтримку гуманітарної діяльності, фінансову інклюзію та збереження довіри до благодійного сектору.

Висновки:

- **Документ демонструє, що ризики фінансування тероризму у секторі НПО мають не системний, а концентрований характер і зосереджені у дуже невеликій групі організацій, які здійснюють міжнародні перекази до високоризикових юрисдикцій або працюють у зонах конфліктів.** Нобхідне застосування ризик-орієнтованого нагляду замість універсальних обмежень для всього сектору.
- **AUSTRAC підтверджує, що найбільш поширеною загрозою є відволікання благодійних коштів через посередників, партнерські організації або осіб, які мають доступ до фінансових ресурсів.** Це вимагає посилення перевірки партнерів, контролю кінцевого використання коштів та моніторингу транскордонних переказів у зони конфліктів.
- **Дослідження показує, що збір благодійних коштів через цифрові платформи, соціальні мережі та краудфандингові платформи стають дедалі важливішими каналами потенційного фінансування тероризму.** Для мінімізації ризиків необхідно розвивати механізми моніторингу онлайн-зборів коштів, цифрових платіжних сервісів та операцій через рахунки посередників.
- **Документ підкреслює, що надмірний де-ріскінг з боку банків може мати зворотний ефект і сприяти переходу організацій до менш прозорих неформальних каналів переказу коштів.** Необхідно підтримувати НПО, що здійснюють законну діяльність в межах регульованої фінансової системи, поєднуючи фінансову інклюзію з ефективними заходами ПВК/ФТ.

Національна стратегія безпеки Великої Британії: пріоритети, виклики та механізми реалізації [2]

Документ, підготовлений Спільним комітетом Палати громад і Палати лордів Великої Британії з питань національної безпеки, є масштабною парламентською оцінкою Національної стратегії безпеки Великої Британії 2025 року та одночасно виступає аналізом здатності держави адаптуватися до принципово нового безпекового середовища. У центрі документа знаходиться теза про те, що Велика Британія та її союзники вступили в епоху радикальної невизначеності, коли багато фундаментальних припущень, на яких будувалася система європейської та трансатлантичної безпеки після завершення Холодної війни, більше не можуть вважатися стабільними. Автори наголошують, що сучасне безпекове середовище характеризується одночасним посиленням геополітичного суперництва великих держав, послабленням міжнародних правил і норм, зростанням ролі гібридних інструментів впливу, використанням новітніх технологій як інструменту конфронтації, збільшенням економічного примусу та поступовим руйнуванням традиційних бар'єрів, які раніше стримували агресивну поведінку держав. У цьому контексті росія визначається як найбільш безпосередня та гостра загроза національній безпеці Великої Британії, тоді як Китай розглядається як довгостроковий системний виклик, здатний впливати на глобальні економічні, технологічні та політичні процеси.

Комітет позитивно оцінює те, що Національна стратегія безпеки достатньо реалістично відображає масштаби сучасних загроз та правильно визначає ключові напрями державної політики. Водночас центральним висновком усього звіту є існування суттєвого розриву між стратегічними деклараціями та практичними механізмами їх реалізації. Автори неодноразово підкреслюють, що уряд сформулював амбітні цілі, проте недостатньо чітко пояснив, яким саме чином вони будуть досягатися, які органи влади відповідатимуть за їх виконання, які ресурси будуть залучені та якими показниками оцінюватиметься успіх. На думку Комітету, саме питання реалізації та координації є головною слабкістю нової стратегії. У документі наголошується, що навіть найточніша оцінка ризиків не матиме практичного значення без ефективної системи управління, міжвідомчої взаємодії та підзвітності.

Окремий розділ присвячений процесу підготовки самої Національної стратегії безпеки. Комітет звертає увагу на те, що консультації із зацікавленими сторонами були значно менш масштабними, ніж під час підготовки Стратегічного оборонного огляду. Представники технологічного сектору, бізнесу, наукових установ та громадянського суспільства вказували на недостатній рівень залучення до процесу формування стратегічних рішень. Автори вважають, що така ситуація створює ризики недостатнього врахування окремих аспектів безпеки та ускладнює формування широкої суспільної підтримки майбутніх заходів у сфері національної безпеки. Особливо критично оцінюється недостатня прозорість уряду щодо результатів так званого China Audit – комплексної міжвідомчої оцінки політики стосовно Китаю. Незважаючи на завершення аудиту, його результати залишилися переважно закритими для громадськості та бізнесу. Комітет наголошує, що надмірна закритість може призводити до втрати довіри з боку суспільства, а також ускладнює підготовку приватного сектору до потенційних ризиків, пов'язаних із китайським економічним та технологічним впливом.

Значна увага приділяється ролі так званої «м'якої сили» та міжнародної допомоги як інструментів забезпечення національної безпеки. Автори висловлюють занепокоєння рішенням уряду скоротити обсяги офіційної допомоги розвитку (ODA) та зазначають, що такі кроки можуть мати довгострокові негативні наслідки для британських стратегічних інтересів. Документ підкреслює, що програми розвитку, підтримка стабільності та запобігання конфліктам нерідко є більш ефективними інструментами забезпечення безпеки, ніж подальше нарощування військових спроможностей. Особливу увагу приділено Африці, де скорочення західної допомоги створює можливості для розширення впливу росії та Китаю. У цьому

[2] https://committees.parliament.uk/publications/52388/documents/290773/default/

контексті автори підкреслюють значення таких інструментів британської «м'якої сили», як Всесвітня служба BBC, Британська Рада та програми офіційної допомоги розвитку, які сприяють зміцненню міжнародних позицій Великої Британії, розширенню її дипломатичного впливу та підтримці стабільності у стратегічно важливих регіонах світу.

Окремий блок звіту присвячений питанням управління та контролю за реалізацією Національної стратегії безпеки. Комітет детально аналізує існуючу модель розподілу відповідальності між урядовими структурами та доходить висновку, що нинішня система не забезпечує достатньої прозорості та підзвітності. Незважаючи на наявність Ради національної безпеки та Національного радника з безпеки, залишається незрозумілим, які саме міністерства відповідають за конкретні напрями реалізації стратегії. Така ситуація створює ризики дублювання функцій, втрати відповідальності та фрагментації державної політики. Комітет наголошує на необхідності створення більш чітких механізмів моніторингу, регулярного звітування та парламентського контролю за виконанням стратегічних завдань.

У межах напряму «Безпека вдома» основний акцент зроблено на питаннях захисту критичної національної інфраструктури та розвитку загальнонаціональної стійкості. Документ виходить із того, що сучасні загрози дедалі частіше спрямовані не на військові об'єкти, а на цивільні системи, від функціонування яких залежить життєздатність держави. Йдеться про енергетичну інфраструктуру, транспортні мережі, телекомунікації, підводні кабелі, фінансову систему та цифрові сервіси. Автори звертають увагу на стрімке зростання кількості гібридних атак на такі об'єкти в Європі та наголошують на необхідності комплексного підходу до їх захисту. Особливий акцент робиться на кібербезпеці, розвитку механізмів раннього виявлення загроз, проведенні регулярних оцінок вразливостей, підвищенні відповідальності операторів критичної інфраструктури та розширенні переліку об'єктів, які мають отримати статус критично важливих.

Важливе місце у звіті займають питання цивільної готовності до криз та війни. Комітет підтримує створення Академії стійкості Великої Британії, яка повинна стати ключовим інструментом оцінки готовності державних структур до надзвичайних ситуацій, однак наголошує, що її повноваження, механізми роботи та зв'язки з урядом залишаються недостатньо визначеними. Автори також звертають увагу на необхідність активнішого використання резервних сил для захисту критичної інфраструктури та підтримання функціонування держави у кризових ситуаціях. Водночас вони зазначають, що уряд поки не представив достатньо конкретного бачення ролі резервістів у разі масштабного конфлікту чи надзвичайної ситуації. Значна увага приділяється концепції загальносуспільного підходу, відповідно до якої забезпечення національної безпеки та стійкості розглядається як спільна відповідальність держави, бізнесу, місцевих громад та громадянського суспільства. Водночас Комітет наголошує, що уряд поки перебуває на початковому етапі впровадження цього підходу та не запропонував комплексного плану його практичної реалізації.

У міжнародному вимірі особливу увагу приділено зміні безпекового середовища в Європі та поступовому зростанню невизначеності щодо майбутньої ролі Сполучених Штатів у гарантуванні європейської безпеки. Автори визнають, що США залишаються найважливішим союзником Великої Британії, однак наголошують на необхідності готуватися до сценаріїв, за яких рівень американської підтримки може зменшитися або стати менш передбачуваним. У зв'язку з цим особливого значення набуває розвиток європейських оборонних спроможностей, посилення ролі НАТО та формування нових форматів співпраці між європейськими державами. Документ підкреслює, що росія залишається найбільшою загрозою для безпеки Великої Британії та її союзників, а тому політика стримування має залишатися одним із ключових напрямів державної політики. Водночас наголошується на необхідності підтримання довгострокового тиску на росію через санкції, дипломатичну ізоляцію та підтримку України.

Особливе місце у звіті займає аналіз відносин із Китаєм. Комітет підтримує прагнення уряду підтримувати економічні зв'язки з КНР, однак наголошує, що будь-які рішення у цій сфері

повинні супроводжуватися прозорою оцінкою ризиків для національної безпеки. Автори закликають уряд чіткіше визначити власне бачення Китаю як стратегічного виклику та забезпечити більшу відкритість щодо того, як саме питання безпеки враховуються під час укладення міжнародних угод та розвитку економічного співробітництва.

Висновки:

- **Документ показує, що головною проблемою британської Національної стратегії безпеки є не оцінка загроз, а відсутність достатньо деталізованих механізмів реалізації.** Необхідне запровадження чіткої системи відповідальності, показників виконання та регулярної звітності щодо досягнення цілей національної безпеки.
- **Комітет наголошує, що захист критичної інфраструктури стає одним із ключових пріоритетів сучасної безпекової політики.** Це вимагає розширення вимог до операторів інфраструктури, посилення кіберзахисту, проведення регулярних оцінок вразливостей та інтеграції приватного сектору у систему національної стійкості.
- **Документ підкреслює необхідність підготовки Європи до сценаріїв зменшення американської безпекової підтримки та водночас закликає до збереження максимального тиску на росію до припинення агресії проти України.** Необхідний розвиток європейських оборонних спроможностей та посиленні ролі НАТО в системі стримування**.**
- **Автори доходять висновку, що технологічний та оборонний суверенітет стає ключовим фактором національної безпеки.** Для цього уряд має чітко визначити перелік критичних технологій і спроможностей, які повинні залишатися під національним контролем, а також сформувати довгострокові механізми підтримки оборонно-промислового сектору та інновацій.

Завершальна частина документа присвячена концепції суверенних спроможностей. Комітет зазначає, що уряд постійно використовує цей термін як один із центральних елементів нової стратегії, проте досі не надав його чіткого визначення. Відсутність ясності щодо того, які саме технології, виробництва та системи повинні перебувати під національним контролем, створює невизначеність для оборонної промисловості, інвесторів та науково-дослідного сектору. Автори наголошують, що в умовах геополітичної нестабільності технологічна та промислова автономія стає одним із ключових чинників національної безпеки. Саме тому уряд має сформувати чітке бачення того, які критичні технології та спроможності повинні бути захищені від зовнішньої залежності, визначити рівні допустимої залежності від союзників та створити довгострокову систему підтримки оборонно-промислового комплексу, інновацій та наукових досліджень.

ЄБА консолідує тлумачення вимог PSD2 [3]

12 червня 2026 року Європейський банківський орган (EBA) опублікував шість остаточних відповідей на запитання (Q&A) в рамках механізму «Єдиного зведення правил» (Single Rulebook Q&A). Усі шість прийняті за результатами запитів чеської компанії ZNPay a.s. та стосуються тлумачення Директиви 2015/2366/ЄС (PSD2), зокрема вимог до посиленої автентифікації клієнта (SCA) та захищеного зв'язку відповідно до Делегованого регламенту Комісії (ЄС) 2018/389 (RTS). Опублікована сукупність Q&A формує консолідовану позицію EBA щодо ключових операційних суперечностей відкритого банкінгу між надавачами платіжних послуг, що обслуговують рахунки (ASPSP), надавачами послуг ініціювання платежів (PISP) та надавачами послуг з надання інформації про рахунки (AISP), і відображає проблеми, що системно виникають при реалізації PSD2.

Q&A 2025_7602 і 2025_7607 формують цілісну доктрину щодо мінімізації перешкод у маршрутах автентифікації та принципів порівняльного аналізу. У Q&A 2025_7602 EBA

[3] https://www.eba.europa.eu/system/files/15062026_122841_EBA_QAs.pdf

кваліфікує обов'язковий екран вибору клієнтського сегмента (роздрібний або корпоративний) в рамках редиректного маршруту як перешкоду в розумінні статті 32(3) RTS, якщо аналогічний крок відсутній при безпосередньому доступі користувача до рахунку через нативний мобільний додаток банку. Відповідно до Думки EBA про перешкоди (EBA/OP/2020/10), взаємодія між користувачем та ASPSP у рамках AIS або PIS має бути зведена до необхідного мінімуму, а маршрут автентифікації не повинен містити надлишкових кроків порівняно з аналогічним прямим доступом. Q&A 2025_7607 встановлює принцип відповідності контексту: якщо користувач використовує послуги AISP або PISP через мобільний додаток і ASPSP надає можливість прямої автентифікації через власний мобільний банківський застосунок, то саме мобільний маршрут є правильним еталоном для порівняння. Перенаправлення користувача до мобільного браузерного середовища в такому контексті, так само як і відсутність автоматичного повернення користувача до TPP-додатку після автентифікації, може становити перешкоду за статтею 32(3) RTS.

Q&A 2025_7606 роз'яснює обсяг поняття «процедури автентифікації» у розумінні Думки EBA про перешкоди. EBA відкидає вузьке тлумачення, що зводить цей термін до фінального методу SCA (наприклад, біометрії або PIN), і чітко встановлює: поняття охоплює всі дії, необхідні для перевірки ідентичності користувача або дійсності використання ним платіжного інструменту, – тобто весь наскрізний маршрут автентифікації. Відповідно, додаткові обтяжливі кроки, які вимагаються виключно в TPP-маршруті та відсутні при прямому доступі – наприклад, необхідність натиснути на неочевидне зображення QR-коду або вручну ввести ім'я користувача для ініціювання push-сповіщення автентифікації – порушують вимогу статті 30(2) RTS щодо підтримки всіх процедур автентифікації через спеціалізований інтерфейс. Це тлумачення закриває практичну лазівку, якою користувались деякі ASPSP, формально заявляючи про підтримку тих самих SCA-методів при одночасному запровадженні суттєво більш обтяжливого маршруту в TPP-каналі.

Q&A 2025_7644 стосується зобов'язань ASPSP щодо інформування PISP про статус виконання окремих платежів за постійними дорученнями (standing orders). EBA роз'яснює, що вимога статті 66(4)(b) PSD2 та статті 36(1)(b) Делегованого регламенту щодо надання PISP інформації про ініціювання та виконання платежу застосовується виключно на момент «негайний після отримання платіжного доручення», і не зобов'язує ASPSP надавати оновлення на пізніших стадіях. Оскільки встановлення постійного доручення є підставою для здійснення множинних майбутніх платежів, а на момент отримання такого доручення інформація про статус майбутніх окремих транзакцій ASPSP ще не відома, зобов'язання щодо їх окремого інформування PISP відсутнє. Ця позиція підтверджує раніше сформульовані Q&A 4601 і Q&A 7261 і встановлює чіткий правовий кордон між зобов'язанням надати PISP інформацію «негайно після отримання» та будь-яким наступним постійним інформаційним потоком.

Q&A 2025_7672 і 2025_7675 уточнюють обсяг інформаційних зобов'язань ASPSP в контексті підтримки та відмов у платежах. У Q&A 2025_7672 EBA проводить важливе концептуальне розмежування: посилання на «підтримку» в статті 32(1) RTS стосується технічної підтримки, що надається ASPSP третім постачальникам (TPP – AISP та PISP), а не клієнтської підтримки для користувачів. Оскільки спеціалізований інтерфейс є інтерфейсом доступу для TPP, а не клієнтським інтерфейсом для користувачів, відсутність для користувачів каналів підтримки під час автентифікації в рамках AIS/PIS не є перешкодою за статтею 32(3), якщо аналогічна ситуація має місце і при прямому доступі користувача до рахунку. Водночас відсутність або нерівноцінність підтримки для TPP через спеціалізований інтерфейс становить порушення статті 32(1). Q&A 2025_7675 роз'яснює питання інформаційної асиметрії при відмовах: ASPSP зобов'язаний надати PISP ту саму інформацію про причини відмови у виконанні платіжного доручення, що надається користувачу при безпосередньому ініціюванні, – якщо вона відома ASPSP негайно після отримання доручення. EBA уточнює, що стаття 79(1) PSD2 регулює порядок та строки інформування користувача про відмову з боку ASPSP, однак не вимагає, щоб це інформування відбувалось безпосередньо через інтерфейс ініціювання платежу; до

того ж відмова стає відомою ASPSP, як правило, лише після завершення процедури автентифікації.

Від оцінки ризиків до вимірювання економії: міжнародний підхід до протидії шахрайству [4]

Документ, підготовлений Міжнародним форумом з питань шахрайства у державному секторі (IPSFF) у співпраці з Управлінням з протидії шахрайству в державному секторі Великої Британії (PSFA) та Центром запобігання шахрайству Співдружності Австралії (CFPC), присвячений створенню єдиної методологічної основи для оцінки фінансових та нефінансових вигод від заходів із запобігання шахрайству в державному секторі. Автори виходять із того, що шахрайство є однією з найбільш прихованих форм втрат державних ресурсів, масштаби якої часто залишаються недооціненими через складність виявлення та вимірювання. Саме тому державні органи нерідко інвестують більше ресурсів у виявлення та розслідування вже скоєних порушень, ніж у їх попередження. Документ прагне змінити цей підхід шляхом формування практичного інструментарію, який дозволяє кількісно доводити економічну доцільність профілактичних заходів і демонструвати їхню реальну віддачу для державного бюджету.

Центральною концепцією документа є поняття оцінки економії від запобігання шахрайству – системного процесу оцінки економії коштів, досягнутої внаслідок впровадження заходів із запобігання шахрайству та порушенням. Автори наголошують, що така оцінка повинна здійснюватися за єдиними, послідовними та обґрунтованими принципами, які дозволяють не лише демонструвати результати вже реалізованих заходів, але й прогнозувати майбутній ефект від нових ініціатив. Документ розглядає оцінку економії від запобігання шахрайству як невід'ємний елемент комплексної системи управління ризиками шахрайства, що включає оцінку ризиків, вимірювання втрат від шахрайства, аналітику даних, тестування контрольних заходів, управлінську звітність та інші складові сучасної системи управління протидією шахрайству.

Особлива увага приділяється економічній логіці профілактики. Документ зазначає, що профілактичні заходи традиційно складніше обґрунтовувати перед керівництвом та бюджетними органами, оскільки вони спрямовані на запобігання потенційним порушенням і втратам, які фактично не відбулися. Однак саме профілактика дозволяє уникати найбільших втрат. У документі наводяться приклади аналізу британського досвіду, які свідчать про значно вищу рентабельність проактивних заходів порівняно з реактивними підходами. При цьому автори підкреслюють, що навіть фінансові показники не відображають повною мірою вигоди від запобігання шахрайству, оскільки не враховують репутаційні наслідки, зниження довіри громадян до держави, додаткові адміністративні витрати та суспільну шкоду, яка виникає внаслідок невиявлених зловживань.

Методологічний підхід, викладений у документі, побудований навколо трьох взаємопов'язаних елементів. Перший із них передбачає проведення попередніх підготовчих заходів, метою яких є збір і аналіз інформації, необхідної для формування обґрунтованої бази подальших розрахунків та оцінок. Автори підкреслюють, що будь-які оцінки економії повинні починатися з визначення масштабу проблеми, аналізу причин шахрайства та встановлення базового рівня втрат. Для цього пропонуються різні інструменти, включаючи аналіз аналогічних програм, збір і аналіз наявних даних, проведення оцінки ризиків шахрайства, тестування контрольних механізмів та вимірювання фактичних втрат від шахрайства. Особливо наголошується, що якість базового рівня безпосередньо впливає на достовірність усіх подальших розрахунків. Саме тому документ рекомендує, за можливості, спиратися на

[4] https://assets.publishing.service.gov.uk/media/69fc95b98cc72d2f863ea5c9/International_Public_Sector_Fraud_Forum__Fraud_Prevention_Savings_Framework.pdf

кількісні дані та результати спеціалізованих заходів з вимірювання втрат від шахрайства, оскільки вони забезпечують найбільш обґрунтовану основу для оцінки ефективності профілактичних заходів.

Документ детально висвітлює значення оцінки ризиків шахрайства (FRA) та вимірювання втрат від шахрайства (FLM) як ключових інструментів формування обґрунтованої базової оцінки шахрайських ризиків, їхніх джерел, масштабу та потенційного впливу. Оцінка ризиків дозволяє виявити потенційні сценарії шахрайства, визначити їхню ймовірність та потенційний вплив, а також оцінити залишковий ризик після впровадження наявних контролів. Водночас вимірювання втрат від шахрайства розглядається як найбільш точний інструмент встановлення фактичного рівня порушень, оскільки воно базується на статистично обґрунтованому аналізі транзакцій та використанні зовнішніх джерел даних для перевірки їхньої правомірності. Автори вважають, що саме поєднання цих підходів забезпечує найбільш надійну основу для розрахунку економії від майбутніх втручань.

Наступним етапом запропонованої методології є визначення профілактичних заходів, які мають бути спрямовані на усунення або зменшення впливу виявлених причин і чинників шахрайства та помилок. Документ пропонує розглядати втручання через призму чотирьох рівнів профілактики. Документ виділяє чотири рівні профілактики шахрайства. Перший рівень – первинне проєктування системи запобігання (primordial prevention) – передбачає формування ефективного контрольного середовища ще на етапі розроблення нової програми, процесу або послуги. Другий рівень – безпосереднє запобігання (primary prevention) – охоплює контрольні та організаційні заходи, спрямовані на зниження ймовірності виникнення шахрайства чи помилок. Третій рівень – раннє виявлення (secondary prevention) – включає механізми своєчасного виявлення порушень з метою обмеження їх тривалості та мінімізації подальших втрат. Четвертий рівень – реагування та відшкодування збитків (tertiary prevention) – передбачає проведення розслідувань, стягнення неправомірно отриманих коштів та повернення активів після вчинення порушення. Автори наголошують, що найбільша довгострокова економічна цінність досягається саме завдяки розвитку перших двох рівнів профілактики, тоді як третинні заходи виконують переважно компенсаційну функцію.

Окремий великий розділ присвячений методам розрахунку економії. В основі підходу лежить концепція контрфактичного підходу, який використовується для визначення базового сценарію розвитку подій та передбачає оцінку того, якими були б рівень шахрайства, обсяг втрат і пов’язані ризики у разі невпровадження відповідного втручання. Документ розглядає контрфактичний підхід як ключовий елемент оцінки економії від запобігання шахрайству, оскільки саме він формує базу для порівняння та визначення економічного ефекту від впроваджених заходів. Для побудови таких сценаріїв можуть використовуватися історичні дані, статистичні моделі, експертні оцінки, аналіз аналогічних програм або квазіекспериментальні методи. Автори підкреслюють, що незалежно від обраного підходу всі припущення повинні бути логічно обґрунтованими, прозорими та придатними для подальшої перевірки.

Після формування контрфактичного підходу здійснюється оцінка очікуваного впливу відповідного втручання. Для цього документ рекомендує ідентифікувати ключові причини та чинники, що спричиняють втрати від шахрайства і помилок, а також визначити ступінь впливу запланованих заходів на їх усунення або мінімізацію. Документ визнає, що в більшості випадків неможливо усунути ризик повністю, тому оцінка ефективності втручань має враховувати залишкові вразливості та реалістичні припущення щодо рівня зниження ризику. Значну роль у цьому процесі відіграють експертні судження, результати попередніх оцінок ефективності аналогічних заходів, аудиторські перевірки та аналіз історичних даних.

Наступним етапом є безпосередній розрахунок економії, який здійснюється шляхом порівняння прогнозованих втрат у сценарії без втручання з очікуваними або фактичними втратами після його реалізації. Документ приділяє значну увагу поняттю періоду оцінки результатів, тобто часовому проміжку, протягом якого отримані результати та досягнута

економія можуть бути обґрунтовано пов'язані з реалізацією конкретного заходу. Документ звертає увагу на необхідність чітко визначати початок та завершення такого періоду, враховуючи життєвий цикл програми, особливості процесів та характер втручання. Автори також наголошують, що розрахунки повинні охоплювати не лише прямі втрати від шахрайства та помилок, а й супутні адміністративні витрати, яких вдалося уникнути завдяки профілактиці.

Важливою складовою запропонованої методології є оцінка рентабельності інвестицій (ROI). Документ пропонує порівнювати отриману економію з витратами на впровадження відповідного заходу, що дозволяє обґрунтовувати інвестиційні рішення та визначати найбільш ефективні напрямки розвитку системи протидії шахрайству. При цьому автори підкреслюють, що фінансові показники не повинні бути єдиним критерієм оцінки, оскільки багато результатів профілактики мають нематеріальний характер.

Окремий розділ документа присвячений нефінансовим вигодам. Документ наголошує, що значна частина цінності профілактичних заходів проявляється через підвищення довіри громадян до державних програм, покращення якості державних послуг, зміцнення культури доброчесності, зростання рівня добровільного дотримання правил та підвищення загальної ефективності управління. Такі результати складно перевести у грошовий еквівалент, однак їх рекомендується систематично документувати та відображати поряд із фінансовими показниками для формування повної картини впливу заходів.

Висновки:

- **Документ демонструє, що ефективна система протидії шахрайству повинна зміщувати акцент із виявлення вже скоєних порушень на їх раннє попередження.** Необхідно інвестувати у превентивні механізми, оскільки вони забезпечують вищу рентабельність порівняно з реактивними заходами.
- **Документ показує, що достовірна оцінка економії від запобігання шахрайству потребує наявності якісної базової оцінки ризиків і втрат, сформованої за допомогою інструментів оцінки ризиків шахрайства, тестування контрольних механізмів та вимірювання втрат від шахрайства.** Відповідно, розвиток цих напрямів є необхідною передумовою побудови ефективної системи управління ризиками шахрайства.
- **Документ пропонує використовувати контрфактичний підхід як один із ключових інструментів оцінки економії від заходів із запобігання шахрайству.** Практична цінність цього підходу полягає у можливості кількісного обґрунтування доцільності інвестицій у нові контрольні та комплаєнс-механізми шляхом прогнозування їхнього потенційного економічного ефекту ще до фактичного впровадження.
- **Документ підкреслює, що оцінка результативності заходів протидії шахрайству повинна охоплювати не лише прямі фінансові втрати, яких вдалося уникнути,** а й ширші нефінансові ефекти, включаючи підвищення довіри до державних інституцій, покращення якості послуг та зміцнення культури доброчесності.

Завершальна частина методології присвячена питанням управління, верифікації та забезпечення якості оцінок. Автори пропонують створювати спеціалізовані механізми незалежного перегляду методологій, формувати централізовані банки методів, здійснювати ретроспективні перевірки прогнозів та оцінювати довгострокову цінність реалізованих заходів. Особлива увага приділяється прозорості методологічних припущень, управлінню даними, забезпеченню відтворюваності розрахунків та формуванню єдиних стандартів звітності. У підсумку документ формує комплексну систему доказового обґрунтування інвестицій у профілактику шахрайства, яка дозволяє державним органам переходити від декларативних тверджень про користь контролів до кількісно підтверджених результатів, що можуть використовуватися для прийняття управлінських рішень, планування ресурсів та вдосконалення системи управління ризиками шахрайства.

Кібер-шахрайські центри та торгівля людьми: трансформація організованої злочинності в цифрову епоху [5]

Доповідь ОБСЄ присвячена дослідженню одного з найбільш небезпечних новітніх проявів транснаціональної організованої злочинності – торгівлі людьми з метою примусового залучення до кібер-шахрайських операцій. Документ демонструє, що явище, яке донедавна переважно асоціювалося з країнами Південно-Східної Азії, поступово трансформується у глобальну кримінальну модель та дедалі активніше поширюється на регіон ОБСЄ. Автори розглядають кібер-шахрайські центри як складні злочинні екосистеми, де поєднуються торгівля людьми, кіберзлочинність, фінансове шахрайство, відмивання коштів та використання цифрових технологій для масового залучення як жертв експлуатації, так і фінансових жертв шахрайства.

У доповіді наголошується, що масштаби цього явища набули безпрецедентного характеру. За оцінками міжнародних організацій, шахрайські центри Східної та Південно-Східної Азії лише у 2023 році могли генерувати від 18 до 37 млрд доларів США незаконних доходів, тоді як глобальні втрати від різних форм онлайн-шахрайства у 2024 році перевищили 1 трлн доларів США. Одночасно сотні тисяч людей можуть перебувати під контролем злочинних мереж та виконувати шахрайські операції під примусом. Автори підкреслюють, що йдеться не лише про фінансові злочини, а й про масштабну гуманітарну проблему, оскільки численні розслідування та свідчення потерпілих документують випадки фізичного насильства, катувань, сексуальної експлуатації, боргової залежності, ізоляції, психологічного тиску та інших форм жорстокого поводження щодо осіб, які були завербовані до таких схем.

Одним із ключових аспектів дослідження є аналіз механізмів вербування жертв. Доповідь показує, що злочинні мережі активно використовують соціальні мережі, сайти пошуку роботи, месенджери та цифрові платформи для розміщення вакансій, які зовні практично не відрізняються від легітимних пропозицій працевлаштування. Переважно такі пропозиції працевлаштування стосуються посад у сферах підтримки клієнтів, функціонування контакт-центрів, онлайн-гемблінгу, дистанційних гральних сервісів, операцій на валютному (Forex) та криптовалютному ринках, маркетингу, реалізації товарів і послуг, а також роботи з клієнтами. Потенційним працівникам пропонуються високі заробітні плати, швидке працевлаштування, допомога з отриманням візи, безкоштовне житло, оплату переїзду та інші вигідні умови. Саме поєднання таких елементів робить вакансії привабливими для молодих людей, які шукають можливості міжнародного працевлаштування.

Автори детально описують типову схему переходу від рекрутингу до експлуатації. Спочатку особа знаходить вакансію через соціальні мережі або тематичні канали, після чого комунікація швидко переводиться у приватні месенджери, зокрема Telegram, WhatsApp або Viber. Далі роботодавець організовує процес релокації, бронювання житла та оформлення необхідних документів. Після прибуття до місця роботи людина поступово втрачає можливість вільно залишити робоче місце, у неї можуть вилучатися документи, обмежуватися пересування, а сам працівник фактично потрапляє під контроль організаторів схеми. Надалі особа залучається до проведення шахрайських операцій, які можуть включати романтичні шахрайства, інвестиційне шахрайство, криптовалютні схеми, телефонне шахрайство або інші види фінансового обману.

Важливим внеском дослідження є аналіз організаційної структури шахрайських центрів. Автори встановлюють, що такі операції функціонують як добре організовані корпоративні структури з чіткою вертикаллю управління. На верхньому рівні знаходяться власники та інвестори, які можуть мати зв'язки з політичними або кримінальними елітами. Нижче розташовані операційні менеджери та керівники підрозділів, які контролюють виконання планів, показники прибутковості та дисципліну персоналу. Безпосередні виконавці поділяються на окремі функціональні групи, які займаються пошуком жертв, встановленням

[5] https://cthb.osce.org/sites/default/files/documents/publications/2026/04/Cyber%20Scam_Screen_260429.pdf

контакту, підтриманням довіри, переконанням інвестувати додаткові кошти або супроводом шахрайських операцій. Для контролю персоналу використовуються системи відеоспостереження, обмеження пересування, контроль доступу, а також спеціалізоване програмне забезпечення для масового управління акаунтами та комунікації з потенційними жертвами.

Особлива увага приділяється використанню криптовалют та цифрової інфраструктури. У доповіді зазначається, що переважна більшість фінансових потоків у таких схемах проходить через криптовалютні активи, зокрема стейблкоїни. Фінансові жертви часто переводять кошти через легальні криптовалютні платформи, після чого активи спрямовуються на контрольовані злочинцями рахунки або псевдоінвестиційні платформи. Така модель значно ускладнює відстеження коштів та сприяє міжнародному переміщенню незаконних доходів.

Окремий блок дослідження присвячений регіону ОБСЄ. Автори констатують, що ознаки функціонування або формування шахрайських центрів вже були зафіксовані у низці держав регіону. Особливої уваги набули випадки у Польщі, Північній Македонії та Чорногорії, де правоохоронні органи викривали організовані структури, які використовували елементи моделі, характерної для шахрайських центрів Південно-Східної Азії. Наведені кейси демонструють використання фальшивих вакансій, транскордонного переміщення працівників, вилучення документів та примусу до участі у шахрайських схемах. Водночас значна кількість громадян держав ОБСЄ залишається серед основних груп жертв, яких вербують для роботи у таких центрах за межами регіону.

Дослідження містить масштабний аналіз онлайн-рекрутингу. Для цього було проаналізовано 82 оголошення про працевлаштування та 750 повідомлень із Telegram-каналів. Встановлено, що найбільш поширеними мовами рекрутингу є англійська та російська, хоча також зустрічаються вакансії турецькою, румунською, італійською та іншими мовами. Найбільшу концентрацію ризикових індикаторів автори виявили у Східній та Південно-Східній Європі, тоді як Південний Кавказ демонструє помітні ознаки розвитку відповідної інфраструктури. Центральна Азія характеризується значним рівнем шахрайської активності, однак з

Висновки:

- **Документ демонструє, що торгівля людьми для примусового залучення до кібер-шахрайства перетворюється з регіонального феномену Південно-Східної Азії на глобальну модель організованої злочинності, яка вже активно поширюється на регіон ОБСЄ.** Необхідне включення кібер-шахрайських центрів до національних оцінок ризиків торгівлі людьми та стратегій протидії організованій злочинності.
- **Дослідження показує, що основним інструментом рекрутингу залишаються соціальні мережі та месенджери, а найбільш поширеними індикаторами ризику є релокаційні пакети, надання житла, швидке працевлаштування, відсутність прозорої інформації про роботодавця та комунікація виключно через Telegram, WhatsApp або Viber.** Це вимагає розроблення систем раннього виявлення ризикових вакансій та посилення моніторингу онлайн-рекрутингу.
- **Автори встановили, що шахрайські центри функціонують як високоструктуровані транснаціональні бізнес-моделі з використанням криптовалют, спеціалізованого програмного забезпечення, міжнародних мереж відмивання коштів та складних схем управління персоналом.** Це означає, що протидія таким мережам повинна поєднувати інструменти боротьби з торгівлею людьми, кіберзлочинністю, ВК/ФТ та організованою злочинністю.
- **Дослідження підтверджує, що значна частина операцій орієнтована на транскордонне залучення працівників зі знанням іноземних мов для подальшого здійснення шахрайства щодо громадян інших країн.** Необхідне посилення міжнародного обміну інформацією між правоохоронними органами, ПФР, міграційними службами та цифровими платформами для виявлення та припинення таких схем на ранніх стадіях.

меншою кількістю ознак транскордонної торгівлі людьми.

Особливу роль у дослідженні відіграє аналіз Telegram як інструменту рекрутингу. Автори встановили, що саме Telegram дедалі частіше використовується як центральний елемент рекрутингової інфраструктури. Канали активно поширюють вакансії для фахівців із утримання та повторного залучення клієнтів, конверсії потенційних клієнтів, супроводу фінансових операцій та роботи з криптовалютними й валютними інструментами. Аналіз функціонального наповнення таких посад свідчить, що їхні завдання часто пов'язані з маніпулятивним впливом на жертв шахрайства, підтриманням їхньої участі у схемах та переконанням здійснювати додаткові фінансові перекази. Значний попит на працівників зі знанням англійської, французької, німецької, португальської та інших мов свідчить про орієнтацію шахрайських операцій на заможні ринки Західної Європи та інших економічно розвинених регіонів.

Важливим результатом дослідження стало створення комплексної системи індикаторів ризику, яка дозволяє виявляти потенційно небезпечні вакансії ще на етапі рекрутингу. До найбільш характерних індикаторів віднесено пропозицію релокації та житла, швидке працевлаштування без перевірки кваліфікації, використання виключно месенджерів для комунікації, відсутність прозорої інформації про роботодавця, шаблонний зміст вакансій, обіцянки надмірно високих доходів, а також роботу у сферах iGaming, Forex або криптовалют. Автори підкреслюють, що окремо кожен із цих факторів не є доказом злочинної діяльності, однак їх сукупність може свідчити про високий ризик торгівлі людьми або примусової злочинної діяльності.

У підсумку доповідь доходить висновку, що торгівля людьми для залучення до кібер-шахрайства стає однією з найсерйозніших нових загроз безпеці в цифрову епоху. Вона поєднує ознаки організованої злочинності, торгівлі людьми, кіберзлочинності та незаконних фінансових потоків, що вимагає принципово нового міжсекторального підходу до протидії. Автори наголошують на необхідності посилення співпраці між правоохоронними органами, підрозділами фінансової розвідки, міграційними службами, платформами соціальних мереж, фінансовими установами та міжнародними організаціями. Лише поєднання заходів із попередження, раннього виявлення, захисту жертв, міжнародного обміну інформацією та притягнення організаторів до відповідальності здатне стримати подальше поширення цієї моделі злочинної діяльності в регіоні ОБСЄ та за його межами.

Регулювання

Системна реформа швейцарського антилегалізаційного законодавства [6]

12 червня 2026 року Федеральна рада Швейцарії оголосила дату набуття чинності двох ключових законодавчих актів, ухвалених Парламентом 26 вересня 2025 року, – переглянутого Закону про боротьбу з відмиванням коштів (AMLA) та нового Федерального закону про прозорість юридичних осіб і ідентифікацію кінцевих бенефіціарних власників (TJPG). Обидва акти набудуть чинності 1 жовтня 2026 року, що знаменує найбільш фундаментальну структурну реформу системи ПВК/ФТ Швейцарії за останні десятиліття. Дата обрана стратегічно: вона синхронізована з наступною оцінкою Швейцарії з боку FATF, запланованою на 2027–2028 роки, і покликана продемонструвати ефективність нових заходів безпосередньо в момент оцінювання. Положення щодо державних нотаріусів (Amtsnotare) відкладено в часі, надаючи кантонам можливість адаптувати власне законодавство; стосовно порогових значень для визначення «професійної консультаційної діяльності» запроваджено чітку нормативну регламентацію за підсумками консультацій.

Центральним інструментальним елементом реформи є запровадження централізованого електронного реєстру прозорості, що перебуватиме в управлінні Федерального офісу юстиції.

[6] https://www.sif.admin.ch/en/newnsb/x3sKLxCJ6S3dQJtfvy0Tb

Це принципова інновація: Швейцарія досі не мала єдиного централізованого реєстру бенефіціарних власників на федеральному рівні. На відміну від моделей, прийнятих у низці держав-членів ЄС, швейцарський реєстр не є публічно доступним – коло осіб, уповноважених на доступ до нього, суворо обмежене законом. Повний доступ мають правоохоронні, адміністративні та кримінальні органи, Управління звітності з питань відмивання коштів (MROS), органи міжнародного податкового співробітництва та виконання санкцій. Наглядові органи в рамках AMLA, саморегулюючі організації, служба розвідки та ряд інших спеціалізованих інститутів можуть здійснювати запити виключно в обсязі, необхідному для виконання їхніх статутних функцій. Фінансові посередники та певна категорія консультантів отримують право онлайн-запиту до реєстру, однак лише при виконанні зобов'язань з належної перевірки в рамках антилегалізаційного законодавства.

Предметна сфера застосування TJPG охоплює більшість швейцарських компаній – корпорацій, товариств з обмеженою відповідальністю, кооперативів, командитних акціонерних товариств, – а також іноземних суб'єктів із відчутною прив'язкою до Швейцарії: через зареєстровану філію, фактичне місцезнаходження адміністрації або нерухоме майно на її території. До сфери дії закону належать і трасти, довірені особи яких є резидентами Швейцарії або управляють ними на її території. Водночас передбачено низку винятків: асоціації, фонди, прості та командитні товариства вилучені зі сфери дії закону. Не підпадають під його вимоги пенсійні фонди, суб'єкти, що щонайменше на 75 відсотків прямо або опосередковано перебувають у власності державних органів, компанії з акціями, що публічно торгуються на біржі, і їхні дочірні структури з аналогічним пороговим значенням.

Поняття «кінцевий бенефіціарний власник» (КБВ) відтворює міжнародні стандарти: це будь-яка фізична особа, яка контролює суб'єкт через пряме або опосередковане володіння, індивідуальне або спільне утримання не менш ніж 25 відсотків капіталу або права голосу або через здійснення контролю в інший спосіб. Якщо жодна особа не відповідає цим критеріям, КБВ вважається найвищий за посадою член виконавчого органу. Зобов'язання щодо ідентифікації КБВ покладаються безпосередньо на юридичні особи: вони зобов'язані встановити, верифікувати та задокументувати своїх КБВ, збираючи деталізовану персональну інформацію (ім'я, дату народження, громадянство, місце проживання та характер контролю). Якщо компанія не може ідентифікувати КБВ або задовільним чином верифікувати його ідентичність чи статус, вона зобов'язана зафіксувати цей факт разом з описом невдалих спроб ідентифікації. Зібрані дані підлягають внесенню до реєстру прозорості протягом одного місяця після інкорпорації або виникнення зобов'язань та оперативному оновленню за будь-яких змін. Санкції є суттєвими: за навмисні порушення зобов'язань щодо повідомлення або співпраці передбачено штраф до 500 000 швейцарських франків (із семирічним строком давності), за невиконання остаточного рішення наглядового органу – до 100 000 швейцарських франків.

Паралельна реформа AMLA здійснює якісне розширення кола підзвітних суб'єктів шляхом включення до нього «консультантів» – категорії, що раніше майже повністю залишалась поза межами антилегалізаційного регулювання. Консультантами в розумінні закону є фізичні та юридичні особи, що на професійній основі та від імені або в інтересах третіх осіб беруть участь у фінансових операціях у зв'язку з визначеними видами діяльності. Ці операції охоплюють: купівлю та продаж нерухомого майна; створення, заснування, управління та адміністрування юридичних осіб, зареєстрованих у Швейцарії, або будь-яких юридичних осіб за кордоном; внески до капіталу та розподіл із нього щодо неопераційних суб'єктів; купівлю та продаж юридичних осіб через неопераційні структури. Такий підхід цілеспрямовано усуває прогалину, неодноразово фіксовану FATF: нерегульовану роль гейткіперів – юристів, нотаріусів, бізнес-консультантів – у потенційно ризикових операціях.

Нові зобов'язання консультантів включають ключові елементи системи належної перевірки: ідентифікацію клієнта, встановлення КБВ, документування операцій, а також з'ясування мети і контексту транзакцій з посиленою перевіркою у випадках підвищеного ризику. Консультанти зобов'язані невідкладно повідомляти MROS про підозри щодо відмивання коштів або фінансування тероризму та вступати в членство саморегулюючої організації, що

здійснюватиме нагляд за дотриманням ними вимог AMLA і матиме право накладати санкції; FINMA веде публічний реєстр афільованих консультантів. Для адвокатів і нотаріусів встановлено спеціальні гарантії збереження адвокатської таємниці: контрольні функції можуть виконуватись виключно незалежними кваліфікованими фахівцями, а розкриття захищеної інформації допускається лише за наявності об'єктивних ознак порушення зобов'язань, абсолютної необхідності розкриття та зняття режиму таємниці судом або самим клієнтом. Реформа в сукупності є системним зсувом регуляторної парадигми: від традиційного зосередження всіх AML-зобов'язань на фінансових посередниках до розподіленої відповідальності, що охоплює всіх, хто сприяє структуруванню юридичних осіб і здійсненню транзакцій із підвищеним ризиком.

Суд ЄС визначає межі застосування санкційних списків третіх країн при відмові в доступі до платіжних рахунків [7]

11 червня 2026 року Суд Європейського Союзу (четверта палата) виніс рішення у справі C-81/24 «Jenec» за клопотанням про попередній висновок від Окружного суду м. Марібор (Словенія) у справі LH проти OTP banka d.d.. Справа розкриває одну з центральних колізій сучасної AML-архітектури ЄС: баланс між правом споживача на відкриття платіжного рахунку, закріпленим Директивою 2014/92/ЄС, та зобов'язаннями банків у сфері ПВК/ФТ відповідно до Директиви 2015/849/ЄС (4-та Директива ПВК/ФТ). Фактичні обставини: у 2022 році словенський банк відмовив споживачу LH у відкритті базового платіжного рахунку, посилаючись на його включення до санкційного списку Управління з контролю іноземних активів Міністерства фінансів США (OFAC). При цьому LH не мав жодного обвинувального вироку за правопорушення, що стало підставою для внесення до списку OFAC, в той час як ані ООН, ані ЄС, ані Словенія не запровадили стосовно нього будь-яких обмежувальних заходів. Словенський суд звернувся до Суду ЄС із ключовим питанням: чи допускає стаття 16(4) Директиви 2014/92/ЄС у взаємозв'язку з Директивою 2015/849/ЄС, щоб держави-члени зобов'язували банки відмовляти у відкритті базового платіжного рахунку виключно на підставі факту перебування споживача в санкційному списку третьої держави?

Відповідь Суду ЄС є однозначною: право ЄС не допускає автоматичної відмови у відкритті базового платіжного рахунку на підставі одного лише факту включення особи до списку OFAC або аналогічного переліку третьої країни. Суд підтвердив, що кожен споживач, який законно проживає в ЄС, має право на доступ до базового платіжного рахунку відповідно до Директиви 2014/92/ЄС, що охоплює депозити, зняття коштів, перекази та карткові платежі. Водночас це право не є абсолютним: воно підлягає узгодженню з нормами ЄС і національного права у сфері ПВК/ФТ. Ключовий висновок рішення такий: включення до санкційного списку OFAC може бути релевантним фактором при оцінці ризику, однак лише одним із факторів, а не автономною підставою для відмови. Банк зобов'язаний провести індивідуальну оцінку конкретного ризику відмивання коштів або фінансування тероризму, пов'язаного з цим клієнтом.

Правовий стандарт, встановлений Судом, ґрунтується на принципах пропорційності та індивідуальної оцінки: відмова у відкритті базового платіжного рахунку є сумісною з правом ЄС лише тоді, коли після проведення конкретної та індивідуалізованої оцінки банк доходить висновку, що він не може ефективно управляти виявленим ризиком за допомогою пропорційних заходів, з урахуванням природи та масштабу установи. Суд ЄС також зазначив, що обмежений функціонал базового платіжного рахунку є юридично значимою обставиною, що може знижувати відповідний ризик, хоча Суд не виключив можливості того, що навіть базовий рахунок у конкретному випадку може становити ризик, яким банк не може адекватно управляти. Практичний наслідок рішення: банки зобов'язані документувати, чому конкретний

[7] https://infocuria.curia.europa.eu/tabs/jurisprudence?sort=DOC_DATE-DESC&searchTerm=%22C-81%2F24%22&publishedId=C-81%2F24

клієнт становить специфічний ризик і чому цей ризик не може бути нейтралізований пропорційними заходами – посилання виключно на іноземний санкційний список принципово недостатньо.

Значення цього рішення виявляється щонайменше в трьох вимірах. По-перше, воно захищає ефективність права ЄС на доступ до базових банківських послуг: базовий платіжний рахунок є необхідним інструментом участі в економічному та соціальному житті, а не привілейованим фінансовим продуктом. По-друге, рішення обмежує автоматичний екстериторіальний ефект санкцій третіх країн у правовому порядку ЄС: включення до санкційного списку OFAC може мати значення, але не визначає автоматично правову позицію за правом ЄС. По-третє, рішення підтверджує центральне місце принципів пропорційності та індивідуальної оцінки в антилегалізаційному праві ЄС: зобов'язання з комплаєнсу не можуть бути зведені до механічного виключення без реального аналізу ризиків.

Для практиків у сфері ПВК/ФТ рішення у справі «Jenec» встановлює чіткий стандарт підзвітності: банки, що діють на території ЄС, повинні мати задокументовану систему індивідуальної оцінки ризиків, здатну обґрунтувати відмову в наданні послуг не лише посиланням на санкційний перелік третьої країни, але й конкретним аналізом того, чому виявлений ризик не піддається управлінню пропорційними інструментами. Це рішення є черговим підтвердженням того, що автоматизовані скринінгові системи, які генерують відмови виключно на підставі санкційного статусу без подальшого аналізу ризику, не відповідають вимогам права ЄС, особливо щодо осіб, включених до санкційних списків третіх країн за відсутності паралельних заходів з боку ЄС, ООН або держав-членів.

Санкції

Оновлення санкційного списку Мінфіну США [8]

У червні 2026 року Управління з контролю за іноземними активами Міністерства фінансів США завдало потужного удару по фінансовій інфраструктурі Ірану, додавши до списку спеціально позначених громадян та підсанкційних осіб одразу чотири ключові платформи для торгівлі криптовалютами. Під обмеження потрапили найбільша іранська біржа Nobitex, а також Wallex, Bitpin та Ramzinex. Це рішення не є формальним жестом – воно фактично відрізає зазначені майданчики від глобальної фінансової системи, блокує всі їхні активи на території США та створює катастрофічні ризики для будь-якої фінансової установи у світі, яка продовжить із ними співпрацювати.

Головна проблема, яку намагається вирішити американський регулятор, полягає в тому, що іранський режим системно використовує криптовалютні біржі для обходу міжнародних торговельних обмежень, фінансування терористичних угруповань та легалізації доходів від кіберзлочинності. Nobitex, яка контролює понад п’ятдесят відсотків усього вхідного трафіку цифрових активів в Ірані, стала справжнім фінансовим хабом для Корпусу вартових ісламської революції та пов’язаних із ним кіберзлочинців. Через цю біржу державні кошти, номіновані в знеціненому та ізольованому іранському ріалі, конвертуються у стейблкоїни, прив’язані до долара, й отримують доступ до міжнародної ліквідності в обхід системи SWIFT.

За даними регуляторних органів, Nobitex діяла в тісній координації з Центральним банком Ірану, забезпечуючи доступ до сотень мільйонів доларів у вигляді стейблкоїнів. Це дозволяло режиму створювати паралельну економічну інфраструктуру, повністю нейтралізуючи класичні банківські блокади. Але навіть це не найтривожніший аспект. Біржа слугувала прямим розрахунковим центром для спеціалізованих злочинних мереж, зокрема для операторів програм-вимагачів, афілійованих з іранською державою. Ці хакери отримували викупи від жертв по всьому світу, спрямовували кошти на гаманці, підконтрольні біржі, де ті

[8] https://fincrimecentral.com/us-sanctions-iranian-crypto-exchanges-nobitex/
https://ofac.treasury.gov/recent-actions/sanctions-list-updates

змішувалися із загальним пулом ліквідності, а потім конвертувалися у фіат або альтернативні токени. Така схема робить неможливим відстеження походження коштів стандартними засобами комплаєнсу.

Особливої уваги заслуговує архітектура всієї іранської «криптомережі». Вона не обмежується однією платформою. Wallex, друга за розміром біржа регіону, контролювала приблизно дванадцять відсотків вхідних потоків віртуальної валюти та слугувала резервним каналом для великих транзакцій. Bitpin та Ramzinex разом забезпечували дедалі більші обсяги, причому лише Ramzinex із моменту свого заснування провела транзакції на суму понад два з половиною мільярди доларів. Це не просто окремі біржі – це взаємопов'язана надлишкова система, спроєктована так, щоб витримувати точкові регуляторні удари. Якщо одна платформа блокується, кошти миттєво перетікають через інші.

Найтривожнішим у цій історії є глибоке проникнення правлячої політичної еліти в управління цими майданчиками. Розслідування показали, що кілька співзасновників та ключових технічних фахівців, зокрема керівник блокчейн-напрямку Сеєд Мохаммад Агамір Алі підтримує прямі зв'язки з найближчим оточенням верховного лідера Ірану. Це означає, що корпоративні цілі платформ підпорядковані стратегічним фінансовим потребам держави. Під час міжнародних конфліктів або внутрішньої нестабільності ці біржі активно ініціювали переміщення капіталу, виводячи величезні обсяги багатства режиму за кордон для захисту від замороження активів. Вражає, що цей процес тривав навіть під час державних відключень інтернету в Ірані – платформи продовжували працювати через альтернативні канали.

Юридичним підґрунтям для блокування стали два виконавчі накази – 13224, спрямований проти міжнародного тероризму, та 13902, який цілеспрямовано б'є по фінансовому сектору економіки, що не виконує вимоги. Наслідки для будь-якої фінансової установи за межами США є абсолютними. Регуляторний механізм працює на засадах суворої відповідальності – організації можуть отримати величезні цивільні штрафи за обробку заборонених транзакцій навіть без доведення їхнього наміру чи обізнаності. Більше того, іноземні фінансові інституції, які свідомо проводять значні операції для цих бірж, ризикують бути повністю відрізаними від американської фінансової системи через вторинні санкції. Це змушує міжнародний бізнес обирати: або ризиковане співробітництво з регіональними майданчиками, або доступ до глобальної розрахункової мережі.

Для фахівців з протидії відмиванню коштів стаття наводить конкретні індикатори ризику. Серед них – аномальна активність на вкладених біржах, коли постачальники віртуальних активів відкривають рахунки під неоднозначними корпоративними назвами з обсягами, що дзеркалять великих комерційних гравців; великі надходження стейблкоїнів з некастодіальних гаманців з негайним спрямуванням на платформи в юрисдикціях високого ризику; збіг шляхів транзакцій з відомими гаманцями програм-вимагачів; використання VPN або Tor для доступу з регіонів, суміжних із підсанкційними територіями; та раптові сплески вихідних цифрових переказів у періоди геополітичної нестабільності.

Висновки:

- **Іран системно використовує криптобіржі** (Nobitex, Wallex, Bitpin, Ramzinex) як державний інструмент для обходу міжнародних торговельних обмежень, забезпечуючи конвертацію знеціненого ріалу в ліквідні стейблкоїни в обхід SWIFT.
- **Ці платформи безпосередньо обслуговують фінансові потоки** Корпусу вартових ісламської революції та афілійованих з Іраном угруповань програм-вимагачів, змішуючи злочинні доходи із загальним пулом ліквідності.
- **Архітектура іранської криптомережі є надлишковою та розподіленою:** друга за розміром біржа Wallex контролює 12% вхідного трафіку, а Ramzinex провела транзакції на понад $2,5 млрд, що робить систему стійкою до точкових ударів.
- **Ключові особи цих бірж мають прямі зв'язки з представниками найвищого політичного керівництва Ірану**, що підтверджує державний характер цієї фінансової інфраструктури.

Іран створив складну, керовану державою систему цифрових активів, яка дозволяє обходити традиційні банківські блокади. У відповідь США застосовують не лише чорні списки, а й потужні фінансові стимули для знищення цієї інфраструктури зсередини. Для міжнародних фінансових інституцій це означає один однозначний висновок: будь-яка взаємодія з іранськими крипто-платформами тепер не просто ризикована, а смертельно небезпечна з точки зору регуляторних наслідків.

Звіти окремих інституцій та експертів

Наркотрафік нової ери: шлях до Європи [9]

Першого травня 2026 року іспанська цивільна гвардія, здійснюючи патрулювання неподалік від берегів Західної Сахари поблизу міста Дахла, отримала певну розвідувальну інформацію. Об'єктом уваги стало суховантажне судно «Arconian», яке ходило під прапором Коморських островів.

Коли спецпризначенці піднялися на борт, вони ще не усвідомлювали, що стали свідками найбільшого в історії вилучення кокаїну. За металевими дверима, яку охороняли шестеро озброєних чоловіків – п'ятеро громадян Нідерландів і один із Суринаму, – виявилася довжелезна галерея, повністю заставлена тюками з кокаїном. Загальна вага перевищила 30,2 тонни. Це більше, ніж багато країн вилучають за кілька років сукупно. І що особливо важливо, ця подія сталася не біля берегів Колумбії чи Мексики, які традиційно вважаються епіцентром світової торгівлі кокаїном, а біля узбережжя Африки, неподалік від Західної Сахари.

Для того щоб зрозуміти справжні масштаби цього відкриття, варто поглянути на ширший контекст трансатлантичного наркотрафіку. Починаючи приблизно з 2019 року обсяги кокаїну, що прямують через Західну Африку до Європи, зазнали вибухового зростання. Це пов'язано одразу з кількома чинниками. По-перше, світовий ринок кокаїну досяг небачених масштабів через стрімке нарощування виробництва в країнах Андського регіону. По-друге, Західна Африка стала дедалі привабливішою для витончених злочинних мереж завдяки прогалинам у системах державного управління, слабкому правосуддю та, що дуже важливо, масовим інвестиціям у портову інфраструктуру, яка тепер з'єднує цей регіон з основними світовими ринками.

Дані міжнародних правоохоронних органів свідчать про семикратне збільшення вилучень кокаїну на маршрутах з Латинської Америки до Західної Африки між 2022 та 2024 роками, причому середній розмір однієї партії на неконтейнерних суднах зріс з 2,4 тонни у 2024-му до 5,6 тонни у 2025 році. Але парадокс полягав у тому, що вилучення на зворотному шляху – з Африки до Європи – залишалися приголомшливо низькими. Європейські порти, насамперед Антверпен та Роттердам, повідомляли про зменшення обсягів конфіскацій, хоча роздрібні ціни на кокаїн у Нідерландах та Бельгії впали з 28 000 євро за кілограм у 2021 році до приблизно 15 000 у 2025 році, а в Іспанії спостерігалася схожа тенденція. Таке падіння цін на тлі скорочення вилучень є класичною ринковою аномалією, що свідчить про структурний надлишок пропозиції та, відповідно, про те, що величезні обсяги кокаїну якимось чином уникають виявлення.

Захисники правопорядку швидко встановили, що за цим перевезенням, імовірно, стоїть Джос Лейдеккерс – нідерландський наркобарон, відомий у кримінальному світі під прізвиськом «Bolle Jos». Від середини 2022 року Лейдеккерс облаштувався в Сьєрра-Леоне, де, уникаючи екстрадиції, створив складну логістичну мережу. Його зв'язки простягаються від Суринаму (звідки походять його коріння) до Туреччини, де він довгий час жив і де залишився його брат

[9] https://globalinitiative.net/wp-content/uploads/2026/06/Josef-Skrdlik-Sarah-Fares-Lucia-Bird-The-Arconian-operation-Anatomy-of-a-record-Atlantic-cocaine-shipment-GI-TOC-June-2026.pdf

Гаррі, якого неодноразово заарештовували, та шурин Абдуллах Алп Устун, який навіть відвідував його в Сьєрра-Леоне.

Важливо зазначити, що, на думку слідства, ця рекордна партія навряд чи належала виключно Лейдеккерсу. Її величезний обсяг свідчить про так званий пулінг – об'єднання ресурсів кількох різних злочинних угруповань, де Лейдеккерс виступав як логістичний провайдер, який забезпечував транспортування, страхування та безпеку, а частка вантажу могла належати різним «клієнтам» з європейських наркоринків.

Розслідування, проведене Global Initiative Against Transnational Organized Crime (GI-TOC), не обмежилося вивченням одного лише «Arconian». Дослідники застосували змішану методологію, що поєднувала аналіз відкритих даних автоматичної ідентифікаційної системи (AIS), супутникове відстеження, вивчення суднових реєстрів (Equasis), корпоративних баз даних (Sayari, Nexis, OpenCorporates), а також інтерв'ю з портовими працівниками, очевидцями та представниками правоохоронних органів кількох країн.

Зіставлення цих даних дозволило виявити щонайменше вісім суден, які демонстрували майже ідентичну поведінку, але найяскравішими прикладами стали два інші судна – «White Eagle» та «White Labelle», хоча кокаїн на них безпосередньо не вилучали.

Ключова ланка в цьому ланцюжку – Сьєрра-Леоне. Хоча уряд цієї країни на офіційному брифінгу 20 травня 2026 року заперечував, що «Arconian» завантажували у Фрітауні, сукупність доказів свідчить про зворотне. Фотографії, отримані від джерел, наближених до мережі Лейдеккерса, показують «White Eagle» біля причалу Єлизавети II, а поруч із судном стоять кілька величезних мішків. Один із портових працівників, який обслуговував судно, розповів слідству, що бачив білий порошок усередині цих мішків. Інша фотографія, зроблена вночі, демонструє колону поліцейських машин, припаркованих поруч, що може свідчити про охорону або, навпаки, про присутність корумпованих правоохоронців. Крім того, відео, нібито зняте всередині «White Eagle», показує філіппінців, одного з яких ідентифікували як капітана судна.

Важливо зазначити, що місцеві рибалки та мешканці прибережних громад Сьєрра-Леоне, опитані в серпні 2025 року, одностайно стверджували, що знаходити плавучі пакунки кокаїну в морі стало звичною справою, особливо з 2022 року, коли Лейдеккерс оселився в країні. Ці пакунки, імовірно, є наслідками помилок під час перевантаження з судна на судно або перекидання невеликих човнів. За даними міжнародних правоохоронних органів, лише за шість місяців, що передували затриманню «Arconian», біля узбережжя Сьєрра-Леоне відбулися дві передачі по 10 тонн кокаїну, а ще 14 тонн відстежили до Гани у лютому 2026 року. Це означає, що сумарний обсяг (34 тонни) навіть дещо перевищує те, що було знайдено на борту «Arconian», що підтверджує наявність достатніх складських запасів у регіоні.

Щодо географії, то дослідження виокремлює кілька критичних точок. Перша – це Північна Африка, зокрема Лівія. Хоча «Arconian» офіційно прямував до Бенгазі на сході країни, реакція лівійських політичних сил виявилася показовою. Прем'єр-міністр уряду національної єдності в Триполі Абд аль-Хамід Дбейба наказав провести розслідування, тоді як східні органи влади, підконтрольні Лівійській арабській армії, спробували подати цю справу як політично мотивовану маніпуляцію, пригрозивши навіть дипломатичними заходами проти Іспанії.

Європейське джерело з безпеки повідомило, що на сході Лівії очікували надходження великої партії кокаїну в часовому проміжку, який збігається з подорожжю «Arconian», хоча прямий зв'язок із цим судном підтвердити не змогли. Джерело GI-TOC на місцях у східній Лівії додало, що, хоча розмір партії викликає подив, цей випадок трапився в чутливий момент, коли високопосадовці, які захищають наркотрафік у регіоні, намагаються відбілити свою репутацію, і таке велике відправлення могло бути останньою спробою проштовхнути величезний вантаж перед зміною маршрутів та партнерств

Друга ключова точка – Канарські острови. Злочинні мережі використовували цей архіпелаг як зручну зупинку ще з 2020-2021 років, коли балканські угруповання вивозили кокаїн із Сьєрра-

Леоне на вітрильниках до Гран-Канарії. Іспанська влада зафіксувала різке зростання трафіку в напрямку архіпелагу з початку 2024 року, а у вересні 2025 року на островах виявили лабораторію з переробки кокаїну.

Нарешті, третя важлива ланка – це Філіппіни. Десятки філіппінських громадян виконують роль як робочих, так і ключових операційних менеджерів. Один із них, за інформацією з його профілю LinkedIn, раніше працював операційним менеджером у судноплавній компанії на Філіппінах. Щомісяця він переказував своїй родині десятки тисяч доларів через Western Union. Рекрутингом, імовірно, займалася філіппінка, яка проживає в Сьєрра-Леоне та регулярно відвідує резиденції Лейдеккерса. Коли «White Eagle» та «White Arrow» були покинуті в Надорі та Бенгазі, їхні філіппінські екіпажі (16 та 15 осіб відповідно) опинилися в пастці, що є типовим явищем у цьому бізнесі, де люди стають розхідним матеріалом.

Отже, операція «Arconian» – це не просто рекордне вилучення. Це анатомічний зріз цілої екосистеми. Вона демонструє, як кокаїн, вироблений в Андах, через Суринам і Гаяну потрапляє в Західну Африку, де накопичується в країнах із крихкими державними інституціями, як-от Сьєрра-Леоне та Гвінея-Бісау. Далі він вирушає на північ, уникаючи великих європейських портів, і розвантажується біля берегів Марокко, Канарських островів чи Лівії на швидкісні катери, які доставляють його безпосередньо на споживчі ринки.

Те, що європейські ціни на кокаїн падають, а вилучення в портах скорочуються, отримало своє пояснення. Європейські правоохоронці виявилися неготовими до тієї гнучкості, яку демонструють злочинні мережі, перемістивши логістику з контейнерних терміналів Роттердама у відкрите море. Перехоплення «Arconian», безсумнівно, є величезним ударом по мережі Лейдеккерса та, ймовірно, тимчасово підірве їхню впевненість. Але, як свідчить аналіз повторних рейсів інших суден, цей механізм уже відпрацьований до автоматизму. Він продовжуватиме діяти, доки зберігатимуться три умови: величезний попит у Європі, слабкість контролю в портах Західної Африки та існування юрисдикцій, готових за гроші закривати очі.

Висновки:

- **Нова домінуюча логістична модель.** Кокаїн вивозять із Західної Африки до Європи не через великі порти, а на невеликих вантажних суднах, які розвантажуються в морі поблизу Канарських островів, узбережжя Марокко чи Лівії, передаючи вантаж швидкісним катерам.
- **Сьєрра-Леоне як хаб Європи.** Ця невелика країна, де осів нідерландський наркобарон Джос Лейдеккерс, перетворилася на гігантський транзитний хаб. Місцеві рибалки регулярно знаходять пакунки кокаїну в морі.
- **Системне використання «зручних прапорів» та спільних управлінських структур.** Три основні судна, задіяні в цій схемі мають спільних менеджерів — німецьку компанію з Фленсбурга та турецьку компанію з Газіантепу. Це свідчить про довгострокове планування та консолідацію ресурсів у межах однієї злочинної мережі.
- **Філіппінські екіпажі як вразлива ланка та маркер.** Усі судна мережі комплектуються філіппінськими моряками, які часто працюють у рабських умовах, не мають змоги залишити. Наявність філіппінської команди може бути індикатором для правоохоронців.

Як шахраї використовують ЧС-2026 для викрадення особистих даних[10]

У той час як світ із нетерпінням чекає на старт Чемпіонату світу з футболу 2026 року, готуючись до видовищних матчів і мільйонних натовпів уболівальників, у тіньовому сегменті інтернету розгорнулася не менш масштабна кримінальна кампанія.

[10] https://www.occrp.org/en/news/as-the-2026-world-cup-looms-a-shadow-tournament-of-cyber-fraud-begins
https://www.ic3.gov/PSA/2026/PSA260527

За даними OCCRP та Федерального бюро розслідувань США, кількість підроблених вебсайтів, що імітують офіційні ресурси Міжнародної федерації футболу (FIFA), уже сягнула приблизно 4300, і це лише ті, що вдалося виявити спеціалістам із кібербезпеки. Ситуація стала настільки загрозливою, що наприкінці травня 2026 року ФБР випустило офіційне публічне попередження (PSA), у якому прямо заявило: зловмисники проводять масовані атаки на вебсайт FIFA, використовуючи очікування чемпіонату для виманювання персональних даних і грошей.

Йдеться не просто про дрібне шахрайство з продажем фальшивих квитків – хоча й воно теж є частиною схеми. Перед нами багатошарова, технологічно зріла злочинна екосистема, що включає фальшиві туристичні пакети, підроблені мерчендайзингові портали, нелегальні беттингові застосунки, які крадуть фінансові дані, а також стрімінгові програми, що встановлюють на пристрої жертв шпигунське програмне забезпечення.

Як зазначає Девід Гонсалес Куаутле, керівник відділу досліджень та підвищення обізнаності в компанії ESET, кіберзлочинці діють за сезонним принципом, прив'язуючись до тем, які хвилюють суспільство. Чемпіонат світу з футболу – це «ідеальна принада», яка дозволяє їм закинути найширші сіті. Уболівальники, осліплені передчуттям свята, значно менш пильні, ніж зазвичай, і охоче вводять свої банківські реквізити на сайтах, які виглядають абсолютно автентично.

Основним інструментом атаки є метод, відомий як тайпсквотинг (typosquatting) заснований на помилках користувачів під час введення URL-адрес. Зловмисники реєструють домени, які відрізняються від справжнього www.fifa.com на одну-дві літери, використовують альтернативні домени верхнього рівня, або створюють складні композитні адреси. ФБР опублікувло список подібних шахрайських сайтів. Як можна побачити, зловмисники використовують не лише класичні помилки (подвоєння літер, заміна «i» на «l», зміна порядку букв, але й цілі фрази, що імітують працевлаштування («jobs», «hiring», «careerhub») або продаж квитків («ticket», «sale»). Це означає, що шахраї орієнтуються на різні категорії жертв: одні шукають квитки, інші – роботу на чемпіонаті, треті – просто хочуть переглянути розклад.

Але найтривожнішим аспектом є те, що візуально ці сайти є майже ідеальними копіями офіційного порталу. Вони мають ті самі логотипи, фірмові кольори, типографіку, структуру навігації та навіть підроблені сертифікати безпеки. Експерти ESET провели експеримент: вони проаналізували вибірку з десяти таких фальшивих порталів і виявили, що більшість із них не є одноразовими пастками, а працюють як повноцінні центри збору даних. Коли жертва вводить своє ім'я, домашню адресу, номер телефону, електронну пошту, а головне – банківські реквізити або дані кредитної картки, ця інформація не йде на купівлю квитка, а одразу потрапляє до рук зловмисників. Далі можливі кілька сценаріїв: перший – безпосереднє списання коштів, другий – продаж цих даних на чорному ринку третім особам, третій, найнебезпечніший – використання отриманої персональної інформації (PII) для створення нових акаунтів на ім'я жертви, отримання кредитів, оформлення позик або навіть для шантажу.

Ключовий момент, на який звертають увагу і ФБР, і ESET, полягає в тому, що традиційний маркер безпеки – «зелений замок» у браузері, який свідчить про наявність SSL-сертифіката, – більше не є надійним індикатором. Сьогодні будь-який шахрай може отримати безкоштовний або дешевий SSL-сертифікат для свого фейкового сайту, і браузер показуватиме той самий значок замка, що й на справжньому fifa.com. Це руйнує базове уявлення пересічного користувача про безпеку в мережі. Людина звикла думати: якщо є замок – значить, сайту можна довіряти. Але тепер це не так. Зловмисники використовують цю психологічну пастку, додаючи до своїх ресурсів підроблені сертифікати або навіть справжні, видані на фіктивні компанії.

Ще одним тривожним трендом, який фіксують аналітики, є локалізація атак. Якщо на початковому етапі переважна більшість фальшивих доменів була англомовною, то тепер з'являються сайти іншими мовами. Це свідчить про те, що шахрайські мережі діють

регіонально, створюючи копії для вболівальників з Німеччини, Франції, Іспанії, країн Латинської Америки. Вони використовують місцеві платіжні системи, враховують культурні особливості та навіть пишуть тексти звернень без граматичних помилок – те, що раніше могло видати підробку, нині практично зникло. У деяких випадках шахраї створюють цілі багатомовні сайти, де користувач може обрати свою мову, що ще більше підвищує рівень довіри.

Не менш небезпечним є канал мобільних застосунків. ФБР та OCCRP попереджають про існування фальшивих додатків, які маскуються під портали трансляцій матчів або букмекерські платформи. Коли користувач встановлює такий застосунок, він запитує дозволи, які далеко виходять за межі необхідних: доступ до контактів, SMS, геолокації, камери, мікрофона, а іноді – навіть прав адміністратора. Після отримання цих дозволів додаток може непомітно надсилати всі введені дані на сервер зловмисників, перехоплювати банківські повідомлення, робити скріншоти екрану або активувати камеру без відома власника. Окремою категорією є підроблені застосунки для ставок: вони виглядають як звичайні беттингові платформи, але замість виплат виграшів просто крадуть гроші та дані.

Фінансові втрати від придбання неіснуючого квитка – це лише верхівка айсберга, і, можливо, найменша проблема. Справжньою катастрофою для жертви стає довготривала компрометація її цифрової ідентичності. Отримавши доступ до персональних даних, зловмисники можуть протягом багатьох місяців або навіть років використовувати їх для відкриття нових кредитних ліній, реєстрації фіктивних компаній, отримання медичних послуг або навіть участі в схемах відмивання грошей. Жертва може дізнатися про це лише тоді, коли отримає лист від колекторської агенції або вимогу сплатити податки за «свій» бізнес, про який вона ніколи не чула.

У відповідь на цю загрозу ФБР опублікувало чіткі рекомендації, які ґрунтуються на тому, що єдиним абсолютно надійним способом потрапити на справжній сайт ФІФА є ручне введення адреси fifa.com безпосередньо в адресний рядок браузера. Не варто використовувати пошукові системи, оскільки перші результати часто є платними «спонсорованими» посиланнями – саме там шахраї купують рекламу, щоб перенаправляти трафік на свої підробки. Якщо ви все ж користуєтеся пошуковою системою, уникайте будь-яких результатів із позначкою «Реклама» або «Спонсоровано». Перевіряйте, що URL закінчується саме на .com і що він правильно введений як www.fifa.com. Не клікайте на жодне посилання, чия адреса відрізняється від канонічної. Крім того, фахівці радять використовувати закладки або список обраного для входу на критично важливі сайти, а не покладатися на результати пошуку чи рекламні банери. Для доступу до субдоменів, наприклад plus.fifa.com, варто спочатку зайти на головну сторінку fifa.com і вже звідти переходити за внутрішніми посиланнями, а не вводити адресу субдомену вручну.

Висновки:

- **Масштабна кампанія.** Станом на травень 2026 року кіберзлочинці створили близько 4300 фальшивих доменів, що імітують офіційний сайт FIFA, використовуючи незначні зміни в написанні адреси для обману вболівальників.
- **Крадіжка даних як основна мета.** Підроблені сайти не лише продають фальшиві квитки, але й системно збирають персональну та банківську інформацію, яка згодом використовується для відкриття акаунтів на ім’я жертви, оформлення кредитів або продажу на чорному ринку.
- **Традиційні маркери безпеки більше не працюють.** Наявність SSL-сертифіката в адресному рядку браузера більше не гарантує легітимність сайту, оскільки зловмисники навчилися клонувати або отримувати справжні сертифікати на підроблені ресурси.
- **Багатовекторність загроз.** Окрім вебсайтів, шахраї активно використовують фальшиві мобільні застосунки, які запитують надмірні дозволи та встановлюють шпигунське програмне забезпечення, а також локалізують атаки різними мовами для окремих країн.

Окрема порада стосується реклами. Шахраї часто купують таргетовану рекламу в соціальних мережах і пошукових системах, яка веде на підроблені сайти. Перед тим, як натиснути на будь-який банер, навіть якщо він виглядає привабливо, наведіть курсор на посилання, щоб побачити справжню URL-адресу. Найчастіше виявляється, що вона не має жодного стосунку до FIFA. Також не варто переходити за посиланнями з небажаних електронних листів, повідомлень у месенджерах або SMS, навіть якщо вони виглядають так, ніби надіслані офіційними представниками чемпіонату. FIFA ніколи не розсилає листи з проханням ввести банківські дані.

ФБР також закликає звертати увагу на якість графіки та тексту. Хоча сучасні підробки дуже реалістичні, все ж іноді можна помітити дрібні невідповідності: нечіткі логотипи, граматичні помилки в малопомітних місцях, нестандартні шрифти або дивні URL-адреси. Якщо у вас виникла найменша підозра, не вводьте жодної особистої інформації. Краще витратити кілька додаткових секунд на перевірку, ніж потім місяцями розбиратися з наслідками крадіжки інформації.

Якщо ви або хтось із ваших знайомих усе ж стали жертвою такого шахрайства, ФБР наполегливо рекомендує негайно подати скаргу до Центру скарг на кіберзлочини (IC3) за адресою www.ic3.gov. Чим більше деталей ви надасте, тим вищою є ймовірність, що правоохоронні органи зможуть відстежити зловмисників і запобігти подальшим злочинам.

Таким чином, кожен уболівальник, який шукає квитки, планує поїздку або просто хоче дізнатися розклад матчів, має розуміти: уважність до URL-адреси, недовіра до реклами та звичка вручну вводити адреси – це не параноя, а необхідний мінімальний захист у світі, де навіть «зелений замок» більше не є гарантією безпеки. Перемога над кібершахраями починається не з роботи спецслужб, а з одного простого звичного руху: зупинитися, перевірити і подумати, чи справді той сайт, на який ви збираєтесь натиснути, є тим, за кого себе видає.

Як російські військові опиняються на борту танкерів «тіньового флоту» [11]

У міжнародному судноплавствф, де під прапорами зручних юрисдикцій ховаються танкери з російською нафтою, формується новий, тривожний феномен.

Розслідування, проведене консорціумом європейських медіа OCCRP, Dossier Center та Follow the Money, виявило системну практику: на борту суден, які транспортують санкційну російську нафту, постійно присутні люди з військовим або силовим минулим. Їхня роль – не охорона в класичному розумінні, а цілодобовий нагляд за діями капітанів та іноземних екіпажів, особливо в моменти, коли судна можуть бути зупинені європейськими правоохоронцями. Цих людей називають «наглядачами» (watchmen), і їхнє існування розмиває межу між комерційним судноплавством і військовою логістикою.

Хто ж ці люди? Їхній профіль разюче відрізняється від звичайних моряків. Якщо в списках екіпажу вони значаться як «техніки» або «позаштатні» (supernumeraries), то реальне минуле свідчить про інше. Серед них – ветерани російських збройних сил, співробітники приватних військових компаній, зокрема відомого угруповання «Вагнер» та підсанкційного «Редуту», а також колишні співробітники спецпідрозділів.

У звіті наведено характерний приклад: Андрій, колишній командир елітного російського повітряно-десантного підрозділу, ветеран бойових дій у Чечні, що працював особистим охоронцем і обіймав керівні посади в корпоративній безпеці. Його завдання на борту танкера, за власними словами, полягало в тому, щоб «спостерігати, своєчасно доповідати і, так би мовити, не дозволяти судну відхилятися від курсу». Інший фігурант розслідування, Михайло,

[11] https://www.occrp.org/en/investigation/eyes-on-the-crew-the-russian-watchmen-aboard-moscows-sanctioned-shadow-fleet-tankers

закінчив провідний навчальний центр офіцерів для ВДВ і вісім років провів у Сирії, очолюючи службу безпеки приватного військового підрядника. На борту санкційного танкера він був записаний як «технік», однак його справжня функція – моніторинг екіпажу, капітана та старшого помічника.

Журналісти використали метод прихованого інтерв'ю, видаючи себе за рекрутерів, які шукають охоронців для майбутніх рейсів тіньового флоту. Це дозволило отримати безцінні свідчення з перших вуст. Андрій, спілкуючись у відеодзвінку з «рекрутером», пояснив, що його місія полягала в тому, щоб капітани, особливо під час ризику огляду європейськими службами, не «піддавалися» і не робили «неправильних дій». Він відверто порівнював поведінку капітанів: одні трималися правильно, інші – «здавали позиції». Іншими словами, присутність наглядача мала гарантувати, що судну не буде змінено курс, не будуть надані «вигідні Заходу» свідчення чи допущена співпраця з правоохоронцями. Михайло доповнив цю картину, зазначивши, що він виявляв, «хто здає інформацію, на кого вони працюють, які дані йдуть з корабля на берег – індійській владі чи, можливо, навіть країнам НАТО». Це свідчить про те, що російські наглядачі виконують не лише функцію стримування, а й контррозвідувальну роль на борту, відстежуючи потенційних інформаторів серед іноземних моряків.

Використовуючи витік даних із 757 танкерів тіньового флоту за період із січня 2023 по квітень 2026 року, дослідники ідентифікували 83 особи, які підпадають під опис «наглядачів». Всі вони – росіяни, які працювали разом із переважно іноземними екіпажами. Їхні подорожі різко активізувалися влітку 2025 року, після інцидентів в Естонії, коли було затримано один танкер і майже проведено обшук на іншому. Однак, починаючи з січня 2026 року, кількість таких подорожей почала знижуватися – причина залишається предметом дискусій аналітиків. Найчастіше маршрути цих суден пролягали з російських портів Балтійського моря через Середземне море до Індії – одного з ключових напрямків для російського нафтового експорту в умовах санкцій.

Серед ідентифікованих наглядачів виділяються такі постаті, як Юрій Ржевський, 52-річний ветеран ПВК «Вагнер», який воював у Сирії командиром відділення та інженером-сапером під позивним «Поруччик». У листопаді 2025 року він працював на санкційному танкері Selva під прапором Оману. Інший приклад – Євген Скороваров, 45 років, який служив у спеціальному підрозділі швидкого реагування російської митної служби. Хоча він заперечував роботу в морській безпеці, його профіль у російському месенджері містив фото на борту великого судна, а дата народження збігалася з даними в суднових ролях. Ці приклади ілюструють, як державні структури росії, включно з митницею та збройними силами, делегують своїх колишніх або діючих співробітників для контролю над «тіньовим флотом».

Роль наглядачів не обмежувалася пасивним спостереженням. Як зазначив один з них, «стандартні обов'язки» включають моніторинг дотримання екіпажем усіх протоколів, спрямованих на запобігання затриманню або захопленню судна. У європейських водах, наприклад, під час проходження Ла-Маншем або поблизу Данії, напруга сягала піку. Михайло розповів про інцидент із двома французькими лоцманами, які піднялися на борт. Один із них одразу запитав: «Хто ти? Чому ти на містку?». Михайло назвався радіоінженером, але змушений був покинути місток і простояти всю ніч на палубі, спостерігаючи за лоцманами крізь вікно, побоюючись провокації або висадки штурмової групи. Це свідчить про глибоку недовіру та готовність до силового протистояння.

Спілкування зі звичайними моряками, зокрема з «Леєм», який дев'ять місяців працював на танкері тіньового флоту, малює напружену атмосферу всередині суден. За його словами, росіяни з гордістю демонстрували фотографії з минулих військових місій, позуючи зі зброєю та бронетехнікою. Один із них мав «дуже високе звання». Згодом Лей дійшов висновку, що наглядачі мають не стільки моніторити, скільки бути сполучною ланкою між судном та російським військовим командуванням. Цю гіпотезу підтверджує аналітик Фінської служби безпеки (SUPO). Наймають їх, за даними розвідки України, російські охоронні компанії, як-от

Moran Security Group, яку Андрій вказав своїм останнім місцем роботи. Віктор Александров, ще один «наглядач» із числа колишніх вагнерівців, розмістив у соцмережах світлину 2021 року в камуфляжі в сирійському Хомсі – наочне свідчення географії «відряджень» цих людей.

Взаємини між наглядачами та іноземними екіпажами були складними. Лей зазначав, що багато моряків обурювалися: росіяни споживали багато їжі, але мало робили для роботи судна, створюючи враження, ніби «вони приїхали на свято, насолоджуючись пікніком». Водночас наглядачі самі скаржилися на недоречні умови: Михайло безуспішно просив індійського кухаря готувати «по-європейськи», оскільки гостра їжа була «неможливою до споживання». Навіть інтернет був суворо лімітований, чого вистачало лише для кількох щоденних звітів на берег.

Найбільш драматичний епізод, який сплив під час розмови – це атаки безпілотників з боку України. Андрій описав одну з таких атак. Деталі його розповіді збігаються з атакою на танкер Qendil під прапором Оману в грудні 2025 року. Судно щойно доставило нафту в порт Сікка (Індія) і поверталося до росії через Середземне море, коли його вразили дрони Служби безпеки України. Оприлюднені кадри з ураження показують яскраві вибухи на палубі. Андрій назвав подальшу подорож «випробуванням»: судно стало на ремонт біля турецького берега, де під час шторму втратило якір і було викинуте на мілину на півтора-два тижні. Примітно, що після цього удару – першого в історії ураження тіньового флоту на відстані 2000 кілометрів від кордонів України – в даних журналістів різко скоротилася кількість рейсів за участі «наглядачів».

Експерти досі сперечаються про причини такого падіння. За однією з версій, вартість розміщення «наглядачів» стала надто високою через падіння нафтових доходів росії. Інший погляд, висловлений представником однієї з західних розвідок, цинічніший: «Дешевше їх не розгортати, бо всі так чи інакше знають, що вони на борту». Натомість російська сторона, за традицією, відмовчується або заперечує факти: Андрій назвав будь-яку згадку про його роботу на тіньовому флоті «брехнею», а Михайло – що ніколи не був на нафтовому танкері.

Попри ці заперечення, зібрані докази формують тривожний пазл. Присутність військових на комерційних суднах, які перевозять санкційні вантажі, є не просто спробою убезпечити логістику. Це – частина гібридної стратегії, що дозволяє росії, не вдаючись до відкритої військової ескалації на морі, контролювати критичні ланки своєї економіки, залякувати іноземних моряків і підвищувати ціну будь-якої потенційної операції західних служб із затримання порушників санкцій.

Така практика створює нові ризики безпеки на морі, адже на борту танкерів, які, й без того, часто є екологічно небезпечними через вік та стан, тепер знаходяться люди, чиєю основною професією є війна.

Висновки:

- **Системна присутність військових «наглядачів»:** росія цілеспрямовано розміщує на борту танкерів свого «тіньового флоту» військових, які офіційно значаться як «техніки» або «позаштатні», але реально виконують функції контролю.
- **Контроль над іноземними екіпажами:** Головне завдання цих «наглядачів» – моніторинг капітанів та іноземних екіпажів, недопущення відхилення судна від курсу, а також виявлення потенційних інформаторів, які могли б співпрацювати з європейськими чи українськими структурами.
- **Реакція на європейські затримання та українські атаки:** Присутність «наглядачів» різко посилилася після інцидентів із затриманням танкерів Естонією у 2025 році, але суттєво знизилася після успішної атаки українських дронів на танкер Qendil у грудні 2025 року в Середземному морі.
- **Розмивання межі між комерцією та військом:** Залучення структур, пов'язаних із російськими оборонними відомствами, до супроводу цивільних нафтовозів створює небезпечний прецедент «гібридного» флоту, де військові елементи використовуються для обходу санкцій і тиску на міжнародне судноплавство.

Внутрішнє шахрайство як системний ризик для організацій: ключові висновки глобального дослідження ACFE 2026 [12]

Звіт є одним із найавторитетніших і наймасштабніших міжнародних досліджень у сфері внутрішнього шахрайства та відображає результати аналізу 2402 реальних випадків шахрайства, розслідуваних сертифікованими експертами з розслідування шахрайства у 143 країнах і територіях світу. Документ продовжує тридцятирічну серію досліджень «Звіт для країн світу» (Report to the Nations), яка протягом тривалого часу слугує міжнародним орієнтиром для оцінки масштабів, тенденцій та механізмів внутрішнього шахрайства, акумулювавши результати аналізу майже 25 тисяч розслідуваних випадків із сукупними втратами понад 65 млрд доларів США. У дослідженні внутрішнє шахрайство розглядається як одна з найбільш поширених та економічно руйнівних форм фінансової злочинності, що становить загрозу для будь-якої організації незалежно від її галузевої належності, форми власності, розміру чи географічного розташування. Автори наголошують, що проблема внутрішнього шахрайства виходить далеко за межі окремих фінансових втрат, оскільки впливає на стійкість організацій, інвестиційну привабливість, якість корпоративного управління, ефективність використання ресурсів та довіру до інституцій загалом.

Одним із ключових результатів дослідження є оцінка глобальної вартості шахрайства. На підставі накопичених даних ACFE робить висновок, що організації у світі щорічно втрачають близько 5% своїх доходів через різні форми внутрішнього шахрайства. З урахуванням обсягів світової економіки це еквівалентно потенційним глобальним втратам понад 5,5 трлн доларів США на рік. Досліджені у звіті випадки призвели до сукупних втрат понад 3,4 млрд доларів США, тоді як середній розмір збитків на один випадок становив 1,457 млн доларів США, а медіанний збиток – 104 тис. доларів США. Водночас кожен п’ятий випадок супроводжувався втратами понад 1 млн доларів США, що демонструє високий потенціал окремих шахрайських схем до завдання критичної шкоди організаціям.

Значна частина документа присвячена аналізу способів вчинення внутрішнього шахрайства. В основу аналізу покладено класифікаційну модель «Дерево шахрайства» (Fraud Tree), відповідно до якої всі форми внутрішнього шахрайства групуються у три базові категорії: привласнення активів, корупцію та шахрайство з фінансовою звітністю. Результати дослідження показують, що привласнення активів залишається найбільш поширеною формою внутрішнього шахрайства та зустрічається у дев’яти з десяти випадків. До цієї категорії належать викрадення готівки, активів компанії, маніпуляції з виплатами, закупівлями, рахунками та іншими господарськими процесами. Хоча такі схеми є найчастішими, вони характеризуються порівняно нижчим рівнем фінансових втрат. Натомість корупційні правопорушення були присутні майже у половині всіх випадків і включали конфлікти інтересів, хабарництво, відкатні схеми, змови під час закупівель та інші форми зловживання службовим становищем. Найбільш небезпечним видом правопорушень залишалося шахрайство з фінансовою звітністю, яке хоча й було зафіксоване лише у незначній кількості випадків, супроводжувалося найвищими фінансовими втратами та мало потенціал завдавати багатомільйонних збитків організаціям, інвесторам і кредиторам.

Автори приділяють окрему увагу тому факту, що сучасне внутрішнє шахрайство дедалі рідше обмежується одним видом протиправної діяльності. Майже 40% випадків включали одночасно декілька категорій шахрайства. Найпоширенішим поєднанням стало одночасне використання схем привласнення активів та корупції. Це свідчить про поступове ускладнення шахрайських механізмів та необхідність комплексного підходу до оцінки ризиків, який враховує взаємозв’язок різних форм економічних зловживань.

Суттєвий аналітичний блок присвячений підсхемам привласнення активів. Найбільш ризиковими з точки зору поєднання частоти виникнення та обсягу фінансових втрат визнано викрадення нефінансових активів, шахрайство у сфері закупівель і рахунків, а також

[12] https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2026/2026-report-to-the-nations.pdf

маніпуляції з платіжними документами та чеками. Дослідження демонструє, що сучасні шахрайські схеми дедалі більше інтегруються у звичайні бізнес-процеси та використовують прогалини у внутрішніх процедурах закупівель, погодження платежів, обліку активів та контролю витрат. Такий висновок є особливо важливим для організацій, які традиційно концентрують увагу на захисті фінансових операцій, недооцінюючи ризики, пов'язані з управлінням матеріальними активами, логістикою чи договірними відносинами.

Вагоме місце у звіті займає аналіз корупційних ризиків. Дослідження демонструє значні регіональні відмінності у поширеності корупційних схем. Найвищі показники зафіксовані у країнах Південної Азії, Азійсько-Тихоокеанського регіону, Латинської Америки та Близького Сходу. Водночас навіть у регіонах із порівняно нижчими показниками корупція залишається одним із ключових ризиків внутрішнього шахрайства. Автори роблять висновок, що корупція є не лише етичним чи правовим питанням, а й значним фактором фінансових втрат, який безпосередньо впливає на ефективність використання ресурсів організацій.

Окремий розділ присвячений тривалості шахрайських схем та її впливу на фінансові наслідки. Дослідження підтверджує стабільну закономірність, яка простежується протягом усіх років існування Report to the Nations: чим довше шахрайство залишається невиявленим, тим більших збитків воно завдає. Типова схема існувала близько одного року до моменту її викриття. Водночас шахрайства, які виявлялися протягом перших шести місяців, супроводжувалися відносно невеликими втратами, тоді як випадки, що залишалися невиявленими понад п'ять років, призводили до багатократного збільшення збитків. Найдовше зазвичай тривали схеми маніпулювання фінансовою звітністю, що пояснюється складністю їх виявлення та високим рівнем доступу правопорушників до фінансових процесів організації.

Для більш глибокого розуміння масштабів проблеми автори аналізують швидкість накопичення збитків від різних видів шахрайства. Було встановлено, що в середньому кожен місяць невиявленого шахрайства додає організації майже 10 тисяч доларів нових втрат. Найвищу швидкість завдання фінансової шкоди продемонстрували шахрайства з фінансовою звітністю та корупційні схеми. Крім того, суттєве значення має кількість учасників шахрайства. Змови за участю кількох осіб завдають організаціям набагато більших втрат та розвиваються значно швидше, ніж схеми, реалізовані одним правопорушником. Аналогічна тенденція спостерігається щодо службового становища правопорушника: чим вищу посаду займає особа, тим масштабнішими є наслідки її шахрайських дій.

Особливий інтерес для практиків становить розділ, присвячений механізмам виявлення шахрайства. Дослідження вкотре підтверджує, що найефективнішим інструментом викриття шахрайських схем залишаються повідомлення викривачів. Саме завдяки таким повідомленням було виявлено понад 40% усіх випадків. Понад половину повідомлень надали працівники організацій, тоді як значна частина інформації надходила від клієнтів, постачальників та інших зовнішніх контрагентів. Автори звертають увагу на поступову зміну каналів комунікації: традиційні телефонні гарячі лінії втрачають популярність, поступаючись електронній пошті та вебпорталам для повідомлень про порушення. Це свідчить про необхідність модернізації систем роботи з викривачами та адаптації їх до сучасних цифрових каналів взаємодії.

Документ також порівнює ефективність різних способів виявлення шахрайства. Результати показують, що проактивні інструменти, такі як внутрішній аудит, аналіз даних, автоматизований моніторинг транзакцій, перевірка документів та управлінський контроль, дозволяють виявляти шахрайство значно швидше та з меншими фінансовими наслідками. Натомість пасивні способи виявлення, включаючи випадкове викриття, втручання правоохоронних органів або зізнання правопорушника, зазвичай пов'язані з набагато більшими втратами. Таким чином, звіт переконливо демонструє економічну доцільність інвестицій у системи раннього виявлення шахрайства.

Важливий напрям дослідження стосується способів приховування шахрайських схем. Найчастіше правопорушники створювали або змінювали паперові документи, фальсифікували

електронні записи, приховували документи чи маніпулювали бухгалтерськими системами. Це свідчить про те, що сучасне шахрайство майже завжди супроводжується елементами маскування та потребує від організацій не лише контролю операцій, а й забезпечення цілісності документів, бухгалтерських записів та інформаційних систем.

Висновки:

- **Документ підтверджує, що найбільші фінансові втрати організаціям завдає не масове дрібне шахрайство, а порівняно рідкісні випадки шахрайства з фінансовою звітністю та корупції.** Необхідно приділяти особливу увагу контролям у сфері фінансової звітності, корпоративного управління та управлінських рішень, а не лише операційним ризикам.
- **Дослідження демонструє, що швидкість виявлення шахрайства є одним із головних факторів мінімізації збитків.** Організаціям доцільно інвестувати у проактивні механізми моніторингу, внутрішній аудит, аналіз даних та автоматизовані системи контролю, оскільки кожен додатковий місяць невиявленого шахрайства суттєво збільшує фінансові втрати.
- **Викривачі залишаються найефективнішим інструментом виявлення шахрайства.** Є необхідність у розвитку захищених багатоканальних механізмів повідомлення про порушення, включаючи вебпортали, електронні канали зв'язку та програми захисту викривачів.
- **Більшість випадків шахрайства виникають через слабкість або обходження внутрішніх контролів.** Це означає, що ефективна стратегія запобігання та протидії шахрайству повинна базуватися на регулярному тестуванні контролів, незалежному внутрішньому аудиті, оцінці ризиків шахрайства та системному моніторингу поведінкових індикаторів ризику серед персоналу.

Окремий розділ присвячено використанню криптовалют у схемах внутрішнього шахрайства. Хоча частка таких випадків поки що залишається відносно невеликою, автори фіксують їх стабільну присутність. Найчастіше криптоактиви використовувалися для легалізації коштів, отриманих у результаті шахрайства, або для передачі неправомірної вигоди в межах корупційних схем. Цей висновок демонструє поступову інтеграцію цифрових активів у сучасну економічну злочинність та необхідність врахування відповідних ризиків у системах внутрішнього контролю та ПВК/ФТ.

Загалом звіт формує комплексне уявлення про внутрішнє шахрайство як про багатофакторний ризик, що виникає на перетині людського фактору, недосконалості внутрішнього контролю, слабкого корпоративного управління та недостатньої культури доброчесності. Основний меседж дослідження полягає в тому, що жодна організація не може повністю усунути ризик шахрайства, проте ефективна система внутрішнього контролю, підтримка викривачів, розвиток аналітичних інструментів моніторингу, регулярні оцінки ризиків шахрайства та належне корпоративне управління здатні суттєво знизити як ймовірність виникнення шахрайських схем, так і масштаби їх негативних наслідків.

Для загального розвитку

Сліпа пляма фінансової безпеки: як криптовалюти виходять з-під контролю [13]

У той час як мільярди доларів спрямовуються на відстеження блокчейн-транзакцій, розробляються все складніші інструменти аналітики та посилюється контроль на вході у світ цифрових активів – на крипто-біржах, – справжнє відмивання грошей дедалі частіше відбувається там, де віртуальна валюта перетворюється на звичайні фіатні гроші.

Цей етап, який отримав назву «off-ramp», залишається критично недооціненим як регуляторами, так і приватними комплаєнс-командами. Комплаєнс-відділи провідних бірж

[13] https://fincrimecentral.com/crypto-aml-controls-collapse-fiat-on-off-ramp/

часто святкують перемогу, коли аналітичний інструмент позначає депозит «зеленим». Проте ця впевненість оманлива: фокус виключно на моніторингу блокчейну створює небезпечну сліпу пляму саме в точці виходу.

Проблема полягає в системній фрагментації відповідальності. Більшість крипто-платформ не здійснюють прямий переказ фіатних коштів на банківські рахунки користувачів власними силами. Натомість вони покладаються на заплутану мережу сторонніх платіжних провайдерів, регіональних банків та інших посередників. Цей операційний розрив має вирішальне значення: суб'єкт, який ретельно перевіряв блокчейн-гаманець, не є тим, хто здійснює остаточне кредитування фіатних коштів. Комплаєнс-підрозділи бірж діють у хибній парадигмі, вважаючи, що «чисті» дані реєстру гарантують чистий вихід у фіат. Але досвідчені злочинці чудово усвідомлюють, що саме цю точку передачі даних ніхто не контролює належним чином.

Більше того, аутсорсинг фіатної інфраструктури неминуче означає аутсорсинг життєвого циклу перевірки клієнта, тобто KYC. Кожен посередник – платіжний провайдер, регіональний банк-партнер – використовує власні пороги толерантності до ризиків, правила моніторингу транзакцій та географічні обмеження. Синдикати з відмивання грошей ретельно відстежують ці регуляторні розбіжності, виявляючи конкретні регіональні платіжні шлюзи з найслабшими протоколами скринінгу. Спрямовуючи кошти через такі вразливі маршрути, вони легко обходять жорсткі захисні механізми первинних бірж. У підсумку біржа бачить звичайне фіатне зняття на адресу партнера-провайдера, а сам провайдер фіксує вхідний кредит від довіреного корпоративного клієнта. Жодна зі сторін не володіє повною картиною. Це не просто технічна вада, а фундаментальна прогалина в архітектурі сучасного AML.

Одним із найбільш загрозливих проявів цієї проблеми стало використання так званих «вкладених рахунків» (nested accounts). Менш регульовані, часто офшорні, суб'єкти відкривають корпоративні майстер-рахунки на великих біржах. Через ці рахунки вони проводять фіатні транзакції для тисяч незалежних, неперевірених кінцевих користувачів. Коли такі вкладені юридичні особи ініціюють зняття коштів, транзакції виглядають як легітимні корпоративні переміщення – як у блокчейні, так і в традиційному банкінгу. Первинна біржа не має ані договірних повноважень, ані технічної спроможності перевіряти кінцевих користувачів цих вкладених акаунтів. Фактично платформа стає мимовільним кліринговим центром для коштів, які ніколи не проходили справжньої регуляторної перевірки.

Не меншу загрозу становлять і позабіржові брокери (OTC-брокери), які діють як незалежні мости між світом криптовалют і традиційними фіатними мережами. Ці брокери часто використовують особисті банківські лінії, компанії-оболонки та неформальні розрахункові мережі, цілеспрямовано утримуючи свою діяльність нижче порогів виявлення комерційними банками. Клієнт бажає ліквідувати велику крипто-позицію – брокер приймає цифрові активи та розподіляє відповідну суму фіату через десятки окремих локальних банківських переказів. Цей метод повністю розриває зв'язок між джерелом криптовалюти та фіатним шляхом, унеможливлюючи для банків-отримувачів ідентифікацію коштів як результатів ліквідації цифрових активів. Брокер тут виступає як професійний шар обфускації, що експлуатує відсутність обміну даними між традиційними банками та постачальниками послуг віртуальних активів.

Особливо яскраво структурна вразливість проявляється у сфері крипто-дебетових карток. Багато платформ пропонують брендовані картки, які дозволяють витрачати цифрові активи у звичайних магазинах чи знімати готівку в банкоматах. За цими картками стоїть щільна мережа програмних менеджерів, банків-емітентів і карткових мереж, що працюють на застарілій інфраструктурі, яка фізично не здатна читати блокчейн-дані. Коли користувач поповнює картку криптовалютою, цифровий актив миттєво ліквідується через внутрішній пул, а еквівалент у фіаті зараховується на бухгалтерський рахунок у банку-емітенті. Подальші зняття готівки виглядають для банківської системи як стандартна роздрібна карткова активність,

повністю стираючи цифровий слід і дозволяючи користувачам обходити географічний контроль за рухом капіталу без жодних підозрілих сповіщень.

Вирішення цих структурних вад вимагає фундаментального зрушення в тому, як фінансові інституції концептуалізують моніторинг транзакцій. Справжній комплаєнс не може існувати у вакуумі, де видимість блокчейну закінчується в точці конверсії у фіат, а традиційні банки сліпо приймають вхідні перекази. Платформи повинні вимагати глибшої технічної інтеграції зі своїми платіжними партнерами, гарантуючи, що дані про кінцевого бенефіціара переміщуються разом із фіатним платіжним повідомленням. Це вимагає впровадження передових прикладних програмних інтерфейсів (API), які пов'язують конкретні хеші блокчейн-транзакцій безпосередньо з відповідними банківськими клірингговими даними. Без цього явного криптографічного зв'язку аудиторський слід залишається розірваним, а регуляторні органи продовжуватимуть штрафувати установи за неспроможність запобігти системному зловживанню.

Регулятори вже починають зосереджуватися на юридичній відповідальності банків, які надають базову інфраструктуру крипто-посередникам. Банківські мережі більше не можуть ховатися за аргументом, що вони «просто обробляють стандартні банківські перекази для корпоративного клієнта». Очікування регуляторів сьогодні такі: клірингові банки повинні проводити глибоку належну перевірку можливостей моніторингу транзакцій своїх партнерів-постачальників платіжних послуг, включаючи обов'язковий аудит даних про кінцевих користувачів. Установи, які не впроваджують такі перехресні протоколи верифікації, ризикують отримати значні цивільні грошові штрафи, репутаційні втрати та навіть втрату клірингових привілеїв.

Хавала: операційна реальність проти кримінального міфу [14]

Аналітична стаття д-ра Mariola Marzouk та Quentin Mugg «Hawala: Operational Reality vs Criminal Mythology», опублікована 9 червня 2026 року, є критичною ревізією тридцятирічного масиву інтелектуальних помилок і методологічних хиб, якими оперує AML-система у своєму ставленні до хавали як феномена. Автори цілеспрямовано демонтують п'ять найстійкіших міфів, що пронизують регуляторну доктрину, типологічні посібники, обвинувальні акти та корпоративні комплаєнс-процедури, показуючи, як неточний базовий опис системи неминуче деформує всі наступні похідні інструменти – від систем транзакційного моніторингу до судових наративів і кримінальних розслідувань.

Міф перший – «хавала є за своєю природою злочинною» – є, за оцінкою авторів, фундаментальною помилкою, що породжує всі наступні. Хавала є гнучкою сервісною архітектурою неформального переведення вартості, вкоріненою в соціальне, комерційне та діаспорне середовище, – і не є злочинною категорією самою по собі. Хаваладари є фінансовими утилітами в середовищах, де банківська система відсутня, недостатня, викликає недовіру або є нераціональною. Те, що тією самою мережею послуговуються і члени сімей-мігрантів, і НПО, і суб'єкти малого бізнесу, і злочинні актори, свідчить про «сервісну нейтральність» системи, а не про тотожність системи злочинній мережі. Ілюстрацією є задокументований кейс: у кримінальній справі щодо мережі переведення виручки від кокаїну координатор відкрито позиціонував себе як представник торгової компанії, а кілька його агентів вели реальний легальний бізнес – торгівлю вживаними автомобілями, текстилем і ювелірними прикрасами. Легітимна торгівля не була декорацією, а функціонально злита з нелегальним потоком – саме це і є «сервісна нейтральність».

Міф другий – «хавала базується на довірі» – автори переосмислюють в операційному ключі: хавала не просто покладається на довіру, вона активно виробляє довіру як механізм управління транзакцією. Довіра у хаваладарів є не романтичним фольклором, а формою

[14] https://www.linkedin.com/pulse/hawala-operational-reality-vs-criminal-mythology-dr-mariola-marzouk-ndkxe/

операційної належної перевірки через соціальну та комерційну близькість, а не бюрократичну документацію. Взаємини розвиваються через повторюване виконання зобов'язань, рекомендації, суспільний авторитет і поступову верифікацію надійності. Санкція за невиконання є, як правило, екзистенційною: виключення з мережі, репутаційний колапс, втрата доступу до кореспондентських зв'язків і фактичний кінець бізнесу. Хавала нерідко досягає рівня особистої підзвітності, яку регульовані фінанси часто обіцяють, але рідко реалізують на практиці. Водночас автори не ідеалізують систему: та сама довірча інфраструктура, що забезпечує сімейні перекази та торговельне кредитування, може бути і вже використовується для переміщення коштів від шахрайства, ухилення від сплати податків, обходу санкцій, корупції, наркотрафіку, торгівлі людьми, зброєю та фінансування тероризму.

Міф третій – «хавала важкодоступна для зовнішніх суб'єктів» – розвінчується через конкретну доказову базу. Доступ на нижньому та середньому рівнях може бути разюче простим: журналіст без жодних попередніх зв'язків увійшов до магазину на базарі Касабланки та отримав послугу переведення коштів до Франції майже негайно; інший журналіст зателефонував публічно відомому засудженому відмивачу коштів і отримав пропозицію кількох варіантів переведення великих сум без будь-яких рекомендацій. Проникнення можливе і на значно вищих рівнях: в описаному кейсі панєвропейського розслідування наркотероризму хаваладар-відмивач прийшов до двох оперативників під прикриттям у готельному номері і вже через кілька хвилин розкрив усю операційну схему, включно з щомісячними обсягами та контрабандними зв'язками через імпортний бізнес. Що реально захищає верхній ешелон – це відсутність реалістичного наближення до нього, а не непроникна секретність. Реальна причина регуляторного провалу – не культурна непрозорість, а те, що приватні AML-системи побудовані навколо типологій і логіки транзакційного моніторингу, розрахованих на банківську видиму активність, тоді як хавала функціонує на перетині готівки, спільноти, торгівлі та вибіркового використання формальних інститутів.

Міф четвертий – «хавала існує поза межами легітимної торгівлі» – за оцінкою авторів, несе найбільш шкідливі наслідки. Хавала часто функціонально злита з легальним торговельним бізнесом: обмінними пунктами, магазинами, підприємствами текстильної та автомобільної торгівлі, імпортно-експортними операціями. Розрахунки здійснюються через готівку, банківські перекази, MSB, цифрові платіжні канали або торгівлю товарами. Більше того, те, що переміщується в рамках транзакції, часто є не готівкою, а зобов'язаннями, залишками на рахунках, товарами та еквівалентною вартістю через розподілену інфраструктуру. Задокументовані приклади ілюструють це: готівка, зібрана в Північній Європі, йшла на придбання люксових автомобілів, що відправлялись до Західної Африки (іноді з банкнотами за дверними панелями); той самий ланцюжок забезпечував купівлю годинників у duty-free та їх перепродаж у Бейруті. Готівка, зібрана на паркінгу в Європі, могла ніколи не перетинати кордон: вона перепродавалась у місцевий попит, а еквівалентна вартість ставала доступна в Бейруті протягом доби. Відділити законну торгівлю від відмивання є важким, оскільки шва для відділення ніколи і не існувало: легальний шар нерідко свідомо будується самими відмивачами, бо реальний бізнес є найбільш стійким способом надати брудним грошам легального вигляду.

Міф п'ятий – «хавала стає дедалі досконалішою» – спростовується через повернення до першоджерел її стійкості: хавала зберігається не тому, що технологічно еволюціонує, а тому, що залишається простою, адаптивною, дешевою та соціально кмітливою. Її конкурентна перевага – не новизна, а інституційна відповідність: вона ефективно функціонує в готівкових економіках, середовищах зі слабким банківським охопленням, міграційних коридорах, зонах конфліктів та спільнотах, що надають пріоритет швидкості, знайомості, конфіденційності та гнучкості над регуляторним формалізмом. Те, що описується як «зростаюча досконалість», є здебільшого стратегічною адаптивністю в знайомих операційних умовах; мова про «постійно еволюціонуючий ландшафт» є зручним маркетингом для AML-індустрії, що виправдовує бюджети, консультантів і конференційні кола. Авторки залишають місце для двох застережень: по-перше, простота найбільш характерна для вуличного та коридорного рівня;

на верхньому ешелоні присутня справжня архітектурна інженерія – багатошарові підставні компанії в кількох юрисдикціях і навмисна структурованість задля протидії санкційному та митному контролю. По-друге, класичні прийоми є разюче низькотехнологічними і практично не змінились за покоління.

Методологічний висновок авторів є: хавала є переважно легітимною інфраструктурою з реальним злочинним верхнім ешелоном, що ховається всередині неї саме тому, що решта системи виглядає настільки нормально. Ця конфігурація категорично відкидає спокусу хірургічного видалення злочинного компонента без розуміння більш широкого ринку, в який він вбудований: пулів ліквідності, якими він живиться, і соціальних та комерційних каналів, через які він отримує доступ до клієнтів та розрахункових потужностей. Водночас автори наголошують: коригуючий погляд не повинен переходити в ідеалізацію – у певних коридорах злочинний ешелон є не маргінальним пасажиром на легітимному транспорті, а структурно домінуючим актором, метою якого є рух виручки від серйозних злочинів і, в окремих випадках, фінансування озброєних і підсанкційних осіб. Точний опис хавали означає утримання обох істин одночасно, а не вибір між ними.

Ваша думка важлива!

1. Як українські банки в умовах дії воєнного стану та значного збільшення благодійних платежів, можуть ідентифікувати підозрілі крипто надходження, якщо платіжний провайдер маркує переказ як «благодійну допомогу»?
2. Як державам забезпечити ефективну протидію фінансуванню тероризму через неприбуткові організації, не створюючи надмірного регуляторного тиску на благодійний сектор та не обмежуючи його гуманітарну діяльність?
3. Які інституційні, нормативно-правові та організаційні зміни необхідні Україні для переходу від моделі протидії шахрайству, що переважно ґрунтується на виявленні та реагуванні на вже вчинені порушення, до моделі, орієнтованої на їх попередження та мінімізацію пов'язаних із ними ризиків і втрат?
4. З урахуванням масштабів післявоєнного відновлення України, залучення міжнародної допомоги та великих інвестиційних проєктів, які механізми корпоративного управління, внутрішнього контролю та управління ризиками повинні стати пріоритетними для мінімізації ризиків внутрішнього шахрайства та корупції?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-24

Бюлетень є аналітичною розробкою методологічної команди Департаменту антилегалізаційної політики Міністерства фінансів України, спрямованою на поширення кращих практик, дослідження новітніх типологій та глобальних регуляторних і правоохоронних тенденцій у сфері ПВК/ФТ/ФР. Видання призначене для підвищення інституційної спроможності всіх учасників AML системи України та сприяння ефективному управлінню ризиками ВК/ФТ/ФР з урахуванням міжнародних стандартів та актів права ЄС.

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