Методологічний бюлетень

Серійний номер: МінФін-AML-2025-23

Червень 2025

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

Марія Склодовська-Кюрі

Мета

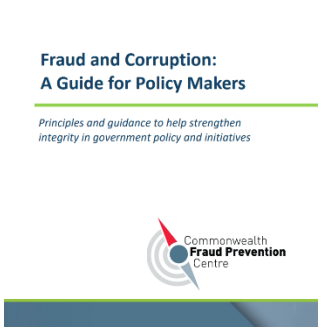
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Шахрайство та корупція: Посібник для нормотворців [1]



Аналітичний документ підготовлений Commonwealth Fraud Prevention Centre є практичним інструментом для політичних і адміністративних рішень у сфері державного управління, що покликаний інтегрувати ризик шахрайства і корупції в усі етапи розробки та реалізації політики. Основна мета посібника — надати посадовим особам підхід, який дозволяє не лише досягати бажаних політичних результатів, а й одночасно забезпечувати сталу доброчесність, запобігати втратам державних ресурсів і підтримувати довіру громадськості.

Документ базується на моделі «Delivering Great Policy» Австралійської публічної служби, яка включає чотири ключові компоненти: чіткість намірів, обґрунтованість,

[1] https://www.counterfraud.gov.au/library/fraud-corruption-guide-for-policy-makers

практичність реалізації та впливовість. У кожному з них «антикорупційна призма» дозволяє виявити приховані загрози, типові помилки політичного дизайну, а також запропонувати конкретні дії для їхнього нейтралізування. Центральною ідеєю є визнання, що ризики шахрайства та корупції мають бути передбачені та враховані ще на етапі задуму ініціативи, а не лише у процесі її виконання чи після виявлення проблем.

Рекомендовано, щоб вже на першому етапі — визначенні намірів — політики формулювали мету не лише з точки зору очікуваного ефекту, а й через аналіз потенційного зловживання. Наприклад, програму державного фінансування необхідно одразу «захищати» через критерії доброчесності, а не зосереджуватися лише на стимулюванні економіки. Далі, для формування обґрунтованої позиції, автори радять активно використовувати досвід попередніх зловживань, дані аудитів, аналітику з корупційних інцидентів, а також проводити консультації з фахівцями з антикорупційного ризик-менеджменту. Визнається, що будь-яка ініціатива — від цифрової трансформації до надання субсидій — має унікальні вразливості, які потребують профільного аналізу.

Третій елемент — практичність — передбачає впровадження конкретних інструментів: верифікацію особи, перевірку достовірності інформації, перехресне зіставлення даних, повідомлення про ризикові транзакції, санкційні механізми, аудит доступу до ресурсів. Наголошено, що ефективне управління ризиками має бути вбудованим у проєктування ініціативи з самого початку, оскільки «запізнілі» заходи стають дорогими та менш результативними. Для цього надається широкий набір ресурсів: понад 70 типів контрольних механізмів, шаблони бізнес-процесів, фреймворки впливу, приклади з інфраструктурних, грантових і надзвичайних програм.

Особливу увагу приділено впливовості політичних рішень у частині доброчесності. Посібник радить позиціонувати боротьбу з шахрайством не як перешкоду, а як стратегічну перевагу — основу громадської довіри, економії державних коштів і відповідності пріоритетам доброчесності уряду. Показовими є дані про щорічні втрати бюджету через шахрайство, які можуть бути використані

Висновки:

- **Ризики шахрайства і корупції повинні бути інтегровані в дизайн політики як окремий елемент мети та результативності**, з конкретними механізмами контролю, починаючи з формулювання намірів.
- **Розробка політик повинна ґрунтуватися на аналізі вразливостей, прикладів попередніх зловживань та консультаціях із фахівцями**, що дозволяє виявити слабкі місця до моменту їх реалізації.
- **Кожна ініціатива повинна містити набір конкретних, практичних інструментів запобігання та виявлення шахрайства**, які підбираються індивідуально залежно від характеру ризиків.
- **Політична підтримка ініціатив посилюється через аргументи про економічні втрати, репутаційні ризики та загрози довірі суспільства**, а також завдяки послідовній комунікації з ключовими стейкхолдерами на основі прозорих даних.

як аргументи у підготовці політичного рішення чи інвестиційної заявки на ресурси для антикорупційної підтримки.

Нормативна основа посібника базується на Законі про державне управління та підзвітність (PGPA Act), Фреймворку протидії шахрайству і корупції, політиці управління ризиками та відповідних вимогах до державних установ щодо попередження, виявлення та реагування на корупцію. Прямим обов'язком є інтеграція аналізу доброчесності у всі державні ініціативи, особливо за умов структурних змін чи нових функцій.

Звіти ПФР Джерсі про підозрілу активність за 1 квартал 2025 року [2]

Аналітичний звіт від Підрозділу фінансової розвідки Джерсі (FIUJ) є не лише статистичним підсумком діяльності щодо виявлення підозрілих фінансових операцій, а й цінним джерелом стратегічної аналітики, що окреслює сучасні загрози та акценти в боротьбі з відмиванням коштів, фінансуванням тероризму та фінансуванням розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Документ охоплює кількісну та якісну оцінку поданих повідомлень про підозрілі операції (SARs), висвітлює злочинні типології, надає зворотний зв'язок ринку та демонструє міжвідомчу координацію у реагуванні на фінансові загрози.

Протягом першого кварталу 2025 року FIUJ отримала 511 повідомлень про підозрілі операції, що становить зростання на 9,9% у порівнянні з аналогічним періодом 2024 року. Основним джерелом SAR залишаються банківські установи (65,5%), далі — постачальники послуг трастів та компаній (TCSP) (16,8%). Ця динаміка підтверджує важливість постійного моніторингу на рівні інституцій, що володіють найбільшим обсягом інформації про клієнтів та структури власності.

Особливої уваги заслуговує категорія SAR, поданих у зв'язку з відмовою в обслуговуванні: у 83 випадках (16,2%) SAR супроводжувались рішенням не вступати в ділові відносини. Половина з них стосувалась фальсифікованої або оманливої інформації при відкритті рахунків, що свідчить про ефективність процедур початкової перевірки (onboarding) та підтверджує їхню критичну роль у виявленні загроз на ранньому етапі.

Основним видом підозрюваної злочинної діяльності у Q1 2025 залишалося шахрайство (37,3%), однак у 41,1% випадків суб'єкти не змогли чітко визначити первинний злочин — категорія «Other – undetermined» потребує окремого регулювання, оскільки вона охоплює ситуації, пов'язані з нетиповою поведінкою клієнтів, зловживанням рахунками, аномаліями операційної діяльності, зокрема щодо клієнтів із Китаю, Гонконгу та Тайваню.

В контексті підстав для подання SAR найбільшу частку займає шахрайство/викривлення фінансової або корпоративної звітності (26,1%), далі — активність, що не відповідає KYC-профілю (14,8%), інформація, отримана в межах фінансової групи або холдингу (13,5%) та дані з відкритих джерел (12,5%). Це підкреслює актуальність поглибленої аналітики поведінкових шаблонів і важливість доступу до зовнішніх джерел інформації у процесі моніторингу.

Окрему увагу у звіті приділено кейсу фінансування тероризму через фіктивну благодійну кампанію, пов'язану з ХАМАС. Злочинці використали платформу GoFundMe та місцеві Facebook-

[2] https://cdn.prod.website-files.com/6464df252c82010a0d5f893f/68133ef565cf0d0ae129d9eb_20250430_1072_V1%20FIU%20SAR%20Q1%202025%20Report.pdf

Висновки:

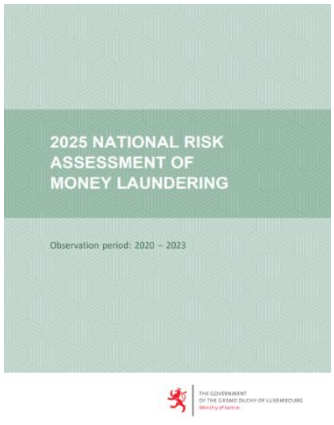
- **Фокус на етапі onboarding залишається критичним — майже половина відмов у бізнесі пов'язані з виявленням шахрайських намірів до початку відносин**. Рекомендовано посилити процедури верифікації на цьому етапі, включно з аналізом соціальних мереж та медіа, санкцій, географічного ризику.
- **Широке використання категорії "Other – undetermined" вказує на необхідність методологічного перегляду шаблонів SAR і додаткових навчань для респондентів**. Варто впровадити приклади типових ситуацій для правильнішої класифікації первинних злочинів.
- **Підвищена увага до криптовалютних операцій, використання міксерів і децентралізованих платформ у схемах ФТ, вимагає розширення технічного інструментарію FIUJ** — блокчейн-аналітика, співпраця з приватними провайдерами, автоматизоване відстеження адрес.
- **Вразливість некомерційного сектору до маніпуляцій через соціальні мережі та краудфандинг потребує мультисекторальної відповіді** — від навчання НПО до укладення угод з платформами та створення механізмів проактивного виявлення фейкових кампаній.

групи, орієнтуючись на жителів Джерсі. Кошти, зібрані через онлайн-кампанію, були переведені на рахунок у банку Джерсі, потім — у криптовалюту і зрештою використані на підтримку терористичної діяльності. Цей кейс ілюструє ефективність використання психологічних маніпуляцій (емоційні меседжі), структурування платежів, використання мультиканальних схем, офшорних рахунків і криптовалют.

FIUJ продемонструвала багатовекторну відповідь: від позначення SAR як "Code 1" до звернень до Revolut, запуску OSINT-досліджень, партнерств із поліцією та TRM Labs, а також планування впровадження аналітичних блокчейн інструментів. Також зазначено про ініціативу щодо підписання меморандуму з Центром кібербезпеки Джерсі та запровадження модулів навчання співробітників FIUJ з фокусом на фінансування тероризму.

Оцінка якості SAR показала позитивну динаміку: 94,1% звітів були визнані такими, що відповідають високим стандартам, що свідчить про підвищення обізнаності та професійного рівня у сфері фінансового моніторингу на острові.

Національна оцінка ризиків ВК у Люксембурзі [3]



У 2025 році Люксембург провів чергову Національну оцінку ризиків (НОР) протидії відмиванню коштів (ПВК), яка охоплює період з 2020 по 2023 рік. Ця оцінка, здійснена під керівництвом Міністерства юстиції та Національного комітету із запобігання відмиванню коштів та фінансуванню тероризму (NPC) , мала на меті поглибити розуміння ризиків відмивання коштів (ВК) та забезпечити застосування ризик-орієнтованого підходу на всіх рівнях — від розробників політики та правоохоронних органів до наглядових органів, підзвітних суб'єктів та фахівців. Це оновлення зосереджується виключно на ризиках ВК, тоді як фінансування тероризму (ФТ) буде розглянуто в окремій оцінці. Методологія звіту передбачає оцінку притаманних ризиків, що

[3] https://gouvernement.lu/dam-assets/images-documents/actualites/2025/05/26-evaluation-risque-blanchiment/2025-nra-vsite-internet.pdf

виникають внаслідок основних загроз ВК та вразливостей різних секторів, після чого враховуються заходи пом'якшення для визначення залишкових ризиків.

Звіт підтверджує, що ВК, що надходить від іноземних злочинів, є найзначнішою загрозою для Люксембургу, враховуючи його позицію як глобального фінансового центру. Основними зовнішніми загрозами залишаються шахрайство та підробка, податкові злочини, а також корупція та хабарництво. Зокрема, кібершахрайство значно зросло, часто здійснюючись транснаціональними організованими злочинними групами. Цифровізація та нові технології прискорили швидкість та масштаб кібершахрайства, що призвело до швидкого відмивання коштів через мережі рахунків, які часто охоплюють кілька юрисдикцій. Звіт наголошує на використанні криптоактивів у шахрайстві з інвестиціями та зловживанні віртуальними IBAN (vIBAN) для приховування незаконних коштів, що ускладнює їхнє відстеження правоохоронними органами. Прокуратура Європейського Союзу (EPPO), що базується в Люксембурзі, відіграє вирішальну роль у розслідуванні злочинів проти фінансових інтересів ЄС, таких як транскордонне шахрайство з ПДВ, яке часто пов'язане з ВК та використовує люксембурзькі компанії як посередників. Внутрішній рівень ВК значно нижчий через низький рівень злочинності в країні. Основними внутрішніми загрозами є шахрайство та підробка, розбій та крадіжки, а також незаконний обіг наркотиків.

З точки зору вразливостей, фінансовий сектор демонструє високий притаманний ризик. Банки, включаючи роздрібні та ті, що працюють онлайн, а також оптові, корпоративні та інвестиційні банки, становлять «Високий» притаманний ризик, тоді як приватні банківські послуги становлять «Дуже високий» ризик через складність послуг та клієнтської бази. Зберігачі та субзберігачі становлять «Середній» ризик. Інвестиційний сектор також має високий ризик, особливо фірми, що надають інвестиційні консультації та послуги з управління портфелем. Постачальники послуг з віртуальними активами (VASP) також були оцінені як такі, що мають «Високий» притаманний ризик, причому ключовими факторами ризику є обсяг транзакцій та канали

Висновки:

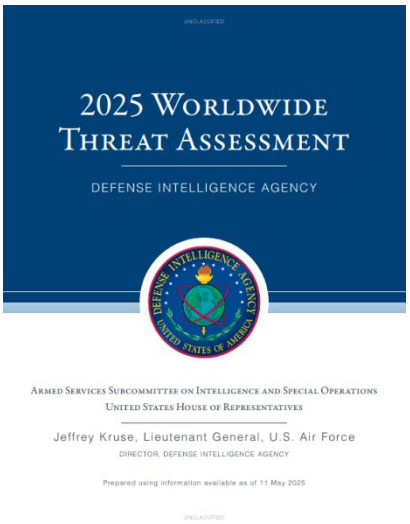
- **Цільовий нагляд та ресурси для високоризикових секторів**: Люксембург повинен продовжувати цільове застосування ризик-орієнтованого нагляду та надавати адекватні ресурси для секторів з високим притаманним ризиком, таким як приватне банківське обслуговування, інвестиційні фірми, VASP, а також юридичні особи та правові утворення, особливо трасти, для ефективного управління залишковими ризиками відмивання коштів.
- **Боротьба з кіберзлочинністю та новими технологіями**: Необхідно посилити можливості щодо виявлення та переслідування кіберзлочинності, що є джерелом значних обсягів відмитих коштів, з акцентом на зловживання віртуальними активами та віртуальними IBAN, а також на транскордонне шахрайство з ПДВ. Це вимагає вдосконалення технологічних інструментів та міжнародної співпраці з EPPO та іншими органами.
- **Підвищення прозорості юридичних структур**: Подальше зміцнення прозорості юридичних осіб та правових утворень, зокрема щодо бенефіціарної власності, є критично важливим. Це включає забезпечення повного дотримання вимог щодо реєстру бенефіціарних власників та сприяння відповідальності TCSP щоб запобігти використанню складних структур для приховування незаконних коштів.
- **Запобігання необґрунтованому дерейтингу**: Вжити заходів для пом'якшення негативних наслідків необґрунтованого дерейтингу для юридичних осіб, таких як малі та середні підприємства та НПО, шляхом надання рекомендацій та сприяння діалогу між фінансовими установами та постраждалими сторонами, щоб забезпечити доступ до фінансових послуг та запобігти переходу до нерегульованих каналів.

розподілу. Нефінансовий сектор, включаючи більшість юридичних та бухгалтерських професій, зберігає «Високий» притаманний ризик, за винятком аудиторської професії та судових виконавців, які мають «Середній» ризик. Юридичні особи та правові утворення, зокрема трасти, були визнані такими, що несуть найвищий притаманний ризик через їхню схильність до використання у складних схемах ВК.

Щодо факторів пом'якшення, звіт відзначає надійну систему ПВК/ФТ Люксембургу, що відповідає рекомендаціям FATF та директивам ЄС. Позитивна оцінка FATF у 2023 році підкреслює «надійну основу та добре розуміння ризиків ВК/ФТ» в Люксембурзі. Національна координація та співпраця між компетентними органами, включаючи створення Міжміністерського керівного комітету з питань протидії відмиванню грошей та фінансуванню тероризму (ISC) , визнані сильною стороною. CRF відіграє центральну роль у виявленні, отримуючи та аналізуючи звіти про підозрілі операції та діяльність (STR/SAR), а також співпрацюючи з міжнародними партнерами. Повноваження CRF щодо заморожування коштів були посилені, а кількість STR/SAR, особливо від ВНУП, постійно зростає, що свідчить про підвищення обізнаності. Впровадження центрального електронного реєстру рахунків IBAN та сейфів є ключовим інструментом, що надає правоохоронним органам прямий доступ до інформації про власників рахунків. Крім того, Закон про неприбуткові асоціації та фонди 2023 року має на меті підвищити прозорість та запобігти зловживанням цими організаціями.

Попри ці заходи, залишковий ризик ВК зберігається. Сектори, що мають високий притаманний ризик, такі як приватне банківське обслуговування та трасти, все ще мають значні залишкові ризики, навіть після застосування заходів пом'якшення. Явища, такі як дерейтинг та фінансова ізоляція, хоч і впливають на фізичних осіб меншою мірою, можуть мати негативний вплив на юридичні особи, такі як стартапи, малі та середні підприємства (МСП) та неприбуткові організації (НПО), що працюють у високоризикових юрисдикціях, змушуючи їх звертатися до нерегульованих каналів.

2025: Рік гібридної нестабільності — аналіз глобальної оцінки загроз DIA[4]



Документ, підготовлений Агентством воєнної розвідки США (Defense Intelligence Agency, DIA), детально висвітлює поточну та прогнозовану конфігурацію глобального безпекового середовища, в якому діють Сполучені Штати та їхні союзники. Цей документ, презентований Конгресу США, репрезентує аналітичну позицію DIA щодо стратегічних викликів, які формуються на перетині міждержавного суперництва, транснаціональних загроз, зростання значущості високих технологій і деструктивної ролі недержавних учасників. Звіт є структурно комплексним, логічно вибудованим і охоплює 39 основних тематичних напрямів — від розвитку ракетних програм і кіберзагроз до аналізу регіональних дестабілізацій і технологічної трансформації потенціалу противників.

Одним із головних висновків звіту є констатація того, що характер глобальної конкуренції трансформується з традиційної воєнної логіки у гібридно-технологічну парадигму, де домінують багатовимірні впливи, а лінія між війною та миром розмита. США стикаються із супротивниками, які все частіше співпрацюють, зокрема в обхід санкцій, у галузі зброї масового ураження, а також у рамках багатосторонніх організацій (БРІКС,

[4] https://armedservices.house.gov/uploadedfiles/2025_dia_statement_for_the_record.pdf

ШОС), не лише для посилення своїх геополітичних позицій, а й для прямого підриву впливу Заходу. Ключовими державами, що формують ядро цієї коаліції, є Китай, росія, Іран і КНДР, які, попри історичні та ідеологічні відмінності, діють прагматично, розвиваючи двосторонні обміни озброєнням, бойовим досвідом, технологіями подвійного призначення та спільною інформаційною політикою проти США.

Особливий акцент зроблено на Китаї, який визначається як найбільш стратегічно послідовний і системно небезпечний суперник. Він продовжує реалізовувати цілі щодо лідерства в Азійсько-Тихоокеанському регіоні та в перспективі — глобального домінування. Під керівництвом Сі Цзіньпіна Китай інвестує у військову модернізацію, нарощування кіберспроможностей, розбудову космічних платформ і розвиток технологій штучного інтелекту. Значне занепокоєння викликає стрімке зростання китайського ядерного арсеналу — понад 600 активних боєголовок на 2025 рік, із прогнозом перевищити 1 000 до кінця десятиліття. КНР також активно просуває дипломатичну ізоляцію Тайваню, проводячи багатодоменні навчання поблизу його узбережжя, тестує блокадні сценарії, здійснює вторгнення у повітряний простір сусідніх держав, зокрема Філіппін, та паралельно розвиває глобальну логістичну інфраструктуру PLA, відкриваючи військові об’єкти за кордоном — у Камбоджі, Танзанії, потенційно в Кубі, ОАЕ, Бірмі.

Дуже детально аналізовано роль російської федерації, яка продовжує агресивну війну проти України. Війна розглядається Кремлем як екзистенційне протистояння із Заходом, а не як регіональний конфлікт. Незважаючи на важкі втрати (близько 700 000 загиблих і поранених, знищення понад 10 000 одиниць техніки), рф не демонструє ознак згортання агресії. Її стратегія базується на виснаженні України та створенні умов, за яких буде нав’язано «мир на умовах Кремля». У цьому контексті росія отримує значну допомогу від Північної Кореї (артилерія, ракети, 12 000 військовослужбовців), Ірану (БПЛА Shahed, ракети), а у відповідь постачає високотехнологічні компоненти — від електроніки до супутникових технологій. DIA також фіксує нарощування росією кібероперацій, орбітальних можливостей, застосування систем радіоелектронної боротьби та експерименти з протисупутниковою зброєю, включно з випробуванням носіїв ядерного заряду в космосі. У політико-дипломатичній площині рф інтенсифікує вплив у Латинській Америці, на Кавказі, в Африці та Центральній Азії, просуваючи моделі субординованого «партнерства» з білоруссю, Грузією, Вірменією та африканськими державами.

У звіті детально аналізується роль Ірану як регіонального хабу загроз у Західній Азії. Зокрема, з 2023 року Іран перейшов від проксі-моделі до прямого застосування збройних сил проти Ізраїлю, завдавши серій масованих ракетно-дронових ударів, а також активізував спроби знищення ізраїльських, єврейських і американських цілей у всьому світі. Іран суттєво наблизився до можливості виготовлення ядерної зброї, зберігаючи здатність створити перший боєзаряд менш ніж за тиждень. Водночас він активно досліджує біологічні та хімічні компоненти, що потенційно можуть бути використані в збройних конфліктах. Значного удару зазнала проксі-мережа Ірану в Сирії після краху режиму Асада та втрати логістичного коридору для поповнення Хезболли.

Не менш важливою є оцінка Північної Кореї, яка демонструє підвищену впевненість у своїй геополітичній суб’єктності, розвиває співпрацю з рф, модернізує арсенал МБР, і зберігає активну кіберзлочинну діяльність, включно з крадіжками криптоактивів. Її стратегічна мета — зміцнення режиму та створення умов для переговорів на власних умовах. КНДР зберігає потужності з виробництва хімічної, біологічної та ядерної зброї, і готова до нових випробувань на Пунгері.

У сфері транснаціональних загроз особливо вирізняється проблема фентанілу: попри зниження його потоку на 30% у 2025 році, США зазнали понад 86 000 смертей, що свідчить про значну гуманітарну та кримінальну кризу. Мексиканські картелі (Сіналоа, Халіско, MS-13, Tren de Aragua) і надалі становлять загрозу безпеці США, контролюючи ключові канали постачання наркотиків, зокрема через південний кордон.

Висновки:

- **Глобальна конкуренція зростає в усіх доменах (кібер, космос, AI, військова сфера), і держави-противники активно використовують технології подвійного призначення.**
  Рекомендація: інвестувати в контртехнології, особливо у сфері AI, безпілотних систем та захисту від кібервторгнень.
- **Китай активно готується до потенційного воєнного сценарію щодо Тайваню та блокує санкції проти КНДР.**
  Практична дія: зміцнення оборонної співпраці з союзниками в Індо-Тихоокеанському регіоні (зокрема Японією, Філіппінами, Тайванем).
- **росія зберігає стратегічні цілі в Україні, розраховуючи на війну на виснаження та зменшення підтримки Заходу.**
  Висновок: США та союзникам варто переглянути стратегію довгострокової підтримки України, зокрема щодо витривалості ресурсів, логістики та інформаційної підтримки.
- **Іран та КНДР активізують військово-технічну співпрацю з рф, що сприятиме модернізації їхніх програм зброї масового ураження.**
  Порада: застосування більш жорсткого моніторингу та обмеження доступу до технологій подвійного призначення в регіоні.

Висвітлюється також глобальна терористична загроза з боку ІДІЛ, Аль-Каїди та афілійованих структур, зокрема в Африці. Відзначено, що ці організації адаптувалися до нових умов — децентралізовані, технологічно підготовлені, здатні використовувати AI, БПЛА, криптовалюти, а також успішно вербувати нові кадри через соціальні мережі. Значну загрозу становить можливість прихованого проникнення осіб з терористичним бекграундом через латиноамериканські маршрути.

Таким чином, звіт DIA демонструє системне ускладнення глобального безпекового ландшафту, в якому кількість одночасно діючих державних і недержавних викликів зростає, технологічний компонент стає ключовим рушієм конфліктів, а багатополярний світ перетворюється на арену нестабільності, гібридного протистояння і конкуренції ідеологій. Він прямо вказує на необхідність підвищення технологічної стійкості, посилення оборонного партнерства, модернізації протиракетної та кіберзахисної інфраструктури, а також переосмислення глобальної стратегії протидії системним противникам.

Віртуальні загрози: Фінансування тероризму через онлайн-ігри [5]

Project craaft
Collaboration, Research & Analysis Against the Financing of Terrorism

Документ підготовлений Гонсало Саїзом у рамках проєкту CRAAFT II (Collaborative Responses to the Role of New Technologies in Terrorist Financing) за підтримки Програми НАТО «Наука заради миру та безпеки» у 2025 році, є першим дослідницьким брифінгом, що аналізує використання онлайн-ігор терористами та екстремістами для фінансування їхньої діяльності.

[5] https://www.projectcraaft.eu/s/594-CRAAFT-II-BP1-Terrorist-Financing-Inzr.pdf

Дослідження зосереджується на тому, як ігрова індустрія, попри свою популярність і економічний потенціал, стає вразливою до зловживань через слабке регулювання фінансових злочинів, зокрема фінансування тероризму. Автор детально розглядає регуляторні прогалини, фінансові ризики, пов'язані з мікротранзакціями та продажем екстремістських ігор, а також нові загрози, що виникають із появою технологій, таких як блокчейн і метавсесвіт. Документ пропонує рекомендації для посилення протидії фінансуванню тероризму (CTF) в ігровій індустрії.

Проєкт CRAAFT, який розпочався з першої фази (CRAAFT I) і продовжується у 2025 році в рамках CRAAFT II, спрямований на зміцнення глобальних зусиль із протидії фінансуванню тероризму шляхом аналізу впливу нових технологій. Дослідження проводиться Центром фінансів і безпеки (CFS) при Королівському інституті об'єднаних служб (RUSI) у співпраці з RUSI Europe та Регіональним інститутом досліджень безпеки (RISS) у Тбілісі. Воно підкреслює, що ігрова індустрія, яка у 2024 році охоплювала 3,4 мільярда користувачів і генерувала 187,7 мільярда доларів доходу з прогнозом зростання до 213,3 мільярда до 2027 року, привертає увагу терористів і екстремістів через свою доступність і слабке регулювання. Платформи онлайн-ігор використовуються для поширення пропаганди, вербування та збору коштів, що робить їх потенційним інструментом для фінансових злочинів.

Регуляторні зусилля в ігровій індустрії зосереджені переважно на протидії екстремістському контенту, тоді як фінансування тероризму залишається поза увагою. Наприклад, Друга та Третя директиви ЄС щодо боротьби з відмиванням грошей (AMLD) регулюють онлайн-гемблінг, але не поширюються на онлайн-ігри. П'ята директива AMLD охоплює обмін віртуальних валют на фіатні, але виключає ігрові валюти, які не конвертуються в реальні гроші, що створює прогалини в нагляді. Ігрові платформи часто покладаються на платіжні сервіси для проведення перевірок клієнтів, але відсутність вимог «Знай свого клієнта» (KYC) у самих платформ призводить до «перекладання відповідальності» між сторонами, що знижує ефективність моніторингу. Автор зазначає, що розмитість між поняттями «тероризм» і «екстремізм» ускладнює визначення обов'язків платформ, оскільки екстремістські дії не завжди підпадають під чітке визначення тероризму, що ускладнює виявлення фінансових потоків.

Одним із ключових ризиків є мікротранзакції, які дозволяють купувати віртуальні предмети чи валюти за фіатні гроші. Ці транзакції створюють можливості для відмивання грошей, коли злочинці використовують вкрадені картки для покупки ігрових активів, які потім продаються на сторонніх платформах за нижчими цінами, конвертуючись у фіатну валюту чи криптовалюту. Наприклад, у 2018 році Valve повідомила, що більшість мікротранзакцій у грі Counter-Strike: Global Offensive використовувалися для відмивання грошей. Лутбокси, які функціонують за принципом азартних ігор, також створюють ризики, оскільки їхній вміст розкривається лише після покупки. Хоча доказів прямого використання таких схем терористами поки що мало, потенціал для зловживань залишається високим через відсутність належного регулювання.

Терористичні та екстремістські групи активно створюють власні ігри або модифікують популярні, щоб поширювати ідеологію та збирати кошти. Наприклад, Хезболла випустила ігри Special Forces (2003) та Holy Defence (2018), де гравці можуть виступати в ролі бійців Хезболли. Ультраправі групи, такі як National Alliance, розробили гру Ethnic Cleansing (2002), яка продавалася за 14,88 долара, що є символічним числом у правоекстремістських колах. У 2020 році австрійський розробник Kvltgames за підтримки ультраправої організації Ein Prozent випустив гру Heimat Defender: Rebellion, а у 2024 році — The Great Rebellion, яка зібрала 94 500 доларів на платформі Steam. Модифікації популярних ігор, таких як Roblox, Minecraft чи Grand Theft Auto, також використовуються для пропаганди, наприклад, відтворюючи терористичні атаки. Окрім продажів, екстремісти отримують кошти через пожертви під час стрімінгу ігор, як у випадку Ніка Фуентеса, який зібрав 163 000 доларів через турнір у Fortnite у 2023 році.

Ігрові та суміжні платформи, такі як Discord, Twitch і DLive, стають майданчиками для комунікації та збору коштів екстремістами. Голосові та текстові чати, часто із шифруванням, дозволяють екстремістам спілкуватися, вербувати та просити пожертви, переводячи користувачів на безпечніші канали для подальших інструкцій. Дослідження показують, що 16% геймерів стикалися зі спробами збору пожертв екстремістами на ігрових платформах. Платформа DLive, яка використовує криптовалюту на основі блокчейну, стала осередком для збору коштів, де деякі канали у 2020 році заробляли від 150 000 до 550 000 доларів. Discord також використовувався для планування подій, таких як мітинг Unite the Right у Шарлоттсвіллі у 2017 році. Зростання модерації на цих платформах змушує екстремістів діяти більш приховано, що ускладнює їх виявлення.

Нові технології, такі як блокчейн, невзаємозамінні токени (NFT) та метавсесвіт, створюють додаткові ризики. Метавсесвіт може використовуватися для віртуальних подій, таких як концерти чи бої, де екстремісти можуть продавати NFT із символікою чи членські токени для доступу до спільнот. Ці децентралізовані платформи стають менш прозорими, що ускладнює регуляторний нагляд. Хоча метавсесвіт більше пов'язаний із відмиванням грошей, ніж фінансуванням тероризму, його потенціал для зловживань зростає, що вимагає пильної уваги.

Документ наголошує на необхідності глибшого аналізу ризиків ігрової індустрії та вдосконалення регулювання. FATF рекомендовано провести секторальний аналіз ризиків, а Європейській Комісії — оцінити ризики відмивання грошей і фінансування тероризму в онлайн-іграх у наступному звіті щодо ПВК/ФТ. Пропонується чітко розподілити обов'язки між ігровими платформами та платіжними провайдерами, запровадити механізми звітності та використовувати штучний інтелект для модерації голосового чату. Регулювання має бути пропорційним і базуватися на оцінці ризиків, щоб не перешкоджати розвитку індустрії. Автор підкреслює, що швидка еволюція ігрової індустрії вимагає від ЄС та національних регуляторів глибшого розуміння нових ризиків, щоб запобігти зловживанням терористами та екстремістами.

Висновки:

- **Проведення секторального аналізу ризиків:** FATF має ініціювати опитування серед своїх членів та доручити робочій групі з ризиків, трендів і методів підготувати звіт про ризики фінансування тероризму в ігровій індустрії, щоб визначити, чи потрібне розширення AML регулювання.
- **Чіткий розподіл обов'язків:** Необхідно законодавчо визначити відповідальність ігрових платформ і платіжних провайдерів щодо моніторингу транзакцій, запровадивши вимоги KYC для зменшення «перекладання відповідальності».
- **Запровадження звітності та модерації:** Ігрові платформи повинні впровадити механізми звітності про підозрілу діяльність і використовувати ШІ для модерації голосового та текстового контенту, щоб виявляти екстремістські наративи та фінансові транзакції.
- **Моніторинг нових технологій:** Регулятори повинні приділити увагу метавсесвіту та блокчейн-платформам, щоб запобігти використанню NFT, криптовалют і віртуальних подій для фінансування тероризму, розробивши відповідні регуляторні рамки.

Eurojust 2024: Глобальний центр судової співпраці та відповідальності за міжнародні злочини [6]

Річний звіт Eurojust Annual Report 2024 є комплексним оглядом діяльності Агентства Європейського Союзу з питань кримінального правосуддя у сфері боротьби з тяжкими транскордонними злочинами. Упродовж 2024 року Eurojust підтримав майже 13 000 кримінальних проваджень, з яких понад 5 300 були новими справами, а інші — такими, що тривали з попередніх років. Ці справи охоплювали всі основні категорії тяжкої злочинності: від економічних злочинів і торгівлі наркотиками до тероризму, кіберзлочинів, злочинів проти довкілля та торгівлі людьми. У звіті особливо підкреслюється, що у 2024 році було здійснено понад 1 200 арештів, заморожено або конфісковано злочинні активи на суму понад 1,3 млрд євро, а вартість вилучених наркотичних засобів сягнула 19,6 млрд євро. Крім того, агентство зафіксувало участь у справах, які стосуються понад 1,3 млн потерпілих та спричинили понад 32 млрд євро збитків.

Особливої уваги в звіті надано розширенню міжнародного партнерства Eurojust. У 2024 році Агентство уклало нові меморандуми з шістьма країнами Латинської Америки (зокрема, Болівією, Чилі, Коста-Рикою, Еквадором, Панамою та Перу) для поглиблення співпраці у сферах боротьби з наркоторгівлею, торгівлею людьми, відмиванням коштів та кіберзлочинністю. Підписано угоду про співпрацю з Вірменією, активізовано діалог з Алжиром, Ліваном, Колумбією та Бразилією. Водночас, Євроюст продовжив зміцнення своєї мережі контактних пунктів, які вже охоплюють понад 70 країн, і прийняв нового прокурора з Ісландії. Загалом у 2024 році з третіми країнами було відкрито понад 1 000 нових справ, а найактивнішими серед них були Велика Британія, Швейцарія, Албанія та Україна.

Окремий блок звіту присвячено розбудові нової Європейської судової мережі у сфері організованої злочинності (EJOCN), започаткованої Радою міністрів юстиції ЄС у 2024 році. Eurojust став координатором і технічним оператором цієї мережі, яка має на меті забезпечити обмін оперативною інформацією, розбудову спільних стратегій переслідування організованих злочинних груп та формування JIT (спільних слідчих груп) для протидії найбільш загрозливим формам злочинності — насамперед, наркоторгівлі через порти ЄС. EJOCN має стратегічну функцію з розробки методичних матеріалів, виявлення правових проблем і трендів, координації слідчих дій у Європі та за її межами.

У контексті війни в Україні звіт фіксує значну активність Євроюсту у підтримці національних та міжнародних розслідувань щодо воєнних злочинів, злочинів проти людяності та геноциду. У звіті описується робота JIT з розслідування основних міжнародних злочинів, який діє з 2022 року за участі України, Литви, Польщі та інших країн. У 2024 році цей JIT було продовжено до 2026 року. Також триває робота Міжнародного центру з переслідування злочину агресії проти України (ICPA) та функціонування бази доказів CICED, яку поповнюють національні органи слідства. Протягом року зібрано десятки тисяч свідчень, а також винесено підозри кільком підозрюваним у воєнних злочинах.

В аналітичній частині звіту докладно проаналізовано основні категорії злочинів, з якими працював Eurojust: економічні (найпоширеніші — шахрайство та відмивання коштів),

[6] https://www.eurojust.europa.eu/annual-report-2024

наркоторгівля (особливо кокаїном з Латинської Америки), торгівля людьми (з акцентом на сексуальну експлуатацію та примусову працю), кіберзлочинність (зокрема, пов'язана з криптовалютами та хакерськими атаками), а також злочини проти навколишнього середовища та інтелектуальної власності. В багатьох із цих сфер відзначається зростання цифрових загроз, використання закритих платформ зв'язку (EncroChat, SkyECC), а також гібридні форми злочинності (наприклад, наркоторгівля через фіктивний бізнес).

Висновки:

- **Eurojust став незамінним інструментом для транскордонної координації розслідувань у ЄС і за його межами.** Національним прокуратурам доцільно системно ініціювати спільні слідчі групи (JIT), особливо у складних справах з міжнародним елементом, зважаючи на доступ до фінансування, експертів і оперативної підтримки від Eurojust.
- **Розширення партнерств із третіми країнами суттєво підвищує ефективність боротьби з транснаціональною злочинністю.** Україна має просувати укладення повноцінної міжнародної угоди з Eurojust (із можливістю обміну персональними даними) для інтеграції у європейську судову інфраструктуру.
- **У відповідь на війну в Україні створено нові постійні інституції для документування та переслідування міжнародних злочинів.** Необхідно системно передавати докази до CICED, активно взаємодіяти з ICPA, та ініціювати координаційні зустрічі з іншими країнами для узгодження стратегій розслідування.
- **Стрімке зростання кіберзлочинів і цифрових форм злочинності вимагає модернізації інструментів міжнародного правосуддя.** Необхідно впроваджувати новітні інструменти, розширювати навчання суддів і прокурорів щодо доказів у цифровому середовищі.

У 2024 році Eurojust також значно активізував співпрацю з іншими структурами ЄС, зокрема Europol, OLAF та EPPO. Особливо важливою була спільна робота з Європейською прокуратурою над справами щодо шахрайства з ПДВ та злочинами проти фінансових інтересів ЄС. Водночас, спостерігався приріст кількості координаційних зустрічей та проведення днів спільних дій у реальному часі, що дозволило забезпечити арешти, обшуки й вилучення активів у декількох країнах одночасно.

Таким чином, звіт демонструє, що Eurojust є не лише координатором судового співробітництва, а й стратегічним інституційним майданчиком для європейської та глобальної взаємодії у протидії злочинності. Його ключові інструменти — JIT, Європейський ордер на арешт, Європейський наказ на розслідування, координаційні центри та мережі прокурорів — стали ядром сучасного підходу до правосуддя у глобалізованому світі.

Огляд перших результатів політики відшкодування APP-шахрайства [7]

Документ, опублікований Payment Systems Regulator (PSR), є детальним звітом, що аналізує перші результати впровадження новаторських вимог щодо відшкодування збитків жертвам шахрайства типу Authorised Push Payment (APP) у Великій Британії.

[7] https://psr.org.uk/news-and-updates/thought-pieces/thought-pieces/the-story-so-far-a-snapshot-of-what-we-ve-seen-since-our-app-scams-reimbursement-requirement-went-live/

Ці вимоги, які набули чинності 7 жовтня 2024 року, стали першим у світі комплексним регуляторним механізмом, спрямованим на захист споживачів від фінансових та емоційних наслідків APP-шахрайства, коли жертви свідомо переказують кошти шахраям, вважаючи транзакції легітимними. Звіт охоплює перші три місяці дії політики (з жовтня по грудень 2024 року) і базується на офіційних даних про дотримання вимог, отриманих від постачальників платіжних послуг (PSPs) через Pay.UK, а також на відгуках стейкхолдерів, включаючи банки, споживачів та регуляторні органи.

Політика передбачає, що відповідальність за відшкодування збитків жертвам APP-шахрайства розподіляється між відправником (банк або платіжна фірма жертви) та отримувачем (банк або платіжна фірма шахрая). Такий підхід створює фінансові стимули для обох сторін активно запобігати шахрайству, що є ключовою відмінністю від попередніх практик, коли відшкодування залежало від добровільної участі банків у Contingent Reimbursement Model Code (CRM). Велика Британія стала піонером у впровадженні такого підходу, встановивши світовий стандарт захисту споживачів від цього виду шахрайства.

За перші три місяці дії політики PSR відзначає успішне впровадження, попри виклики, пов'язані з необхідністю навчання персоналу PSPs та адаптації споживачів до нових правил. Дані свідчать, що 86% коштів, втрачених через APP-шахрайство, було повернуто жертвам, що становить приблизно £27 млн. Для порівняння, у 2023 році, за даними UK Finance, рівень відшкодування складав 68%, хоча прямі порівняння ускладнені через зміни в методології та визначенні APP-шахрайства. Особливу увагу приділено вразливим споживачам, на яких припало 14% заяв (£7 млн), що підкреслює ефективність додаткових заходів захисту для цієї групи.

Раніше відшкодування залежало від того, чи був банк учасником добровільного CRM-кодексу, що створювало нерівність між споживачами різних PSPs. Нова політика усунула цю проблему: усі 60 фірм, які отримали заяви в перші три місяці, відшкодовували збитки, створюючи більш справедливі умови. Співпраця між відправниками та отримувачами також демонструє позитивну динаміку: 86% заяв повідомляються відправником отримувачу протягом двох робочих годин, а 84% заяв закриваються протягом п'яти робочих днів. Це свідчить про оперативну взаємодію, яка сприяє швидкому вирішенню справ та підвищенню довіри споживачів. Однак стейкхолдери зазначають, що інформація, якою обмінюються PSPs, іноді є недостатньою для ефективного запобігання шахрайству, що вимагає подальшого вдосконалення.

Побоювання щодо різкого зростання кількості заяв не справдилися: за три місяці було подано 46 000 заяв, що нижче середнього показника за аналогічний період 2023 року (56 000, за даними UK Finance). Це може бути пов'язано з тим, що дані не включають шахрайства, скоєні до 7 жовтня 2024 року, а також із поступовим зростанням обізнаності споживачів про нову політику. Очікується, що кількість заяв зростатиме в коротко- та середньостроковій перспективі. Банк Англії, Financial Ombudsman Service та FCA також не зафіксували сплеску скарг, пов'язаних із відшкодуванням, хоча PSR зазначає, що скарги можуть з'явитися пізніше.

Ще одним аспектом, який викликав занепокоєння перед впровадженням політики, був потенційний моральний ризик: побоювання, що споживачі діятимуть менш обережно, знаючи про можливість відшкодування. Для протидії цьому PSPs можуть застосовувати виняток «стандарт обережності споживача» (якщо жертва діяла з грубою недбалістю) або стягувати £100 надлишку. Проте лише 2% заяв було відхилено через невідповідність стандарту обережності, а 23% фірм використовували цей виняток, що вказує на нерівномірне застосування правил. PSR планує співпрацювати з PSPs та Financial Ombudsman Service, щоб уточнити, коли цей виняток доцільно застосовувати. Дані також не підтверджують значних змін у поведінці споживачів, що спростовує побоювання щодо морального ризику.

Звіт включає анонімізовані кейс-стаді (історії Баррі, Кірана, Язмін та Джорджіни), які ілюструють реальний вплив шахрайства та ефективність політики. PSR наголошує на важливості захисту реальних людей від емоційних та фінансових наслідків шахрайства, а також закликає споживачів залишатись пильними, особливо під час використання соціальних мереж, технологічних платформ і телекомунікацій, які є поширеними каналами для шахраїв, згідно з їхнім звітом про походження шахрайства 2024 року.

Наступні кроки включають продовження моніторингу ефективності політики спільно з FCA. У жовтні 2025 року розпочнеться незалежний огляд, який оцінить результати після року дії політики. PSR також активно взаємодіє з індустрією та представниками споживачів, щоб зібрати відгуки та вдосконалити механізми. Документ завершується закликом до співпраці між усіма сторонами для забезпечення захисту жертв та створення сильних стимулів для запобігання шахрайству.

Висновки:

- **Високий рівень відшкодування та захист вразливих споживачів:** 86% втрачених через APP-шахрайство коштів (£27 млн) повернуто жертвам, з особливим акцентом на захист вразливих груп (14% заяв, £7 млн).
- **Ефективна співпраця між PSPs:** 86% заяв обробляються протягом двох робочих годин, а 84% закриваються протягом п’яти робочих днів.
- **Відсутність сплеску заяв:** Кількість заяв (46 000) не зросла порівняно з 2023 роком, що спростовує побоювання щодо надмірного навантаження на PSPs. Необхідно посилити просвітницьку роботу серед споживачів для підвищення обізнаності про політику, що може поступово збільшити кількість заяв.
- **Нерівномірне застосування винятків:** Лише 23% фірм використовують виняток «стандарт обережності», що вказує на потребу в чіткіших вказівках. Необхідно розробити детальніші інструкції для PSPs щодо застосування винятків, щоб забезпечити однаковий підхід.

Регулювання

Поглиблення конкурентоспроможності та сталого розвитку внутрішнього ринку ЄС [8]

Запропонований Регламент Європейського парламенту і Ради ЄС від 21 травня 2025 року (COM(2025) 501 final) є частиною пакета реформ, спрямованого на поглиблення конкурентоспроможності та сталого розвитку внутрішнього ринку ЄС. Основна мета ініціативи — розширити чинні регуляторні послаблення і спрощення, які наразі застосовуються до малих та середніх підприємств (МСП), на категорію малих та середніх підприємств (SMC, Small Mid-Caps). Ідеться про підприємства, що вже вийшли за межі визначення МСП, але ще не досягли рівня великих корпорацій, зазвичай — це компанії з чисельністю персоналу до 750 осіб або річним обігом до 150 мільйонів євро.

Документ відображає зростаючу роль таких підприємств в інноваційних, стратегічно важливих секторах — оборона, електроніка, відновлювана енергетика — та потребу в регуляторній гнучкості для підтримки їхнього зростання. Згідно зі звітами Маріо Драгі та Енріко Летти, які

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0501R%2801%29

надали стратегічне підґрунтя ініціативі, SMC зазнають непропорційно високого адміністративного навантаження, не маючи при цьому доступу до полегшених режимів, передбачених для МСП. Це створює так званий "ефект урвища" (cliff-effect), коли зростаючі компанії опиняються у значно менш сприятливому правовому полі лише через незначне перевищення порогів, передбачених у дефініції МСП.

Регламент пропонує внести зміни до шести чинних регламентів ЄС, включно з Загальним регламентом про захист даних (GDPR). У кожному з них передбачається розширення кола адресатів певних спрощень, зокрема звільнення від ведення облікової документації, обов'язків щорічного звітування, вимог щодо сертифікації або полегшеного доступу до інструментів захисту торгівлі. Для SMC встановлюється окрема дефініція, яка, попри спільну логіку з МСП, формалізує їх як особливу групу підприємств із відповідними порогами.

Регламент також передбачає перехід до трирічного циклу звітування замість щорічного, удосконалення принципів пропорційності в GDPR щодо обов'язків ведення реєстрів обробки даних, а також надання SMC можливості використовувати спрощену форму проспекту EU Growth у рамках залучення капіталу.

Особливу увагу приділено також усуненню надмірних процедур у Регламенті щодо фторованих газів — зокрема, скасовується обов'язкова реєстрація для імпортерів та експортерів, якщо обіг їхньої продукції не підпадає під режими звітності чи обмежень, що дозволяє уникнути блокування поставок на митниці. Усі зміни покликані не тільки забезпечити відповідність принципу пропорційності, а й стимулювати економічне зростання шляхом зниження адміністративних витрат без шкоди для ефективності регуляторних режимів.

Ініціатива відображає підхід Єврокомісії до вдосконалення регуляторної екосистеми — так звану програму REFIT — і реалізує зобов'язання щодо зменшення загального адміністративного навантаження на 25%, а для МСП — на 35%. Проект також отримав схвалення в результаті консультацій з бізнес-спільнотою, яка послідовно наголошувала на необхідності врахування специфіки SMC під час формування нових норм.

У контексті Загального регламенту про захист даних (GDPR), запропоновані зміни стосуються удосконалення принципу пропорційності з метою зменшення надмірного адміністративного навантаження на SMC.

Зокрема, йдеться про те, що SMC отримають можливість спрощеного ведення реєстрів обробки персональних даних, а також потенційно інші регуляторні полегшення, які вже діють для МСП. Це дозволить уникнути

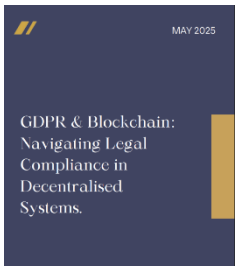
Висновки:

- **Усі держави-члени мають актуалізувати свої національні правові та адміністративні рамки**, аби забезпечити практичну реалізацію нової категорії SMC і застосування до них передбачених спрощень, зокрема шляхом внесення змін до реєстрів, баз даних та процедур нагляду.
- **Регуляторним органам варто оперативно переглянути підходи до взаємодії з підприємствами**, що виходять за межі дефініції МСП, щоб уникнути "ефекту урвища" та забезпечити безперервність підтримки, зокрема у сферах захисту даних, доступу до ринків капіталу, торгового захисту та екологічного комплаєнсу.
- **Бізнес-асоціаціям рекомендовано посилити адвокацію інтересів SMC у діалозі з регуляторами** та ініціювати розробку кодексів поведінки та галузевих стандартів із врахуванням нових можливостей, передбачених цим регламентом.
- **Контролюючі органи та наглядові структури мають адаптувати свої IT-системи та процеси реєстрації й звітності**, включаючи створення фільтрів та шаблонів, які автоматично ідентифікують SMC та застосовують до них релевантні виключення чи полегшення.

ситуації, коли підприємства, що трохи перевищують пороги, визначені для МСП, змушені виконувати всі вимоги GDPR без будь-яких послаблень, навіть якщо їхні ризики є порівняно низькими.

Звіти окремих інституцій та експертів

Навігація у сфері дотримання законодавства в децентралізованих системах [9]



Документ є вичерпним правовим аналізом перетину технології блокчейн із вимогами Загального регламенту про захист даних (GDPR). Документ зосереджено на ключових викликах, які виникають при обробці персональних даних у децентралізованих середовищах, особливо у контексті публічних блокчейнів, смарт-контрактів, DAO і DeFi. Центральним предметом розгляду є суперечність між природними характеристиками блокчейн-систем—такими як незмінність, глобальність, відсутність централізованого контролю—та принципами GDPR, зокрема правом на забуття, обмеженням мети та мінімізацією даних.

У вступі висвітлюється технічна природа блокчейн-технології та її ключові атрибути: незмінність записів, криптографічна ідентифікація через публічні/приватні ключі, консенсусні механізми, розподілене зберігання. Далі подано юридичний контекст: принципи GDPR, що включають законність, прозорість, обмеження мети, точність, мінімізацію, збереження та підзвітність. Автори наголошують, що псевдонімізовані дані, які можна пов'язати з фізичною особою через додаткову інформацію (напр. IP-адреси чи поведінкові шаблони), розглядаються як персональні і підлягають регулюванню відповідно до GDPR.

Основна частина аналізу зосереджена на шести юридичних питаннях. По-перше, незмінність баз даних на блокчейн суттєво ускладнює реалізацію права на виправлення чи видалення даних. Застосування жорстких чи м'яких форків не забезпечує відповідності вимогам статей 16 і 17 GDPR, оскільки оригінальні записи зберігаються у старих версіях ланцюга. По-друге, через розподілену природу блокчейнів визначення контролера даних є

Висновки:

- **Зберігання персональних даних безпосередньо на блокчейні слід розглядати лише як виняткове рішення** — пріоритет має надаватися зовнішньому (off-chain) зберіганню, а в разі необхідності використання блокчейну — застосовувати перевірені криптографічні засоби захисту (такі як технології підвищення конфіденційності), обов'язково оцінюючи потенційні ризики повторної ідентифікації особи.
- **Ідентифікація контролера даних у блокчейн-середовищі повинна бути закладена в дизайн** — через використання permissioned моделей, ролей адміністраторів, або контрактних механізмів, що чітко визначають відповідальність.
- **Оцінка впливу на захист даних (DPIA) є обов'язковою для всіх випадків обробки персональних даних через блокчейн**, особливо якщо дані є чутливими або передаються за межі ЄС, і має включати аналіз альтернатив, технічних засобів і ступеня ризику для суб'єктів даних.
- **Право на заперечення проти автоматизованого прийняття рішень має бути забезпечене навіть у DAO чи DeFi екосистемах**, шляхом вбудованих механізмів оскарження, людського перегляду або пост-фактум впливу на наслідки смарт-контракту.

[9] https://www.patsalides.com.cy/wp-content/uploads/2025/05/NAVIGATING-LEGAL-COMPLIANCE-IN-DECENTRALISED-SYSTEMS-CHRISTOS-PATSALIDES-LLC-2.pdf

складним: у permissionless мережах це майже неможливо, тоді як у permissioned системах такі функції можуть бути централізовані, наприклад, у межах консорціуму. Третє питання—правові підстави для обробки: згода є проблематичною через її відкличність та труднощі з реалізацією в децентралізованих системах, тому автори рекомендують зважати на законні інтереси або виконання юридичних зобов'язань (наприклад, ПВК/ФТ).

Четвертим викликом є дотримання принципів обмеження мети та мінімізації даних. Із врахуванням незворотності записів та їхньої доступності для усіх учасників мережі, забезпечити обмеження обробки виключно первісною метою стає технічно неможливо. П'ятим є проблема міжнародної передачі даних: оскільки блокчейн за своєю природою передбачає транскордонне дублювання даних, контролювати відповідність трансферам положенням Розділу V GDPR (зокрема, забезпечення "еквівалентного рівня захисту") практично не вдається. Нарешті, автоматизоване прийняття рішень (напр., через смарт-контракти) може суперечити правам суб'єктів даних за статтею 22 GDPR, якщо не забезпечити можливість людського втручання чи оскарження рішень.

Особливу увагу документ приділяє новим настановам EDPB (Керівні принципи 02/2025), які, попри те що ще перебувають на етапі громадського обговорення, вже окреслюють очікування регулятора. Згідно з ними, ключовими заходами для бізнесу є впровадження чіткої структури відповідальності (розмежування ролей контролера і процесора), використання оф-чейн рішень для зберігання персональних даних, реалізація принципів «конфіденційності за дизайном» і обов'язковість проведення оцінки впливу на захист даних (DPIA) для високоризикових процесів. Також важливо впроваджувати технічні й організаційні механізми виявлення вразливостей, забезпечення зворотного зв'язку із суб'єктами даних та підготовки до інцидентів безпеки.

Документ завершують практичні рекомендації для компаній, що працюють у сфері блокчейн, закликаючи до проактивного підходу в оцінці ризиків, застосуванні PETs (технологій підвищення конфіденційності) та залученні до регуляторного діалогу.

Стандарт для токенізації боргових інструментів з використанням технології розподіленого реєстру [10]

Документ розкриває повноцінний регуляторний та технічний каркас для випуску боргових інструментів у вигляді реєстрових цінних паперів на основі блокчейн-технології відповідно до швейцарського законодавства. Стандарт побудовано на базі попереднього документа щодо токенізації акцій (Equity Standard) і має за мету поширити подібну модель на боргові цінні папери — облігації, структуровані продукти, похідні інструменти тощо.

Ключовим є те, що токенізований борговий інструмент у розумінні цього Стандарту — це цінний папір, прирівняний до ledger-based security згідно зі статтями 973d і наступними Швейцарського кодексу зобов'язань (CO), що означає юридично визнане право, яке не може бути передане без відповідного токена, і навпаки. Для цього необхідна реалізація смарт-контракту (зокрема CMTAT), який забезпечує надійне створення, передачу та знищення токенів, їхній зв'язок із умовами інструменту та наявність

[10] https://cmta.ch/standards/standard-for-the-tokenization-of-debt-instruments-using-distributed-ledger-technology

механізмів захисту, таких як обмеження на передачу, заморожування адрес, деактивація контракту тощо.

Весь процес поділяється на три етапи: передумови, емісія та дії після токенізації. На етапі передумов основними вимогами є: підтвердження правоздатності емітента, наявність дозволу на випуск токенізованих інструментів, сумісність із швейцарським правом та вибір розподіленого реєстру, який відповідає вимогам CO. Підкреслюється необхідність, щоб сам реєстр не контролювався емітентом, містив захищений механізм валідації (наприклад, консенсус Proof-of-Stake), а також дозволяв користувачам безперешкодний доступ до інформації про власні записи.

Етап емісії передбачає прийняття офіційного рішення компетентним органом емітента, формалізацію умов випуску (tokenization terms), оприлюднення ключової інформації (включно з умовами позики, описом смарт-контракту і реєстру, публічними адресами тощо), використання перевіреного смарт-контракту (CMTAT або альтернативи, схваленої CMTA), і розподіл токенів на адресу відповідних власників. Документ чітко описує вимоги до оприлюднення умов інструменту (зокрема, використання хешів або цифрового підпису), а також підкреслює необхідність машино зчитуваних форматів із можливістю надійного перекладу.

Висновки:

- **Токенізація боргових інструментів допускається лише для юридично переносимих прав**, які можуть бути пов’язані з токеном, та не потребують третьої сторони (реєстру, згоди тощо) для передачі — винятки (наприклад, іпотечні папери) не підпадають під дію стандарту.
- **Емітенти зобов’язані закласти контроль за AML/CFT шляхом попереднього або наступного контролю над власниками**, з технічною реалізацією через смарт-контракт — у вигляді умовної передачі, списків адрес або обмежень на реалізацію прав.
- **Smart contract повинен бути затверджений CMTA, прозорий, документований і пройти незалежний аудит** — використання CMTAT є рекомендованим базовим варіантом.
- **Перехід на іншу форму обліку, анулювання або перевипуск токенів можливі, але мають передбачатися в умовах та реалізовуватися згідно з процедурою, що мінімізує правову невизначеність**, зокрема через наявність "pause" або "deactivate" функцій у контракті.

Після емісії реалізуються механізми контролю та комплаєнсу. Центральне місце займає ідентифікація власників. Тут запропоновано дві моделі: ex ante контроль (дозвіл на передачу виключно попередньо схваленим адресам — whitelisting, що обмежує торгівлю, але підвищує відповідність вимогам з ПВК/ФТ), або ex post контроль (вільна передача токенів, але обмежене здійснення прав до верифікації особи). CMTA рекомендує детально прописувати механізми таких контролів у смарт-контракті, зокрема, через функції RuleEngine у CMTAT.

Окремо розглянуто ситуації, коли потрібно перейти на нетокенізовану форму, або перевипустити токени, зокрема через втрату приватного ключа. У такому разі за рішенням суду Швейцарії (відповідно до статті 973h CO) можлива судова ануляція та перевипуск токенів. Стандарт передбачає спрощену процедуру: достатньо одного публічного оголошення в Офіційному віснику Швейцарії та одного місяця для подання відповіді. Крім того, у разі хардфорку або технічної несправності допускається використання функції деактивації смарт-контракту.

Наприкінці, документ встановлює сертифікаційний механізм CMTA: емітенти можуть отримати марку «CMTA Tokenized Debt» після проходження юридичної та технічної перевірки з боку

визнаних експертів, подання документації та оплати зборів. Це не замінює державного регулювання, але посилює довіру ринку.

Боротьба з фінансовим шахрайством у Великій Британії: аналіз загроз, змін та системної відповіді у 2024 році [11]

Звіт є комплексним аналізом стану, динаміки та ключових викликів у сфері фінансового шахрайства у Великій Британії за 2024 рік. Документ охоплює як несанкціоноване шахрайство, коли транзакція здійснюється без дозволу власника рахунку, так і авторизоване шахрайство, зокрема вид APP (authorised push payment fraud), коли особа під впливом соціального інжинірингу самостійно переказує гроші злочинцям. Загальна вартість втрачених коштів становить 1,172 мільярда фунтів стерлінгів, що є майже незмінним показником порівняно з 2023 роком. Але, що тривожніше — загальна кількість зафіксованих випадків шахрайства зросла на 12% і перевищила 3,3 мільйона, що є найвищим зафіксованим рівнем за весь період статистичного спостереження.

Це свідчить про зміну моделей поведінки зловмисників — від стратегій високих разових сум до високочастотних атак на дрібні цілі. Така тактика особливо характерна для зростаючого сегмента віддалених покупок, що є підкатегорією карткового шахрайства. У 2024 році цей вид шахрайства зріс на 22% за кількістю випадків, перевищивши 2,58 мільйона, а втрати зросли на 11% до 399,6 млн фунтів. Цей тип шахрайства здебільшого пов’язаний із компрометацією одноразових паролів (OTP), що використовуються для підтвердження покупок в інтернет-магазинах або підключення до цифрових гаманців. Попри те, що OTP сприймається як ефективний захист, звіт підкреслює, що шахраї все частіше вдаються до складних сценаріїв соціального інжинірингу, аби змусити користувача самостійно ввести цей код. Така тенденція формує нову реальність, в якій безпека онлайн-транзакцій потребує перегляду на рівні архітектури.

Водночас найбільш обнадійливою динамікою звіт відзначає сектор APP-шахрайства. Загальна сума втрат зменшилась на 2% (до 450,7 млн фунтів), а кількість підтверджених випадків впала на вражаючі 20%. Це найнижчий рівень із 2021 року, і така позитивна динаміка була досягнута ще до набуття чинності обов’язковими правилами відшкодування, запровадженими Регулятором платіжних систем (PSR) у жовтні 2024 року. Автори звіту наголошують, що результат є наслідком системної багаторівневої роботи — посилення інструментів виявлення ризиків, інвестицій у поведінкову аналітику, просвітницьких кампаній («Take Five», «Don’t Be Fooled»), а також взаємодії з технологічними платформами і телеком-операторами, через які найчастіше і відбувається початковий контакт із жертвами.

Особливу увагу звіт приділяє новим технологічним викликам, зокрема зростанню потенціалу використання злочинцями агентного штучного інтелекту (Agentic AI) — автономних систем, які можуть самостійно будувати шахрайські сценарії, проводити фішингові кампанії та адаптуватися до поведінки жертв. Злочинці, за аналогією з легальними бізнесами, використовують ці інструменти для масштабування, здешевлення та автоматизації атак. У цьому контексті UK Finance особливо наголошує на важливості реального часу виявлення поведінкових аномалій,

[11] https://www.ukfinance.org.uk/system/files/2025-05/UK%20Finance%20Annual%20Fraud%20report%202025.pdf

коли система може розпізнати відхилення у діях користувача і ініціювати превентивні заходи ще до завершення транзакції.

Звіт також висвітлює значні успіхи міжвідомчої співпраці. Зокрема, діяльність спеціалізованого підрозділу DCPCU (Dedicated Card and Payment Crime Unit), створеного у партнерстві з поліцією Лондона і Метрополітенською поліцією (Met Police), призвела до запобігання втратам на суму понад £64,9 млн, арешту 90 злочинних угруповань і винесення 75 обвинувальних вироків. Суттєвим є розвиток системи Banking Protocol, яка дозволяє банківським працівникам, виявивши ознаки можливого шахрайства, негайно викликати поліцію — у 2024 році це дозволило запобігти втратам ще на £61 млн і стало причиною понад 12 тисяч викликів.

Ще однією важливою частиною документа є розгляд проблеми вразливих клієнтів, які можуть стати жертвами шахраїв через свій психічний чи соціальний стан. Банк і поліція розробили механізм сповіщення про таких осіб, і за рік кількість таких повідомлень зросла вдвічі. У цьому ж контексті згадується про кампанії, розраховані на молодь, людей з особливими освітніми потребами та тих, для кого англійська не є рідною мовою.

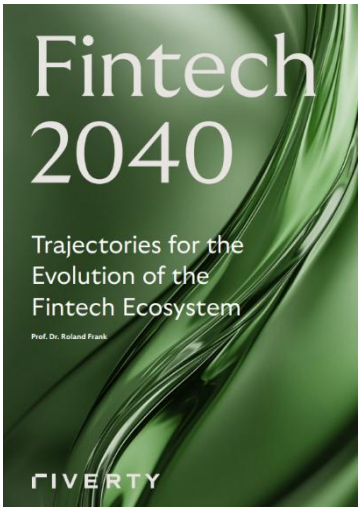
На рівні політики звіт закликає розглядати шахрайство не лише як економічний чи споживчий ризик, а як загрозу національній безпеці. Автори наголошують, що багато злочинців діють з-за меж юрисдикції Великої Британії, і класична кримінальна відповідальність тут часто не застосовується. Відтак, необхідно об'єднувати зусилля приватного сектору, регуляторів, телеком-компаній та міжнародних партнерів для побудови спільної інфраструктури попередження і реагування.

Загалом, документ демонструє високий ступінь усвідомлення галуззю нових ризиків та необхідності переходу до проактивної моделі боротьби з шахрайством, заснованої на превенції, інтелектуальному аналізі даних, інтеграції технологій і співпраці всіх гравців цифрової екосистеми. У фокусі не лише захист активів, а й збереження довіри до фінансової системи в епоху стрімкої цифровізації, яка, хоча й відкриває нові можливості, водночас породжує безпрецедентні загрози.

Висновки:

- **APP-шахрайство скорочується, але адаптація злочинців вимагає безперервної превенції:** зменшення кількості випадків на 20% і втрат на 2% свідчить про ефективність багаторівневих заходів, зокрема обов'язкового відшкодування (PSR), але зростання середніх сум шахрайства під час покупок вимагає подальшої уваги до масштабних схем.
- **Шахрайство під час дистанційних покупок— нова «епідемія» у сфері шахрайства:** 2,6 млн випадків і зростання втрат до £400 млн зумовлені масштабним використанням скомпрометованих OTP-кодів і відсутністю належного захисту в e-commerce (особливо за межами Великої Британії).
- **Спільні дії галузі, правоохоронців і держави дали змогу запобігти втратам на £1,45 млрд,** але основне завдання — не відшкодування, а запобігання та ідентифікація ризиків у реальному часі (наприклад, завдяки поведінковій аналітиці).
- **Поширення шахрайства як послуги і використання AI злочинцями створює новий рівень загроз**, що не можна ігнорувати. Використання Agentic AI вимагає радикального оновлення інструментів виявлення аномалій та законодавчих змін у сфері кібербезпеки.

Майбутнє фінансів: сценарії еволюції Fintech до 2040 року[12]



Документ, створений професором Роландом Франком у співпраці з Riverty Group, є системним і глибоко аналітичним дослідженням, присвяченим трансформації фінансових технологій у період до 2040 року. Основна мета дослідження — не лише окреслити технологічні тенденції, а й сформулювати цілісне бачення майбутньої фінтех-екосистеми, зосереджуючись на її архітектурі, динаміці, ключових учасниках і очікуваних змінах у поведінці споживачів. Центральним аналітичним інструментом виступає концепція Order-to-Cash (O2C) — наскрізний процес, що охоплює весь цикл взаємодії між клієнтом і компанією: від розміщення замовлення до фінального платежу, включаючи доставку, обробку платежів, визнання доходу та постпродажну комунікацію. Через цю призму автор аналізує, як новітні технології впливають на всі етапи O2C-процесу, і демонструє, як Fintech еволюціонує від цифрового інструменту до повноцінної інфраструктури повсякденного життя.

Звіт ідентифікує шість ключових технологічних рушіїв, які формуватимуть фінансову екосистему до 2040 року: AI-агенти, AI-орієнтована кібербезпека, криптовалюти та DeFi, вбудовані фінансові послуги, фінансова прозорість, грамотність та інклюзія, а також квантові обчислення. Кожна з цих технологій аналізується у двох вимірах — персоналізація та автоматизація — що дозволяє автору побудувати матрицю майбутнього: фінансові сервіси стають одночасно більш персоналізованими для кожного користувача та автономними у своїй роботі. У майбутньому, як передбачається, AI-агенти перейдуть від функцій внутрішніх операційних процесів до повноцінної взаємодії з клієнтом — від виявлення шахрайства до формування персоналізованих фінансових рішень у реальному часі. DeFi, у свою чергу, замінює традиційні фінансові структури смарт-контрактами, що усувають посередників і забезпечують прозорість, масштабованість і контроль з боку користувача. Вбудовані фінансові послуги трансформують будь-який нефінансовий продукт або платформу в канал надання фінансових послуг, а квантові

Висновки:

- **Фінансові ШІ-агенти до 2040 року** стануть основним інтерфейсом взаємодії споживача з фінансами — компаніям слід інвестувати у розробку моделей «персоналізації на рівні однієї особи», які об’єднують інвестиції, бюджетування, кредитування та страхування в одному розумному помічнику.
- **RegTech та AI-based Cybersecurity** повинні стати основним напрямом стратегічних інвестицій: до 2040 року понад 70% кіберзахисту буде автоматизовано, а фінансові установи мають впровадити нову архітектуру довіри на основі біометрії та безперервної автентифікації.
- **DeFi, криптовалюти та CBDC** створять нові моделі транзакцій без посередників — регуляторам та компаніям необхідно адаптувати моделі комплаєнсу до смарт-контрактів, мультивалютного середовища та фінансової самостійності користувачів.
- **Інклюзія та Explainable AI стануть базовими очікуваннями користувача** — тому Fintech-компанії мають створювати відкриті, прозорі та освітні рішення, які не лише дають послугу, а й навчають користувача взаємодіяти з нею усвідомлено.

[12] https://www.riverty.com/49a2b2/globalassets/media-images/insights/fintech-2040/riverty_fintech2040.pdf

обчислення відкривають нові горизонти для оптимізації ризиків, портфельного управління та криптографії.

Звіт приділяє окрему увагу адаптаційній моделі, яка дозволяє класифікувати нові технології за ступенем їхнього впливу на клієнта (інкрементальний чи проривний) і характером завдань (операційні чи стратегічні). Це дозволяє компаніям розрізняти технології, які можна швидко впровадити з відчутним ефектом («оперативні досягнення»), від тих, що потребують довгострокових інвестицій. Наприклад, біометричні сканери ідентифікуються як технологія, що швидко дає користувацьку цінність, тоді як квантова криптографія — як стратегічна інвестиція, що забезпечить безпеку в постквантовому середовищі.

Документ базується на двох методологічних стовпах: аналітичному огляді наукової та галузевої літератури і так званому підході орієнованому на клієнті — оцінці впливу кожної технології через призму зручності, користі та цінності для кінцевого користувача. Таким чином, автор зберігає баланс між концептуальним баченням і практичною орієнтацією. У центрі уваги — як технології трансформують реальний фінансовий досвід людини, від способу здійснення платежів до прийняття рішень про інвестиції чи кредитування.

На завершення автор формулює заклик до дій: Fintech 2040 не є просто спробою прогнозування — це запрошення до міжсекторної співпраці, спільного моделювання фінансової інфраструктури майбутнього, яка буде одночасно цифровою, прозорою, етичною та інклюзивною. Сформульовані у звіті сценарії та інструменти можуть бути використані як стратегічна дорожня карта для компаній, що прагнуть не лише адаптуватися до майбутнього, а активно його формувати.

ВНУП

Переосмислення нагляду за визначеними нефінансовими установами та професіями [13]

Стаття, присвячена новим акцентам у міжнародній системі протидії відмиванню коштів, висвітлює кардинальний зсув у підході до нагляду за визначеними нефінансовими установами та професіями. Упродовж тривалого часу ці сектори – зокрема юристи, бухгалтери, агенти з нерухомості, надавачі трастових та корпоративних послуг, казино, а також дилери дорогоцінних металів і каміння – залишалися на периферії уваги національних та міжнародних режимів ПВК/ФТ. Увага концентрувалася насамперед на фінансових установах, залишаючи ВНУП у сфері обмеженого або формального нагляду, який часто делегувався саморегулівним органам без належних повноважень і ресурсів.

Поворотною точкою стала оновлена редакція Безпосереднього результату 4 (БР4) у методології FATF у 2024 році, яка поставила ВНУП у центр оцінювання ефективності. Якщо раніше оцінювання фокусувалося переважно на формальному нагляді загалом, тепер ключова увага приділяється наглядовим практикам саме щодо ВНУП: від ризик-орієнтованих підходів до інспекційної діяльності, режимів санкціонування і наявності дієвих оцінок ризиків. Цей зсув відображає усвідомлення ролі ВНУП як системних "воріт" до зловживань у фінансовій системі, з огляду на їхню участь у створенні та обслуговуванні складних утворень і фінансових структур.

[13] https://sites.google.com/view/dnfbp?usp=sharing

Стаття демонструє, що слабкий нагляд за ВНУП є історично обумовленим явищем. Поєднання політичної чутливості (особливо у відношенні до юридичної спільноти), фрагментації сектору, обмежених ресурсів саморегулівних організацій (ОСР) та фокусування на банківському секторі призвело до нерівномірного розвитку механізмів нагляду. У результаті спостерігається низька якість оцінок ризиків, відсутність системної інспекційної роботи та майже повна неспроможність забезпечення виконання вимог.

Автор статті наводить переконливі приклади кращих та гірших практик на підставі останніх Звітів про взаємну оцінку. Зокрема, виділено успішні юрисдикції, як-от Сінгапур і Ірландія, які застосовують оновлені ризик-орієнтовані підходи, використовують тематичні перевірки для виявлення крос-секторальних вразливостей, інтегрують AML-нагляд із пруденційним, та інвестують у SupTech-рішення. Навпаки, у 44% оцінених країн нагляд за ВНУП було визнано неефективним: лише 7% наглядових органів мали актуальні оцінки ризиків, значна частина наглядачів не володіла належними повноваженнями або аналітичними інструментами.

Особливо критично виглядає ситуація у випадках, коли ОСР номінально здійснюють нагляд, але фактично виконують лише реєстраційні функції без можливості застосування санкцій. У таких випадках нагляд набуває суто декоративного характеру. Додаткові труднощі створюють особливості окремих секторів ВНУП. Наприклад, ринок нерухомості часто роздроблений, що ускладнює контроль, а адвокати можуть посилатися на професійну таємницю для уникнення інспекцій.

Стаття підсумовує ключові уроки, які мають бути засвоєні наглядовими органами: необхідність повної імплементації ризик-орієнтованого підходу; чіткий розподіл повноважень між державними органами та ОСР з відповідними гарантіями ефективності; інвестування в навчання, роз'яснення та постійний контакт з піднаглядними суб'єктами; а також запровадження реального режиму застосування санкцій, який має бути видимим, пропорційним і стримуючим.

Висновки:

- **Юрисдикціям слід терміново оновити та інституціоналізувати секторальні оцінки ризиків ВНУП**, забезпечивши їх регулярне оновлення та інтеграцію у наглядову діяльність, включно з тематичними перевірками та плануванням інспекцій.
- **Потрібно забезпечити, щоб ОСР, які виконують функції нагляду, мали законодавчо закріплені повноваження щодо доступу до інформації**, проведення інспекцій і застосування санкцій, або ж розглянути перехід до прямого державного нагляду.
- **Наглядові органи мають розвивати цифрові інструменти SupTech для збору, аналізу та візуалізації даних** про відповідність, що дозволить ефективніше розподіляти ресурси відповідно до ризику та оперативно реагувати на виявлені вразливості.
- **Слід запровадити стратегії постійної комунікації з піднаглядними суб'єктами**: роз'яснення вимог мовою, зрозумілою для відповідного сектора, розробка прикладних посібників і обов'язкове навчання для підвищення рівня обізнаності та відповідального ставлення до виконання вимог ПВК/ФТ.

Нарешті, з урахуванням початку п'ятого раунду взаємних оцінок, усі юрисдикції мають розглядати нагляд за ВНУП як стратегічну складову національної системи ПВК/ФТ, а не як другорядний обов'язок. Йдеться не лише про дотримання формальних стандартів FATF, а про побудову стійких інституційних механізмів, здатних адаптуватися до нових загроз і захищати цілісність правової та фінансової систем.

Інші новини

Необґрунтовані звіти про підозрілі транзакції: Нові виклики для фінансових установ у світлі рішення BaFin [14]

Новина, підготовлена юридичною фірмою White & Case LLP, аналізує рішення Федерального управління фінансового нагляду Німеччини (BaFin) від 6 березня 2025 року, яке стосувалося накладення санкцій на платіжну установу за недоліки в організації бізнес-процесів, зокрема у сфері виявлення та звітування про підозрілі транзакції (Suspicious Transaction Reports, STR).

Ця новина є важливою, оскільки вона відображає нову тенденцію в регуляторній практиці BaFin, яка вперше застосувала санкції за подання "необґрунтованих" STR, сигналізуючи про посилення вимог до якості звітів та необхідність балансу між надмірним і недостатнім звітуванням. Це рішення має значні практичні наслідки для фінансових установ, які змушені переглядати свої системи моніторингу транзакцій, калібрування критеріїв підозрілості та внутрішні процеси, щоб відповідати оновленим очікуванням регулятора, уникати санкцій і забезпечувати ефективне виконання вимог щодо боротьби з відмиванням грошей.

У ширшому контексті новина підкреслює контраст між підготовкою фінансових установ Європейського Союзу до впровадження нового пакету регуляцій щодо боротьби з відмиванням грошей (AML Package), який набуде чинності з середини 2027 року, та певним послабленням вимог до AML-відповідності в США. У Німеччині BaFin посилює контроль за дотриманням вимог до подання STRs, які є обов'язковими для організацій, визначених як "підзвітні установи" відповідно до Закону про боротьбу з відмиванням грошей (Geldwäschegesetz, GwG), що базується на Директиві ЄС 2015/849. Підзвітні установи повинні негайно повідомляти ПФР про транзакції, які викликають підозру щодо походження коштів або пов'язані з фінансуванням тероризму. Рішення BaFin від 6 березня 2025 року є новаторським, оскільки вперше санкції були застосовані не за несвоєчасне подання STRs, а за подання "необґрунтованих" звітів, тобто таких, що не відповідають критеріям підозрілості. Це вказує на зміну підходу регулятора до якості звітів і необхідності уникнення надмірного звітування, яке перевантажує ПФР.

Раніше BaFin штрафувала установи за несвоєчасне подання STRs, що спонукало фінансові організації застосовувати обережний підхід, подаючи звіти навіть за мінімальних підозр, щоб уникнути регуляторних ризиків. Така практика призвела до значного зростання обсягу даних, які обробляє ПФР, створюючи перевантаження системи. У рішенні BaFin наголосила, що фінансові установи повинні впроваджувати IT-системи моніторингу, які ефективно фільтрують транзакції без ознак підозрілості, щоб зменшити кількість необґрунтованих STRs. Це рішення відображає очікування регулятора щодо більш точного та виваженого підходу до виявлення підозрілих транзакцій, що вимагає від установ перегляду їхніх внутрішніх процесів і технологій.

Відповідно до секції 43 GwG, звіт про підозрілу транзакцію необхідно подавати, якщо є підстави вважати, що активи, пов'язані з діловими відносинами, посередництвом чи транзакцією, походять від злочинної діяльності, яка може бути предикатним злочином для відмивання грошей, якщо транзакція чи активи пов'язані з фінансуванням тероризму, або якщо контрагент не виконує обов'язок розкрити інформацію про бенефіціарного власника. У своїх рекомендаціях

[14] https://www.whitecase.com/insight-alert/unsubstantiated-suspicious-transaction-reports

(Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, AuA) BaFin зазначає, що підозрілі транзакції визначаються на основі мети та характеру ділових відносин, а також типових моделей транзакцій на ринку. Транзакція вважається підозрілою, якщо вона не відповідає звичайній діяльності клієнта, є особливо складною, великою за обсягом або незвичною. Поріг для подання STRs є дуже низьким: достатньо "обґрунтованих підстав" для підозри, а підзвітні установи не повинні проводити детальне розслідування, а лише оцінювати транзакцію на основі "загального досвіду" та "професійних знань". Німеччина застосовує "all-crimes approach", що означає, що будь-який злочин може бути предикатним для відмивання грошей, що розширює спектр транзакцій, які потенційно підлягають звітуванню.

Рішення BaFin підкреслює критичну важливість правильного калібрування критеріїв для виявлення підозрілих транзакцій у системах моніторингу. Надто широкі критерії призводять до генерації великої кількості сповіщень, що може перевантажити як внутрішні процеси установи, так і ПФР, тоді як надто вузькі критерії створюють ризик пропуску підозрілих транзакцій, що також загрожує регуляторними санкціями. Після виявлення потенційно підозрілої транзакції IT-системою, установа повинна оцінити сповіщення, враховуючи мету ділових відносин, попередні транзакції клієнта та типові моделі транзакцій у відповідному сегменті клієнтів. Хоча автоматизовані процедури є допустимими, необхідні спеціальні процеси перевірки та вибіркові перевірки для забезпечення точності.

Надмірне подання STRs створює практичні проблеми, зокрема внутрішні затримки та невизначеність щодо виконання транзакцій. Згідно з GwG, транзакцію можна виконати через три робочі дні після подання STR, якщо ПФР не надає зворотного зв'язку, але в практиці залишаються невирішені юридичні питання щодо цього процесу, що ускладнює операційну діяльність установ. Рішення BaFin, ймовірно, спричинить дискусії серед учасників ринку щодо оптимального визначення підозрілих транзакцій та необхідності балансу між надмірним і недостатнім звітуванням. Фінансові установи повинні переглянути свої процеси звітування, калібрування критеріїв і оцінки сповіщень, щоб відповідати новим очікуванням BaFin. Критерії підозрілості мають бути чітко задокументовані, регулярно переглядатися та адаптуватися на основі подій чи накопиченого досвіду.

Трансформація злочинності: як кримінальні групи Латинської Америки адаптуються до цифрової ери [15]

Стаття InSight Crime досліджує, як злочинні групи в Латинській Америці адаптуються до цифрової ери, використовуючи технологічні інновації для вдосконалення своїх незаконних операцій. Автор Сара Гарсія, спираючись на інтерв'ю з Антоніо Нікасо, професором Університету Квінз у Канаді та директором Центру дослідження кіберзлочинності Фонду Magna Grecia в Італії, детально аналізує трансформацію злочинних економік у регіоні, зокрема таких діяльностей, як торгівля наркотиками, відмивання грошей, кіберзлочини та онлайн-шахрайство.

У цифрову еру, інтернет кардинально змінив методи діяльності злочинних організацій у Латинській Америці. Технологічні інновації відкрили нові можливості для таких груп, як мексиканські картелі Сіналоа та Халіско (CJNG), а також бразильська організація Primeiro

[15] https://insightcrime.org/news/how-have-criminal-groups-adapted-digital-age/

Comando da Capital (PCC). Злочинці використовують відкритий інтернет і дарк-веб для закупівлі прекурсорів для виробництва синтетичних наркотиків, таких як фентаніл і метамфетамін, через продавців, які забезпечують доставку до будь-якої точки світу. Криптовалюти стали ключовим інструментом для відмивання грошей, отриманих від наркоторгівлі, а також для фінансування інших незаконних операцій. Наприклад, у 2018 році бразильська PCC ще не володіла достатніми знаннями для операцій із біткойнами, але до 2025 року організація активно інвестує в криптовалюти та бере участь у кіберзлочинах, таких як онлайн-шахрайство. Подібну активність демонструє й інша бразильська група, Comando Vermelho, яка також інвестує в цифрові валюти.

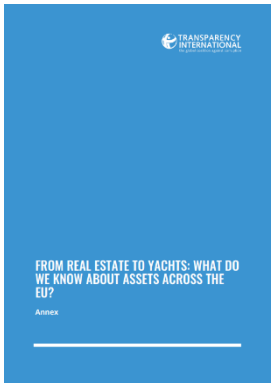
Антоніо Нікасо підкреслює, що злочинні групи адаптуються до цифрового світу, змінюючи свою структуру та підходи. Їхній "соціальний капітал" — мережа зовнішніх зв'язків, яка раніше спиралася на юристів, бухгалтерів і брокерів, — тепер включає нових спеціалістів, таких як інженери штучного інтелекту (ШІ), які розробляють зашифровані системи для обміну повідомленнями, та експерти з криптовалют, які використовують спеціалізоване обладнання для майнінгу. Ці фахівці дозволяють злочинним групам діяти в гібридному форматі, поєднуючи традиційні офлайн-методи з віртуальними онлайн-інструментами. Такий підхід ускладнює їх відстеження та вимагає від правоохоронних органів перегляду стратегій боротьби зі злочинністю.

Соціальні мережі стали ще одним важливим інструментом для злочинних організацій. Вони використовують їх як продовження фізичного контролю над територією, створюючи віртуальний простір для просування власного бренду. Злочинці демонструють багатство та вплив, щоб залучати нових членів, особливо молодь, пропонуючи їм "успішний" спосіб життя. Через соціальні платформи вони також поширюють наративи про боротьбу з маргіналізацією чи протистояння державі, формуючи нову ідентичність і почуття приналежності серед своїх послідовників. Це дозволяє не лише зміцнювати їхню присутність, але й ефективно вербувати нових учасників.

Стаття також звертає увагу на серйозні виклики для правоохоронних органів. Технологічний розрив між злочинцями та владою залишається значним. У багатьох країнах, наприклад в Італії, правоохоронці обмежені у використанні хакерів для протидії кіберзлочинності, тоді як злочинні групи активно залучають таких фахівців. Нікасо наголошує на необхідності глобальної стратегії, яка включає використання ШІ та алгоритмів для аналізу даних і відстеження гібридної злочинної діяльності. Без таких інновацій правоохоронні органи залишатимуться позаду, оскільки традиційні методи боротьби зі злочинністю вже не відповідають сучасним реаліям.

Для загального розвитку

Прозорість під мікроскопом: огляд реєстрів активів у дев'яти країнах ЄС[16]



Документ є фактично технічним додатком до ширшого дослідження, проведеного Transparency International з метою картографування та оцінки стану обліку активів у державах-членах Європейського Союзу. Він фокусується на дев'яти країнах: Франції, Німеччині, Ірландії, Італії, Латвії, Литві, Португалії, Словенії та Іспанії — і презентує їхні національні реєстри у системному порівняльному вигляді. Документ зосереджено на ідентифікації офіційних державних баз даних, які покликані забезпечити прозорість власності над ключовими видами активів, що мають значення у контексті боротьби з відмиванням коштів, фінансуванням тероризму,

[16] https://images.transparencycdn.org/images/ANNEX_What-do-we-know-about-assets-across-the-EU_2025.pdf

ухиленням від сплати податків та відстеженням незаконно набутого майна.

Структурно документ розділено на кілька великих секцій, відповідно до типів активів: бенефіціарна власність, юридичні особи, банківські рахунки, нерухомість, автотранспорт, водні судна, повітряні судна, інвестиційні частки та спеціалізовані майнові реєстри. У кожному сегменті автори подають порівняльну таблицю з назвами реєстрів, установами, відповідальними за їх ведення, та коротким описом або коментарем щодо особливостей функціонування. Паралельно документ надає посилання на національне законодавство, офіційні урядові портали, нормативні акти Європейського Союзу та письмові відповіді органів влади, отримані Transparency International упродовж 2024–2025 років.

Однією з головних тем документа є реєстри бенефіціарних власників, які розглядаються у трьох площинах: для юридичних осіб, для колективних інвестиційних структур і для правових утворень (зокрема трастів, довірених осіб та інших подібних структур). Значна увага приділена відмінностям у підходах держав: у Німеччині функціонує централізований Transparenzregister, у Франції — RBE, тоді як в Італії відповідний реєстр станом на травень 2025 року було офіційно призупинено. Деякі держави створили спеціальні реєстри для трастів (наприклад, CRBOT в Ірландії), а інші інтегрували інформацію у вже існуючі системи юридичних осіб. Водночас, попри загальноєвропейські вимоги до обов'язковості реєстрації КБВ (зокрема стаття 30 та 31 Директиви (ЄС) 2015/849, у редакції Директиви (ЄС) 2018/843), охоплення трастових і некомерційних структур залишається вибірковим.

У сфері юридичних осіб документ показує наявність чітко визначених реєстрів у всіх країнах, які зазвичай ведуться органами реєстрації компаній або торговими палатами. Наприклад, у Франції діє Національний реєстр підприємств (RNE) та Реєстр комерції та компаній (RCS), які інтегровані з реєстром бенефіціарів. У Литві та Латвії цю функцію виконує державний регістр підприємств, підпорядкований відповідним міністерствам юстиції. Водночас у частині країн, зокрема Італії, ведення реєстрів здійснюється за підтримки регіональних торгових палат, що створює більшу децентралізацію.

У розділі про банківські рахунки виділено ініціативу BARIS — європейську систему обміну даними про банківські рахунки. У більшості країн існує централізований державний реєстр рахунків: у Франції — FICOBA (під контролем DGFIP), у Німеччині — автоматизована процедура отримання інформації з рахунків під наглядом BaFin, в Італії — Архів фінансових відносин (Archivio dei rapporti finanziari), в Ірландії — ISBAR. Проте рівень доступу до цих систем, регулярність оновлення та глибина даних істотно відрізняються.

Секція про нерухомість і землю засвідчує, що всі держави мають офіційні земельні реєстри, однак їх структура і ступінь діджиталізації варіюються. Наприклад, у Словенії діє цифрова Земельна книга, адміністрована геодезичним управлінням, тоді як у Німеччині реєстри ведуться судами на місцевому рівні. У більшості випадків інформація є обмежено публічною, з можливістю доступу лише за спеціальними запитами або за участі нотаріусів.

У розділі про автотранспорт документ надає огляд національних реєстрів зареєстрованих транспортних засобів. Наприклад, ZFZR у Німеччині, SIV у Франції, NVDF в Ірландії, PRA та ANV в Італії, CSDD у Латвії, REGITRA у Литві тощо. У більшості випадків дані ведуться централізовано, хоча доступ до реєстрів обмежений.

Реєстри водних суден поділяються на реєстри морських та річкових суден, які у кожній країні мають окреме підпорядкування. У Франції, наприклад, використовується одразу кілька платформ — PUMA (для яхт) і RIF (для комерційних суден). В Італії існує Telematic Archive для човнів для дозвілля та окремий Реєстр міжнародної навігації. Подібна фрагментація спостерігається і в інших державах.

Окрема секція присвячена повітряним суднам — у кожній країні є національний авіаційний регістр, яким опікуються або цивільні авіаційні агентства, або міністерства транспорту. Документ фіксує назви цих реєстрів, відповідальні органи, посилання на нормативні джерела та відомості щодо того, чи охоплюються всі типи літальних апаратів.

У фінальній частині додатку подано великий обсяг нормативних посилань, які охоплюють не лише європейське право (зокрема нові Директиви ЄС 2024 року), а й десятки національних законів, указів, положень та інструкцій — усі з активними посиланнями на офіційні портали законодавства. Також додано перелік джерел, включаючи відповіді органів влади, отримані через інформаційні запити, інтерв'ю з представниками державних установ і витяги з офіційних сайтів реєстрів.

Таким чином, документ є детальною, структурованою, верифікованою технічною базою, що дозволяє не лише оцінити рівень прозорості у кожній окремій країні, а й зрозуміти загальний стан гармонізації в межах ЄС, виявити прогалини в обліку активів та побачити, наскільки державні інфраструктури здатні ефективно виявляти майно та встановлювати справжніх бенефіціарів. Це потужний аналітичний інструмент для оцінювання ефективності систем запобігання зловживанням фінансовою системою Європейського Союзу.

Сім ключових тенденцій, на які варто звернути увагу в 2025 році

Глобальний ландшафт фінансової злочинності швидко змінюється. Якщо ви працюєте у сфері комплаєнсу, ризиків, криптовалют або фінтех, ось тенденції, які формують наш світ зараз:

1. Штучний інтелект бере на себе ініціативу в моніторингу

Регулятори очікують систем з ПВК на основі штучного інтелекту. Йдеться про швидше виявлення, розумніші сповіщення та меншу кількість хибнопозитивних результатів.

2. FATF перемикає фокус на ефективність

У своєму 5-му раунді взаємних оцінок FATF запитує: Чи дійсно ваші засоби контролю працюють на практиці?

3. Запущено новий орган ЄС з ПВК (AMLA)

ЄС офіційно запустив AMLA, централізований наглядовий орган з прямими повноваженнями щодо нагляду за високоризиковими організаціями по всьому блоку. Транскордонна гармонізація нарешті стає реальною.

4. Китай вперше за 17 років оновлює закон про боротьбу з відмиванням коштів

Закон Китаю про боротьбу з відмиванням коштів 2025 року розширює охоплення на нефінансові установи, посилює зобов'язання щодо звітності та посилює правозастосування, передбачаючи суворіші штрафи.

5. Регулювання криптовалют стає серйознішим

DeFi, міксери та гаманці стикаються з новими правилами в ЄС, Сполученому Королівстві та Азії. Правило подорожей тепер діє в більшій кількості юрисдикцій і виконується.

6. ESG + AML = Новий рубіж

Злочини проти довкілля є зростаючим ризиком ПВК. Незаконний видобуток корисних копалин, лісозаготівля та торгівля відходами тепер є частиною оцінки ризиків відповідності.

7. Прозорість КБВ стає глобальною

Публічні реєстри бенефіціарної власності поширюються. Дні анонімних фіктивних компаній добігають завершення.

Що це означає для працівників з питань комплаєнсу:

- ✓ Переосмисліть свої моделі ризиків
- ✓ Відстежуйте транскордонні регуляторні зміни
- ✓ Вбудуйте ESG-ризики та криптовалютні ризики у свою програму з ПВК

Ваша думка важлива!

1. Чи слід посилити вимоги до перевірки на етапі onboarding з урахуванням кейсів ПФР Джерсі? Наскільки обґрунтованим є використання OSINT і соціальних мереж як інструментів верифікації?
2. Яким чином країни мають реагувати на виклики дерейтингу щодо суб'єктів з високоризикових юрисдикцій, щоб забезпечити доступ до фінансових послуг без шкоди для безпеки фінансової системи?
3. Яким має бути оптимальний регуляторний режим для геймінг-індустрії у сфері ПВК/ФТ: які елементи (вимоги до KYC, обов'язки звітності, модерація ШІ-контенту тощо) мають бути ключовими, щоб забезпечити ефективне попередження зловживань без надмірного навантаження на галузь?
4. Як геополітична співпраця між державами-ізгоями (росією, Іраном, КНДР) трансформує ризики у сфері фінансування тероризму та розповсюдження ЗМЗ? Наскільки ефективними є наявні механізми виявлення фінансування через посередників, складні ланцюги транзакцій та постачання товарів подвійного призначення?
5. Наскільки застосовна модель відшкодування збитків від APP-шахрайства для інших країн, включно з Україною? Чи є ризик того, що подібна модель стимулюватиме недобросовісні звернення?
6. Як соціальні мережі використовуються злочинними або ворожими організаціями для вербування, дестабілізації ситуації чи просування проросійських наративів, і яким чином українські правоохоронні органи можуть ефективніше виявляти та протидіяти таким загрозам?
7. Як українським правоохоронним органам адаптувати національні механізми боротьби з кіберзлочинністю та відмиванням коштів до нових викликів цифрового середовища, враховуючи практичний досвід Eurojust у розслідуванні таких злочинів?

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-2025-23

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

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