Методологічний бюлетень

Серійний номер: МінФін-AML-2025-05

Січень 2025

Мета

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи 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.

Включає 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

Як Росія обходить санкції: новий посібник для експортерів від уряду Великобританії [1]

Документ, опублікований урядом Великобританії у 2025 році, є вичерпним керівництвом для експортерів щодо виявлення, запобігання та протидії ухиленню Росії від міжнародних санкцій. Він розроблений Департаментом бізнесу та торгівлі Великобританії у співпраці з Офісом реалізації торгових санкцій і містить конкретні рекомендації для компаній, які можуть бути залучені до схем обходу санкцій або зазнавати ризику зловживань з боку контрагентів.

Документ розпочинається із загального огляду проблеми обходу санкцій, наголошуючи, що з моменту початку повномасштабного вторгнення РФ в Україну у 2022 році Великобританія запровадила масштабні експортні обмеження, які мають на меті заблокувати доступ Росії до критично важливих товарів і технологій. Проте, попри зниження обсягів прямої торгівлі з РФ, британська влада виявила зростання випадків непрямого постачання санкційних товарів через треті країни, зокрема Китай, Туреччину, Казахстан, Вірменію, ОАЕ та інші держави. Росія використовує складні механізми обходу санкцій, включаючи фіктивні компанії, підставних осіб, нелегальні маршрути постачання та зміну кінцевих споживачів у документації.

[1] https://www.gov.uk/government/publications/countering-russian-sanctions-evasion-and-circumvention/countering-russian-sanctions-evasion-guidance-for-exporters

У документі представлений так званий Common High Priority List (CHPL) – список критично важливих товарів, які РФ намагається отримати для підтримки своїх військових можливостей. Він розроблений у співпраці з ЄС, США та Японією і містить понад 50 найменувань, які розподілені за чотирма категоріями ризику. До них належать мікроелектроніка (інтегральні схеми, мікропроцесори, напівпровідники), електронні компоненти для комунікаційних систем, обладнання для виробництва та тестування електроніки, верстати з ЧПУ, а також механічні та електромеханічні компоненти для військової техніки. Крім того, до списку входять промислове обладнання, компоненти для аерокосмічної галузі, автомобільні деталі, мастильні матеріали, нафтопереробні продукти, друкарські фарби та деякі види програмного забезпечення.

Окремий розділ присвячено методам ухилення від санкцій, які найчастіше використовує Росія. До них відносяться багатоетапні торговельні операції через мережу посередників, замовлення товарів через компанії у третіх країнах, зміна кінцевих споживачів у документації, штучне заниження або завищення вартості товарів для обходу контролю, використання складних фінансових схем, включаючи криптовалютні платежі. Також підкреслюється, що РФ активно створює нові компанії-посередники у дружніх країнах, використовуючи непрозорі корпоративні структури для приховування реальних отримувачів товарів.

Документ містить детальний перелік червоних прапорців (red flags) – індикаторів можливого порушення санкцій. Вони поділені на чотири основні категорії: ризики, пов’язані з товаром, клієнтом, фінансовими транзакціями та експортним маршрутом. До них належать невідповідність товару заявленому призначенню, замовлення високотехнологічної продукції компаніями, що не мають відповідної спеціалізації, невідповідність кінцевого отримувача типу товару, використання підставних компаній, раптове збільшення закупівель від нового клієнта, підозрілі фінансові операції (наприклад, платежі з третіх країн або використання готівки для великих закупівель), відсутність онлайн-присутності у замовника та складні логістичні маршрути, що вказують на можливість реекспорту товарів у Росію.

Окрема увага приділяється найкращим практикам комплаєнсу та перевірки контрагентів. Рекомендується проводити розширену процедуру «знай свого клієнта» (KYC), перевіряти бенефіціарну структуру замовників, ретельно аналізувати фінансові операції та маршрути поставок. Підприємствам рекомендовано використовувати міжнародні санкційні бази, включати у договори пункт про заборону реекспорту в Росію («No Russia Clause») і проводити регулярний моніторинг змін у торговельній активності своїх клієнтів.

Документ також роз’яснює відповідальність компаній за порушення санкцій. Вказується, що ненавмисне або умисне постачання товарів, що можуть бути використані у військових цілях РФ, може призвести до кримінальної відповідальності, значних штрафів та репутаційних ризиків. Органами контролю за дотриманням санкцій у Великобританії є HM Revenue & Customs (митна служба) та Офіс реалізації торгових санкцій. Компанії, що підозрюють потенційне порушення санкцій, зобов’язані повідомляти відповідні органи, зокрема через систему добровільного розкриття інформації.

Завершальна частина документа містить корисні ресурси для бізнесу, включаючи посилання на британські, європейські та американські регуляторні органи, бази даних підсанкційних компаній та інструменти для перевірки контрагентів. Окремо вказані міжнародні дослідницькі ініціативи, такі як RUSI (Royal United Services Institute) та KSE (Kyiv School of Economics), що займаються аналізом схем обходу санкцій і впливу західних технологій на російський військовий комплекс.

Таким чином, документ є комплексним посібником для експортерів, що не лише пояснює механізми ухилення від санкцій, а й пропонує конкретні інструменти для мінімізації ризиків та забезпечення відповідності законодавству. Він підкреслює важливість міжнародної

координації та підвищення обізнаності бізнесу щодо сучасних загроз санкційного обходу, а також закликає компанії до активного залучення у процес контролю за експортом, що є ключовим елементом стратегічного обмеження військових можливостей Росії.

Операція MATRIX: новий удар по організованій злочинності [2]

Міністерство юстиції США оголосило про публікацію четвертого і фінального тому National Firearms Commerce and Trafficking Assessment (NFCTA), підготовленого Бюро алкоголю, тютюну, вогнепальної зброї та вибухових речовин (ATF). Це дослідження є найбільш комплексним аналізом обігу вогнепальної зброї у США та її потрапляння до незаконного ринку. Ініціатива була започаткована у 2021 році за дорученням президента Джо Байдена та Генерального прокурора Мерріка Гарланда з метою розробки ефективних механізмів боротьби з незаконним обігом зброї, оскільки зростання злочинності та поширення нелегальної зброї стали серйозною загрозою національній безпеці.

Четвертий том дослідження зосереджений на аналізі сучасних тенденцій незаконного обігу зброї, механізмів її потрапляння до рук злочинців, а також рекомендаціях щодо політики протидії цьому явищу. Однією з головних проблем є різке зростання кількості так званої "привласненої" зброї (Privately Made Firearms), яка виготовляється без серійних номерів і не проходить через офіційні канали продажу. В період з 2017 по 2023 роки правоохоронні органи США вилучили 92 702 одиниці такої зброї, причому її використання у злочинах зросло на 1600%. Серед вилученої зброї значна частка була пов'язана з випадками домашнього насилля та іншими насильницькими злочинами. Також було зафіксовано зростання виробництва компонентів для таких зразків зброї (рамок та ресиверів), що свідчить про їхнє активне поширення серед злочинців.

Ще однією серйозною загрозою стали пристрої для перетворення напівавтоматичної зброї в автоматичну (Machinegun Conversion Devices), які перетворюють звичайні пістолети та гвинтівки на повноцінні автоматичні зразки. Вилучення таких пристроїв зросло на 784% у період з 2019 по 2023 рік. Для боротьби з цією проблемою у 2024 році було створено спеціальну міжвідомчу ANTI-MCD Task Force, яку очолює ATF та федеральні прокурори.

Крім того, документ підкреслює важливість криміналістичної аналітики та роботи ATF у сфері розслідування злочинів, пов'язаних із застосуванням вогнепальної зброї. Інструменти ATF, такі як Національна інтегрована система балістичної інформації (NIBIN) та електронна система простежування зброї (eTrace), значно підвищили ефективність розслідувань. З 2017 по 2023 рік кількість запитів на простежування зброї зросла на 52%, причому 56% випадків показали невідповідність між покупцем і фактичним власником зброї. Це підтверджує, що нелегальний ринок зброї часто починається з легального продажу. У рамках NIBIN було проаналізовано понад 6,5 мільйонів балістичних записів, що призвело до створення понад 1 мільйона слідчих досьє. Також було зафіксовано, що у 14% випадків одна й та ж зброя використовувалася в кількох різних злочинах, що вказує на стійкі схеми обороту нелегальної зброї.

Окрему увагу в дослідженні приділено торгівлі зброєю через кордон між США та Мексикою. З 2017 по 2023 рік кількість вилученої в Мексиці зброї, яка була простежена до США, зросла на

[2] https://www.justice.gov/opa/pr/justice-department-announces-atfs-publication-final-volume-national-firearms-commerce-and

63%. Основними джерелами незаконного постачання стали Техас (43% усієї простеженої зброї), Аризона (22%) і Каліфорнія (9%). Виявлено п'ять основних каналів постачання зброї до Мексики, де основними кінцевими споживачами є наркокартелі, зокрема Сіналоа та Jalisco New Generation Cartel (CJNG). У відповідь ATF активізувало заходи з перехоплення контрабандної зброї, що призвело до 86% зростання успішних операцій з перехоплення у 2023 році.

Ще однією важливою темою документа є тенденції у виробництві та продажу вогнепальної зброї у США. Було зафіксовано, що між 2000 і 2023 роками виробництво зброї зросло на 113%, що значно перевищує темпи зростання населення (19%). Також різко зросло виробництво глушників, їх випуск збільшився більш ніж на 8000%. Лише у період з 2017 по 2023 рік через ліцензованих продавців до громадян було передано понад 106 мільйонів одиниць вогнепальної зброї.

На основі отриманих даних у документі подані ключові рекомендації для покращення боротьби з незаконним обігом зброї. Однією з основних рекомендацій є розширення системи перевірки покупців зброї (background checks), оскільки дані дослідження доводять, що така практика зменшує ймовірність потрапляння зброї до злочинців. Також запропоновано збільшити відповідальність за перепродаж службової зброї з боку правоохоронних органів, оскільки понад 25 000 одиниць такої зброї були використані у злочинах за останні п'ять років. ATF рекомендує впровадження обов'язкового знищення зброї, що перебуває у відомчому користуванні, після закінчення її експлуатації. Ще однією рекомендацією є розширення використання криміналістичних інструментів ATF у всіх правоохоронних органах США, що дозволить значно підвищити ефективність боротьби зі злочинами, пов'язаними зі зброєю.

Висновки:

- **Нелегальний обіг "ghost guns" та пристроїв для автоматизації зброї різко зріс,** що призвело до тисяч злочинів та створило нові виклики для правоохоронців.
- **Криміналістичні інструменти ATF підтвердили масштаб нелегального трафіку зброї,** зокрема через масовий перепродаж та використання однієї і тієї ж зброї у кількох злочинах.
- **Торгівля зброєю через кордон з Мексикою зросла на 63%,** забезпечуючи картелі вогнепальною зброєю зі США через основні контрабандні маршрути.
- **Необхідно розширити перевірки покупців,** посилити контроль за відомчою зброєю та збільшити фінансування ATF, щоб ефективно протидіяти нелегальному обігу.

Таким чином, фінальний том NFCTA є детальним аналізом проблеми незаконного обігу зброї у США та пропонує низку конкретних заходів для її подолання. Документ наголошує на необхідності подальшого фінансування ATF, розширення використання технологічних рішень та удосконалення правового регулювання, спрямованого на зниження рівня насильства та боротьбу з трафіком вогнепальної зброї.

Відмивання коштів через ринки капіталу: ризики, типології та нові підходи до протидії[3]

Документ є детальним звітом, що аналізує ризики відмивання коштів через фінансові ринки, зокрема капітальні ринки, та містить рекомендації щодо мінімізації цих загроз. Він був

[3] https://www.fca.org.uk/publication/corporate/money-laundering-through-markets-review-january-2025.pdf

підготовлений у січні 2025 року як продовження попередньої тематичної оцінки TR19/4, проведеної у 2019 році, та базується на додаткових наглядових заходах, консультаціях із галузевими експертами, а також вивченні новітніх методів боротьби з фінансовими злочинами.

У документі визначено, що відмивання коштів через ринки капіталу (MLTM) передбачає використання фінансових інструментів, таких як акції, облігації, деривативи та інші активи, для маскування походження злочинних доходів. Це відбувається через складні фінансові операції, які ускладнюють виявлення кінцевого бенефіціара та створюють ілюзію законного походження коштів. Основними ризиками у цій сфері є високий рівень анонімності торгівлі, велика швидкість і обсяг транзакцій, складність фінансових ланцюгів та використання міжнародних юрисдикцій, що обмежують можливість регуляторного нагляду. Звіт базується на аналізі фінансових установ, насамперед брокерських компаній, які відіграють ключову роль у забезпеченні ліквідності ринку, але водночас можуть бути використані злочинцями для відмивання коштів.

Документ містить детальний огляд сучасних типологій ВК через ринки капіталу. Серед виявлених схем відзначаються попередньо узгоджені торги, коли дві сторони заздалегідь домовляються про умови угод з метою переміщення коштів між рахунками, а також так звані Free of Payment (FoP) перекази, що використовуються для обходу санкцій. Аналізується практика використання брокерів та фінансових посередників для приховування кінцевих бенефіціарів угод, маніпуляції з фінансовими деривативами та підозрілі торгові стратегії, такі як дзеркальні та циклічні угоди, де однакові фінансові інструменти купуються і продаються між пов'язаними контрагентами без економічного сенсу.

Оцінюючи ефективність заходів боротьби з MLTM, документ наголошує на важливості впровадження ризик-орієнтованого підходу, який має включати якісний аналіз бізнес-ризиків (BWRA) та оцінку ризику клієнтів (CRA). Багато компаній недооцінюють загрози фінансових злочинів, недостатньо документують власні ризики або не

Висновки:

- **Посилення інтегрованої оцінки ризиків на рівні компаній:**
  - Впровадження регулярного перегляду бізнес-ризиків (BWRA), що включає аналіз типологій MLTM та використання індикаторів підозрілих операцій.
  - Розширення практики оцінки клієнтів (CRA), з урахуванням динамічних змін в їхній поведінці.
- **Покращення моніторингу транзакцій через персоналізовані алгоритми:**
  - Використання багаторівневого моніторингу транзакцій з урахуванням специфіки MLTM, інтегруючи аналіз поведінки клієнтів.
  - Запровадження нових критеріїв автоматизованого виявлення ризиків, що фокусуються на взаємозв'язках клієнтів.
- **Посилення якості подачі SAR-звітності:**
  - Підвищення рівню внутрішньої перевірки якості підозрілих звітів (SAR) перед їх поданням до фінансової розвідки.
  - Використання коду «XXMLTMXX» у всіх релевантних випадках, що стосуються підозр MLTM.
- **Сприяння співпраці між ринковими учасниками та держорганами:**
  - Використання розширених можливостей обміну інформацією відповідно до ECCTA 2023.
  - Запровадження регулярного обміну аналітичними даними між компаніями та UKFIU для виявлення системних ризиків.

оновлюють їх відповідно до змін ринку. Також встановлено, що процес перевірки клієнтів (KYC/CDD) часто має недоліки, зокрема надмірну залежність від інших учасників угод у проведенні належної перевірки контрагентів. Виявлено, що деякі компанії не документують очікуваний характер діяльності клієнтів та не відстежують транзакційні аномалії, що ускладнює виявлення підозрілих операцій.

Моніторинг транзакцій залишається однією з найскладніших ділянок у боротьбі з MLTM. Більшість компаній використовують автоматизовані системи для виявлення підозрілих операцій, однак їх ефективність часто є низькою через високий рівень хибнопозитивних спрацювань. У багатьох випадках системи контролю більше адаптовані до запобігання ринковим зловживанням (market abuse), ніж до виявлення ВК. Регулятори наголошують на необхідності інтегрованого підходу до фінансового моніторингу, що має поєднувати аналіз транзакцій із інформацією про клієнтів, історією торгівлі та можливими зв'язками між контрагентами.

Документ акцентує увагу на необхідності покращення якості звітності про підозрілі операції (SAR). Багато компаній використовують код «XXMLTMXX» неправильно або не подають відповідні звіти взагалі, що ускладнює боротьбу з MLTM на рівні регуляторів. Також зазначається, що інформаційний обмін між компаніями та державними органами є недостатнім, а можливості нових нормативних ініціатив, таких як Economic Crime and Corporate Transparency Act 2023 (ECCTA), ще не використовуються повною мірою.

На підставі отриманих висновків документ пропонує конкретні кроки для мінімізації ризиків MLTM. Серед основних рекомендацій – посилення ризик-орієнтованого підходу на рівні компаній, зокрема через запровадження більш деталізованої оцінки клієнтів і транзакцій. Фінансові установи повинні оновлювати свої системи моніторингу, використовуючи штучний інтелект та аналітику великих даних для точнішого виявлення ризиків. Також рекомендується розширити співпрацю між ринковими учасниками та правоохоронними органами шляхом активного обміну аналітичними даними та інформацією про підозрілі угоди.

У підсумку звіт підкреслює, що ефективна протидія MLTM потребує комплексного підходу, що включає покращене корпоративне управління, підвищення якості підозрілих звітів, зміцнення співпраці між державними та приватними інституціями, а також використання новітніх технологій для аналітики ринкових ризиків. Регулятори очікують від компаній не лише формального дотримання вимог, а й активного впровадження найкращих практик для зменшення загроз фінансових злочинів.

Звіт Європейської Комісії щодо контролю за експортом, посередництвом, технічною допомогою, транзитом і передачею товарів подвійного використання[4]


EUROPEAN COMMISSION

Brussels, 30.1.2025
COM(2025) 19 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items

{SWD(2025) 6 final}

У звіті Європейської Комісії оцінюється реалізація Регламенту (ЄС) 2021/821 щодо контролю експорту, посередництва, технічної допомоги, транзиту та передачі товарів подвійного використання. Документ охоплює період 2022–2023 років і включає деякі ключові події 2024 року, а також надає консолідовані статистичні дані щодо експортного контролю в ЄС. Це перший щорічний звіт такого характеру, який спрямований на підвищення прозорості у сфері експортного контролю шляхом розширення інформаційного обміну між державами-членами щодо рішень з ліцензування експорту.

[4] https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2025)19&lang=en

У звіті розглядаються основні зміни у політиці та нормативно-правовій базі контролю експорту. Однією з ключових реформ стало посилення контролю над кіберспостережними технологіями, які можуть використовуватися для порушення прав людини або гуманітарного права. Для цього Європейська Комісія 16 жовтня 2024 року опублікувала рекомендації для експортерів щодо заходів належної перевірки та відповідності. Крім того, у межах модернізації контролю запроваджено нові механізми взаємодії, зокрема Групу експертів з новітніх технологій (ETEG), Механізм координації правозастосування (ECM) та електронну систему контролю подвійного використання (DUeS) для обміну даними між Європейською Комісією та державами-членами.

Важливою частиною звіту є міжнародна співпраця у сфері експортного контролю. Зокрема, в рамках Торговельно-технологічної ради ЄС-США (TTC) було розширено співпрацю щодо контролю за технологіями подвійного використання та узгодження санкцій проти Росії та Білорусі. Також ЄС відіграє активну роль у Глобальній коаліції санкцій проти Росії (GECC), яка об'єднує 39 країн, що запровадили експортні обмеження для ослаблення військового потенціалу РФ. У рамках діалогу ЄС-Норвегія сторони обговорили питання обмежень щодо експорту технологій подвійного використання та авіаційних технологій.

Оновлення контрольного списку ЄС відбулося відповідно до змін у міжнародних експортних режимах, таких як Васенаарська угода, Група ядерних постачальників та Режим контролю ракетних технологій (MTCR). Особливу увагу було приділено обмеженням на експорт до Росії, зокрема вилученню РФ зі списку країн, які мають доступ до спрощеного експорту за загальними експортними авторизаціями ЄС.

Згідно зі звітом, у 2022 році загальний обсяг дозволеного експорту товарів подвійного використання склав 57,3 млрд євро, що становить 2% від загального експорту ЄС. Було видано 138 764 експортних дозволів, серед яких переважали загальні експортні дозволи ЄС (93 311), національні загальні експортні дозволи (26 953) та індивідуальні ліцензії (17 072). Найбільшими ринками для експорту товарів подвійного використання стали Китай (5,6 млрд євро), Південна Корея (1,7 млрд євро), США (1,3 млрд євро), Японія (1,04 млрд євро) та Сінгапур (994 млн євро).

Висновки:

- **Зміцнення експортного контролю**: ЄС посилив обмеження на експорт товарів подвійного використання, зокрема кіберспостережних технологій, та розширив механізми моніторингу через нові експертні групи та цифрові системи.
- **Міжнародна координація санкцій**: через TTC, GECC та інші механізми ЄС синхронізував заходи експортного контролю із США та іншими партнерами, зокрема в контексті санкцій проти Росії та Білорусі.
- **Значний вплив на торгівлю**: загальний обсяг дозволеного експорту товарів подвійного використання у 2022 році склав 57,3 млрд євро, а кількість відмов у ліцензуванні зросла до 813 випадків.
- **Розширення цифрових інструментів контролю**: електронна система eLicensing поступово інтегрується з національними митними системами, що підвищує ефективність та прозорість експортного контролю в ЄС.

Кількість відмов у видачі експортних ліцензій у 2022 році склала 813 випадків на суму 0,98 млрд євро, що становить 0,04% від загального експорту ЄС. Зростає кількість ліцензій на експорт кіберспостережних технологій, що свідчить про посилення контролю в цій сфері. У 2022 році подано 288 заявок на експорт таких товарів, з яких 224 було схвалено, а 37 відмовлено.

Для забезпечення ефективності експортного контролю в ЄС запроваджено цифрові інструменти, такі як електронна система ліцензування eLicensing, яка вже працює в кількох країнах-членах і поступово інтегрується з національними митними

системами. Ці технологічні рішення сприяють зменшенню адміністративного навантаження та підвищенню ефективності експортного контролю.

Загалом, звіт підкреслює зростаючу роль контролю за товарами подвійного використання в умовах геополітичної нестабільності, посилення обмежувальних заходів щодо Росії та Білорусі, а також необхідність подальшого посилення співпраці з міжнародними партнерами для забезпечення безпеки та стабільності у світі.

Регулювання

Політика захисту даних в ЄС: виклики, досягнення та майбутні перспективи[5]

Документ є ґрунтовним аналітичним дослідженням Європейської парламентської дослідницької служби (EPRS), присвяченим політиці захисту персональних даних у Європейському Союзі. Він висвітлює історичний розвиток цієї сфери, ключові законодавчі акти, роль інституцій ЄС, а також основні виклики, що стоять перед цифровою приватністю в умовах сучасних технологічних реалій.

У зв'язку з глобальним зростанням обсягу даних та частими скандалами, пов'язаними з їхнім неналежним використанням (наприклад, випадок Facebook–Cambridge Analytica), захист персональної інформації набув статусу важливого соціального, правового та політичного питання. ЄС відповів на ці виклики створенням сучасного правового режиму захисту даних, закріпленого в Загальному регламенті про захист даних (GDPR), Директиві щодо обробки даних у правоохоронних органах (LED), Регламенті щодо захисту даних в установах ЄС та Директиві про електронну приватність (e-Privacy Directive). Ці документи формують комплексний підхід до регулювання обробки персональних даних, як у приватному секторі, так і в державних установах.

GDPR став революційним кроком у європейському правовому регулюванні, запровадивши такі основоположні принципи, як прозорість обробки даних, обов'язковість отримання явної згоди користувачів, право на доступ, виправлення та видалення персональних даних, обов'язок компаній швидко повідомляти про витоки даних, а також механізм суворого нагляду через незалежних національних регуляторів. Важливою рисою GDPR є його екстериторіальний ефект, що означає поширення регламенту на компанії, які працюють з даними громадян ЄС, незалежно від їхньої фізичної присутності в межах Союзу. Це дозволило ЄС встановити глобальні стандарти у сфері захисту даних, які впливають на законодавство багатьох країн світу.

Європейський парламент відіграв вирішальну роль у формуванні та прийнятті GDPR, забезпечуючи політичну підтримку високих стандартів приватності, а Європейський суд справедливості (CJEU) через свою судову практику закріпив ключові принципи тлумачення цього регламенту. Наприклад, саме суд підтвердив право на забуття, визнавши можливість громадян вимагати видалення застарілих або неточних особистих даних з пошукових систем. Судові рішення також торкнулися проблеми правомірності масового збирання даних, що стало предметом дискусій між інтересами безпеки та правами людини.

Попри успіхи GDPR, документ наголошує на значних викликах у його реалізації. Насамперед це проблеми з його виконанням, оскільки багато великих технологічних компаній намагаються мінімізувати відповідальність, а національні органи з захисту даних часто мають обмежені ресурси для ефективного контролю. Одним із можливих рішень є посилення міждержавної

[5] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf

співпраці регуляторів, збільшення фінансування та застосування більш жорстких санкцій проти порушників. Другим викликом є баланс між приватністю та безпекою, оскільки правоохоронні органи потребують доступу до персональних даних для боротьби зі злочинністю та тероризмом, що створює ризик надмірного державного нагляду. У зв'язку з цим виникає необхідність чіткішого регулювання питань доступу до даних для правоохоронних цілей.

Окремий розділ присвячено впливу новітніх технологій, таких як штучний інтелект, біометричне розпізнавання, інтернет речей, які несуть нові загрози для приватності. Наприклад, використання алгоритмів машинного навчання може призводити до дискримінації або несанкціонованого використання персональних даних, а розпізнавання облич викликає занепокоєння щодо масового стеження. Документ наголошує на необхідності запровадження чітких правил для нових технологій з метою запобігання порушенню прав громадян.

Також розглянуто проблему надмірного регуляторного тягаря для малого та середнього бізнесу. Незважаючи на те, що GDPR передбачає спрощені механізми для малих компаній, вони часто стикаються з труднощами у виконанні вимог регламенту. Одним із можливих рішень може стати запровадження галузевих кодексів поведінки та надання бізнесу практичних рекомендацій щодо відповідності GDPR.

У сфері міжнародного обміну даними ЄС застосовує механізм «рішень про адекватність», що дозволяє передавати персональні дані в країни, які забезпечують належний рівень захисту. Проте судова практика вже скасовувала попередні угоди з США через надмірне втручання американських спецслужб у персональні дані європейців. Нині ЄС шукає нові юридичні механізми для захисту даних своїх громадян при міжнародних передаваннях.

Зрештою, документ окреслює ключові майбутні виклики у сфері захисту даних, серед яких необхідність посилення виконання GDPR, адаптація законодавства до новітніх технологій, забезпечення справедливого балансу між приватністю та безпекою, а також підтримка малого бізнесу у виконанні регуляторних вимог. ЄС має амбітні плани щодо подальшого розвитку своєї цифрової політики, проте їхня реалізація потребуватиме ефективної взаємодії між країнами-членами, регуляторами, бізнесом та громадянським суспільством.

Висновки:

- **Підвищення ефективності виконання GDPR:**
  - Необхідно посилити контроль над великими технологічними компаніями та забезпечити достатнє фінансування національних регуляторів.
  - Впровадження механізму **спільних розслідувань** між країнами-членами ЄС.
- **Оновлення підходів до обробки даних у правоохоронній сфері**
  - Чітке визначення меж допустимого державного нагляду за даними громадян.
  - Забезпечення **пропорційності заходів** відповідно до рішень CJEU.
- **Регулювання новітніх технологій (ШІ, біометрія, IoT)**
  - Впровадження спеціальних правил для обробки персональних даних у штучному інтелекті та технологіях розпізнавання облич.
  - Заборона **неконтрольованого збору біометричних даних** без згоди користувачів.
- **Спрощення регулювання для малого бізнесу**
  - Розробка спрощених процедур для відповідності GDPR.
  - Запровадження **секторальних кодексів поведінки** для різних галузей.

Звіти окремих інституцій та експертів

Кримінальні тенденції 2025: ключові індикатори, що визначають майбутнє організованої злочинності [6]

Стаття від InSight Crime аналізує п’ять ключових тенденцій, які визначатимуть розвиток організованої злочинності у 2025 році. Автори дослідження спираються на великі масиви даних, отримані шляхом моніторингу, збору офіційної інформації та досліджень, щоб простежити закономірності у динаміці злочинної діяльності. Основний акцент зроблено на насильницькі злочини, наркоторгівлю, зростання використання криптовалют у кримінальних фінансах, а також збільшення масштабів вимагання та рекету.

Організована злочинність залишається основним каталізатором насильства в Латинській Америці та Карибському басейні, і у 2025 році очікується подальше зростання рівня вбивств у регіоні. Це явище тісно пов’язане із фрагментацією злочинних угруповань, які вступають у конфлікти через перерозподіл впливу та ресурсів. Еквадор і Колумбія є прикладами країн, де такі процеси особливо виразні: в Еквадорі внутрішні розколи між бандами Choneros та Lobos призвели до серії жорстоких зіткнень, зокрема у тюрмах, а в Колумбії боротьба за контроль над нелегальними ринками спричинила сплеск насильства у таких містах, як Калі, Богота, Кукута та Барранкілья. Дослідники з InSight Crime збирали дані про вбивства за допомогою моніторингу новин, запитів на публічну інформацію та державних баз даних, щоб визначити географічні «гарячі точки» насильства та виявити зв’язки між рівнем вбивств, процесами фрагментації злочинних структур і особливостями функціонування кримінальних економік.

Наркоторгівля залишається основним джерелом фінансування організованої злочинності, і у 2024 році світ зіткнувся з рекордними обсягами поставок кокаїну. Незважаючи на посилення правоохоронних заходів, у таких країнах, як Болівія, Перу, Домініканська Республіка та Гайана, вилучення кокаїну досягли історичних максимумів. Іспанія знову закріпилася як головний європейський вхідний пункт для цього наркотика, а зростаючий попит на ринках США та Європи стимулює ще більш активне виробництво та розширення транспортних мереж. InSight Crime відстежують обсяги вилучень кокаїну та картографують ключові маршрути його постачання, зокрема аналізуючи роль портів, методи транспортування та мережі, що оперують на різних рівнях.

Ще одним критично важливим фактором є розширення мережі нелегальних злітно-посадкових смуг, які використовуються для транспортування наркотиків та підтримки інших злочинних операцій. Наприклад, у лісових районах Перу відзначено посилення насильства проти корінних громад, оскільки наркоторговці захоплюють території та будують там аеродроми для відправлення наркотиків у транзитні країни. Водночас у Центральній Америці зафіксовано зниження кількості незаконних повітряних перевезень, що може свідчити про зміну тактики контрабандистів.

Окремо досліджується динаміка вимагання та рекету, які стали одними з найпоширеніших злочинів у регіоні. Простота реалізації цих схем дозволяє навіть малим злочинним групам отримувати прибутки, що може спричинити подальшу атомізацію кримінального середовища. Прикладом є Перу, де кількість випадків вимагання зросла на 370% між 2021 і 2023 роками. З одного боку, зростання кількості подібних злочинів може свідчити про децентралізацію

[6] https://insightcrime.org/news/mapping-criminal-trends-five-indicators-watch-2025/

організованої злочинності, а з іншого – про появу нових гравців у кримінальному світі, які можуть поступово перетворитися на великі угруповання. Водночас зменшення кількості таких випадків може означати як успішність державних заходів, так і перехід злочинців до більш витончених економічних злочинів.

Останній важливий фактор – це активне використання криптовалют у фінансових схемах організованої злочинності. Дедалі більше злочинних угруповань відмовляються від готівкових операцій і переходять на цифрові активи, щоб уникати контролю традиційних банківських установ. У 2024 році влада Бразилії заморозила понад 1 мільярд доларів у криптовалюті, що належали кримінальній організації Primeiro Comando da Capital (PCC). Відслідковування транзакцій у цифровій сфері дозволяє аналітикам оцінювати масштаби використання криптовалют у злочинних схемах, а також розуміти, чи відбувається поступова заміна фізичних активів цифровими засобами. Враховуючи, що криптовалюти дедалі частіше застосовуються у фінансуванні наркотрафіку, відмиванні грошей та кібератаках, у 2025 році очікується посилення заходів щодо їхнього регулювання.

Таким чином, у 2025 році головними тенденціями залишаться зростання рівня насильства, розширення незаконного обігу наркотиків, використання криптовалют злочинцями, нарощування незаконної інфраструктури для перевезення наркотиків і збільшення масштабів злочинів. Аналітичні центри, правоохоронні органи та уряди повинні враховувати ці тренди при розробці стратегій боротьби з організованою злочинністю та адаптувати свої підходи до нових викликів.

Висновки:

- **Фрагментація злочинних угруповань веде до зростання насильства та територіальних воєн.** Державним органам слід розвивати аналітичні механізми моніторингу злочинних конфліктів, щоб запобігати їхньому поширенню.
- **Наркоторгівля залишається основним джерелом фінансування організованої злочинності.** Необхідне подальше зміцнення міжнародної співпраці щодо перекриття ключових транзитних маршрутів.
- **Криптовалюти стають критичним фінансовим інструментом для кримінальних структур.** Необхідне посилення регулювання криптовалютних бірж та обов'язковий моніторинг великих цифрових транзакцій.
- **Зростання рекету свідчить про децентралізацію злочинності та її адаптацію.** Необхідно створювати ефективні механізми захисту бізнесу та громадян від вимагань, зокрема через покращення механізмів анонімного повідомлення про злочини.

Тіньовий флот Ірану: Як нафта обходить міжнародні санкційні обмеження [7]

Масштабне журналістське розслідування агентства Reuters висвітлює складну систему ухилення Ірану від міжнародних санкцій шляхом нелегального транспортування нафти. На основі витоку понад 10 000 електронних листів компанії Sahara Thunder, супутникових знімків та аналітичних даних репортери розкривають глобальну мережу

[7] https://www.reuters.com/graphics/IRAN-OIL/zjpqngedmvx/

перевезення підсанкційного іранського пального. Головна увага зосереджена на методах маскування походження нафти, механізмах її транспортування та ключових гравцях цієї схеми.

Центральним елементом розслідування є опис функціонування «тіньового флоту», що складається з 34 танкерів, які систематично змінюють імена, прапори та документи, щоб приховати справжнє походження вантажу. Особливу увагу приділено судну Remy, яке виконувало функцію посередника: воно офіційно декларувало перевезення іракської нафти, тоді як фактично транспортувало нафту з Ірану. Операція була задокументована завдяки супутниковим знімкам, а витік внутрішнього листування Sahara Thunder підтвердив, що це судно отримало вантаж від іранського танкера Sonia 1. При цьому капітан мав два різні сертифікати походження – один від іранської національної нафтової компанії, інший, сфальсифікований, від іракського терміналу в Басрі.

Розслідування також висвітлює методи, які застосовувалися для обходу санкцій. Судна вимикали транспондери AIS (автоматичної ідентифікаційної системи) або використовували підроблені сигнали, щоб створювати ілюзію перебування в інших місцях. Танкер Remy, наприклад, використовував фальшиве ім'я Deep Ocean під час прийому іранської нафти. Крім того, деякі судна перефарбовували, змінювали їхню реєстрацію або використовували підроблені IMO-номери.

Журналісти також простежили маршрути нелегальної торгівлі, які включали перевалки в портах Ірану, Об’єднаних Арабських Еміратів, Венесуели, Мурманська в Росії та китайських гаваней, що були кінцевою точкою більшості поставок. За період із березня 2022 року по лютий 2024 року Sahara Thunder транспортувала близько 20 мільйонів барелів нафти, що еквівалентно 1,7 мільярда доларів США за середньою ринковою ціною 2023 року. Основним покупцем була Китайська Народна Республіка, яка отримала щонайменше 12,6 мільйона барелів. Крім іранської нафти, компанія також допомагала транспортувати паливо з Росії та Венесуели, що вказує на розширення масштабів санкційного ухилення.

Реакція західних урядів на ці схеми була неоднозначною. США у квітні 2024 року запровадили санкції проти Sahara Thunder, назвавши її «підставною компанією», яка працює на уряд Ірану та Корпус вартових Ісламської революції (IRGC). Всього під санкції потрапило 21 із 34 суден, пов’язаних із цією мережею. Тим не менш, 13 танкерів, включно з Remy, продовжують свою діяльність, змінивши назви та реєстрацію.

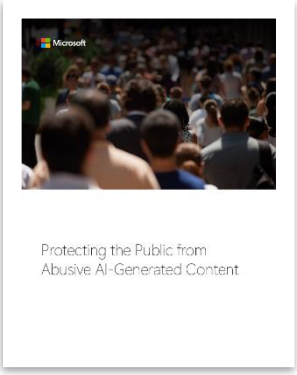
Одним із найбільш вражаючих епізодів у матеріалі є викриття фінансових схем, що дозволяли компанії Sahara Thunder оплачувати послуги, попри санкції, які блокували доступ до міжнародної банківської системи. Наприклад, у листуванні зафіксовано, що компанія оплачувала заправку суден у портах ОАЕ готівкою через посередників. Один із платежів, зафіксований у витоку, становив 1,2 мільйона доларів США в дирхамах ОАЕ, які мали бути передані готівкою агенту.

Документ також містить підтвердження того, що іранські постачальники активно співпрацювали з російськими компаніями після введення санкцій проти Москви у 2022 році через повномасштабне вторгнення в Україну. У грудні 2023 року Remy здійснював останній задокументований рейс у рамках схеми Sahara Thunder, транспортуючи російську нафту, яка, ймовірно, також призначалася для китайських покупців.

Важливою частиною розслідування є аналіз методів збору інформації, що включав використання витоків електронної пошти, супутникових знімків та алгоритмічного аналізу руху суден. Дані витоку були оброблені за допомогою інструментів штучного інтелекту, які дозволили виявити закономірності в маршрутах і маніпуляціях із документами. Незалежна перевірка результатів проводилася аналітичною компанією Roke Intelligence, яка підтвердила більшість викритих схем шляхом аналізу супутникових знімків та баз даних судноплавства.

Висновки документа вказують на те, що, попри жорсткі санкції, Іран зумів налагодити ефективний механізм прихованого продажу нафти завдяки складній системі фальсифікацій, використанню «тіньового флоту» та залученню альтернативних фінансових механізмів. Це дозволяє країні продовжувати отримувати мільярдні доходи від експорту пального, фінансуючи власну економіку та підтримуючи союзницькі військово-політичні групи в регіоні. Розслідування підкреслює необхідність посилення заходів контролю, запровадження нових механізмів ідентифікації санкційних схем та посилення міжнародного співробітництва для унеможливлення подібних дій у майбутньому.

Боротьба зі зловживаннями ШІ: як захистити суспільство від загроз генеративного контенту [8]



Документ від компанії Microsoft є ґрунтовним дослідженням проблеми зловживання штучним інтелектом (ШІ) для створення шкідливого контенту та пропонує комплексні рішення на рівні політики, технологій та суспільної освіти. Він наголошує, що сучасні генеративні моделі ШІ стали інструментом не лише для творчості та інновацій, а й для маніпуляцій, шахрайства, поширення дезінформації та підриву суспільної довіри.

Документ починається з передмови Бреда Сміта, віцепрезидента Microsoft, який окреслює масштаби загрози та необхідність негайних дій. Він наголошує, що небезпека полягає не в надмірній регуляції, а навпаки – у занадто повільній реакції держав і технологічних компаній. Наводяться приклади, як ШІ вже використовується для дестабілізації суспільств і впливу на геополітичні процеси, зокрема через фейкові новини, маніпулятивні відео та аудіозаписи, шахрайські схеми та порушення цифрових прав людини.

У першій частині документ детально аналізує проблематику шкідливого ШІ-генерованого контенту. Розглядаються чотири основні категорії загроз: шахрайство, створення штучного контенту сексуального характеру, політична дезінформація та використання ШІ для створення маніпулятивних або шкідливих зображень. Наводяться реальні кейси, серед яких випадки фінансового шахрайства, коли через deepfake-відео компанії втрачали мільйони доларів, або поширення фальшивих політичних заяв перед виборами, як це сталося, наприклад, у Словаччині. Окремо наголошується на зростаючій загрозі ШІ-створеного контенту сексуального характеру, зокрема використання deepfake-технологій для створення матеріалів, що дискредитують жінок, дітей та публічних осіб.

Друга частина описує підхід Microsoft до боротьби з цією загрозою. Компанія пропонує комплексну систему захисту, яка включає шість ключових напрямків: посилення безпеки на рівні ШІ-моделей та платформ, забезпечення автентичності цифрового контенту через watermarking та криптографічні маркери, моніторинг зловживань, співпрацю з урядами та громадськими організаціями, оновлення законодавчої бази та проведення освітніх кампаній. Microsoft уже впроваджує рішення, такі як автоматичне маркування контенту, створеного моделлю DALL-E 3, а також використання стандартів C2PA для перевірки походження цифрових зображень у LinkedIn.

Окремий розділ присвячено нормативно-правовим ініціативам та рекомендаціям, які мають на меті зменшити ризики, пов’язані зі ШІ-генерованим контентом. Microsoft закликає уряди ухвалити законодавчі акти, які б:

[8] https://aka.ms/ProtectThePublic

- Запровадили вимогу маркування синтетичного контенту;
- Захищали вибори від маніпуляцій через deepfake-технології;
- Передбачали оновлення законодавства щодо боротьби з експлуатацією дітей та порушенням цифрових прав людини;
- Впроваджували кримінальну відповідальність за створення та поширення шахрайського ШІ-контенту.

Висновки:

- **Впровадження стандартів прозорості,** таких як C2PA, watermarking та криптографічні маркери, має стати обов'язковим для всіх постачальників послуг ШІ, щоб запобігти маніпуляціям і дезінформації.
- **Необхідно ухвалити закон про «шахрайство за допомогою deepfake»,** який дозволить ефективно притягати до відповідальності осіб, що використовують ШІ для фінансових махінацій, підробки голосів, зображень і документів.
- **Чинні закони щодо експлуатації дітей та нелегального контенту повинні бути оновлені** для включення штучно створених матеріалів, а також забезпечення суворих санкцій за поширення несанкціонованих зображень.
- **Уряди, технологічні компанії та громадські організації мають координувати зусилля** для виявлення та нейтралізації спроб використання deepfake-контенту з метою впливу на вибори, що передбачає створення оперативних моніторингових груп та механізмів швидкого реагування.

Microsoft також пропонує створити партнерства між державним і приватним секторами для моніторингу випадків зловживань та розширити державне фінансування освітніх програм, спрямованих на підвищення медіаграмотності. Компанія бере активну участь у міжнародних ініціативах, зокрема у Tech Accord to Combat Deceptive Use of AI in 2024 Elections, що об'єднує провідні технологічні компанії для спільної боротьби з маніпуляціями на виборах.

Документ завершується закликом до негайних дій. Автори наголошують, що зволікання лише ускладнить проблему, тоді як комплексний підхід, що включає технологічні, нормативні та освітні заходи, може ефективно зменшити загрози, пов'язані зі зловживанням генеративним ШІ.

Токенізація активів: як блокчейн змінює фінансовий сектор та відкриває нові можливості для інвесторів[9]

Звіт глибоко аналізує токенізацію активів, її потенціал у трансформації фінансового сектору та виклики, які необхідно подолати для повноцінного впровадження. Основна увага приділена фінансовим установам, які можуть використовувати блокчейн не тільки для операцій із криптовалютами, а й для створення більш ефективних фінансових рішень, включаючи випуск та обіг токенізованих активів. Особливу увагу приділено Латинській Америці, де токенізація може вирішити проблеми низької фінансової інклюзії та сприяти економічному розвитку.

Звіт починається з історичного контексту та пояснює технологічний розвиток блокчейну, починаючи від Bitcoin (2009) як першої децентралізованої цифрової валюти, до Ethereum (2015), який запровадив смарт-контракти та суттєво розширив

[9] https://b2b.mastercard.com/media/xg1bnu3l/asset-tokenization_a-comprehensive-report-and-why-you-should-start-caring-about-the-technology.pdf

можливості використання блокчейну. Технологія еволюціонувала від простого запису транзакцій до універсального інструменту для зберігання, обліку та переміщення будь-яких активів у цифровій формі. Це дозволяє фінансовим установам розглядати токенізацію як спосіб підвищення ефективності, зниження витрат, автоматизації процесів та підвищення прозорості.

Токенізація активів – це процес перетворення прав власності на будь-який актив у цифрові токени, які зберігаються у блокчейні. Це дозволяє активам бути більш ліквідними, доступними для швидкого обігу та інтегрованими у фінансові екосистеми на глобальному рівні. Використання смарт-контрактів дає змогу автоматизувати виконання зобов'язань та зменшити потребу у посередниках. Наприклад, облігації, акції, нерухомість, дорогоцінні метали та навіть мистецтво можуть бути представлені у вигляді токенів, що дозволяє нові форми володіння, включаючи фрагментарну власність, коли один актив може належати багатьом інвесторам одночасно.

Фінансові установи вже активно досліджують потенціал токенізації. Провідні банки та інвестиційні компанії, такі як J.P. Morgan, BlackRock, Citi, Apollo, впроваджують рішення для токенізації облігацій, депозитів та фондових активів. Наприклад, J.P. Morgan створив платформу Liink, що дозволяє здійснювати миттєві міжбанківські платежі. BlackRock та Apollo тестують токенізовані ринки альтернативних інвестицій, що дозволяє знизити витрати та спростити механізми обліку активів. Hamilton Lane та KKR співпрацюють із платформами на базі блокчейну для надання доступу до інвестицій у приватні ринки через токенізовані активи.

Важливим є питання регулювання, яке залишається невизначеним у багатьох юрисдикціях, що гальмує масштабне впровадження токенізації. У звіті наголошується, що деякі країни, зокрема Сінгапур, Об'єднані Арабські Емірати та Велика Британія, активно тестують регуляторні підходи через пісочниці – спеціальні середовища для випробування інноваційних фінансових технологій під контролем регуляторів. У США регулятори демонструють жорстку позицію щодо криптовалют, проте зацікавлені у використанні блокчейну як інструменту для підвищення прозорості фінансових операцій.

Значну увагу звіт приділяє Латинській Америці, де фінансова система має свої унікальні виклики. У багатьох країнах регіону, зокрема у Бразилії, Мексиці та Перу, великий відсоток населення не має доступу до банківських послуг. Це спричинено низьким рівнем довіри до фінансових установ, високою інфляцією та історичною нестабільністю. Блокчейн може вирішити ці проблеми, дозволяючи громадянам мати прямий доступ до фінансових інструментів, оминаючи традиційні банки. Наприклад, Центральний банк Бразилії запустив платформу Drex, яка дозволяє токенізувати активи та використовувати блокчейн для фінансових розрахунків між установами.

Попри значний потенціал, впровадження токенізації стикається з кількома технічними та організаційними викликами. Головні серед них:

- Інтероперабельність блокчейнів – існує багато різних блокчейн-платформ, які не завжди сумісні між собою, що ускладнює переміщення активів.
- Кастодіальні послуги – зберігання та управління цифровими активами вимагає нових моделей управління безпекою та відповідності нормативним вимогам.
- Проблеми масштабування – для використання блокчейну у фінансових операціях необхідна висока пропускна здатність мережі.
- Необоротність транзакцій – традиційні фінансові системи допускають скасування операцій у разі помилки або шахрайства, що складніше реалізувати у децентралізованих системах.

Рішенням цих проблем можуть стати глобальні стандарти, нові технології з управління доступом та розвиток інституційних платформ, які спрощують процес токенізації для банків та корпорацій. У звіті зазначається, що великі технологічні компанії, такі як Mastercard, активно працюють над створенням платформ «compliance-first», що поєднують переваги блокчейну із сучасними механізмами регулювання, включаючи ідентифікацію користувачів та моніторинг транзакцій.

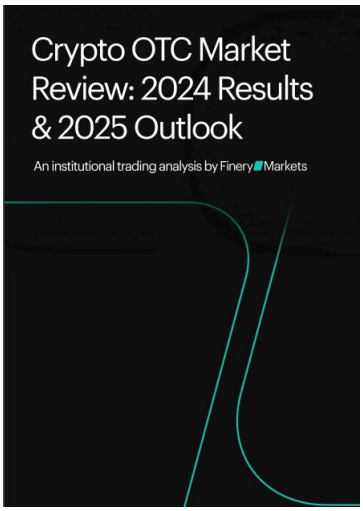
Висновки:

- **Фінансові установи можуть впроваджувати блокчейн-рішення вже зараз**, не чекаючи остаточного регулювання, що дає змогу отримати конкурентну перевагу.
- **Токенізація дозволяє створювати нові фінансові продукти,** включаючи **фрагментарну власність,** автоматизовані смарт-контракти та більш ліквідні активи.
- **Регуляторні бар'єри залишаються головним викликом для масштабування,** однак деякі юрисдикції (Сінгапур, Бразилія, Великобританія) вже розробляють **експериментальні регуляторні середовища** для тестування рішень.
- **Латинська Америка – один із ключових регіонів для впровадження токенізації,** де технологія може допомогти **закрити економічні розриви** та підвищити рівень фінансової інклюзії.

Звіт також включає прогнози щодо майбутнього ринку токенізації. За оцінками аналітиків, до 2030 року обсяг токенізованих активів може перевищити 10 трлн доларів. Найбільше зростання очікується у секторі фінансових активів, зокрема облігацій, акцій та інвестиційних фондів. Очікується, що цифрові валюти центрального банку (CBDC) стануть каталізатором масового впровадження блокчейну у фінансових операціях. Також активно розвиваються нові класи токенізованих активів, включаючи ліцензії на інтелектуальну власність, музичні роялті та навіть права на відеоконтент.

Загальний висновок звіту – токенізація стає не лише технологічним трендом, а й реальним стратегічним напрямом для фінансових установ, що прагнуть підвищити ефективність, знизити витрати та залучити нових інвесторів. Проте для її повноцінного впровадження потрібні чіткі регуляторні рамки, нові технологічні рішення та готовність фінансових установ адаптуватися до змін.

Еволюція OTC-торгівлі криптовалютами: Підсумки 2024 року та інституційні тренди 2025[10]



Звіт від Finery Markets є детальним аналізом ринку позабіржової (OTC) криптовалютної торгівлі, заснованим на даних 4 мільйонів спотових угод, укладених у 2024 році інституційними учасниками. Дослідження включає аналіз торгівельних тенденцій, ролі стейблкоїнів, впливу політичних і регуляторних змін, а також прогноз на 2025 рік.

2024 рік став знаковим для криптовалютного ринку, оскільки загальний обсяг OTC-торгівлі зріс на 106% у річному вимірі. Зростання було викликано кількома ключовими факторами: історичними ціновими максимумами Bitcoin (BTC), запуском біржових фондів (ETF) на BTC і Ethereum (ETH), а також стрімким розвитком стейблкоїнів, які почали відігравати домінуючу роль у фінансових операціях. В грудні 2024 року Bitcoin перевищив

[10] https://finerymarkets.com/assets/files/FM_2024_OTC_review.pdf

позначку у $100,000, що стало каталізатором для всього ринку та сприяло рекордному квартальному зростанню. Інституційні інвестори отримали можливість входу у крипторинок через регульовані ETF на BTC та ETH, що забезпечило безпрецедентний притік капіталу. За даними звіту, обсяг інвестицій у BTC ETF перевищив потоки в традиційні золоті ETF, що стало найбільш успішним запуском біржового продукту в історії.

Поступове прийняття криптовалют великими фінансовими установами у 2024 році змінило загальне ставлення до цифрових активів. Якщо раніше банки та інші традиційні фінансові учасники демонстрували скептицизм, то у 2024 році багато установ перейшли до нейтрального або позитивного ставлення. Деякі навіть оголосили про плани інвестування у криптовалютні проєкти або створення спеціалізованих підрозділів для роботи з цифровими активами. Це стало можливим завдяки поступовому формуванню регуляторної ясності та інституційного прийняття цифрових активів. Хоча законодавчі рамки все ще залишаються неповністю визначеними, звіт підкреслює, що про-крипто позиція адміністрації Дональда Трампа позитивно вплинула на ринок у четвертому кварталі, що сприяло рекордним обсягам торгівлі.

Стейблкоїни стали основним елементом фінансових транзакцій у 2024 році, оскільки їх використання в OTC-торгівлі зросло на 147% рік до року. Це дозволило ефективно подолати недоліки традиційної банківської інфраструктури, забезпечивши швидкі та масштабовані транзакції. Дані показують, що обсяг трансакцій у стейблкоїнах перевищив операції, проведені через Visa, що демонструє їхню перевагу для міжнародних платежів. Звіт наголошує, що зростаюча роль стейблкоїнів як містка між традиційними та цифровими фінансами підтверджує їхню необхідність у майбутньому регуляторному середовищі.

У розрізі позабіржової торгівлі, 2024 рік відзначився історично високим зростанням обсягів у четвертому кварталі, особливо після виборів у США. Загальний річний приріст OTC-торгівлі сягнув 177% YoY, при цьому торгівля криптовалютами між собою зросла у 5,4 рази, а крипто-стейблкоїнові операції — на 311%. Найбільш динамічним кварталом став саме Q4, коли обсяги торгівлі суттєво перевищили попередні показники через активізацію інвесторів після виборів у США. Єдиним іншим кварталом з трипроцентним зростанням став Q2, що був спричинений успішним запуском

Висновки:

- **Інституційні інвестори будуть ключовими драйверами ринку у 2025 році.**
  - Варто стежити за змінами в політиці США та впливом BTC/ETH ETF на традиційні ринки.
  - Потенційний розвиток крипто-забезпечених кредитів створить нові можливості для ліквідності.
- **Стейблкоїни та токенізовані активи продовжать витісняти традиційні фінансові механізми.**
  - Бізнес, що працює із міжнародними транзакціями, повинен розглянути інтеграцію стейблкоїнів.
  - Токенізація нерухомості, облігацій та інших активів може змінити структуру капіталовкладень.
- **Децентралізовані фінанси (DeFi) та регульовані ринки будуть дедалі більше інтегруватися.**
  - Очікується створення **гібридних DeFi-CeFi платформ,** що забезпечать нові можливості арбітражу та генерації прибутку.
  - Великі фінансові установи почнуть тестувати DeFi-інструменти, що може змінити правила гри.
- **Регуляторні зміни у ЄС (MiCA) можуть спричинити ліквідність кризи для дрібних CEX.**
  - Менші централізовані біржі змушені будуть адаптуватися, використовуючи нові моделі брокер-дилерських послуг або покращені рішення з ліквідності.

BTC ETF.

Щодо торгівлі альткоїнами, звіт підтверджує, що, попри домінування BTC, частка альтернативних криптовалют у позабіржових операціях поступово зростає. У 2024 році альткоїни складали 29% від загального обсягу торгівлі проти 13% у 2023 році. Найбільш помітні зміни відбулися у сегменті XRP, Solana (SOL) та Litecoin (LTC). XRP став третьою за капіталізацією криптовалютою, хоча його зростання ще не встигло суттєво вплинути на динаміку ринку. SOL демонстрував вражаюче зростання у дев'ять разів за рік, а в четвертому кварталі — у 43 рази, що пов'язано з розвитком екосистеми Solana та популярністю мемкоїнів. Litecoin (LTC) залишався стабільним вибором для інституційних інвесторів, зрісши на 149% у річному вимірі.

Прогноз на 2025 рік базується на тенденціях, які спостерігалися у 2024-му, та очікуваних змінах у регулюванні та технологічному розвитку. Про-крипто політика США створює передумови для масового прийняття цифрових активів, особливо серед традиційних фінансових установ. Очікується, що успіх BTC та ETH ETF може спричинити появу крипто-забезпечених кредитів, що дозволить розширити ліквідність ринку. Також прогнозується зростання ролі токенізованих традиційних активів, що може змінити структуру глобальної торгівлі через доступність 24/7, можливість дробового володіння активами та покращену ліквідність.

Одним із важливих змінних факторів залишається регуляторне середовище. У звіті зазначено, що з подальшим уточненням глобальних регуляторних норм зросте прийняття DeFi серед інституційних інвесторів. Очікується формування гібридних платформ, де централізовані установи взаємодіятимуть з DeFi-рішеннями, що відкриє нові можливості для арбітражу та прибуткових стратегій. Окрему увагу приділено можливості BTC стати резервним активом, що може призвести до перегляду глобальної стратегії ризик-менеджменту корпорацій та урядів.

Також у звіті акцентується на проблемах, з якими можуть зіткнутися Tier 2 і Tier 3 централізовані біржі в ЄС через впровадження регламенту MiCA. Це може призвести до проблем із ліквідністю, що змусить їх або змінювати бізнес-моделі, або шукати нові брокер-дилерські рішення.

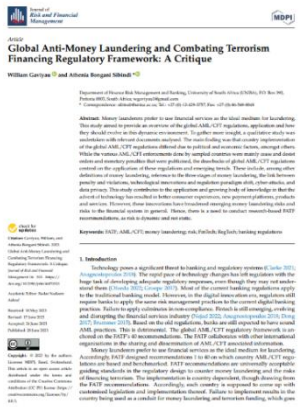
Загалом, звіт Finery Markets демонструє, що криптовалютний ринок вступає у фазу інституційного прийняття та структурної трансформації, де взаємодія традиційних фінансів та криптоіндустрії стає все більш інтегрованою, а регуляторна ясність поступово формує нові можливості для учасників ринку.

Рекомендовані матеріали та заходи

Еволюція глобальної системи протидії відмиванню коштів: виклики, недоліки та перспективи регулювання у цифрову епоху [11]

Стаття присвячена аналізу сучасного глобального регулювання у сфері протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ). Автори розглядають роль FATF у формуванні міжнародних стандартів та критично оцінюють ефективність їх застосування різними країнами. Основний фокус зроблено на тому, як глобальна нормативно-правова база адаптується (або не адаптується) до технологічних змін та сучасних викликів, пов'язаних із цифровими фінансами.

[11] https://www.mdpi.com/1911-8074/16/7/313



Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique

З початку дослідження автори зазначають, що регулювання ПВК/ФТ базується на 40 рекомендаціях FATF, які були прийняті як загальний стандарт для більшості країн. Однак впровадження цих стандартів є неоднорідним: у той час як розвинені країни частіше мають жорсткіші механізми дотримання, країни, що розвиваються, стикаються з проблемами у їх імплементації через політичні, економічні та технічні фактори. Крім того, регулятори змушені враховувати нові загрози, які виникли через розвиток фінансових технологій (FinTech) і регуляторних технологій (RegTech). Впровадження цифрових фінансових послуг, таких як мобільні платежі, криптовалюти та децентралізовані фінансові платформи, створює нові можливості для відмивання коштів, які не завжди ефективно охоплюються традиційними підходами FATF.

Автори також аналізують класичну трирівневу модель відмивання коштів (розміщення, розшарування, інтеграція) та підкреслюють її обмеження в умовах цифрової економіки. У сучасних схемах ВК операції можуть проходити миттєво через цифрові транзакції, що ускладнює виявлення підозрілих активностей за допомогою традиційних методів фінансового моніторингу. Крім того, вони звертають увагу на те, що сучасне регулювання ПВК/ФТ має бути ризик-орієнтованим, а не просто дотримуватися формальних вимог. Це означає, що фінансові установи та регулятори повинні використовувати передові аналітичні інструменти, такі як машинне навчання, великі дані та аналіз поведінкових патернів, щоб ідентифікувати потенційні загрози.

Важливою частиною дослідження є аналіз практики регуляторного правозастосування у різних країнах. Автори розглядають випадки накладення штрафів та застосування санкцій у США, Великій Британії, Намібії, ПАР та інших країнах. Найпоширенішими видами санкцій є накази про припинення діяльності (cease and desist orders), штрафи та вимоги щодо покращення комплаєнсу. Вони підкреслюють, що штрафи часто мають недостатньо чіткий зв'язок із конкретними порушеннями, що створює ризик правової невизначеності та змушує фінансові установи діяти занадто консервативно. Це, у свою чергу, може негативно впливати на фінансову інклюзію, оскільки банки можуть відмовлятися від обслуговування клієнтів

Висновки:

- **Необхідність оновлення стандартів FATF.** Поточна нормативно-правова база застаріла для цифрової епохи. FATF повинна розробити стандарти для боротьби з ВК/ФТ в умовах фінансових інновацій, включаючи криптовалюти та цифрові платіжні системи.
- **Ризик-орієнтований підхід як основа регулювання.** Банки та фінансові установи повинні змістити фокус з дотримання формальних процедур на аналіз реальних загроз. Використання штучного інтелекту та машинного навчання для моніторингу транзакцій може зменшити хибні спрацьовування та підвищити ефективність контролю.
- **Розвиток регуляторних технологій (RegTech).** Запровадження автоматизованих систем аналізу ризиків дозволить регуляторам більш ефективно виявляти та запобігати схемам ВК/ФТ. Потрібне інтегроване використання великих даних (Big Data) та аналізу поведінкових моделей.
- **Посилення міжнародної співпраці та регуляторного арбітражу.** Окремі країни залишають «сірі зони» у своїх законах, що дозволяє ВК/ФТ. Встановлення єдиних міжнародних стандартів та обов'язкових механізмів обміну даними між фінансовими установами та регуляторами критично необхідне для ефективної боротьби з глобальними фінансовими злочинами.

із високим ризиком замість належного управління їхніми ризиками.

Ще одним важливим аспектом є аналіз взаємодії між технологіями та регулюванням. Автори наголошують, що розвиток криптовалют і блокчейн-технологій створює як нові виклики, так і можливості для ефективнішої боротьби з ВК/ФТ. Наприклад, хоча криптовалюти можуть бути використані для приховування незаконних фінансових потоків, вони також дають можливість створення прозорих систем фінансового моніторингу. Регулятори повинні бути готовими до швидкого реагування на ці виклики, а також до розробки нових підходів, які б інтегрували технології у процеси комплаєнсу.

У підсумку автори пропонують кілька рекомендацій щодо покращення глобальної системи ПВК/ФТ. Вони наголошують на необхідності оновлення рекомендацій FATF з урахуванням цифрової економіки, використання ризик-орієнтованого підходу замість формальних перевірок, розвитку технологій RegTech для автоматизації процесів моніторингу та підвищення рівня міжнародної співпраці у сфері фінансового моніторингу. Крім того, вони підкреслюють важливість подальшого дослідження впливу цифрових інновацій на фінансову злочинність та можливості застосування передових технологій для запобігання ВК/ФТ.

Таким чином, стаття є глибоким аналізом сучасної глобальної системи протидії відмиванню коштів та фінансуванню тероризму. Вона не лише демонструє її недоліки, але й пропонує стратегічні напрями розвитку для підвищення ефективності боротьби з фінансовими злочинами у швидко змінюваному цифровому світі.

Вебінар: Запуск Центру кібермоніторингу[12]

6 лютого 2025 року відбудеться онлайн-захід, присвячений запуску Cyber Monitoring Centre—незалежної ініціативи страхової індустрії, яка займається моніторингом та класифікацією кіберінцидентів.

Центр використовує перевірені дані та оцінки експертів для аналізу кіберзагроз і створення більшої прозорості щодо їхнього впливу.

Що обговорюватимуть на вебінарі?

- Як працює система класифікації кіберподій та які методи оцінки використовуються
- Огляд кіберінцидентів за 2024 рік
- Як нова шкала оцінки кіберзагроз може покращити реагування та планування

Спікери заходу:

- Ciaran Martin - професор у Blavatnik School of Government, Оксфорд
- Sadie Creese - професор кібербезпеки, Оксфордський університет
- Will Mayes - генеральний директор Cyber Monitoring Centre

Дата: 6 лютого 2025 року

Час: 10:30–11:30 GMT

Формат: Онлайн через Zoom + офлайн у RUSI (Лондон)

Цей вебінар буде корисним для фахівців у сфері кібербезпеки, аналітиків ризиків, представників страхових компаній та всіх, хто цікавиться класифікацією кіберінцидентів.

[12] https://my.rusi.org/events/online-launch-of-the-cyber-monitoring-centre.html

FinSec25: Фінанси та безпека у світі, що змінюється[13]

11 лютого 2025 року в Лондоні відбудеться конференція FinSec25, організована Королівським об'єднаним інститутом оборонних досліджень (RUSI). Захід присвячений актуальним викликам у сфері фінансової безпеки, боротьбі з фінансовими злочинами, геополітичним ризикам та впливу нових технологій на фінансовий сектор.

Про що цей захід?

Конференція FinSec25 об'єднає експертів з усього світу для аналізу еволюції фінансової безпеки за останнє десятиліття, впливу технологій на фінансові злочини, геополітичних змін та майбутніх загроз у сфері фінансів. Учасники матимуть змогу обговорити стратегії протидії фінансовим злочинам та забезпечення економічної безпеки.

Хто організовує захід?

Організатором конференції є RUSI—провідний британський аналітичний центр у сфері оборони та безпеки. Захід відбудеться за адресою: RUSI, 61 Whitehall, Лондон.

Серед підтверджених спікерів:

Justin Baldacchino — Dubai Financial Services Authority (DFSA)

Catherine Belton — The Washington Post

Andrea Bowe — Financial Conduct Authority (FCA)

J. Edward Conway — The Wolfsberg Group

Wendy Ennis — Standard Chartered

Tom Keatinge — директор Центру досліджень фінансових злочинів та безпеки (CFS), RUSI

Eliza Lockhart — науковий співробітник CFS, RUSI

William Lyne — Національне агентство по боротьбі зі злочинністю (NCA)

David O'Sullivan — спеціальний представник ЄС з питань санкцій

Tom Tugendhat — депутат парламенту Великобританії

Kathryn Westmore — старший науковий співробітник CFS, RUSI

Elad Wieder — Управління з протидії відмиванню грошей та фінансуванню тероризму Ізраїлю (IMPA)

Кому буде корисний цей захід?

Конференція буде корисною для фахівців у сфері фінансів, безпеки, регулювання, комплаєнсу, а також для дослідників, політиків та всіх, хто цікавиться питаннями фінансової безпеки та протидії фінансовим злочинам.

Як і коли долучитися?

[13] https://my.rusi.org/events/finsec25-conference.html

Захід відбудеться 11 лютого 2025 року з 08:00 до 20:00 GMT у гібридному форматі. Місце проведення: RUSI, 61 Whitehall, Лондон. Онлайн-участь: через платформу Zoom. Для участі необхідно зареєструватися на офіційному сайті заходу.

Інші новини

Європейська Комісія пропонує запровадити тарифи на сільськогосподарську продукцію та на добрива з Росії та Білорусі[14]


EUROPEAN COMMISSION

Brussels, 28.1.2025
COM(2025) 34 final
2025/0021 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the modification of customs duties applicable to imports of certain goods originating in or exported directly or indirectly from the Russian Federation and the Republic of Belarus

Європейська комісія запропонувала новий регламент, спрямований на підвищення митних тарифів на імпорт певних сільськогосподарських товарів та добрив з Російської Федерації та Республіки Білорусь. Ця ініціатива має на меті зменшити залежність Європейського Союзу від цих країн та зміцнити продовольчу безпеку Союзу.

Згідно з пропозицією, митні тарифи на імпорт сільськогосподарських товарів будуть негайно підвищені до 50%. Тарифи на добрива зростатимуть поступово протягом трьох років, досягаючи заборонного рівня. Ці заходи спрямовані на обмеження економічного впливу Росії та Білорусі на ринок ЄС та запобігання можливим економічним і політичним маніпуляціям з їхнього боку.

Документ підкреслює, що запропоновані заходи не матимуть негативного впливу на глобальну продовольчу безпеку, оскільки вони стосуються лише імпорту в ЄС і не зачіпають транзит товарів через його територію. Очікується, що підвищення митних зборів сприятиме диверсифікації джерел постачання та посиленню внутрішнього виробництва в ЄС.

Також передбачено моніторинг цін на добрива протягом перших трьох років застосування регламенту. У разі значного зростання цін можливе призупинення тарифів на добрива з інших країн, окрім Росії та Білорусі, для забезпечення стабільності ринку добрив у ЄС.

Ця пропозиція узгоджується із санкційною політикою ЄС проти Росії та Білорусі у відповідь на агресію проти України та спрямована на зміцнення продовольчої безпеки та стабільності ринку ЄС.

[14] https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2025)34&lang=en

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-2025-05

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].