Методологічний бюлетень

Серійний номер: МінФін-AML-2025-08

Лютий 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

Зростання шахрайства з чеками через крадіжку пошти: методи, наслідки та заходи протидії [1]

Документ, опублікований Інтернет-центром скарг на кіберзлочини (IC3) 27 січня 2025 року, привертає увагу до стрімкого зростання шахрайства з чеками, пов’язаного з крадіжкою пошти. Федеральне бюро розслідувань (FBI) та Поштова інспекційна служба США (USPIS) попереджають, що масштаби цієї проблеми значно збільшилися, а звіти про підозрілі операції (SARs), пов’язані з чековим шахрайством, майже подвоїлися з 2021 по 2023 рік. Основною причиною цього явища є вразливість фінансових механізмів: відповідно до регламентованих строків обробки чеків, фінансові установи змушені швидко робити кошти доступними, що дає шахраям можливість отримати їх ще до того, як факт підробки чи крадіжки буде виявлений.

Основний механізм шахрайства починається зі зламу або фізичного викрадення чеків під час їхньої доставки або зберігання. Зловмисники отримують доступ до легітимних чеків шляхом крадіжки пошти безпосередньо з поштових скриньок, викрадення з USPS або через підставних осіб. Після отримання чеків вони піддаються подальшій обробці для того, щоб змінити їхній зміст або створити підроблені дублікати. Найпоширеніші методи фальсифікації включають "check washing" — процес хімічного зняття первинної інформації з чека, що дозволяє змінювати

[1] https://www.ic3.gov/PSA/2025/PSA250127

отримувача та суму виплати, а також "check cooking" — метод цифрової обробки викраденого чека за допомогою сучасного програмного забезпечення та друку підробок на високотехнологічних принтерах. Ці техніки дозволяють зловмисникам або підробити оригінальний чек, або створити його цифровий аналог, який потім друкується у великій кількості та використовується для численних незаконних транзакцій. Найчастіше підроблені чеки виписуються на відносно невеликі суми, щоб уникнути негайного виявлення фінансовими установами.

Після підготовки змінених або підроблених чеків вони вносяться в обіг через систему фінансових установ. Шахраї використовують або власні підставні рахунки, або продають підроблені чеки іншим злочинним угрупованням через темні канали інтернету. В багатьох випадках до злочинних схем залучають "фінансових мулів" – людей, які добровільно або через обман надають свої рахунки для прийому та переведення в готівку коштів. Оскільки виявлення фальсифікації зазвичай займає певний час, до моменту виявлення шахрайства зловмисники вже встигають зняти кошти, а фінансові установи та законні власники рахунків несуть збитки.

Шахрайство з чеками завдає серйозних економічних і соціальних збитків різним категоріям суб'єктів. Бізнеси можуть стикатися з фінансовими втратами, репутаційними ризиками та порушенням нормальних бізнес-процесів через шахрайські платежі. Споживачі також відчувають негативні наслідки, такі як негативний вплив на кредитну історію, втрату власних активів, незаконне розкриття особистих даних та втрату коштів через підроблені фінансові операції. Державні установи страждають через викрадення коштів, призначених для соціальних виплат, що призводить до затримок виплат, необхідності проведення додаткових розслідувань та фінансових витрат на усунення наслідків шахрайства.

У зв’язку з цим документ надає детальні рекомендації щодо захисту від шахрайства як для окремих осіб, так і для бізнесу та урядових установ. З метою мінімізації ризику крадіжки пошти рекомендовано не залишати пошту у відкритому доступі, своєчасно забирати кореспонденцію та використовувати такі послуги, як Informed Delivery®, що дозволяє отримувати попередні сповіщення про вхідну пошту. Крім того, рекомендується використовувати спеціальні захищені конверти та уникати відправлення важливих документів через стандартні поштові скриньки, особливо вразливі до зламу.

Захист чеків також є ключовим аспектом протидії шахрайству. Зокрема, документ рекомендує використовувати незмивні чорнила при заповненні чеків, уникати залишення порожніх рядків у чеках, не зазначати на них особисту інформацію (номер соціального страхування, водійське посвідчення тощо) та активно перевіряти банківські виписки на наявність підозрілих транзакцій. Замість паперових чеків рекомендується використовувати електронні платіжні методи (e-check, ACH, мобільні платежі), які забезпечують більший рівень безпеки та меншу ймовірність підробки.

Висновки:

- **Перехід на електронні платежі –** Використання e-check, ACH та мобільних платежів значно знижує ризик шахрайства порівняно з паперовими чеками.
- **Запровадження банківських механізмів перевірки –** Використання "Positive Pay" та автоматизованих систем виявлення шахрайських чеків допомагає запобігти фальсифікаціям.
- **Підвищення безпеки поштових відправлень –** Використання послуги Informed Delivery®, закритих поштових скриньок та мінімізація використання стандартних поштових відправлень для цінних документів зменшує ризик крадіжки.
- **Застосування чеків із захисними елементами –** Використання чеків із водяними знаками, термочорнилом та іншими технологіями ускладнює їхню фальсифікацію.

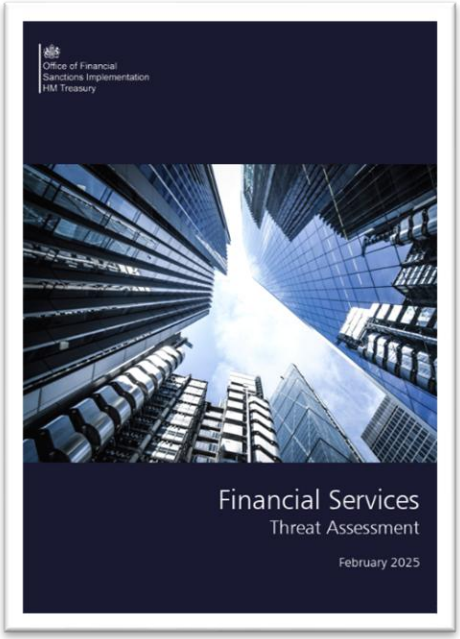
Окремо наголошується на важливості використання "Positive Pay", спеціальної банківської програми, що дозволяє автоматично перевіряти чеки перед їх обробкою, виявляючи можливі шахрайські спроби. Додатково рекомендується застосовувати чеки з розширеними захисними елементами, такими як мікродрук, водяні знаки, термоактивні чорнила та голографічні елементи.

Якщо особа стала жертвою шахрайства, їй рекомендовано негайно зв'язатися зі своїм банком, вимагати копії всіх підроблених чеків та розглянути можливість закриття скомпрометованого рахунку. Крім того, варто негайно подати офіційну скаргу до FBI Internet Crime Complaint Center (IC3) та United States Postal Inspection Service (USPIS) для проведення розслідування та вжиття відповідних заходів.

Документ підкреслює, що шахраї активно використовують сучасні технології, включаючи AI-інструменти, що дозволяють створювати підроблені голосові дзвінки та підроблені документи, що робить їхні схеми ще більш витонченими. У зв'язку з цим рекомендовано особливо уважно ставитися до захисту літніх людей та інших вразливих груп населення, які можуть стати мішенню для шахраїв.

Загалом, документ наголошує на необхідності підвищення фінансової грамотності серед споживачів, впровадження нових технологій безпеки в банківському секторі та посилення міжвідомчої координації між фінансовими установами, правоохоронними органами та поштовими службами для ефективної боротьби з шахрайством з чеками.

Еволюція фінансових санкцій: як російські підсанкційні особи обходять обмеження та які загрози це створює для британського фінансового сектору [2]



Звіт, підготовлений Управлінням з реалізації фінансових санкцій Великої Британії (OFSI) у лютому 2025 року, є комплексною аналітичною оцінкою загроз дотримання санкційного режиму у фінансовому секторі після повномасштабного вторгнення Росії в Україну. Документ спрямований на виявлення ризиків, з якими стикаються британські фінансові установи під час забезпечення санкційного контролю, а також розкриває складні методи обходу санкцій, що використовуються підсанкційними особами та їхніми посередниками.

У вступній частині звіту наголошується, що ландшафт фінансових санкцій Великої Британії значно змінився після 2022 року через запровадження масштабних обмежувальних заходів проти Росії. Це ускладнило діяльність фінансових установ, оскільки вони змушені адаптувати свої процеси для забезпечення належного дотримання санкційного законодавства. OFSI визнає, що санкційна політика є динамічною і змінюється відповідно до нових викликів, тому оцінка загроз у фінансовому секторі є важливим інструментом для посилення контролю та зменшення ризиків порушень. Звіт базується на даних, отриманих з різних джерел між січнем 2022 і березнем 2024 року, включаючи випадки підозрілих транзакцій, самостійні повідомлення

[2] https://assets.publishing.service.gov.uk/media/67ae21a9e270ceae39f9e1b7/OFSI_Financial_Services_Threat_Assessment_Report.pdf

фінансових установ про потенційні порушення санкцій, а також розслідування, проведені самим OFSI.

Окрему увагу у звіті приділено оцінці поширеності порушень санкційного законодавства у фінансовому секторі Великої Британії. Близько 65% усіх зареєстрованих випадків підозрюваних порушень були пов'язані з діяльністю британських фінансових установ, зокрема банків та небанківських платіжних сервісів (NBPSPs), які становили понад 80% усіх випадків. Найбільша частка порушень була пов'язана з активами, які належать або контролюються підсанкційними російськими особами. Крім того, було виявлено значні проблеми з адмініструванням заморожених активів, що призводило до ненавмисних порушень санкцій, зокрема через автоматичне списання коштів за страховими полісами, комунальними платежами чи іншими регулярними витратами.

Документ містить розгорнутий аналіз діяльності "сприячів" (enablers), які допомагають російським підсанкційним особам обходити фінансові обмеження. У звіті визначено дві основні групи таких посередників: професійні та непрофесійні "сприячі". Професійні "сприячі" включають компанії та консультантів, які свідомо беруть участь у схемах приховування активів та забезпечення фінансування осіб, які перебувають під санкціями. До таких посередників належать трастові компанії, адвокатські фірми, фінансові консультанти та інші організації, що надають послуги з управління статками. Непрофесійні "сприячі" – це переважно члени родин підсанкційних осіб або їхні близькі знайомі, які беруть на себе роль номінальних власників активів або здійснюють платежі на користь підсанкційних осіб.

У звіті наводиться кілька механізмів обходу санкцій, які використовуються підсанкційними російськими особами. Один із ключових способів – фінансування витрат, пов'язаних із підтримкою розкішного способу життя, включаючи утримання супер'яхт, елітної нерухомості у Великій Британії, персональних послуг, навчання дітей у приватних школах та придбання предметів розкоші. Ці платежі часто здійснюються через "сприячів", що дає змогу приховати їхнє походження. Значну роль у схемах обходу санкцій відіграє використання криптовалют, оскільки вони дозволяють переводити кошти між юрисдикціями з мінімальним контролем з боку фінансових регуляторів.

Окремо розглянуто роль посередницьких країн у схемах обходу санкцій. OFSI зафіксувало, що понад 25% усіх підозрілих транзакцій так чи інакше були пов'язані з офшорними юрисдикціями та країнами, які пропонують сприятливі умови для ухилення від санкцій. Серед таких держав виокремлено Британські Віргінські Острови, Кіпр, Швейцарію, ОАЕ, Люксембург, Австрію та Туреччину. Спостерігається зміна географії санкційних порушень: у 2022 році переважно використовувалися офшорні компанії на BVI та в Швейцарії, тоді як у 2024 році значно зросла роль ОАЕ та Туреччини, які не мають жорстких санкційних обмежень щодо Росії. Встановлено, що через ці країни підсанкційні особи структурують власність активів, відкривають рахунки для приховування транзакцій та використовують криптобіржі, які не дотримуються санкційного контролю.

Особливу увагу у звіті приділено незаконним схемам передачі прав власності на активи підсанкційних осіб. OFSI зафіксував випадки, коли номінальні власники (переважно професійні посередники) заявляли про право власності на заморожені активи, щоб обійти санкційні обмеження. Це особливо актуально у випадках, коли активи належать складним корпоративним структурам або перебувають у стані фінансової нестабільності, наприклад, через процедури банкрутства. Такі маніпуляції дозволяють фактичним власникам зберігати контроль над активами, попри їхню формальну заморозку.

Звіт містить конкретні рекомендації для фінансових установ щодо посилення санкційного контролю. Зокрема, OFSI рекомендує впровадження детальнішого аналізу транзакцій, що можуть свідчити про фінансування витрат підсанкційних осіб третіми сторонами. Також

Висновки:

- **Британські фінансові установи недостатньо повідомляють про підозрілі транзакції**, що вимагає посилення механізмів самозвітування та внутрішнього моніторингу.
- **Російські підсанкційні особи активно використовують професійних та непрофесійних посередників для обходу санкцій**, фінансування активів та приховування джерел коштів.
- **Криптовалюти та посередницькі країни, такі як ОАЕ та Туреччина, стали ключовими інструментами обходу санкцій**, що потребує посиленого контролю та перевірок транзакцій із цих юрисдикцій.
- **Фінансові установи повинні вдосконалити механізми ідентифікації складних схем обходу санкцій**, зокрема шляхом розширення моніторингу власності активів та посилення міжнародної співпраці.

особливої уваги потребують операції з криптовалютами, оскільки вони часто використовуються для приховування джерел коштів. Крім того, у звіті наголошується на необхідності розширення моніторингу транзакцій, що проходять через посередницькі юрисдикції, та проведення ретельного аналізу структури власності клієнтів фінансових установ для виявлення прихованих зв'язків із підсанкційними особами.

У цілому, звіт Financial Services Threat Assessment акцентує увагу на тому, що механізми обходу санкцій стають дедалі складнішими та вимагають посилення контролю з боку фінансових установ, правоохоронних органів і регуляторів. OFSI закликає до активнішого самозвітування про підозрілі транзакції, впровадження комплексних перевірок клієнтів та зміцнення міжнародного співробітництва для ефективної боротьби з фінансовими порушеннями санкційного режиму.

CPI 2024: Як корупція загрожує кліматичній безпеці та глобальній стабільності [3]

Індекс сприйняття корупції (CPI) 2024 від Transparency International пропонує комплексний аналіз глобального стану корупції, оцінюючи 180 країн та територій за рівнем корумпованості державного сектора. Оцінка здійснюється за шкалою від 0 до 100, де 0 означає найвищий рівень корупції, а 100 – найнижчий. Загальний середній світовий показник CPI у 2024 році становить 43 бали зі 100, що свідчить про стійко високий рівень корупції у більшості країн. Близько двох третин держав мають оцінку нижче 50 балів, що вказує на серйозні проблеми з корупцією у державному управлінні.

Серед лідерів рейтингу найменш корумпованих країн знову опинилися Данія (90 балів), Фінляндія (88), Сінгапур (84) та Нова Зеландія (83). Високі результати цих країн пов'язані з наявністю ефективних демократичних інститутів, незалежних судових систем, а також розвиненими механізмами прозорості та підзвітності. Водночас на іншому кінці спектра залишаються країни з активними конфліктами або авторитарними режимами: Південний Судан (8 балів), Сомалі (9), Венесуела (10) та Сирія (12). Вони характеризуються слабкістю державних інституцій, значною корупцією у сфері розподілу ресурсів та повною відсутністю демократичної підзвітності.

[3] https://www.transparency.org/en/cpi/2024

Одна з центральних тем CPI 2024 – взаємозв'язок корупції та кліматичної кризи. Документ наголошує, що корупція стає потужним гальмом для міжнародних зусиль з боротьби зі змінами клімату. Корупційні схеми у сфері кліматичного фінансування призводять до розкрадання коштів, виділених на екологічні ініціативи, та сприяють ухваленню політичних рішень, що вигідні насамперед великим забруднювачам довкілля. Одним із прикладів є Росія, де виявлено масштабну корупційну схему в рамках проекту Глобального екологічного фонду (GEF), що мав на меті скорочення викидів, але зрештою не виконав жодного з поставлених завдань через неефективне управління коштами. Лівія є іншим прикладом країни, де корупція у поєднанні зі слабкістю державних механізмів призвела до катастрофічних наслідків: руйнування інфраструктури внаслідок шторму «Даніель» та загибель тисяч людей можна частково пояснити корупційними схемами у будівництві та обслуговуванні гідротехнічних споруд.

Документ також аналізує вплив корупції на формування політичних рішень у країнах із різними рівнями демократії. У розвинених країнах, таких як США (65 балів) та Канада (75 балів), корупція часто проявляється у формі недобросовісного лобіювання та політичного впливу великих корпорацій. У Сполучених Штатах масштабна корупційна схема в енергетичному секторі призвела до сповільнення переходу на відновлювані джерела енергії, оскільки окремі політики отримували фінансування від компаній, що намагалися зберегти свій контроль над енергетичним ринком. У той же час в авторитарних країнах корупція має більш класичні форми – через прямий підкуп чиновників, непрозорі тендери та розкрадання бюджетних коштів.

Ще один важливий аспект CPI 2024 – ризики, з якими стикаються екологічні активісти та журналісти, що викривають корупційні схеми у сфері довкілля. За останні п'ять років понад 1 000 екологічних активістів були вбиті у країнах із високим рівнем корупції, зокрема у Бразилії (34 бали), на Філіппінах (33) та у Демократичній Республіці Конго (20). Документ наголошує, що боротьба з корупцією має бути невід'ємною частиною екологічних реформ, оскільки без цього будь-які ініціативи щодо захисту навколишнього середовища будуть заблоковані або знівельовані інтересами корумпованих еліт.

Transparency International пропонує ряд стратегічних заходів для протидії корупції та посилення підзвітності у сфері кліматичних змін. Серед них – інтеграція антикорупційних механізмів у розподіл міжнародного фінансування, створення незалежних органів моніторингу витрат на кліматичні проекти, посилення правового захисту активістів та журналістів, що викривають корупційні злочини. Організація наголошує, що лише забезпечення прозорості у прийнятті рішень на міжнародному, національному та місцевому рівнях допоможе зробити зусилля у боротьбі зі змінами клімату ефективними.

Загалом, CPI 2024 демонструє, що корупція залишається глобальною загрозою, яка впливає не лише на політичну та

Висновки:

- **Посилення контролю за кліматичними фондами** – необхідно впроваджувати жорсткі механізми прозорості та підзвітності для запобігання розкраданню коштів, виділених на боротьбу зі змінами клімату.
- **Регулювання лобізму та політичного впливу** – країни мають забезпечити ефективний контроль за корпоративним лобіюванням, щоб запобігти маніпуляціям державними екологічними політиками.
- **Захист екологічних активістів і викривачів корупції** – необхідно створити правові гарантії безпеки для осіб, які розслідують корупцію у сфері довкілля, особливо у країнах із низьким рівнем демократичних свобод.
- **Розвиток демократичних інститутів** – країни з незалежною судовою системою та вільною пресою демонструють нижчий рівень корупції, що підтверджує необхідність зміцнення демократичних процесів для ефективної боротьби з корупцією.

економічну стабільність, але й на здатність людства протистояти найгострішим викликам, таким як кліматична криза. Документ підкреслює необхідність посилення міжнародного співробітництва та використання нових інструментів контролю для зменшення впливу корупції на критично важливі глобальні процеси.

Нові стандарти компетентності в криптоіндустрії: Аналіз консультаційного документу ESMA за MiCA[4]

Консультаційний документ Європейського управління з цінних паперів та ринків (ESMA) розроблений у рамках виконання положень Регламенту ЄС 2023/1114 про ринки криптоактивів (MiCA). Основною метою документа є встановлення критеріїв оцінки знань і компетентності фахівців, які надають інформацію або консультації щодо криптоактивів і криптовалютних послуг. ESMA наголошує на необхідності підвищення рівня кваліфікації персоналу через зростаючий вплив крипторинку на роздрібних інвесторів, який супроводжується високими ризиками, волатильністю та низьким рівнем обізнаності серед користувачів. Документ містить набір рекомендацій, спрямованих на гармонізацію підходів до оцінки кваліфікації в межах ЄС, та встановлює мінімальні вимоги до професійної підготовки та досвіду персоналу криптосервісних провайдерів.

Регламент MiCA передбачає, що всі криптовалютні провайдери, які надають послуги консультацій або інформування клієнтів, зобов'язані забезпечити належний рівень знань і компетентності своїх співробітників. Відповідно до статті 81(15) MiCA, ESMA отримала повноваження на розробку рекомендацій, які конкретизують ці вимоги. У документі розглядається необхідність підвищення якості інформаційних та консультаційних послуг у сфері криптоактивів, оскільки низький рівень обізнаності інвесторів і складність криптовалютного ринку створюють значні ризики для клієнтів. Зокрема, зазначається, що багато криптоактивів мають нестабільну ціну, високу чутливість до ринкових маніпуляцій і відсутність традиційних механізмів захисту, характерних для фінансових інструментів під регулюванням MiFID II.

Документ передбачає розробку чотирьох основних принципів, які повинні лягти в основу регулювання знань і компетентності персоналу криптовалютних сервісних провайдерів. Перший принцип встановлює загальні вимоги, що полягають у необхідності регулярного контролю кваліфікації співробітників, а також у підвищених вимогах до тих, хто надає консультаційні послуги, на відміну від осіб, які лише поширюють інформацію про криптоактиви. Особливу увагу приділено питанням автоматизованих консультацій та роботи алгоритмічних платформ: у таких випадках вимоги до знань і компетентності поширюються також на розробників, які створюють механізми ухвалення рішень.

Другий принцип визначає мінімальні вимоги до фахівців, які надають інформацію про криптоактиви. Вони повинні мати розуміння ключових характеристик, ризиків і ринкових особливостей криптовалютних активів, включаючи їхню волатильність, загрози кібератак, можливість втрати активів через неправильне зберігання приватних ключів, а також регуляторні ризики. До обов'язкових знань входять питання розподілених реєстрів (DLT), методів оцінки криптоактивів, економічних факторів, що впливають на їх вартість, а також механізмів ціноутворення на ринку. Для таких спеціалістів встановлено мінімальні кваліфікаційні вимоги:

[4] https://www.esma.europa.eu/sites/default/files/2025-02/ESMA35-1872330276-2004_MiCA_-_Consultation_Paper_-_Guidelines_on_knowledge_and_competence.pdf

або проходження щонайменше 80 годин професійного навчання та 6 місяців роботи під наглядом, або 1 рік відповідного досвіду. Також передбачено обов'язкове щорічне підвищення кваліфікації на рівні не менше 10 годин.

Третій принцип регламентує вимоги до осіб, які надають консультації щодо криптоактивів. На додаток до вищезгаданих компетенцій, такі фахівці повинні володіти знаннями у сфері управління інвестиційним портфелем, принципів диверсифікації та оцінки ризиків для клієнтів. Консультанти мають усвідомлювати, як відмінності між MiCA та MiFID II впливають на рівень захисту інвесторів, а також знати особливості оподаткування та комісійних зборів, що можуть виникати при інвестуванні в криптоактиви. Мінімальні кваліфікаційні вимоги для таких спеціалістів є значно жорсткішими: вони повинні мати або трирічну вищу освіту та річний досвід роботи, або середню освіту, доповнену трирічною професійною підготовкою та річним досвідом, або пройти 160 годин спеціалізованого навчання та мати принаймні рік роботи в сфері криптоактивів. Крім того, для консультантів встановлено підвищені вимоги до безперервного навчання – не менше 20 годин щорічного підвищення кваліфікації.

Четвертий принцип зосереджений на організаційних вимогах до оцінки, підтримки та оновлення знань персоналу. Криптовалютні провайдери повинні регулярно перевіряти відповідність своїх працівників встановленим критеріям, проводити внутрішній контроль та вести облік кваліфікацій і сертифікацій. Запроваджується вимога документування всіх процесів, пов'язаних із підвищенням компетентності персоналу, що має бути доступним для регуляторних органів. Також встановлено граничний термін роботи під наглядом для нових працівників – не більше 4 років. Якщо співробітник не відповідає встановленим вимогам, він може працювати виключно під керівництвом компетентного наставника, який повинен відповідати всім критеріям знань і досвіду.

Висновки:

- **ESMA встановлює жорсткі вимоги до кваліфікації персоналу криптосервісів.** Всі фахівці, що надають інформацію або консультації про криптоактиви, повинні мати професійну освіту або досвід роботи в цій сфері.
- **Консультанти з криптоактивів повинні мати вищий рівень компетентності, ніж ті, хто лише надає інформацію.** Вимоги включають не лише знання про ринок криптоактивів, але й розуміння інвестиційних стратегій та ризик-менеджменту.
- **Введено обов'язкову систему підвищення кваліфікації –** мінімальні стандарти: 10 годин CPD для інформування, 20 годин CPD для консультування.
- **Компанії повинні створити систему контролю за знаннями та компетентністю персоналу –** щорічні перевірки, ведення записів, а також навчання та сертифікація відповідно до вимог регулятора.

Документ підкреслює, що ESMA прагне забезпечити гармонізовану систему оцінки знань і компетентності персоналу криптосервісів по всьому ЄС, щоб уникнути ситуацій, коли різні юрисдикції встановлюють суперечливі або недостатньо суворі вимоги. Водночас підхід ESMA є гнучким: компаніям надається можливість самостійно визначати внутрішні критерії відповідності своїх співробітників загальноєвропейським вимогам. Важливим нововведенням є інтеграція принципів MiFID II, що використовуються у сфері традиційних фінансових ринків, для забезпечення високого рівня захисту інвесторів у криптовалютній сфері.

Окрему увагу ESMA приділяє практичним питанням впровадження цих стандартів, пропонуючи конкретні приклади, які допоможуть учасникам ринку адаптуватися до нових вимог. Також регулятор закликає зацікавлені сторони висловити свою позицію щодо запропонованих рекомендацій та надати коментарі до 22 квітня 2025 року. Після опрацювання зібраних відгуків ESMA планує опублікувати фінальний звіт у третьому кварталі 2025 року.

Регулювання

MiCAR [5]

Документ є детальним посібником щодо регулювання ринку криптоактивів у Європейському Союзі відповідно до Markets in Crypto-Assets Regulation (MiCAR), першого всеосяжного нормативного акту, що спрямований на врегулювання крипторинку в межах ЄС. Він містить аналіз передумов його запровадження, основних положень, вимог до суб'єктів ринку та ключових регуляторних аспектів.

Посібник починається з огляду нормативного середовища до прийняття MiCAR, зокрема Директиви 5AMLD, яка регулювала криптоактиви переважно у сфері протидії відмиванню коштів (AML). Проте ця директива лише встановлювала мінімальні вимоги, що призвело до різних підходів у країнах ЄС. Деякі держави розширили сферу дії законодавства, включивши до нього крипто біржі або ж запровадивши власні регуляторні моделі (як-от Франція, Німеччина та Мальта). Така фрагментація створила нерівні умови та потребу в єдиній нормативній базі.

MiCAR, запропонований у 2020 році та офіційно впроваджений у 2023 році, покликаний забезпечити уніфікований регуляторний режим для криптоактивів у всіх країнах ЄС. Його головною відмінністю від попередніх ініціатив є те, що це регламент, а не директива, що означає його пряму дію без необхідності транспозиц її в національне законодавство. Це значно скорочує регуляторні розбіжності між країнами.

Документ висвітлює основні положення MiCAR, включаючи визначення та класифікацію криптоактивів. Визначено три основні категорії:

- Електронні грошові токени (EMT), які прив'язані до однієї офіційної валюти.
- Токени, прив'язані до активів (ART), які забезпечені різними активами, включаючи товари, індекси чи інші криптоактиви.
- Інші криптоактиви, які не підпадають під EMT чи ART.

MiCAR запроваджує суворі вимоги до емітентів стейблкоїнів (EMT та ART), включаючи обов'язкову авторизацію для випуску, вимоги до резервного забезпечення та право власників на викуп токенів. Для EMT емітентами можуть бути лише банківські установи або компанії з ліцензією на випуск електронних грошей, тоді як ART можуть випускати лише суб'єкти, що мають спеціальний дозвіл відповідно до MiCAR. Встановлено вимоги до забезпечення мінімальних власних коштів та управління ризиками ліквідності.

Документ детально аналізує регулювання постачальників послуг з криптоактивами (CASPs), які надають послуги з обміну криптоактивів, кастодіальні послуги, послуги трейдингу, фінансового консалтингу тощо. Всі CASPs зобов’язані отримати ліцензію в ЄС, а також дотримуватися AML-вимог, стандартів ринкової поведінки та правил прозорості. Важливою новацією є можливість паспортингу, яка дозволяє CASPs, що мають ліцензію в одній країні ЄС, працювати у всіх державах-членах без додаткових дозволів.

MiCAR також передбачає санкції за маніпуляції ринком криптоактивів та порушення нормативних вимог. Регулювання охоплює підозрілі транзакції, інсайдерську торгівлю та

[5] https://info.merklescience.com/eu-micar-guide-2025?utm_campaign=6438145-EU%20MiCAR%20%7C%20Guide%20%7C%20Jan%2025&utm_source=Natalia&utm_medium=Internal%20Sales

маніпулятивні схеми. Вперше у законодавстві ЄС щодо криптоактивів передбачено захист інвесторів та споживачів шляхом обов'язкового розкриття інформації в білих книгах проектів.

Документ наголошує на територіальному аспекті застосування MiCAR, зокрема на вимозі для криптокомпаній, що обслуговують клієнтів з ЄС, мати юридичну присутність у ЄС. Водночас визначено механізм зворотного запиту (reverse solicitation), який дозволяє інвесторам із ЄС звертатися до нерегульованих провайдерів за межами ЄС без активного просування їхніх послуг у Союзі.

Окремий розділ присвячено правилам перехідного періоду, що діятимуть до 2026 року. Вони передбачають можливість продовження діяльності для CASPs, які вже працювали до кінця 2024 року, якщо національні регулятори надають їм таку можливість.

Завершальний розділ документу підкреслює довгостроковий вплив MiCAR на ринок криптоактивів в ЄС, включаючи перспективи інтеграції з міжнародними стандартами та можливість розширення регуляторних норм на нові форми цифрових активів, таких як CBDC та токенізовані цінні папери.

MiCAR знаменує нову еру в регулюванні криптоактивів у ЄС, створюючи єдині правила для всіх країн-членів, посилюючи нагляд, спрощуючи крос-юрисдикційну діяльність та підвищуючи довіру інвесторів до крипторинку.

Висновки:

- **Всі постачальники послуг з криптоактивами у ЄС зобов'язані отримати ліцензію CASP, а емітенти стейблкоїнів — спеціальний дозвіл**. Це створює єдину правову основу для ринку, але також встановлює високий бар'єр для нових учасників.
- **Введено єдині правила протидії ринковим маніпуляціям, фінансуванню тероризму та відмиванню коштів**. Всі криптокомпанії повинні дотримуватися AML-законодавства, публікувати звітність та забезпечувати прозорість операцій.
- **Застосування правил залежить від територіального зв'язку з ЄС**. Усі емітенти та провайдери, що прагнуть працювати в ЄС, мають юридично зареєструватися в державі-члені. Водночас механізм reverse solicitation дозволяє користувачам звертатися до нерегульованих закордонних компаній за власною ініціативою.
- **Перехідний період до 2026 року дозволяє CASPs, що працювали до кінця 2024 року, продовжувати діяльність за національним регулюванням, але без права паспортингу**. Всі нові CASPs повинні негайно отримати MiCAR-ліцензію.

Санкції

Час скасувати міжнародні санкції щодо Сирії?[6]

Документ аналізує питання можливого зняття міжнародних санкцій із Сирії після несподіваного повалення режиму Башара Асада в грудні 2024 року. Основну увагу приділено політичним змінам у країні, позиції міжнародної спільноти та оцінці санкційного тиску. Внаслідок швидкої військової кампанії, очолюваної угрупованням Хаят Тахрір аш-Шам (HTS), опозиційні сили взяли під контроль Дамаск, змусивши Асада втекти до Москви. Новий уряд, сформований HTS, заявляє про наміри провести інклюзивну політичну трансформацію, зберегти державні інституції та розпочати діалог із міжнародною спільнотою.

Значна частина документа присвячена детальному розгляду міжнародних санкцій, що були накладені на Сирію за останні десятиліття. США наклали найбільш комплексні санкції,

[6] https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/767245/EPRS_BRI(2025)767245_EN.pdf


BRIEFING

European Parliament

Time to lift the international sanctions on Syria?

SUMMARY

Since the unexpected overthrow of Bashar al-Assad's regime in early December 2024, Syria has embarked on an uncertain trajectory. Hayat Tahrir al-Sham (HTS), the armed jihadi group leading the offensive against the Assad forces, has now taken charge of the country and set up a caretaker government. Scepticism abounds in international circles about HTS owing to the group's terrorist credentials and Salafist ideology. However, the new Syrian authorities have declared plans to establish a political transition inclusive of all minorities and segments of Syrian society, as well as increased engagement with neighbouring countries and other foreign players, offering the international community some reassurance.

One of the main demands in the current context from all sides, within Syria as well as from other states and organisations, has been to lift the complex web of international economic, financial and trade sanctions against the country. Most of these sanctions were imposed after Assad's brutal crackdown on protesters in 2011. Moreover, calls have been made to remove the designations of HTS and its leader Ahmed al-Sharaa from the international terrorist lists. Such steps are believed to be essential in addressing the significant economic and humanitarian challenges facing the country after nearly 14 years of civil war.

The United States (US) imposes the most comprehensive sanctions on Syria, including secondary sanctions on foreign governments, non-US individuals and entities doing business with the Syrian government and sanctioned entities in Syria. The European Union (EU) has also imposed restrictive measures on certain Syrian economic sectors, along with asset freezes and travel bans on individuals or entities supporting the Assad regime. In January 2025, the US granted short-term waivers relating to the provision of basic services in response to requests for sanctions relief for Syria. Similarly, the EU Member States reached a political agreement to suspend certain restrictions gradually and conditionally. The UN Security Council has the authority to remove the terrorist designations of HTS and its leader from the ISIL (Da'esh)/Al-Qaida list.

IN THIS BRIEFING

- Upheaval in Syria: The emerging order post-Assad
- Overview of international sanctions on Syria
- Lifting of international sanctions against Syria
- European Parliament

EPRS | European Parliamentary Research Service

Author: Carmen-Cristina Cîrlig
Members' Research Service
PE 737.245 – February 2025

EN

включаючи вторинні обмеження для осіб і компаній, що взаємодіють із сирійським урядом. ЄС, зі свого боку, запровадив ембарго на постачання озброєнь, фінансові обмеження, заборону на торгівлю нафтою, а також санкції проти окремих осіб і компаній, пов'язаних із режимом Асада. У січні 2025 року США та ЄС ухвалили рішення про поступове та умовне послаблення санкцій, зокрема шляхом тимчасових винятків для надання гуманітарної допомоги та базових послуг.

Документ розглядає основні аргументи на користь зняття санкцій, включаючи необхідність економічного відновлення Сирії, покращення гуманітарної ситуації та підтримку нового уряду в забезпеченні стабільності. Уряд HTS наголошує на важливості отримання міжнародного фінансування для відбудови інфраструктури та повернення біженців. Проте міжнародна спільнота залишається обережною через терористичні зв'язки HTS, що офіційно внесене до списків санкцій ООН, США та ЄС.

Деякі країни, зокрема Туреччина, Саудівська Аравія та Йорданія, висловлюють готовність до співпраці з новою владою Сирії та закликають до перегляду санкційної політики. Європейський Союз веде переговори щодо поступового скасування обмежень, зберігаючи водночас тиск на Дамаск з метою забезпечення інклюзивного політичного процесу. США, хоча й надали тимчасові ліцензії на окремі економічні операції, загалом продовжують дотримуватися жорсткої санкційної політики, зокрема щодо HTS.

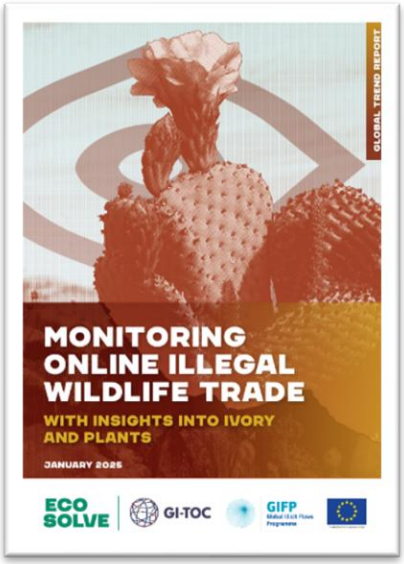
Документ аналізує можливі сценарії майбутнього санкційного режиму, включаючи умови для повного зняття санкцій, які можуть включати поступову демократизацію Сирії, забезпечення прав меншин і жінок, а також відмову HTS від радикальних ідеологічних настанов. Окремо розглянуто потенційні наслідки для міжнародної безпеки, якщо HTS залишиться при владі без проведення глибоких політичних реформ.

Висновки:

- **Поступове пом'якшення санкцій залежить від політичної інклюзивності** – ЄС та США готові послабити санкційний режим лише за умови, що нова влада Сирії продемонструє реальні кроки до інклюзивної політичної трансформації, захисту прав меншин і жінок, а також уникнення радикалізації.
- **HTS залишається у фокусі міжнародної уваги через терористичні зв'язки** – Незважаючи на заяви нового уряду про прагнення до політичної інтеграції, міжнародна спільнота не поспішає скасовувати його статус як терористичної організації, що обмежує можливості економічної інтеграції Сирії.
- **Економічне відновлення країни залежить від зовнішнього фінансування** – Відбудова критичної інфраструктури та повернення біженців потребують значних фінансових вливань, які наразі обмежені санкціями, а також відсутністю довіри з боку міжнародних кредиторів.
- **Ризики дестабілізації та геополітичні наслідки** – Якщо міжнародні санкції залишаться в силі, це може спричинити подальший економічний занепад і гуманітарну кризу, що матиме наслідки для сусідніх країн та може створити вакуум, який використають інші радикальні угруповання.

Звіти окремих інституцій та експертів

Цифрові сліди контрабанди: як онлайн-ринок підживлює незаконну торгівлю слоновою кісткою та рідкісними рослинами [7]



Документ, підготовлений Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC), є частиною серії Global Trend Reports, що висвітлює поточні тенденції незаконної торгівлі видами дикої природи через онлайн-платформи. У ньому зосереджено увагу на двох основних напрямах: торгівлі слоновою кісткою, зокрема в Таїланді, та незаконній торгівлі рідкісними рослинами у глобальному масштабі. Дослідження базується на даних Глобальної системи моніторингу (GMS), що аналізує онлайн-ринок через регіональні хаби в Бразилії, Південній Африці та Таїланді, фіксуючи масштаби нелегальної торгівлі та адаптацію злочинних схем до сучасних умов.

Останні дані, зібрані за період серпня—жовтня 2024 року, вказують на різке зростання обсягів онлайн-торгівлі видами, що перебувають під міжнародним захистом. Протягом зазначеного періоду GMS ідентифікувала 1 741 оголошення про продаж 34 захищених видів. Найбільшу частку (77%) таких оголошень було зафіксовано в Таїланді, що свідчить про масштабний тіньовий ринок у країні, тоді як у Бразилії та ПАР ситуація є відносно стабільною, хоча й викликає занепокоєння. Більшість незаконної торгівлі ведеться через соціальні мережі, зокрема Facebook, на який припадає 91% усіх зафіксованих оголошень. Значно менше використовується e-commerce-платформи, проте спостерігається збільшення активності на таких сайтах, як OLX (Бразилія) та PublicAds (ПАР).

Значну увагу приділено аналізу торгівлі слоновою кісткою в Таїланді, де цей ринок має історично сформовані корені та пов'язаний із культурними традиціями. Хоча законодавство країни значно посилило контроль над продажем слонової кістки, незаконний ринок перейшов у цифровий формат, використовуючи онлайн-платформи та месенджери. Найбільш популярними категоріями товарів є необроблена слонова кістка (45,1% оголошень), ювелірні вироби (36,1%), фігурки та статуетки (10,8%), що свідчить про високий попит на сировину для подальшої обробки та продажу. Важливим аспектом є використання шифрованих месенджерів (WhatsApp, Telegram) та прихованої термінології, що ускладнює моніторинг. Наприклад, у багатьох оголошеннях використовується емодзі слона «🐘» замість слів «слонова кістка», що є однією зі стратегій уникнення автоматичного виявлення.

Таїландське законодавство передбачає жорсткі обмеження на торгівлю слоновою кісткою, проте має певні юридичні прогалини, що дозволяють легальну реалізацію кістки, отриманої від домашніх азійських слонів, що ускладнює контроль за походженням продукції. Крім того, відсутність механізму ретроспективної сертифікації дозволяє певним продавцям реалізовувати нелегальну продукцію під виглядом старих запасів. Законодавчі ініціативи останніх років, включно із посиленням відповідальності та введенням суворіших правил реєстрації слонів, покращили ситуацію, однак слабкий контроль у цифровому середовищі продовжує сприяти розвитку нелегальної торгівлі.

[7] https://globalinitiative.net/wp-content/uploads/2025/01/Monitoring-illegal-wildlife-trade-Ivory-and-plants-GI-TOC-January-2025.pdf

Другий ключовий аспект документа присвячений незаконній торгівлі рідкісними рослинами, що є менш обговорюваною, але не менш серйозною загрозою. На світовому рівні попит на сукуленти, рідкісні орхідеї, кактуси та цінні породи деревини постійно зростає, стимулюючи незаконне вилучення рослин з природного середовища. UNODC оцінює річний обсяг легального ринку захищених рослин у $9,3 млрд, але незаконна торгівля залишається переважно невидимою через низький рівень правоохоронного реагування. Основні маршрути контрабанди ведуть з Південної Африки, Латинської Америки та Південно-Східної Азії до споживчих ринків у Європі, США та Китаї.

Контрабандисти активно використовують цифрові технології для координації своїх дій: ботанічні сайти, соціальні мережі та месенджери застосовуються для збору інформації про рідкісні види, тоді як криптовалюти та онлайн-платежі використовуються для приховування незаконних транзакцій. Значна кількість рослин вивозиться через повітряні та морські маршрути, часто підробленими партіями або замаскованими під інші товари. Наприклад, у Південній Африці зафіксовано випадки, коли 12 000 сукулентів були замасковані під гриби для нелегального експорту до Китаю.

Зважаючи на ці виклики, автори документа наголошують на необхідності інноваційних методів боротьби з онлайн-торгівлею дикою природою. До них належать впровадження штучного інтелекту для моніторингу оголошень, розширення міжнародної співпраці, посилення кримінальної відповідальності та розвиток законодавчих ініціатив. Зокрема, важливо створити електронні бази даних зареєстрованих продавців слонової кістки, що дозволить покупцям перевіряти легальність товарів перед купівлею. Також рекомендується використовувати ДНК-тестування та спектроскопічний аналіз для визначення походження слонової кістки та рослин, що допоможе виявляти нелегальні партії.

Загалом, документ підкреслює необхідність багатокомпонентного підходу для боротьби з незаконною торгівлею дикою природою, що включає посилення контролю за онлайн-торгівлею, використання технологій для відстеження транзакцій, підвищення рівня обізнаності громадськості та створення більш ефективних міжнародних механізмів взаємодії між правоохоронними органами та екологічними організаціями. Важливим залишається зниження попиту на нелегальні товари, що може бути досягнуто завдяки активним інформаційним кампаніям та розвитку програм зі сталого вирощування рідкісних видів у контрольованих умовах.

Висновки:

- **Соціальні мережі є головним каналом незаконної торгівлі**, зокрема Facebook (91% оголошень), що вимагає посилення автоматичного моніторингу та співпраці з платформами.
- **Контрабандисти використовують кодові слова,** емодзі та зашифровані месенджери для уникнення контролю, що потребує впровадження AI-аналізу та веб-скрапінгу.
- **Незаконна торгівля рідкісними рослинами зростає,** особливо у сфері онлайн-торгівлі сукулентами, орхідеями та кактусами, що вимагає міжнародного моніторингу e-commerce платформ.
- **Посилення законодавства та правоохоронних заходів** необхідне для ліквідації юридичних прогалин, посилення відповідальності та впровадження електронних баз даних для відстеження торгівлі.

Глобальна імперія шахрайства: як онлайн-злочинність досягла масштабів наркобізнесу [8]

Стаття розкриває феномен глобального шахрайства, яке досягло безпрецедентного масштабу, завдаючи збитків у сотні мільярдів доларів щорічно. Онлайн-шахрайство стало новою формою організованої злочинності, яка порівнянна за розмахом із наркобізнесом, але є ще небезпечнішою через свою масштабованість та складність викриття. Завдяки використанню новітніх технологій, зокрема штучного інтелекту, а також криптовалют, шахраї створили цілу екосистему, що функціонує на міжнародному рівні та залучає до своєї діяльності сотні тисяч людей, зокрема жертв, примусово залучених до злочинних схем.

Основна увага у статті приділяється методу шахрайства, відомому як "pig butchering" (або китайською "ша атемақәа"), що дослівно перекладається як «відгодівля свині». Ця схема передбачає довготривалий процес завоювання довіри жертви через соціальну інженерію. Шахраї, використовуючи підроблені профілі у соціальних мережах та месенджерах, знаходять потенційних жертв і поступово вибудовують з ними дружні або романтичні стосунки. Після того як жертва стає емоційно залежною, її спонукають інвестувати у вигідну фінансову можливість, найчастіше пов’язану з криптовалютою або ринками форекс. Коли жертва довіряє шахраям значні кошти та намагається їх вивести, вона дізнається, що вся схема була фікцією, а гроші безповоротно зникли.

Шахрайські угруповання мають складну структуру та працюють у різних юрисдикціях, що ускладнює їх виявлення та покарання. У статті наводяться випадки, коли жертвами шахрайства ставали навіть висококваліфіковані спеціалісти, такі як науковці або банкіри, а серед великих кейсів — банкрутство американського банку через те, що його директор вклав 47 мільйонів доларів у фальшиву криптовалютну платформу. Розповідається і про випадки, коли шахраї використовували глибокі фейки (deepfake) для імітації голосу та зовнішності керівників компаній, що дозволяло їм викрадати мільйони доларів у корпорацій.

Відзначається, що основні центри шахрайської діяльності розташовані в Південно-Східній Азії, зокрема у М’янмі, Камбоджі та Лаосі, де уряди або не мають достатньої сили для боротьби з такими угрупованнями, або ж активно співпрацюють із ними. Деякі злочинні анклави виглядають як закриті містечка, де працюють тисячі людей, які нерідко стають жертвами примусової праці. Їх утримують у неволі, змушуючи брати участь у шахрайських схемах, а за спробу втечі можуть застосовувати тортури. Один із найбільш показових випадків — історія філіппінки, яку насильно утримували в М’янмі та примушували займатися шахрайством під виглядом інвесторки.

Стаття також висвітлює ключові технологічні загрози, що посилюють проблему. Серед них особливо небезпечними є штучний інтелект, який дозволяє автоматизувати комунікацію з жертвами та адаптувати маніпулятивні техніки, а також анонімні фінансові системи, що дають змогу швидко переказувати кошти, зменшуючи ризик відстеження. Шахраї використовують криптовалюту для відмивання грошей, а їхні операції настільки динамічні, що традиційні методи

[8] https://www.economist.com/leaders/2025/02/06/the-vast-and-sophisticated-global-enterprise-that-is-scam-inc

фінансового моніторингу часто не встигають за їхніми схемами. Вони створюють цілі платформи, що виглядають як легальні трейдингові сервіси, мають професійно зроблені вебсайти та служби підтримки, що підвищує рівень довіри серед потенційних жертв.

Однією з головних проблем, яку виділяє стаття, є відсутність ефективних міжнародних механізмів боротьби з таким шахрайством. Поліція та регулятори у більшості країн продовжують розглядати онлайн-шахрайство як дрібне правопорушення, що ускладнює координацію між державами та робить боротьбу з транснаціональними злочинними угрупованнями вкрай неефективною. У статті наведено приклади того, як великі держави, такі як Китай, проводять масові арешти шахраїв, проте оскільки вони діють у різних юрисдикціях, значна частина злочинців залишається безкарною. Окремо наголошується, що США та Китай, попри загальне геополітичне протистояння, могли б співпрацювати у сфері боротьби з шахрайством, адже ця проблема є спільною загрозою для обох країн.

Автори підкреслюють, що для ефективної боротьби зі світовою мережею шахрайства потрібен комплексний підхід, який включатиме створення міжнародної платформи для обміну інформацією між банками, криптобіржами, правоохоронними органами та технологічними компаніями. У статті розглядається приклад Сінгапуру, де вже створено таку систему, що дозволяє в режимі реального часу відстежувати та блокувати підозрілі транзакції. Також зазначається, що для зменшення кількості жертв необхідно інвестувати у навчальні кампанії, спрямовані на підвищення цифрової грамотності серед населення. Вже сьогодні у деяких країнах, таких як Сінгапур, під час фінансових операцій з'являються автоматичні попередження про можливі шахрайські ризики.

Однак навіть такі заходи можуть виявитися недостатніми через постійну еволюцію шахрайських схем. Злочинні угруповання продовжують удосконалювати свої методи, використовуючи дедалі складніші технології. Однією з найбільших загроз найближчого майбутнього є використання генеративного штучного інтелекту для масового створення фейкових особистостей та шахрайських схем, що ускладнить розпізнавання обману навіть для досвідчених користувачів. Шахраї також починають використовувати аналітичні алгоритми для вибору жертв за психологічними характеристиками, наприклад, шукаючи фінансово нестабільних людей, які переживають емоційні труднощі.

Висновки:

- **Онлайн-шахрайство стало глобальною загрозою**, що дорівнює наркобізнесу, та потребує аналогічних методів боротьби.
- **Штучний інтелект і криптовалюта надають шахраям нові можливості**, тому необхідно впроваджувати контроль за фінансовими потоками та ШІ-захист.
- **Відсутність міжнародної координації дозволяє шахраям діяти безкарно**, що вимагає створення глобальної системи моніторингу та обміну даними.
- **Інформаційна обізнаність громадян є найкращим способом запобігання шахрайству**, тому слід впровадити автоматичні попередження в онлайн-транзакціях.
- **Шахраї використовують передові технології та персональні дані**, тому критично важливо розвивати кібербезпеку та системи раннього виявлення загроз.

Загалом, стаття показує, що онлайн-шахрайство вже зараз є однією з найсерйозніших глобальних загроз, що потребує негайного реагування. Якщо держави та міжнародні організації не розроблять ефективних механізмів боротьби, масштаби шахрайства продовжать зростати, завдаючи все більших економічних і соціальних втрат.

Фінансові технології та регулювання в ЄС: баланс між інноваціями та безпекою[9]

Документ є комплексним аналітичним дослідженням цифрових фінансів у Європейському Союзі. Це друге щорічне видання, створене в межах ініціативи EU Supervisory Digital Finance Academy (EU-SDFA), яка спрямована на підвищення компетенцій фінансових регуляторів у сфері цифрових технологій, інновацій та штучного інтелекту. Основна увага приділяється аналізу ключових макротрендів цифрової фінансової трансформації, впливу нових технологій на регуляторне середовище, використанню штучного інтелекту у фінансовій галузі, ризикам, пов'язаним із його впровадженням, а також глобальним викликам, що формують сучасний фінансовий ландшафт ЄС.

У першій частині досліджується екосистема цифрових фінансів, яка включає аналіз розвитку фінансових технологій (FinTech), ринку криптоактивів, нових моделей цифрових платежів та тенденцій, що визначають динаміку фінансового сектору. Значна увага приділяється регуляторним ініціативам ЄС, таким як Markets in Crypto-Assets Regulation (MiCA), який встановлює єдині правила для ринку криптоактивів у межах ЄС, та Digital Operational Resilience Act (DORA), що забезпечує стандарти кіберстійкості фінансових установ. Окремо розглядається ініціатива Financial Data Access Framework (FiDA), яка спрямована на відкритий доступ до фінансових даних та сприяння розвитку відкритого банкінгу. Досліджується також перспектива впровадження цифрового євро, що має на меті створення цифрового аналога фіатної валюти, регульованого Європейським центральним банком.

Друга частина документа присвячена штучному інтелекту та його впливу на фінансовий сектор. Розглядається потенціал використання ШІ для автоматизації фінансових процесів, управління ризиками, прогнозування ринкових тенденцій та покращення клієнтського досвіду. Визначаються основні сценарії застосування ШІ в банківській сфері, управлінні активами, страхуванні та кібербезпеці. Водночас акцентується увага на ризиках, пов'язаних із використанням штучного інтелекту, зокрема можливостях маніпулювання ринками, підвищенні уразливості до кібератак та проблемах алгоритмічної дискримінації. Розглядається вплив EU AI Act, який встановлює рамкове регулювання використання ШІ, а також глобальні підходи до регулювання цієї технології.

Документ також аналізує геополітичні аспекти цифрових фінансів, зокрема роль США та Китаю у формуванні світового технологічного ландшафту та їхній вплив на європейську фінансову екосистему. Досліджується залежність фінансового сектору ЄС від Big Tech компаній, що домінують у сфері хмарних технологій, цифрових платежів і збору даних. Розглядаються ризики концентрації ринку та сценарії регуляторного втручання для зменшення залежності від зовнішніх технологічних гігантів. Аналізуються виклики, пов'язані із впровадженням цифрових валют центральних банків (CBDC), а також використання технологій розподіленого реєстру (DLT) у міжнародних розрахунках.

[9] https://cadmus.eui.eu/bitstream/handle/1814/77926/QM-01-24-186-EN-N.pdf?sequence=4&isAllowed=y

Завершальна частина документа підбиває підсумки ключових змін у цифрових фінансах, робить висновки щодо ефективності поточного регуляторного підходу та пропонує стратегічні рекомендації для майбутньої політики ЄС у цій сфері. Основний акцент зроблено на необхідності балансу між інноваціями та регулюванням, щоб стимулювати розвиток цифрових фінансів, одночасно забезпечуючи фінансову стабільність, захист прав споживачів та кібербезпеку.

Висновки:

- Стратегічний підхід до регулювання цифрових фінансів:
  - ЄС активно використовує регуляторні ініціативи (зокрема, MiCA, DORA, AI Act) для керованого розвитку цифрових фінансів.
  - Необхідна гармонізація регулювання в межах ЄС для уникнення арбітражу та підвищення кіберстійкості фінансових установ.
- Штучний інтелект змінює фінансовий сектор, але потребує контролю:
  - Використання ШІ у фінансах створює як можливості (автоматизація аналізу ризиків, боротьба з шахрайством), так і ризики (маніпуляції ринками, дискримінація в алгоритмах).
  - Впровадження AI Act стане визначальним для розвитку ШІ в фінансовій сфері ЄС.
- Геополітична конкуренція у фінансових технологіях:
  - США та Китай лідирують у розробці фінансових технологій, що створює виклики для ЄС у сфері Big Tech та цифрових валют.
  - Європі необхідно розвивати власну інфраструктуру цифрових фінансів, зменшуючи залежність від зовнішніх технологічних гігантів.
- Цифровий євро: виклики та перспективи:
  - Розвиток цифрового євро повинен забезпечити баланс між фінансовою інклюзією, контролем грошового обігу та кібербезпекою.
  - Необхідна чітка політика ЄЦБ щодо використання цифрового євро в міжнародних розрахунках, щоб посилити роль євро у глобальній економіці.

Інші новини

Фінансова розвідка у дії: нові загрози, виклики та міжнародні ініціативи у боротьбі з фінансовими злочинами [10]

У 30-му випуску журналу SARs in Action, опублікованому Британським підрозділом фінансової розвідки (UKFIU), висвітлюються ключові питання боротьби з фінансовими злочинами, що впливають на міжнародну безпеку та економічну стабільність. Основними темами цього випуску є посилення заходів протидії незаконній торгівлі дикою природою, використання штучного інтелекту для обходу перевірок клієнтів у фінансовому секторі, цифрова трансформація процесу подання та аналізу підозрілих фінансових операцій, а також результати великомасштабної міжнародної операції «DESTABILISE» щодо ліквідації злочинних фінансових мереж, пов'язаних із Росією.

Випуск починається з аналізу зусиль UKFIU у боротьбі з незаконною торгівлею дикою природою (Illegal Wildlife Trade, IWT) та екологічними злочинами. Оскільки ці види злочинності приносять значні прибутки організованим кримінальним групам, вони становлять серйозну загрозу не лише для екосистем, а й для глобальної фінансової стабільності. UKFIU підтримує кілька

[10] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/739-sars-in-action-issue-30/file

міжнародних ініціатив, зокрема Project Anton, який спрямований на виявлення фінансових потоків, пов'язаних з IWT, та підвищення рівня їх відображення у звітах про підозрілі операції (SARs). Організація також підписала United for Wildlife Statement of Principles, що підкреслює важливість міжнародної співпраці у протидії фінансуванню злочинів проти навколишнього середовища. Крім того, UKFIU стала частиною Europol Financial Intelligence Public-Private Partnership IWT Work Stream, що дозволяє застосовувати європейський підхід до виявлення фінансових злочинів, пов'язаних із незаконним виловом риби, незаконною вирубкою лісів та іншими видами екологічної злочинності.

Окрему увагу у випуску приділено дослідженню використання штучного інтелекту (AI) для обходу процедур ідентифікації клієнтів (KYC/CDD). У жовтні 2024 року Joint Money Laundering Intelligence Taskforce (JMLIT+) оприлюднила Amber Alert, у якому детально описано, як технології deepfake, генерація фальшивих документів та AI-ідентифікація використовуються для реєстрації банківських рахунків та криптовалютних гаманців на підставних осіб. Виявлено, що злочинці активно використовують AI-генеровані паспортні документи та відео для обходу перевірок клієнтів у фінансових установах, що створює новий рівень загроз для міжнародної фінансової системи. У зв'язку з цим планується створення спеціальної публічно-приватної робочої групи, яка покликана розробити ефективні механізми боротьби із цими ризиками.

Ще одним важливим аспектом є цифрова трансформація подання SARs. SARs Digital Transformation Programme повідомляє, що за останній рік через нові цифрові канали було подано майже мільйон звітів. Випуск містить оновлену інформацію про міграцію історичних даних до SARs Digital Service (SDS), що дозволить значно покращити аналітичну роботу UKFIU та правоохоронних органів. Керівник програми Мартін Сідауей наголошує, що цифровізація дозволить забезпечити швидший доступ до фінансової інформації та ефективніше виявлення схем відмивання коштів та фінансування тероризму.

Один із найбільш резонансних матеріалів випуску присвячений результатам операції «DESTABILISE», яку проводило Національне агентство з боротьби зі злочинністю Великої Британії (NCA) спільно з міжнародними партнерами.

Висновки:

- **Фінансові установи повинні посилити моніторинг підозрілих транзакцій**, пов'язаних з незаконною торгівлею дикою природою, оскільки рівень їх звітування залишається критично низьким (<0.2% від загальної кількості SARs).
- **Штучний інтелект активно використовується для обходу перевірок KYC/CDD**, тому фінансовим установам слід запровадити додаткові біометричні верифікаційні заходи та посилене спостереження за онлайн-ідентифікацією клієнтів.
- **Операція «DESTABILISE» довела, що російські злочинні фінансові мережі масово використовують криптовалюти та традиційний банківський сектор для обходу санкцій**, що вимагає розширення санкційних списків і міжнародного співробітництва.
- **Цифрова трансформація процесу подання та аналізу SARs значно покращує ефективність фінансових розслідувань**, тому суб'єктам фінансового моніторингу слід адаптуватися до нових цифрових форматів звітування.

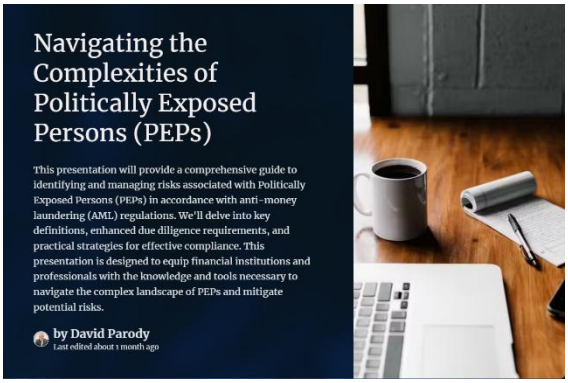
Операція була спрямована на ліквідацію двох великих російськомовних фінансових злочинних угруповань – Smart Group і TGR, що відмивали мільярди доларів щорічно через міжнародні банківські канали та криптовалютні ринки. Ці групи надавали послуги конвертації готівки, що походить від продажу наркотиків, у криптовалюту, допомагали обходити міжнародні санкції, а також фінансували російські шпигунські операції. Завдяки співпраці UKFIU, OFAC (США), JMLIT та інших міжнародних партнерів, було заарештовано 84 особи, заморожено рахунки на суму 20 мільйонів фунтів стерлінгів, а дев'ять ключових учасників угруповань внесені до санкційних списків США. Операція стала однією з найуспішніших в історії міжнародної боротьби з фінансовою злочинністю.

Останній розділ випуску – «Dear UKFIU», нова рубрика, де UKFIU відповідає на запитання читачів щодо процесу подання SARs. Відповідаючи на запитання про те, чому рідко надходять відповіді від правоохоронних органів після подання SARs, UKFIU пояснює, що через величезний обсяг щорічних звітів (понад 800 000) більшість із них стають частиною довготривалих розслідувань, а не одразу призводять до видимих дій. Також пояснюється, що SARs не є офіційними повідомленнями про злочин, а інструментом для виявлення підозрілих фінансових операцій, тому в разі серйозних підозр рекомендовано повідомляти про злочин безпосередньо в поліцію чи податкові органи.

Цей випуск SARs in Action демонструє зростаючу важливість фінансової розвідки у виявленні складних злочинних схем та загроз для глобальної фінансової системи. Особливий акцент робиться на міжнародній співпраці, необхідності використання сучасних цифрових технологій для протидії фінансовим злочинам, а також зростаючій загрозі з боку нових технологій, зокрема штучного інтелекту.

Для загального розвитку

Навігація у складнощах, пов'язаних із політично значущими особами (PEP)[11]



Політично значущі особи (PEP) становлять особливий ризик для фінансових установ та суб'єктів фінансового моніторингу через можливий зв'язок із корупцією, відмиванням коштів та іншими фінансовими злочинами. Виявлення та належне управління ризиками, пов'язаними з PEP, є критично важливими для забезпечення відповідності вимогам міжнародних стандартів та запобігання зловживанням фінансовою системою.

Оскільки PEP мають доступ до значних фінансових ресурсів та впливу, регулювання передбачає посилену належну перевірку. Це включає ідентифікацію джерел їхнього багатства, моніторинг транзакцій та оцінку ризиків взаємодії з ними. Фінансові установи зобов'язані застосовувати ризик-орієнтований підхід, враховуючи фактори, що можуть вказувати на підвищений рівень ризику, наприклад, непрозорі джерела доходів або зв'язки з офшорними структурами.

В матеріалі підкреслюється важливість розрізнення національних та іноземних PEP, а також їхніх близьких родичів і осіб, пов'язаних через ділові відносини. Іноземні PEP, як правило, становлять

[11] https://gamma.app/docs/Navigating-the-Complexities-of-Politically-Exposed-Persons-PEPs-d08cf0o7q8u5z1p?mode=doc

вищий рівень ризику через складність відстеження їхньої діяльності та потенційну залученість у корупційні схеми.

Одним із викликів є динамічний характер статусу PEP – особа може втратити офіційний статус, проте ризики залишаються, оскільки вона могла накопичити активи або зв'язки, що використовуються для збереження впливу. Тому контроль за PEP не завершується автоматично після завершення їхніх офіційних повноважень.

Застосування технологічних рішень для моніторингу та аналізу транзакцій у реальному часі є ключовим інструментом у виявленні підозрілих операцій. Використання автоматизованих систем перевірки санкційних списків та баз даних PEP допомагає фінансовим установам швидко ідентифікувати потенційно ризикових осіб та уникнути порушень регуляторних вимог.

У сучасному регуляторному середовищі навігація у складнощах, пов'язаних із PEP, вимагає комплексного підходу, що поєднує політику внутрішнього контролю, технологічні рішення та міжнародну співпрацю для запобігання фінансовим зловживанням.

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-2025-08

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].