Методологічний бюлетень

Серійний номер: МінФін-AML-2025-10

Березень 2025

Мета

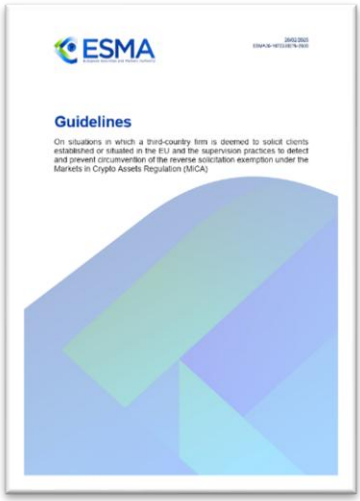
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). 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

Регулювання в ЄС: Рекомендації ESMA щодо діяльності фірм із третіх країн у сфері криптоактивів [1]



Документ, підготовлений Європейським управлінням з цінних паперів і ринків (ESMA), є набором рекомендацій, спрямованих на регулювання ситуацій, коли фірми з третіх країн вважаються такими, що залучають клієнтів, які перебувають або зареєстровані в Європейському Союзі (ЄС), а також наглядових практик для виявлення та запобігання обходу винятку зворотного залучення (reverse solicitation exemption) відповідно до Регламенту про ринки криптоактивів (MiCA). Цей документ має на меті гармонізувати підходи до інтерпретації та застосування положень MiCA, зокрема статті 61, у всіх країнах-членах ЄС, забезпечуючи однакові, ефективні та послідовні наглядові практики в рамках Європейської системи фінансового нагляду (ESFS). Він адресований компетентним органам, як визначено в MiCA, а також частково стосується фірм із третіх країн, які надають послуги, пов’язані з криптоактивами, клієнтам у ЄС без відповідної авторизації.

Рекомендації вступають у дію через 60 календарних днів після їх публікації на вебсайті ESMA усіма офіційними мовами ЄС, що дає чіткий дедлайн для адаптації. Документ спирається на

[1] https://www.esma.europa.eu/sites/default/files/2025-02/ESMA35-1872330276-2030_Guidelines_on_reverse_solicitation_under_MiCA.pdf

ключові законодавчі акти, такі як Регламент ESMA (Regulation (EU) No 1095/2010) та MiCA (Regulation (EU) 2023/1114), і вводить важливе визначення: фірма з третьої країни — це організація, яка підпадала б під вимоги авторизації за статтею 59 MiCA, якби її головний офіс чи зареєстрований офіс розташовувалися в межах ЄС. Основна мета полягає в тому, щоб уточнити, коли такі фірми вважаються такими, що активно залучають клієнтів із ЄС, і запобігти зловживанню винятком зворотного залучення, коли послуги надаються виключно за ініціативою клієнта. Для цього документ пропонує як критерії оцінки залучення, так і конкретні заходи для нагляду.

Щодо зобов'язань, компетентні органи зобов'язані докласти всіх зусиль для дотримання рекомендацій і протягом двох місяців після їх публікації повідомити ESMA про свій статус відповідності — чи то повне дотримання, намір дотримуватися, чи відмова від дотримання з обґрунтуванням причин. Такий підхід підкреслює серйозність впровадження рекомендацій і забезпечує прозорість у процесі їх адаптації на національному рівні. Водночас фірми з третіх країн опосередковано отримують вказівки щодо того, як їхня діяльність може бути класифікована як залучення, що має практичні наслідки для їхньої операційної стратегії в ЄС.

Основна частина документа зосереджена на детальному описі того, як фірми з третіх країн можуть залучати клієнтів із ЄС. Поняття залучення трактується широко і технологічно нейтрально, охоплюючи будь-які форми просування, реклами чи пропозицій криптоактивів або пов'язаних послуг — від інтернет-реклами, соціальних мереж, електронних листів і телефонних дзвінків до фізичних заходів, таких як road shows чи спонсорство подій. Навіть загальна реклама бренду може вважатися залученням, якщо вона орієнтована на аудиторію ЄС. Водночас чисто освітні заходи, наприклад тренінги чи конференції, не класифікуються як залучення, якщо вони не спрямовані на просування послуг фірми чи перенаправлення аудиторії до її вебсайту чи платформи. Для оцінки факту залучення компетентним органам рекомендується враховувати всі обставини конкретної справи, а в додатку наведено приклади, такі як використання SEO-стратегій, орієнтованих на ЄС, чи спонсорство місцевих подій.

Висновки:

- **Чітке визначення «залучення» для регулювання:** Фірми з третіх країн повинні уникати будь-яких форм активного просування (включаючи SEO, рекламу чи інфлюенсерів) у ЄС, якщо не хочуть підпадати під вимоги статті 59 MiCA. Рекомендується використовувати геоблокування чи відмову від нових клієнтів із ЄС як запобіжні заходи.
- **Обмеження винятку зворотного залучення:** Фірми можуть пропонувати послуги лише за ініціативи клієнта і тільки в рамках початкового запиту, без подальшого маркетингу. Вони повинні вести детальні записи взаємодії з клієнтами для доказу їхньої ініціативи.
- **Посилений нагляд:** Компетентні органи повинні активно моніторити онлайн-активність фірм, співпрацювати з іншими відомствами та реагувати на скарги, щоб виявляти порушення. Використання маркетингових інструментів і опитувань є практичними кроками для цього.
- **Технологічна нейтральність:** Регулювання охоплює всі засоби залучення, від традиційних до цифрових, що вимагає від фірм ретельно аналізувати свою діяльність у ЄС незалежно від каналу комунікації.

Залучення може здійснюватися як самою фірмою, так і особами, що діють від її імені, наприклад інфлюенсерами чи афілійованими особами, навіть без формального контракту. Наявність винагороди є сильним доказом такого зв'язку, але її відсутність не виключає факту співпраці. З іншого боку, незалежні огляди послуг фірми, зроблені без її відома чи сприяння, не вважаються залученням. Виняток зворотного залучення застосовується лише тоді, коли клієнт сам

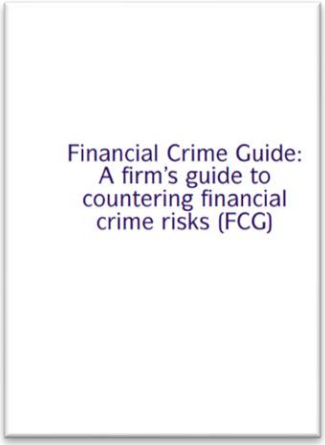
звертається до фірми без будь-якої попередньої ініціативи з її боку, причому це тлумачиться вузько — подальше просування послуг, навіть того ж типу, поза межами початкової транзакції заборонено. Фірми повинні вести облік взаємодії з клієнтами, щоб довести їхню власну ініціативу. Щодо критеріїв "того самого типу" криптоактивів чи послуг, оцінка має бути індивідуальною, враховуючи категорію та ризики, а документ наводить приклади, які не вважаються однаковими, наприклад токени корисності та електронні гроші чи активи з різними технологіями зберігання.

Для запобігання обходу вимог MiCA компетентним органам пропонується низка наглядових практик. Вони включають моніторинг онлайн-активності фірм із третіх країн, наприклад через аналіз їхніх телефонних номерів, адрес чи маркетингових інструментів, орієнтованих на ЄС, а також проведення опитувань споживачів для виявлення фірм, що діють на ринку. Співпраця з іншими органами, такими як поліція чи податкові служби, має допомогти обмінюватися інформацією про діяльність таких фірм, а реагування на скарги клієнтів чи повідомлення викривачів є ще одним важливим інструментом для виявлення порушень. Особлива увага приділяється онлайн-простору, враховуючи, що криптоактиви переважно просуваються через цифрові канали.

Додаток до документа підсилює практичну спрямованість рекомендацій, надаючи невичерпний перелік прикладів ситуацій, коли фірма ймовірно залучає клієнтів із ЄС. Серед них — використання геотаргетованої реклами, вебсайтів із перекладом на офіційні мови ЄС, спонсорство місцевих спортивних подій чи перенаправлення клієнтів через афілійовані структури в ЄС. Ці приклади слугують орієнтиром як для фірм, так і для наглядових органів, допомагаючи уникнути неоднозначностей у тлумаченні.

Загалом документ є комплексним керівництвом, яке поєднує чіткі критерії оцінки залучення з практичними заходами для нагляду, спрямованими на захист споживачів і запобігання регуляторному арбітражу в сфері криптоактивів. Він підкреслює важливість технологічної нейтральності, відповідальності фірм за свою діяльність у ЄС і активної ролі компетентних органів у забезпеченні дотримання MiCA.

Практичний посібник з протидії фінансовим злочинам: аналіз рекомендацій FCA для фінансових установ[2]



Документ є всебічним ресурсом, розробленим Управлінням фінансової поведінки Великої Британії (FCA) для допомоги фінансовим установам у розумінні та протидії ризикам фінансових злочинів. Цей посібник охоплює широкий спектр тем, включаючи відмивання коштів, фінансування тероризму, шахрайство, хабарництво, корупцію, санкції та інсайдерську торгівлю.

У вступі FCG підкреслює важливість впровадження ефективних систем і контролю для виявлення, запобігання та стримування фінансових злочинів. Документ наголошує на необхідності активної участі вищого керівництва у формуванні культури доброчесності та відповідальності в організації. Ризик-орієнтований підхід рекомендується як основа для розробки стратегій протидії фінансовим злочинам, що дозволяє установам адаптувати свої заходи відповідно до специфічних ризиків, з якими вони стикаються.

[2] https://www.handbook.fca.org.uk/handbook/FCG.pdf

Один із ключових аспектів FCG — це акцент на належній перевірці клієнтів (CDD) та посиленій перевірці (EDD) для клієнтів з високим ризиком. Посібник підкреслює важливість постійного моніторингу транзакцій для виявлення підозрілої діяльності, використовуючи як автоматизовані системи, так і ручні процеси. Крім того, FCG надає рекомендації щодо запобігання шахрайству, включаючи впровадження внутрішніх політик, навчання персоналу та обмін інформацією з іншими фінансовими установами.

У розділі, присвяченому захисту даних, FCG наголошує на необхідності впровадження заходів кібербезпеки для захисту конфіденційної інформації клієнтів від несанкціонованого доступу та кібератак. Також посібник охоплює питання дотримання санкційних режимів, підкреслюючи важливість регулярної перевірки санкційних списків та забезпечення відповідності операцій чинним санкціям.

Загалом, FCG служить детальним керівництвом для фінансових установ у розробці та впровадженні ефективних стратегій протидії фінансовим злочинам, забезпечуючи відповідність нормативним вимогам та підтримуючи цілісність фінансової системи.

Висновки:

- Зміцнення системи управління фінансовими злочинами:
  - Необхідно забезпечити активну залученість вищого керівництва до процесів запобігання фінансовим злочинам.
  - Всі фінансові установи мають чітко визначити відповідальних осіб за виконання антикорупційних заходів та заходів, пов'язаних з шахрайством.
- Ризик-орієнтований підхід до перевірки клієнтів (CDD та EDD):
  - Компанії мають впроваджувати адаптивні механізми перевірки клієнтів, базуючись на оцінці ризику.
  - Для високоризикових клієнтів необхідно застосовувати посилену перевірку (EDD) та постійний моніторинг транзакцій.
- Автоматизований моніторинг транзакцій та відповідність санкціям
  - Необхідно використовувати передові технології (зокрема, машинне навчання) для покращення ефективності виявлення підозрілих транзакцій.
  - Важливо забезпечити інтеграцію санкційних списків та миттєву перевірку транзакцій на відповідність міжнародним санкціям.
- Прозорість та ефективний контроль внутрішніх процесів:
  - Внутрішні процедури мають регулярно переглядатися та оновлюватися відповідно до змін у законодавстві та регуляторних вимогах.
  - Організації повинні активно залучати незалежні аудити та проводити внутрішні перевірки на відповідність стандартам фінансової безпеки.

Відкриті технології у швидких платіжних системах: можливості, виклики та стратегічні рішення за даними Світового банку[3]

Документ Світового банку присвячений аналізу використання відкритих цифрових технологій у швидких платіжних системах (FPS) і розглядає ключові аспекти їх впровадження, потенційні переваги, ризики, фінансові наслідки та регуляторні виклики. Він досліджує, яким чином відкриті цифрові платформи можуть бути застосовані в національних і міжнародних системах миттєвих платежів, а також які підходи використовуються різними країнами та фінансовими установами для їхньої інтеграції.

[3] https://fastpayments.worldbank.org/sites/default/files/2025-02/Open%20Source%20FPS_Focus%20Note_Final.pdf

Документ починається з огляду глобального стану використання технологій з відкритим кодом у платіжних системах, наголошуючи на тому, що, хоча такі технології є домінуючим підходом у багатьох секторах IT-індустрії, у сфері FPS їх застосування залишається обмеженим. Єдиним ідентифікованим у дослідженні прикладом використання відкритого коду для основної інфраструктури FPS є ініціатива Mojaloop, яка розроблена для забезпечення фінансової інклюзії у країнах, що розвиваються. У більшості випадків рішення на основі відкритого коду застосовуються для допоміжних або другорядних компонентів платіжних систем, тоді як основні механізми розрахунків і клірингу залишаються закритими.

Далі розглядається концепція відкритих технологій у контексті FPS, пояснюються відмінності між відкритими та закритими технологіями, а також наведена класифікація моделей впровадження таких рішень у швидкі платіжні системи. Виділяються три основні категорії: повністю відкриті системи, пропрієтарні системи з відкритими модулями та повністю закриті рішення. Перший підхід передбачає розробку платіжної інфраструктури з нуля, з відкритим кодом і можливістю вільного модифікування. Другий передбачає використання окремих відкритих компонентів у межах закритої системи, що дозволяє отримати певні переваги відкритого коду без відмови від комерційних механізмів підтримки. Третій підхід – традиційний, із закритим кодом, повністю контрольований комерційним постачальником або центральним банком.

Один із ключових аспектів документа – аналіз переваг і ризиків використання відкритих технологій у FPS. Основні переваги включають зменшення витрат на ліцензування, гнучкість у налаштуванні та можливість використання інноваційного потенціалу спільноти розробників. Відкритий код дає змогу незалежним експертам виявляти вразливості та пропонувати виправлення, що потенційно підвищує рівень безпеки системи. Також використання відкритих рішень може сприяти уникненню залежності від конкретних постачальників (vendor lock-in), що є критичним фактором для операторів FPS у довгостроковій перспективі.

Однак застосування відкритого коду у FPS пов’язане і з низкою ризиків. Ключовий з них – кібербезпека, оскільки відкритий код може зробити систему вразливою для атак, якщо не вжито належних заходів захисту. Відомі випадки, такі як вразливість Log4Shell, показують, що компоненти з відкритим кодом можуть залишатися небезпечними протягом багатьох років, якщо вони не проходять регулярного аудиту та оновлення. Також великою проблемою є необхідність високого рівня технічної експертизи для підтримки та налаштування відкритих рішень, що може компенсувати потенційну економію на ліцензіях. Більше того, міграція з однієї відкритої платформи на іншу або повернення до пропрієтарних рішень може бути складним і дорогим процесом.

Документ також містить детальний аналіз витрат, пов’язаних із застосуванням технологій з відкритим кодом протягом усього життєвого циклу FPS. Основна увага приділяється концепції загальної вартості володіння (Total Cost of Ownership, TCO), що включає не лише первинні витрати на розгортання системи, а й довгострокові витрати на підтримку, оновлення, безпеку та можливі майбутні міграції. Хоча такі рішення можуть мати низьку початкову вартість, подальші витрати на підтримку, навчання персоналу та безпеку можуть виявитися вищими за аналогічні витрати у пропрієтарних рішеннях.

Окремо розглядається питання регуляторного середовища та відповідності технологій з відкритим кодом міжнародним і національним стандартам. Використання відкритого коду не звільняє провайдерів FPS від необхідності дотримання вимог щодо кібербезпеки, збереження конфіденційності даних та відповідності стандартам обміну фінансовими повідомленнями, таким як ISO 20022. Крім того, різні ліцензії для відкритого коду можуть містити обмеження, які впливають на можливість комерційного використання або модифікації коду, що також має враховуватися при ухваленні рішень.

У завершальній частині документа сформульовані ключові висновки та рекомендації для операторів FPS і регуляторів. Світовий банк підкреслює, що ухвалення рішення про використання технологій з відкритим кодом у FPS має базуватися на ретельному аналізі ризиків, технологічної зрілості організації, доступності необхідних технічних ресурсів та довгостроковій стратегії розвитку платіжної інфраструктури. Операторам FPS рекомендується оцінювати як поточні, так і майбутні потреби у безпеці, інтеграції та масштабуванні системи, а також активно взаємодіяти зі спільнотою розробників відкритих технологій для забезпечення стабільності та безперервної підтримки системи.

Світовий банк визнає, що рішення на основі відкритого коду мають значний потенціал для розвитку FPS, особливо у контексті підвищення фінансової інклюзії, розширення конкуренції на ринку платіжних послуг та зниження витрат. Проте, щоб уникнути ризиків, необхідно впроваджувати комплексні заходи контролю та управління безпекою, а також забезпечити належну оцінку загальної вартості володіння системою.

Висновки:

- **Відкритий код у FPS – це тренд, що розвивається, але його використання в ключових фінансових системах ще обмежене.** Важливим прикладом є Mojaloop, але більшість FPS поки що використовують відкритий код тільки для допоміжних компонентів.
- **Оператори та регулятори FPS повинні ретельно оцінювати кібербезпеку та ризики рішень з відкритим кодом.** Відкритий код не завжди означає безпечність: наявні вразливості можуть залишатися невиправленими роками, як у випадку Log4Shell.
- **Попри зменшення витрат на ліцензування, загальна вартість впровадження відкритого коду FPS може бути високою.** Витрати на адаптацію, підтримку, оновлення та безпеку часто перевищують початкову економію.
- **Для успішного використання відкритого коду у FPS, організація повинна мати достатню технічну зрілість.** Без відповідних команд підтримки, тестування та аудиту впровадження відкритого коду може стати значним ризиком для стабільності FPS.

Європейська прокуратура 2024: масштаб фінансових злочинів у ЄС та виклики для антикорупційної системи[4]

Європейська прокуратура (EPPO) у 2024 році зіткнулася з безпрецедентним зростанням навантаження, що свідчить про значне поширення фінансових злочинів, пов'язаних із бюджетом Європейського Союзу. У своїй діяльності EPPO зосередила увагу на розслідуванні шахрайства з фондами ЄС та транскордонних схем ухилення від сплати ПДВ, що часто мають

[4] https://media.licdn.com/dms/document/media/v2/D561FAQFXU1JZ_JBJ5A/feedshare-document-pdf-analyzed/B56ZVcjOJzGQAc-/0/1741014622348?e=1742428800&v=beta&t=dXur5s8nalZCdIitqA4Q0IqyqZBiS14mq6D8pynrDkI

організований характер. Загальний обсяг збитків, зафіксований у відкритих справах, перевищив 24,8 мільярда євро, що підтверджує масштаби економічних злочинів проти бюджету ЄС. Значну частину цих втрат – понад 53% – становить шахрайство з ПДВ, яке дедалі більше приваблює організовані злочинні угруповання. Систематичне використання транскордонних схем свідчить про слабкі місця у правоохоронній координації країн-членів, що дозволяє злочинцям діяти на міжнародному рівні.

Зростання кількості розслідувань у 2024 році супроводжувалося значним збільшенням обсягів повідомлень про підозрілі випадки фінансових злочинів. Загальна кількість отриманих повідомлень досягла 6 547, що на 56% більше, ніж у 2023 році. Найбільший приріст відбувся за рахунок звернень від приватних осіб, що свідчить про посилення громадського контролю та підвищення обізнаності щодо роботи EPPO. Водночас лише 113 повідомлень надійшло від установ і агентств ЄС, що вказує на критично низький рівень внутрішнього контролю та виявлення фінансових порушень з боку європейських інституцій. Це є серйозним викликом для антикорупційної політики ЄС, оскільки демонструє пасивність європейських органів у боротьбі з шахрайством.

У відповідь на ці виклики Європейська прокуратура продовжила активне використання кримінальних переслідувань та замороження активів. У 2024 році було подано 205 обвинувальних актів, що на 47% більше, ніж у попередньому році. Загальна сума заморожених активів склала 849 мільйонів євро, хоча цей показник залишається відносно низьким у порівнянні з оціненими збитками. Суди винесли 102 обвинувальні вироки, що призвело до засудження 196 осіб. Попри це, рівень остаточного повернення незаконно привласнених коштів все ще залишається недостатнім, що вимагає вдосконалення механізмів конфіскації та правозастосування.

EPPO також приділила увагу аналізу типологій злочинів, що дозволило краще ідентифікувати основні загрози та закономірності. Найбільш поширеними схемами шахрайства стали зловживання у сфері непроцедурних витрат, шахрайство у державних закупівлях, корупція, маніпуляції з податковими зобов'язаннями, відмивання коштів та використання фіктивних компаній для здійснення фінансових махінацій. Це свідчить про те, що зловмисники дедалі частіше застосовують складні схеми для уникнення викриття, використовуючи прогалини у регулюванні та недостатню координацію між країнами-членами.

Важливим викликом залишається недостатня ресурсна забезпеченість EPPO, що ускладнює ефективне проведення розслідувань та судових переслідувань. Незважаючи на збільшення кількості розглянутих справ, у багатьох країнах, що беруть участь у діяльності EPPO, все ще бракує спеціалізованих слідчих та аналітиків. Це особливо критично, враховуючи зростання рівня складності фінансових схем шахрайства, які вимагають високого рівня експертизи у сфері цифрових фінансів, криптовалютних операцій та міжнародних фінансових потоків.

У своєму звіті Європейська прокуратура також наголошує на необхідності реформування загальної антикорупційної та антишахрайської архітектури ЄС. Зокрема, ставиться під сумнів ефективність роботи національних податкових і правоохоронних органів у розкритті масштабних схем ухилення від сплати податків. Відзначається, що, попри наявність стратегій боротьби з шахрайством, організовані злочинні угруповання змогли розвинути схеми ПДВ-шахрайства до рівня промислового масштабу, що вимагає радикальних змін у підходах до розслідувань та судового переслідування.

Загалом, звіт EPPO за 2024 рік демонструє суттєве зростання навантаження на орган, що свідчить про велику кількість фінансових злочинів у Європейському Союзі. Однак недостатня

координація між країнами-членами, обмежена кількість спеціалізованих ресурсів та низький рівень повідомлень про злочини з боку європейських інституцій суттєво ускладнюють боротьбу з економічною злочинністю. Для досягнення реального прогресу необхідні кардинальні зміни в підходах до розслідування фінансових злочинів, а також розширення можливостей Європейської прокуратури у залученні спеціалізованих слідчих, фінансових аналітиків та технічних експертів.

Загалом документ показує, що стейблкоїни вже стали важливою частиною глобальної фінансової екосистеми, і їхня роль лише зростатиме в найближчі роки. Їх використання у міжнародних платежах, валютних операціях та фінансовій інфраструктурі може трансформувати традиційні підходи до розрахунків і ліквідності, забезпечуючи швидкість, доступність та прозорість. Проте успіх цього процесу залежить від розвитку регуляторної бази, довіри користувачів та подальшого вдосконалення технологічних механізмів, що підтримують стейблкоїни.

Висновки:

- **Організовані злочинні угруповання активно використовують схеми ПДВ-шахрайства,** що призвело до збитків у 13,15 мільярда євро. Рекомендація: необхідне посилення міждержавної координації та аналітичних можливостей EPPO для виявлення системних схем шахрайства.
- **Рівень повідомлень від установ ЄС є вкрай низьким,** що свідчить про недостатню внутрішню систему контролю та виявлення фінансових порушень. Рекомендація: запровадити жорсткіші вимоги до звітності та перевірки фінансових потоків.
- **Заморожені активи склали лише 3,4% від загальної суми збитків,** що вказує на необхідність вдосконалення механізмів конфіскації активів та повернення незаконно отриманих коштів.
- **Попит на діяльність EPPO значно зріс,** але організація не має достатньо спеціалізованих слідчих та прокурорів у багатьох країнах-учасницях. Рекомендація: збільшити фінансування EPPO та забезпечити держави-члени необхідною кількістю спеціалізованих слідчих.

Регулювання

Регулювання ринку ARTs: Оцінка змін Європейської Комісії до технічних стандартів MiCAR від EBA[5]

Документ містить офіційну позицію Європейського банківського управління (EBA) щодо запропонованих Європейською Комісією змін до Регуляторних технічних стандартів (RTS), які визначають вимоги до інформації, що має бути включена до заявок на отримання дозволу для випуску та допуску до торгів токенів, прив'язаних до активів (ARTs) відповідно до Регламенту про ринки криптоактивів (MiCAR).

EBA розробила ці стандарти у співпраці з ESMA, ґрунтуючись на наявній практиці ліцензування у фінансовому секторі. Остаточний варіант RTS був переданий до Європейської Комісії 6 травня 2024 року. Однак у січні 2025 року ЄК повідомила EBA про свій намір внести поправки, які частково відхиляють початковий варіант RTS. У своїй думці EBA визнає, що запропоновані зміни є суттєвими, але юридично обґрунтованими, оскільки вони спираються на більш вузьке

[5] https://www.bis.org/cpmi/publ/brief7.pdf

тлумачення MiCAR. При цьому EBA наполягає на необхідності майбутніх змін у MiCAR для забезпечення належного регулювання ключових аспектів діяльності емітентів ARTs.

Однією з основних змін, запропонованих ЄК, є виключення з RTS будь-яких посилань на White Paper (стаття 19 MiCAR) у вимогах до програми діяльності емітента ARTs. Це зроблено для уникнення дублювання інформації та чіткішого розмежування вимог. EBA погоджується з цією зміною, оскільки програма діяльності є окремим документом, що має містити специфічну інформацію про бізнес-модель емітента, яка не обов'язково відображена у White Paper.

Ще одна значна зміна стосується внутрішнього управління емітентами ARTs. У первинному варіанті RTS EBA включила вимогу щодо наявності у емітентів політик запобігання ринковим зловживанням і захисту викривачів (whistleblowing). Однак ЄК виключила цю вимогу, аргументуючи тим, що MiCAR прямо не передбачає таких зобов'язань. EBA погоджується з цим обмеженням, але наполягає, що політика боротьби з ринковими зловживаннями є критично важливою для забезпечення прозорості ринку. Відтак EBA рекомендує переглянути MiCAR у майбутньому, щоб включити ці вимоги до загального регуляторного підходу до ARTs.

Окремим важливим аспектом обговорюваних змін є питання технологічного забезпечення операцій з ARTs. У початковому варіанті RTS EBA вимагала від емітентів ARTs проведення незалежного аудиту технологічної та безпекової відповідності блокчейн-мережі (DLT), де здійснюється випуск, зберігання та передача ARTs. ЄК виключила цю вимогу, замінивши її поданням технічного звіту без обов'язкового залучення незалежного аудитора. EBA визнає, що ця зміна ґрунтується на вузькому тлумаченні повноважень, наданих MiCAR, однак наголошує, що без незалежного аудиту оцінка ризиків буде менш ефективною, що може призвести до появи прогалин у регуляторному нагляді за критичною інфраструктурою ринку криптоактивів. Відтак EBA рекомендує майбутнє розширення MiCAR для запровадження вимоги незалежного аудиту, що підвищить рівень довіри до ARTs.

Ще одним аспектом, який зазнав змін, є критерії оцінки доброї репутації членів керівних органів емітентів ARTs. ЄК звузила перелік інформації, яку емітенти мають подавати для підтвердження репутаційної відповідності своїх керівників, залишивши лише ті категорії, що прямо зазначені в MiCAR. Це включає перевірку на відсутність судимостей або санкцій за порушення у сферах комерційного права, банкрутства, фінансових послуг, боротьби з ВК/ФТ, шахрайства та професійної відповідальності. EBA визнає, що ця зміна відповідає букві MiCAR, але водночас підкреслює, що поняття «доброї репутації» є ширшим і має застосовуватися до всього фінансового сектору. Відтак EBA рекомендує змінити MiCAR у майбутньому, щоб розширити критерії оцінки репутації керівників ARTs та узгодити їх із стандартами, що застосовуються до інших фінансових установ.

Окрім цих суттєвих змін, ЄК внесла низку редакційних правок до RTS, які не впливають на змістовну частину документа, але покращують його читабельність. Серед них – видалення визначень у статті 1 RTS, зміна порядку пунктів для поліпшення структури та уточнення посилань на положення MiCAR. Також вилучено положення щодо максимального періоду зберігання персональних даних, оскільки це могло б вплинути на інформаційні системи для перевірки відповідності керівників фінансових установ.

Загалом EBA визнає більшість запропонованих ЄК змін юридично обґрунтованими, оскільки вони базуються на більш вузькому тлумаченні MiCAR. Однак, з погляду регуляторної ефективності та довгострокової стабільності ринку ARTs, EBA вважає, що низка питань має бути врегульована у подальших змінах до MiCAR. Зокрема, EBA рекомендує розширити вимоги щодо внутрішнього управління, запровадити обов'язковий незалежний аудит DLT та переглянути критерії оцінки доброї репутації керівників емітентів ARTs. Водночас EBA наголошує на важливості підтримки високих стандартів прозорості та захисту інвесторів, що є ключовими принципами регулювання ринку криптоактивів у ЄС.

Висновки:

- **Поправки ЄК до RTS обмежують обсяг поданої інформації емітентами ARTs,** виключаючи вимоги щодо ринкових зловживань, політики викривачів та незалежного аудиту блокчейн-мережі.
- **EBA визнає зміни юридично обґрунтованими, але рекомендує розширити регулювання MiCAR** у майбутньому для кращого управління ризиками у сфері криптоактивів.
- **Оцінка доброї репутації членів керівного органу ARTs залишилася обмеженою,** що може створити ризики для довіри до сектору; EBA рекомендує уніфікацію критеріїв з іншими фінансовими установами.
- **Незалежний аудит DLT-платформ залишився добровільним, що може підвищити технологічні ризики;** EBA наполягає на необхідності регуляторного посилення цієї вимоги.

Звіти окремих інституцій та експертів

Тіньові IT-спеціалісти: розкриття північнокорейської кіберстратегії [6]

Документ, підготовлений Insikt Group від Recorded Future і опублікований 13 лютого 2025 року, є детальним дослідженням складної стратегії, яку Північна Корея застосовує для отримання фінансових ресурсів через шахрайське працевлаштування IT-спеціалістів у міжнародних компаніях. У звіті розкривається, як режим використовує зростання популярності віддаленої роботи для проникнення в організації під фальшивими іменами, що дозволяє не лише генерувати доходи в обхід міжнародних санкцій, але й створювати значні кіберзагрози, включаючи крадіжку даних, шахрайство та кібершпигунство. Автори акцентують увагу на тому, що ці операції є частиною ширшої кіберстратегії, яка підтримує фінансові потреби ізольованої держави, зокрема її військові програми, і водночас становить небезпеку для глобальної фінансової системи та національної безпеки.

Звіт розпочинається з резюме, яке описує, як північнокорейські IT-працівники проникають у компанії, використовуючи фальшиві ідентичності для отримання віддалених посад. Ця діяльність не обмежується лише фінансовими махінаціями: такі працівники часто діють як інсайдери, крадуть конфіденційну інформацію, впроваджують бекдори або сприяють масштабнішим кібероперація̈м. Особливу увагу приділено кампанії "Contagious Interview", яку пов'язують із групою PurpleBravo (раніше TAG-120), що зосереджується на розробниках програмного забезпечення в криптовалютній індустрії. Ця кампанія використовує шкідливе

[6] https://www.recordedfuture.com/research/inside-the-scam-north-koreas-it-worker-threat

програмне забезпечення, таке як BeaverTail (інфокрад), InvisibleFerret (бекдор) та OtterCookie (новий бекдор, виявлений у грудні 2024 року), для збору чутливих даних і встановлення контролю над системами жертв. Окрім PurpleBravo, згадується діяльність TAG-121 — іншої групи, яка управляє мережею підставних компаній у Китаї, що імітують легітимні IT-фірми з різних країн, копіюючи їхні вебсайти для маскування своєї діяльності.

Далі документ переходить до передумов, які пояснюють контекст цієї загрози. Зокрема, згадується обвинувачення Міністерства юстиції США від 23 січня 2025 року проти двох північнокорейських громадян і трьох їхніх пособників, які протягом шести років організували схему віддаленої роботи для 64 американських компаній, отримавши щонайменше 866 255 доларів через китайський банк. Ця схема є прикладом того, як Північна Корея адаптувала свої незаконні методи до сучасних реалій. У зв'язку з посиленням санкцій і обмеженням традиційних джерел доходу, таких як контрабанда, режим переключився на кіберзлочини та шахрайське працевлаштування. Зростання віддаленої роботи з 2020 року відкрило нові можливості для розгортання кваліфікованих IT-спеціалістів, які проникають у компанії під вигаданими іменами, підтримуючи таким чином економіку режиму та його військові амбіції.

Кампанія "Contagious Interview", вперше задокументована в листопаді 2023 року, використовує фальшиві вакансії для зараження розробників шкідливим ПЗ. Один із прикладів — випадок із фальшивим рекрутером "Javier Fiesco" від компанії AgencyHill99, який пропонував розробнику завантажити пробне завдання, що містило шкідливу функцію BeaverTail. Дослідження виявило численні фальшиві профілі та вакансії на платформах, таких як LinkedIn, Upwork, Telegram, GitHub і DoraHacks. PurpleBravo активно використовує інфраструктуру, включаючи сервери на хостингах Tier[.]Net, Majestic Hosting і Kaopu Cloud HK, а також VPN-сервіс Astrill для управління командно-контрольними серверами. Жертви цієї групи розташовані щонайменше в шести країнах, включаючи ОАЕ, Коста-Рику, Індію, В'єтнам, Туреччину та Південну Корею, що свідчить про глобальний масштаб загрози.

Технічний аналіз шкідливого програмного забезпечення розкриває його функціонал: BeaverTail краде дані криптовалютних гаманців і браузерів, InvisibleFerret забезпечує віддалений доступ через зворотні шелли, кейлогінг і моніторинг дій користувача, а OtterCookie виконує команди з C2-серверів і викрадає чутливу інформацію, використовуючи регулярні вирази для пошуку цінних файлів. Звіт включає конкретні приклади інфраструктури, такі як IP-адреси серверів і домени, а також аналіз мережевого трафіку, який підтверджує використання Astrill VPN для приховування діяльності. Окремо виділено випадки атак на компанії в криптовалютному секторі, наприклад, на фірму з маркет-мейкінгу в ОАЕ та розробника ПЗ в Індії.

Висновки:

- **Впровадити сувору верифікацію найму:** Компаніям необхідно вимагати відео-співбесіди, нотаріально засвідчені документи та перевіряти IP-адреси віддалених працівників для запобігання проникненню північнокорейських операторів.
- **Посилити кіберзахист:** Встановити системи моніторингу інсайдерських загроз, обмежити доступ до даних і виявляти підозрілі VPN-з'єднання, зокрема через Astrill, для захисту від шкідливого ПЗ типу BeaverTail чи InvisibleFerret.
- **Проводити навчання персоналу:** HR та IT-команди повинні пройти тренінги з розпізнавання фальшивих профілів і вакансій, щоб блокувати спроби шахрайського працевлаштування на ранніх етапах.
- **Міжнародна співпраця:** Урядам і організаціям слід розширити обмін розвідданими про діяльність груп на кшталт PurpleBravo і TAG-121, щоб ефективно протидіяти еволюції північнокорейських кіберзагроз.

Наслідки цієї загрози є багатогранними: компанії, які наймають таких працівників, можуть порушувати санкції, що призводить до юридичних і фінансових ризиків, а також стають жертвами інсайдерських атак, які загрожують їхній інтелектуальній власності та операційній стабільності. Північнокорейські операції становлять ширшу небезпеку для глобальних IT-ланцюгів постачання та фінансової системи. Для протидії автори рекомендують організаціям впроваджувати сувору верифікацію особи під час найму, включаючи відеоспівбесіди та нотаріально засвідчені документи, а також технічні заходи, такі як обмеження доступу до даних, моніторинг аномалій і виявлення підозрілих VPN-з'єднань. Навчання персоналу HR та IT-відділів визнано критично важливим для запобігання проникненню таких акторів. Звіт завершується закликом до співпраці між бізнесом, урядами та організаціями з кібербезпеки для закриття прогалин, які Північна Корея використовує в умовах віддаленої роботи, підкреслюючи, що ця загроза продовжуватиме еволюціонувати.

Майбутнє DeFi: Як регулювання, токенізовані активи та інноваційні стейблкоїни змінюють фінансовий ландшафт [7]

Документ представляє комплексний аналіз сучасних змін та перспектив розвитку децентралізованих фінансів (DeFi), приділяючи особливу увагу регуляторним аспектам, інтеграції реальних активів у блокчейн-екосистему (RWAs) та інноваціям у сфері стейблкоїнів. Основний посил дослідження полягає у тому, що DeFi переживає новий етап еволюції, що передбачає зміщення фокусу з чисто криптовалютних рішень на фінансові механізми, які поєднують переваги блокчейну та традиційних активів.

У першій частині документа розглядаються найважливіші зміни на ринку криптовалют та децентралізованих фінансів. Зокрема, значну увагу приділено прийняттю законодавства про стейблкоїни, що суттєво змінює правила гри для компаній, які працюють у цьому секторі. Це не лише накладає нові вимоги щодо відповідності нормам, але й відкриває можливості для масового використання стейблкоїнів у міжнародних розрахунках. Частка стейблкоїнів у блокчейн-транзакціях вже перевищує 50%, а їхнє використання в окремих країнах (наприклад, Туреччині та Аргентині) досягає 4–30% ВВП. При цьому великі фінансові гравці, такі як Stripe, PayPal та BlackRock, активно інвестують у цей сегмент, що свідчить про його стратегічну важливість.

Окрім цього, у звіті наголошується на очікуваному пом'якшенні регулювання торгівлі безстроковими ф'ючерсами. Децентралізовані біржі деривативів (PerpDEXs), які довгий час стикалися з обмеженнями через відсутність чітких регуляторних рамок, можуть отримати нові можливості для зростання. Особливо цікавими у цьому контексті є ініціативи зі зміни підходу до регулювання криптовалют у США, де роль головного регулятора може перейти від SEC до більш лояльної CFTC.

Також автори досліджують зростаючий інтерес до токенізованих реальних активів (RWAs). Приватне кредитування, державні облігації, дорогоцінні метали та інші активи поступово інтегруються у DeFi-простір, надаючи користувачам можливість отримувати стабільні прибутки.

[7] https://media.licdn.com/dms/document/media/v2/D4D1FAQEQzrdk0sFKzg/feedshare-document-pdf-analyzed/B4DZVRiU6wHIAY-/0/1740829741850?e=1742428800&v=beta&t=j0SstrpfVu55kx6-dvlgMbxmKMLsBaTVd7yS752iE4Q

За останній рік обсяг токенізованих RWAs зріс на 85%, а загальний ринок оцінюється у понад 15 мільярдів доларів. Особливо цікавим є використання RWAs у створенні прибуткових стейблкоїнів, які забезпечені капіталом, що приносить дохід (наприклад, державними облігаціями США).

Окремо розглядається посилення ролі регульованих фінансових установ у криптовалютному секторі. Такі компанії, як JPMorgan, BlackRock та State Street, активно впроваджують блокчейн-рішення для платежів, ліквідності та управління активами. JPMorgan, наприклад, розширює використання цифрового долара JPM Coin та розробляє рішення для автоматизованих розрахунків у мультивалютному середовищі. Паралельно BlackRock запустив перший токенізований фонд державних облігацій BUIDL, що стало значним кроком до масової адаптації RWAs. У свою чергу, компанія Securitize, яка спеціалізується на токенізації активів, залучила мільйони доларів інвестицій та активно співпрацює з BlackRock для розширення можливостей регульованої торгівлі токенізованими цінними паперами.

Друга частина документа присвячена викликам та можливостям у розвитку DeFi. Зокрема, розглядається проблема дефолтів у сфері приватного кредитування, що є ключовим ризиком для DeFi-протоколів, які працюють із RWAs. Автори аналізують приклади таких платформ, як Maple Finance, Goldfinch та Centrifuge, які намагаються вирішити питання ліквідності та управління ризиками за допомогою нових механізмів забезпечення позик. Окремий розділ присвячений перспективам появи прибуткових стейблкоїнів, що дозволяють користувачам отримувати дохід завдяки алгоритмічному управлінню активами або вкладенню у прибуткові RWAs.

Документ також наголошує на взаємопідсилюючій ролі RWAs та DeFi. Токенізовані активи можуть підвищити стійкість децентралізованих фінансових платформ, знижуючи їхню залежність від волатильності ринку криптовалют. Дедалі більше DeFi-проєктів починають використовувати стейблкоїни та інші токенізовані RWAs у якості застави, що підвищує ліквідність та капітальну ефективність платформи.

У заключній частині звіту аналізуються нові перспективні напрями розвитку DeFi. Зокрема, розглядається концепція ончейн-валютного обміну, який може значно знизити вартість конвертації валют у міжнародних розрахунках. Децентралізовані протоколи, такі як Uniswap, вже сьогодні дозволяють виконувати операції з меншими комісіями та більшою швидкістю, ніж традиційні банки. Ще одним важливим трендом є створення кросбордерних платіжних рішень, які використовують стейблкоїни для оптимізації міжнародних переказів. Великі технологічні компанії, такі як Stripe та Ripple, активно розробляють відповідні платформи, що можуть стати серйозною конкуренцією для традиційних SWIFT-платежів.

Висновки:

- **Стейблкоїни стають основою міжнародних фінансів –** їхня частка у блокчейн-транзакціях перевищує 50%, а нове регулювання у США може прискорити їхнє впровадження у глобальні розрахунки.
- **Токенізація реальних активів (RWAs) змінює DeFi –** обсяг ринку RWAs перевищив $15 млрд, а до 2030 року може зрости до $16 трлн, забезпечуючи стабільні прибутки та покращуючи ліквідність DeFi.
- **Фінансові гіганти входять у блокчейн –** JPMorgan, BlackRock і Stripe активно впроваджують цифрові активи, що сприяє злиттю традиційних і децентралізованих фінансів.
- **Прибуткові стейблкоїни – новий етап DeFi –** використання RWAs та алгоритмічного управління ліквідністю дозволяє створювати стейблкоїни, які не лише зберігають вартість, але й приносять дохід.

Останній важливий напрямок – це поява багатопулових агрегаторів стейблкоїнів. Такі рішення дозволяють оптимізувати використання ліквідності у DeFi-секторі, об'єднуючи активи з різних пулів у єдину систему. Це дозволяє не лише підвищити ефективність роботи стейблкоїнів, а й значно покращити користувацький досвід, зменшуючи ризики втрати ліквідності у випадку ринкових потрясінь.

Загальний висновок звіту свідчить про те, що DeFi переживає нову хвилю трансформації, де головний фокус зміщується з криптовалютних експериментів на інтеграцію реальних активів та побудову регульованої фінансової інфраструктури. Це відкриває значні можливості для традиційних фінансових інституцій, які прагнуть увійти у криптовалютний простір, а також для нових гравців, що шукають стійкі бізнес-моделі в умовах зміни регуляторного середовища.

Інші новини

Тіньові ставки: Життя і спадщина кіпріотського гемблінг-короля [8]

Розслідування від OCCRP під назвою, опубліковане 13 лютого 2025 року, занурює читача в історію Халіля Фалялї, турецького кіпріотського бізнесмена, відомого своїм екстравагантним стилем життя та зв'язками з політичною елітою, який був застрелений у лютому 2022 року на сільській дорозі Північного Кіпру. Напад стався, коли його автомобіль обстріляли автоматичною зброєю, убивши водія на місці, а сам Фалялї, хоч і вижив спочатку, помер у лікарні через годину від численних поранень. Ця подія сколихнула турецьку частину острова, де він був відомою постаттю, часто фотографувався з високопосадовцями та відкрито демонстрував багатство через соціальні мережі. Однак за фасадом успішного готельєра та члена правлячої Партії національної єдності (UBP) ховалася, за даними турецьких прокурорів та свідчень його колишнього фінансового директора Джеміля Онала, величезна нелегальна імперія онлайн-гемблінгу, яка діяла в десятках країн і приносила колосальні прибутки.

Розслідування розкриває, що Фалялї, керував організацією, яка щомісяця генерувала щонайменше 80 мільйонів доларів – цифра, яку журналісти не змогли незалежно підтвердити, але яку експерти вважають правдоподібною для подібних мереж. Онал стверджує, що особисто організовував "спонсорські" виплати на суму 15 мільйонів доларів щомісяця чиновникам у Туреччині та на Північному Кіпрі, часто готівкою або через золото й обмінники валюти, щоб уникнути відстеження. Ці зв'язки з владою, зокрема з правлячою Партією справедливості та розвитку (AKP) у Туреччині та UBP, допомагали уникати розслідувань. Водночас журналісти виявили нерухомість у Дубаї вартістю понад 60 мільйонів доларів, що належить вдові Фалялї, Озге Ташкер Фалялї, яку Онал назвав новим осередком діяльності організації після його смерті. Турецькі прокурори стверджують, що мережа завербувала тисячі людей – студентів, пенсіонерів, домогосподарок – для створення банківських, кредитних, криптовалютних і платіжних рахунків, які слугували "мулами" для переміщення доходів від гемблінгу. Згідно з звітом турецького Мінфіну 2022 року, лише частина криптогаманців мережі отримала понад 1,4 мільярда доларів з 2018 року.

Легальний фасад операції забезпечувала компанія Larsen Technologies Ltd., зареєстрована в 2013 році на Північному Кіпрі, яка отримала ліцензію на азартні ігри в 2017 році та управляла

[8] https://www.occrp.org/en/investigation/inside-the-global-online-betting-empire-of-a-slain-turkish-cypriot-businessman

брендом BetCyp. Однак Онал пояснює, що це була лише ширма для прикриття нелегальних сайтів, таких як BeteBet, які пропонували живі казино, слоти та спортивні ставки, залучаючи гравців агресивною рекламою та бонусами. Ці сайти, часто ліцензовані в Кюрасао, блокувалися в країнах на кшталт Туреччини чи Латвії, але швидко замінювалися новими доменами, купленими через сервіси на кшталт GoDaddy. Мережа використовувала складну систему "мульних рахунків", керовану через пірамідальну структуру: "гаранти" контролювали групи власників рахунків, отримуючи 10% комісії, а кошти переміщалися через тисячі транзакцій і переводилися в криптовалюту чи готівку. Один працівник Larsen, заарештований у 2020 році, зняв понад 3 мільйони доларів із 376 рахунків за два місяці через банкомати.

Географічно операція охоплювала численні країни: команди діяли в Мальті, Білорусі, Північній Македонії, а після смерті Фалялї управління перемістилося до ОАЕ. У Білорусі казино Н у Мінську, що належить партнеру Фалялї Мустафі Егемену Шенеру, стало центром збору готівки з європейських ринків, таких як Німеччина чи Польща, а також обробки платежів. Готівка звідти переправлялася до Дубаю або контрабандою через аеропорт Ларнаки до Північного Кіпру за сприяння корумпованих митників і високопосадовців, які брали хабарі – наприклад, 5000 євро за мільйон перевезеної готівки. Північний Кіпр, не визнаний міжнародно (крім Туреччини), із слабким регулюванням і банками, що не відповідають стандартам боротьби з відмиванням грошей, став ідеальним притулком для таких операцій, особливо після заборони казино в Туреччині в 1990-х.

Після вбивства Фалялї турецькі прокурори в 2024 році висунули звинувачення проти 240 осіб, включно з Озге Ташкер Фалялї, якій загрожує понад 50 років ув'язнення. Проте Онал вважає це "попередженням" від уряду, щоб мережа продовжувала платити хабарі, а не справжньою спробою її знищити. Озге залишається на свободі, з'являючись на публічних заходах на Північному Кіпрі, зокрема поруч із лідером регіону на похороні в лютому 2025 року, а операція, за його словами, тепер керується з Дубаю, де легко відкривати рахунки та компанії. Деякі криптогаманці, виявлені в 2022 році, досі активні, а сайти, як BeteBet, продовжують оновлювати домени. Статус Фалялї за життя не постраждав від підозр: США звинуватили його в відмиванні грошей у 2015 році, але зняли обвинувачення після смерті, а на його похороні в 2022 році були присутні високопосадовці, а труну накрили прапорами Туреччини та Північного Кіпру.

Розслідування підкреслює системні проблеми: корупція, слабке регулювання в таких регіонах, як Північний Кіпр чи Білорусь, і використання сучасних технологій для приховування злочинів. Воно базується на 20 годинах інтерв'ю з Оналом, даних прокурорів, аналізі блокчейну та витоках про нерухомість, хоча багато тверджень Онала не підкріплені документами. Стаття створена за участю 14 медіа-партнерів із різних країн і є частиною ширшої роботи OCCRP із викриття організованої злочинності.

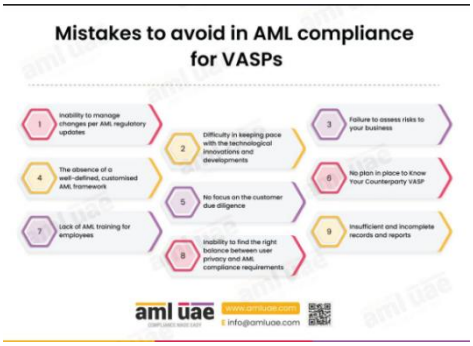
Для загального розвитку

Проблеми антилегалізаційного (AML) комплаєнсу для постачальників віртуальних активів (VASPs) [9]

Інфографічне зображення від компанії AML UAE, має на меті привернути увагу до проблем антилегалізаційного (AML) комплаєнсу для постачальників віртуальних активів (VASPs) у контексті Об'єднаних Арабських Еміратів (ОАЕ). Пост, опублікований Патріком Шахом (Patrick Shah), звертається наголошує на критичній важливості дотримання правил AML для бізнесів, що працюють із віртуальними активами, такими як криптовалюти, підкреслюючи, що недотримання цих норм може поставити компанії в зону серйозного ризику. У повідомленні

[9] https://amluae.com/a-guide-to-avoiding-common-mistakes-in-aml-compliance-for-vasps/

зазначається, що для забезпечення безпечного бізнес-середовища необхідно ретельно вивчити виклики, з якими стикаються VASPs у OAE, і вжити відповідних заходів для їх подолання.



Інфографіка візуально представляє дев'ять ключових помилок, які можуть суттєво підірвати ефективність AML-стратегій. У ній зазначається, що нездатність управляти оновленнями AML політики та регуляторними змінами може призвести до невідповідності сучасним вимогам, а труднощі з адаптацією до технологічних інновацій і пов'язаних із ними ризиків ускладнюють захист від нових загроз у сфері віртуальних активів. Також підкреслюється неспроможність оцінювати ризики, специфічні для бізнесу VASP, що створює вразливості в системі комплаєнсу, та відсутність чітко визначених, індивідуалізованих AML-методологій, що ускладнює створення ефективної програми протидії відмиванню грошей. Недостатня увага до належної перевірки клієнтів підвищує ризик співпраці з ненадійними контрагентами, а відсутність плану дій на випадок критичних ситуацій може призвести до хаосу в управлінні ризиками.

Брак AML-навчання для працівників знижує їхню здатність виявляти підозрілі операції, нездатність знайти баланс між захистом приватності користувачів і вимогами AML-комплаєнсу може спричинити конфлікти з законодавством або незадоволення клієнтів, а недостатнє ведення записів і звітності ускладнює аудит і перевірку відповідності регуляторним стандартам. Загалом інфографіка спрямована на підвищення обізнаності VASPs про критичні помилки в AML-комплаєнсі, пропонуючи практичні рішення через блог компанії та акцентуючи на необхідності активних дій для забезпечення відповідності нормам і захисту бізнесу від фінансових злочинів, таких як відмивання грошей.

Вбудовані фінансові технології: Новий горизонт конкурентних переваг для B2B [10]

Стаття, опублікована PYMNTS 4 березня 2025 року, присвячена зростанню вбудованих фінансових технологій (embedded FinTech) як ключового інструменту для бізнесів у сегменті B2B. Автор спирається на інтерв'ю з Джастіном Дауні, віцепрезидентом із продуктів компанії Maverick, щоб розкрити, як ці технології трансформують бізнес-моделі, створюють нові джерела доходу та підвищують конкурентоспроможність компаній у різних галузях. Стаття констатує, що вбудовані фінансові технології стають "наступною великою річчю" для B2B, дозволяючи інтегрувати фінансові послуги, такі як платежі, кредитування чи страхування, безпосередньо в нефінансові платформи, щоб бізнеси могли пропонувати ці послуги в межах своїх екосистем без звернення клієнтів до окремих фінансових установ. Дауні зазначає, що спостерігається явне зростання кількості B2B-платформ, які прагнуть додати додаткові послуги до своїх продуктів, охоплюючи широкий спектр індустрій — від електронної комерції та роздрібної торгівлі до охорони здоров'я й освіти. Основна перевага полягає в можливості вбудовувати платіжні функції в нефінансові точки взаємодії та інтегрувати їх у наявні системи, що трансформує бізнес-моделі, відкриває нові можливості для монетизації, покращує аналітику даних, підвищує привабливість платформи та створює кращий клієнтський досвід завдяки інтеграції платіжних можливостей у основні продукти.

[10] https://amluae.com/a-guide-to-avoiding-common-mistakes-in-aml-compliance-for-vasps/

Дауні підкреслює ключову роль інтерфейсів прикладного програмування (APIs) у цьому процесі, зазначаючи, що було багато розробок із третіми сторонами та спрощенням інтеграції через APIs, що дозволяє легко додавати платіжні функції до існуючих платформ, роблячи цей процес логічним кроком для багатьох компаній. Хоча кінцева мета embedded FinTech — створити простий і безперебійний користувацький досвід, Дауні наголошує, що за цією простотою стоїть складний фундамент, і одним із головних викликів є безпека, адже обробка конфіденційних даних потребує високого рівня захисту. Він говорить, що безпека буде великим питанням, оскільки компанії мають справу з чутливими даними, а останнім часом зросла увага до регуляторної відповідності, тому бізнеси повинні обирати партнерів, які є експертами в платіжних процесах і можуть гарантувати відповідність стандартам, таким як PCI та SOC 2. Вибір правильного партнера є критично важливим, оскільки FinTech-рішення діють у високорегульованому середовищі, і партнери, які відповідають строгим стандартам, допомагають уникати юридичних і операційних ризиків, а також підтримувати актуальність у питаннях комплаєнсу.

Ще одним важливим аспектом є кастомізація та масштабованість рішень, і Дауні зазначає, що якщо компанії витрачають час і гроші на розробку платіжної системи, вони хочуть, щоб їхня основна пропозиція та користувацький досвід залишалися незмінними, а платіжний досвід був плавним і безперебійним, залишаючись брендованим і злагодженим, щоб не відчужувати користувачів. Масштабованість також важлива, оскільки система має зростати разом із бізнесом, підтримуючи його розвиток без постійних переробок. Дауні формулює кінцеву мету так: компанії хочуть запобігти шахраям, але дозволити хорошим платежам проходити, і щоб досвід виглядав так, ніби це все одна система, що підкреслює баланс між безпекою, зручністю та брендованою ідентичністю. Дивлячись у майбутнє, він прогнозує подальшу інтеграцію штучного інтелекту в вбудовані FinTech-рішення, зазначаючи, що AI автоматизує певні завдання, наприклад, може допомагати в обробці помилок або спрощувати інтеграцію API між системами. Дауні також наголошує на потребі в просвіті, адже незважаючи на ажіотаж довкола embedded FinTech, багато компаній ще не повністю усвідомлюють його можливості, і він бачить значний потенціал у співпраці між спеціалістами з платежів і розробниками програмного забезпечення, де обидві сторони можуть брати участь у доходах, і їм логічно об’єднатися, щоб покращити пропозиції обох. Така співпраця може призвести до створення взаємовигідних рішень, де платіжні компанії надають інфраструктуру, а розробники — платформи для її використання.

Стаття завершується твердженням, що з правильною стратегією компанії можуть не лише оптимізувати свої платіжні процеси, але й відкрити нові можливості для зростання та інновацій, а embedded FinTech розглядається як тренд, що продовжуватиме розвиватися, змінюючи спосіб взаємодії бізнесів із клієнтами та партнерами.

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-2025-10

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].