Методологічний бюлетень

Серійний номер: МінФін-AML-2025-02

Січень 2025

Мета

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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Проекти технічних стандартів, що встановлюють вимоги щодо виявлення та запобігання ринковим зловживанням відповідно до Регламенту про ринки криптоактивів (MiCA)[1]

Фінальний звіт ESMA представляє детальний аналіз проекту регуляторних технічних стандартів (RTS), розроблених для впровадження положень статті 92(2) Регламенту про ринки криптоактивів (MiCA). Цей регламент спрямований на запобігання ринковим зловживанням, включаючи інсайдерську торгівлю, незаконне розголошення конфіденційної інформації та маніпулювання ринком. Звіт детально описує підхід до створення ефективних механізмів моніторингу та звітності, шаблону для повідомлення про підозрілі транзакції (STOR), а також координаційних процедур для забезпечення співпраці між національними компетентними органами (NCA) у транскордонних справах.

Звіт наголошує, що ефективна протидія ринковим зловживанням вимагає від професійних учасників ринку (PPAETs) впровадження належних систем моніторингу. Це стосується як транзакцій, так і інших аспектів функціонування технології розподілених реєстрів (DLT), таких як механізми консенсусу. ESMA акцентує увагу на тому, що вимоги до PPAETs повинні бути

[1] https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75-453128700-1278_Final_Report_STOR_MiCA_Article_92_2_.pdf

пропорційними до їхньої діяльності, масштабу операцій та ризиків, які вони можуть представляти для ринку. З цією метою пропонується систематичне оновлення процедур та їх регулярний перегляд не рідше одного разу на рік. Звіт також визначає важливість документування процесів, включаючи зміни в системах та процедурах, що мають зберігатися протягом п'яти років.

Шаблон STOR розроблено з урахуванням специфіки криптоактивів. Він включає елементи, що дозволяють точно ідентифікувати підозрілу поведінку, таких як тип активу, DLT-технологія, адреси гаманців та деталі транзакцій. ESMA прагнула знайти баланс між забезпеченням достатнього обсягу початкової інформації та гнучкістю у подальшому поданні додаткових даних. Водночас звіт визнає, що зловживання на крипторинках мають свої особливості, наприклад, взаємодія зі смартконтрактами або специфічні форми маніпуляцій, такі як pump-and-dump або rug pull. ESMA адаптувала STOR для таких ситуацій, зберігши ключові аспекти, запозичені з традиційного фінансового сектору.

Координація між NCA вимагає ефективного обміну інформацією у випадках транскордонних зловживань. ESMA пропонує механізм, який дозволяє своєчасно передавати STOR між відповідними органами. Також розглядається роль ESMA у координації розслідувань, якщо цього вимагають зацікавлені сторони. Звіт акцентує, що необхідно уникати дублювання зусиль і створювати чіткі межі відповідальності для кожного компетентного органу. Зокрема, ESMA рекомендує використовувати існуючі рамки співпраці з Регламенту ЄС № 596/2014 (Market Abuse Regulation) як основу для забезпечення координації.

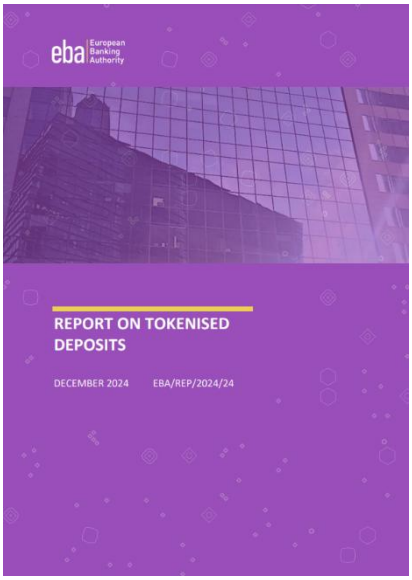
Оцінка витрат та вигод акцентує увагу на необхідності впровадження рішень, що мінімізують витрати для учасників ринку, зокрема через аутсорсинг моніторингу. ESMA також зазначає, що використання автоматизованих систем для виявлення зловживань має бути доповнене людським аналізом, що дозволить зменшити кількість хибнопозитивних сигналів і підвищити ефективність розслідувань. У випадках малих учасників ринку, звіт дозволяє певну гнучкість у впровадженні вимог, але водночас наголошує на необхідності мінімальних стандартів для всіх.

ESMA завершила розробку проекту RTS та передала його до Європейської Комісії для ухвалення. Наступні кроки включають збір додаткових даних і уточнення окремих аспектів регулювання, щоб забезпечити найефективніше впровадження MiCA у практику.

Висновки:

- **Системи запобігання зловживанням повинні бути адаптивними**. Учасники ринку (PPAETs) мають впроваджувати системи моніторингу, що враховують масштаб їх діяльності та ризики ринку. Це включає автоматизовані алгоритми з людським контролем для зменшення хибнопозитивних сигналів.
- **Чіткі критерії для STOR**. Шаблон STOR спрощено, щоб забезпечити швидке подання критичної інформації, залишаючи можливість подання додаткових даних пізніше. Визначено обов'язкові та факультативні елементи звітів.
- **Координація у транскордонних справах**. Важливим є чіткий механізм обміну інформацією між компетентними органами, зокрема для розслідування порушень. ESMA запропоновано координувати ці дії для ефективного розв'язання конфліктів юрисдикцій.
- **Баланс між регуляцією та гнучкістю**. Процедури розроблені з урахуванням потреб малого бізнесу, дозволяючи аутсорсинг моніторингу, але встановлюючи мінімальні стандарти для усіх учасників ринку.

ЗВІТ ПРО ТОКЕНІЗОВАНІ ДЕПОЗИТИ[2]



Звіт Європейського банківського органу (EBA) про токенізовані депозити представляє аналіз поточного стану, потенційних переваг і викликів у використанні токенізованих депозитів, а також рекомендації для регуляторів і зацікавлених сторін. Токенізація депозитів передбачає використання технології розподілених реєстрів (DLT) для фіксації залишків депозитів у цифровій формі, що дозволяє автоматизацію транзакцій і підвищення прозорості. У звіті зазначено, що токенізація не змінює сутності депозиту як фінансового інструменту, а лише змінює спосіб обліку.

У рамках дослідження EBA було проведено опитування регуляторів і фінансових установ у Європейській економічній зоні (EEA), яке виявило лише один активний випадок використання токенізованих депозитів у цьому регіоні. Про екти, що вивчалися, здебільшого спрямовані на оптимізацію розрахунків, включаючи забезпечення моделі "поставка проти платежу" (DvP). Крім того, кілька банківських консорціумів тестують технології DLT для інтеграції токенізованих депозитів у бізнес-процеси.

Висновки:

- **Технологічні переваги DLT.** Токенізовані депозити дозволяють автоматизувати транзакції за допомогою смартконтрактів, що підвищує ефективність і знижує витрати на проведення операцій.
- **Посилення AML/CTF контролю.** Використання DLT забезпечує кращу простежуваність транзакцій та автоматизацію виявлення підозрілих операцій, що сприяє дотриманню вимог протидії відмиванню коштів та фінансуванню тероризму.
- **Необхідність узгодження регуляторних підходів.** Потрібна чітка класифікація токенізованих депозитів у відмінності від EMTs для уникнення регуляторних прогалин і забезпечення захисту споживачів.
- **Потенційні операційні ризики.** Зовнішня залежність від провайдерів технології DLT може збільшити операційні ризики, тому важливо забезпечити стійкість інфраструктури та дотримання стандартів кібербезпеки.

Технологія DLT пропонує нові можливості, такі як програмованість транзакцій, що дозволяє автоматизувати операції за допомогою смартконтрактів. Це може знизити витрати та підвищити ефективність процесів. Крім того, токенізовані депозити можуть полегшити дотримання вимог з AML/CTF, забезпечуючи кращу простежуваність транзакцій та автоматизацію моніторингу.

Однак звіт акцентує увагу на низці викликів, зокрема: захист споживачів, що потребує покращення фінансової грамотності; операційні ризики, пов'язані із зовнішніми залежностями від провайдерів інфраструктури DLT; а також питання ліквідності, які можуть виникнути через зміну поведінки клієнтів і можливу волатильність токенізованих активів. Крім того, необхідно чітко розмежовувати токенізовані депозити та електронні грошові токени (EMTs), оскільки вони підпадають під різні регуляторні режими.

[2] https://www.eba.europa.eu/sites/default/files/2024-12/4b294386-1235-463f-b9b5-08f255160435/Report%20on%20Tokenised%20deposits.pdf

ЕВА не виявила необхідності негайних змін у регуляторній базі через обмежений масштаб впровадження токенізованих депозитів, але підкреслила важливість постійного моніторингу та координації між регуляторами.

Стандарти контролю і захисту інвесторів: нові настанови ESMA щодо "зворотного запиту" у рамках регулювання MiCA[3]

Документ є фінальним звітом Європейського управління з цінних паперів та ринків (ESMA), присвяченим керівним настановам щодо використання винятку "зворотного запиту" (reverse solicitation) у контексті Регламенту про ринки криптоактивів (MiCA). Основна увага приділяється визначенню чітких рамок і обставин, за яких компанії з третіх країн можуть легально пропонувати свої послуги клієнтам у ЄС без необхідності отримання авторизації згідно з MiCA. При цьому особливий акцент зроблено на недопущенні обходу регуляторних вимог через зловживання цим винятком.

Зворотний запит визначається як ситуація, коли клієнт з ЄС самостійно, без жодного зовнішнього впливу, ініціює контакт із фірмою третьої країни для отримання послуг. ESMA підкреслює, що це положення має бути дуже вузько обмеженим та не може використовуватися для обходу авторизаційних вимог MiCA. Документ детально аналізує статтю 61 MiCA, яка регулює зворотний запит, і пояснює, що виняток діє лише в суворо визначених обставинах. Наприклад, навіть якщо клієнт ініціює контакт, фірма третьої країни не може пропонувати йому нові послуги чи криптоактиви, які не були частиною початкової угоди.

Звіт також включає результати консультацій, проведених з учасниками ринку, та коментарі зацікавлених сторін. Більшість відповідей підтверджує необхідність суворого підходу до тлумачення винятку "зворотного запиту". Учасники висловлювали занепокоєння щодо надмірного розширення поняття "зворотного запиту" та ризиків, пов’язаних із недобросовісним використанням цього винятку. ESMA відповідає на ці коментарі та уточнює, що для визначення залучення клієнтів мають враховуватися як активні, так і пасивні форми маркетингу, включаючи непрямі методи, такі як пошукова оптимізація чи рекламні кампанії.

Документ пропонує практичні інструменти для національних компетентних органів (NCAs) з виявлення і запобігання порушенням. Це включає впровадження технологічних рішень для моніторингу ринкової активності та аналізу даних, що дозволяє ефективніше відстежувати рекламу, пропозиції та діяльність криптофірм, які можуть мати на меті обійти вимоги MiCA. Особливу увагу приділено важливості обміну інформацією між регуляторами в різних країнах для забезпечення більшої прозорості та підвищення ефективності нагляду.

Крім того, документ встановлює рамки для інтерпретації поняття "криптоактиви одного типу", які можуть бути запропоновані клієнтам у межах зворотного запиту. ESMA наголошує на ризик-орієнтованому підході до класифікації криптоактивів, підкреслюючи, що ключовими критеріями є категорія активу та пов’язані з ним ризики. Це повинно запобігти маніпуляціям, коли компанії третіх країн могли б пропонувати клієнтам активи, які формально належать до одного типу, але мають суттєво різні профілі ризиків.

[3] https://www.esma.europa.eu/sites/default/files/2024-12/ESMA35-1872330276-1899_-_Final_report_on_GLs_on_reverse_solicitation_under_MiCA.pdf

Документ завершується розглядом потенційних витрат і вигод, пов'язаних із впровадженням цих настанов. Хоча фірми третіх країн можуть нести обмежені адміністративні витрати через необхідність додаткового документування або вжиття запобіжних заходів, вигоди включають посилену захищеність інвесторів, створення рівних умов конкуренції для європейських учасників ринку та зменшення ризиків зловживання. Таким чином, звіт ESMA надає вичерпні рамки для забезпечення дотримання вимог MiCA і захисту інтересів інвесторів у криптоактивах.

Висновки:

- **Суворе обмеження "зворотного запиту":** Використання винятку можливе лише у випадках, коли клієнт самостійно ініціює контакт з фірмою, без жодного маркетингового чи рекламного впливу. Цей механізм має тлумачитися як винятковий і суворо обмежений.
- **Широке визначення "залучення клієнтів":** До залучення відноситься як активний, так і пасивний маркетинг, включаючи непрямі дії, такі як реклама, SEO-оптимізація чи доступність вебсайтів офіційними мовами ЄС.
- **Ризик-орієнтований підхід до класифікації криптоактивів:** Визначення "активів одного типу" має базуватися на категорії активів та рівні пов'язаних ризиків, щоб запобігти маніпуляціям і забезпечити дотримання вимог MiCA.
- **Підсилення моніторингу та співпраці:** Рекомендації для національних органів включають впровадження технологічних рішень для виявлення обходу регулювання, активний обмін інформацією між країнами ЄС та посилений нагляд за діяльністю фірм з третіх країн.

Регулювання ринків криптоактивів: ключові рекомендації ESMA для захисту інвесторів у рамках MiCA [4]

Документ, підготовлений Європейським управлінням з цінних паперів і ринків (ESMA), спрямований на деталізацію вимог щодо захисту інвесторів у сфері криптоактивів, відповідно до Регламенту MiCA. Основна мета цього документа — забезпечення прозорого та уніфікованого підходу до регулювання криптовалютних ринків, що сприятиме гармонізації практик у країнах Європейського Союзу та підвищенню рівня захисту прав інвесторів. Документ містить детальні рекомендації щодо двох ключових аспектів: оцінки придатності криптоактивів для клієнтів та встановлення процедур і політик у контексті послуг трансферу криптоактивів.

Оцінка придатності криптоактивів визначена як важлива складова захисту інвесторів відповідно до положень MiCA. Провайдери послуг мають зібрати достатню інформацію про клієнтів, щоб забезпечити відповідність пропонованих активів їхнім фінансовим цілям, рівню знань та досвіду, а також здатності витримувати потенційні збитки. ESMA підкреслює, що оцінка повинна включати аналіз ризикової толерантності клієнта та його загального розуміння технологій, на яких базуються криптоактиви. Наприклад, клієнтам має бути чітко пояснено ризики, пов'язані з використанням розподілених реєстрів, потенційними зломами та транзакційними помилками. Рекомендації також передбачають застосування процедур, які

[4] https://www.esma.europa.eu/sites/default/files/2024-12/ESMA35-1872330276-1936_MiCA_Final_Report_to_CP3_-_investor_protection_mandates.pdf

дозволять адаптувати вимоги MiCA до специфіки криптоактивів, одночасно враховуючи принципи, що вже діють у рамках MiFID II. Це забезпечує єдиний стандарт захисту інвесторів незалежно від того, чи вони працюють з класичними фінансовими інструментами, чи з криптоактивами.

Ще одним важливим аспектом документа є вимога надання клієнтам регулярної звітності щодо управління їхніми портфелями криптоактивів. Провайдери мають складати детальні періодичні звіти, які включають інформацію про виконані транзакції, продуктивність портфеля, а також оновлені дані щодо відповідності портфеля інвестиційним цілям клієнта. Звіти повинні бути електронними, що відповідає сучасним технологічним стандартам, та надаватися не рідше одного разу на три місяці. У випадках, коли клієнт має доступ до онлайн-систем з актуальною інформацією про свій портфель, вимоги щодо частоти звітності можуть бути адаптовані.

Другий великий блок рекомендацій стосується процедур і політик у контексті послуг трансферу криптоактивів. ESMA наголошує на важливості попереднього інформування клієнтів про основні характеристики та умови виконання трансакцій. Клієнтам має бути надана інформація про можливі ризики, зокрема про незворотність криптовалютних переказів після досягнення певної кількості підтверджень у блокчейні. Також провайдери повинні забезпечити прозорість витрат, чітко розмежовуючи комісії, пов'язані з використанням блокчейн-мережі, та власні збори за надані послуги. Це дозволяє клієнтам приймати зважені рішення на основі повного розуміння витрат і умов.

Висновки:

- **Гармонізація вимог між MiCA та MiFID II:** Рекомендації ESMA забезпечують однаковий рівень захисту клієнтів як на ринку криптоактивів, так і для класичних фінансових інструментів. Такий підхід мінімізує регуляторний арбітраж і створює прозорі умови для учасників ринку.
- **Розширення захисту інвесторів:** Оцінка придатності та вимоги до періодичної звітності покращують прозорість, підвищують довіру до ринку криптоактивів і допомагають уникати надмірних ризиків для клієнтів.
- **Впровадження політик і процедур для послуг трансферу:** Запропоновані вимоги підвищують стандарти управління ризиками, інформованість клієнтів про умови трансферів та зменшують ризики втрати активів.
- **Позитивний вплив на учасників ринку:** Хоча впровадження рекомендацій потребує додаткових витрат на IT-інфраструктуру, навчання персоналу та адаптацію процесів, це сприятиме підвищенню довіри інвесторів і загальному покращенню умов на ринку криптоактивів.

Крім того, ESMA рекомендує провайдерам розробляти політики, які враховують відповідальність у випадках некоректно виконаних або несанкціонованих транзакцій. У документі зазначено, що провайдери мають впровадити процедури для вирішення таких інцидентів, а також забезпечити клієнтам можливість отримувати оперативну інформацію про статус їхніх транзакцій. Це включає повідомлення про причини відхилення, повернення чи затримки переказу, а також про заходи, які клієнт може вжити для вирішення ситуації.

Документ також аналізує витрати та вигоди впровадження рекомендацій. З одного боку, провайдери послуг несуть додаткові витрати на адаптацію IT-систем, навчання персоналу та оновлення процедур. З іншого боку, ці зміни сприятимуть підвищенню довіри до ринку криптоактивів та захисту прав інвесторів. Клієнти отримують вигоди у вигляді кращої

прозорості, більшої безпеки транзакцій та відповідності пропонованих активів їхнім інвестиційним цілям. Гармонізація регулювання в рамках MiCA також зменшує ризики регуляторного арбітражу та створює рівні умови для всіх учасників ринку.

У підсумку, рекомендації ESMA є важливим кроком до забезпечення високого рівня захисту інвесторів і стабільності ринку криптоактивів. Вони сприяють уніфікації регуляторних підходів у країнах ЄС та створюють сприятливі умови для розвитку цього сектора.

"Нові стандарти безпеки в криптоактивах: аналіз рекомендацій ESMA для ринку ЄС [5]

Документ розроблений Європейським органом з цінних паперів та ринків (ESMA), спрямований на впровадження єдиних стандартів управління системами та протоколами безпеки доступу для учасників ринку криптоактивів. Цей документ стосується емітентів криптоактивів та осіб, які прагнуть торгувати такими активами, за винятком токенів, прив'язаних до активів (ART), і токенів електронних грошей (EMT). Розробка цих рекомендацій базується на положеннях регулювання MiCA (Regulation on Markets in Crypto-Assets), яке встановлює основні вимоги до учасників крипторинку, спрямовані на забезпечення безпеки, прозорості та стабільності.

Документ містить рекомендації щодо того, як підтримувати безпеку систем та доступу в контексті зростаючих ризиків кібербезпеки та необхідності дотримання нормативних вимог. Основний акцент зроблено на принципі пропорційності: рекомендації враховують розмір організацій, їхній ризик-профіль, а також складність операцій. Таким чином, малі та середні компанії не будуть зобов'язані впроваджувати надмірно складні чи дорогі заходи, які характерні для великих компаній чи регульованих інституцій, як-от крипто-провайдери (CASPs) або емітенти ART і EMT.

Рекомендації передбачають створення організаційних заходів, що забезпечують належне управління інформаційно-комунікаційними технологіями (ICT). ESMA підкреслює необхідність чіткого розподілу ролей і обов'язків у сфері управління ICT-ризиками, а також забезпечення регулярного навчання персоналу, щоб підвищити рівень компетенцій співробітників. Організації мають визначити ключові функції для моніторингу, оцінки та управління ризиками. Особливу увагу приділено необхідності створення механізмів оцінки ризиків, які виникають через використання послуг сторонніх постачальників ICT.

Важливе місце займають протоколи безпеки доступу, що поділяються на фізичні та логічні. Фізичні протоколи спрямовані на захист приміщень, де зберігаються чутливі дані або розміщені ключові інформаційні системи, від несанкціонованого доступу чи екологічних ризиків. Організації повинні впроваджувати системи обліку фізичного доступу та регулярно переглядати надані дозволи. Логічні протоколи доступу зосереджені на обмеженні доступу до інформаційних систем тільки авторизованими особами, відповідно до їхніх посадових обов'язків. Використання принципів "need-to-know" (необхідність знання) та "least privilege" (мінімальні привілеї) забезпечує мінімізацію ризиків компрометації даних або систем.

Окрему увагу приділено криптографічному захисту. Управління криптографічними ключами передбачає контроль на всіх етапах їхнього життєвого циклу: від створення та резервного копіювання до відкликання та знищення. ESMA рекомендує організаціям впроваджувати

[5] https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75-223375936-6089_Final_Report_-_GLs_on_security_access_protocols_-_Art._14_1__d_.pdf

механізми заміни ключів у разі їх компрометації чи втрати. Для покращення прозорості та контролю організації мають вести реєстр сертифікатів та забезпечувати їхнє своєчасне оновлення. У рекомендаціях також наголошується, що використання криптографічних методів повинно відповідати сучасним стандартам безпеки.

Документ спирається на існуючі нормативи Європейського Союзу, такі як DORA (Digital Operational Resilience Act), NIS2 (Network and Information Security Directive) та міжнародні стандарти, зокрема ISO 27001. ESMA адаптувала рекомендації, щоб уникнути надмірного навантаження на компанії, що не підпадають під дію DORA, але повинні відповідати вимогам MiCA. Цей підхід дозволяє досягти балансу між забезпеченням безпеки та зменшенням адміністративного тиску.

В результаті впровадження цих рекомендацій організації зможуть підвищити свою кіберстійкість, зменшити ризики компрометації систем і активів, а також покращити загальний рівень безпеки. Рекомендації сприятимуть гармонізації регуляторних підходів у Європейському Союзі та забезпеченню довіри до ринку криптоактивів.

Висновки:

- **Пропорційний підхід до стандартів:** Рекомендації адаптовані до масштабу та ризиків компаній, дозволяючи знижувати адміністративне навантаження, особливо для малих і середніх підприємств.
- **Підвищення кіберстійкості:** Використання протоколів безпеки та криптографічних інструментів знижує ризики компрометації систем, захищає активи та дані компаній.
- **Управління ризиками ІКТ:** Організаціям рекомендовано створити ефективні внутрішні структури для управління ІКТ-ризиками, включаючи моніторинг, оцінку та звітування.

Наднаціональні заходи ЄС у сфері протидії відмиванню коштів та фінансуванню тероризму: аналіз ефективності за результатами 5-го раунду оцінок MONEYVAL[6]

Документ присвячений аналізу наднаціональних механізмів Європейського Союзу (ЄС) у сфері протидії відмиванню коштів (ВК) і фінансуванню тероризму (ФТ) на основі 5-го раунду взаємних оцінок MONEYVAL. Головною метою аналізу є оцінка того, як країни-члени MONEYVAL, які входять до ЄС, впроваджують та інтегрують у свою діяльність наднаціональні законодавчі рамки, механізми співпраці й ризикові оцінки. Дослідження акцентує увагу на ключових аспектах ефективності таких механізмів, виявляючи як їхні сильні сторони, так і прогалини у реалізації.

ЄС, як наднаціональна організація, створив спільну правову та інституційну базу для уніфікації підходів у боротьбі з ВК/ФТ серед країн-членів. Основою цих зусиль стали Директиви ЄС (4-та та 5-та Директиви з протидії ВК/ФТ), які встановлюють загальні правила, включаючи вимоги до реєстрації бенефіціарних власників (БВ), проведення належної перевірки клієнтів (CDD), застосування посилених заходів перевірки (EDD) та аналізу ризиків. Попри це, взаємні оцінки MONEYVAL свідчать, що транспозиція цих директив не завжди відповідає національним ризиковим профілям, що призводить до неоднорідності у виконанні.

[6] https://www.coe.int/en/web/moneyval/-/eu-supranational-measures-in-moneyval-5th-round-mutual-evaluation-reports

Одним із ключових аспектів є роль наднаціональних ризикових оцінок (SNRA), які покликані допомогти країнам оцінювати транскордонні загрози. MONEYVAL встановив, що у більшості випадків SNRA не інтегрується належним чином у національні ризикові стратегії. Це спричиняє недостатню увагу до загроз, пов'язаних із транскордонними потоками коштів та географічними ризиками. Лише кілька країн використовували SNRA як джерело для власних національних оцінок ризиків.

Висновки:

- **Інтеграція SNRA в національні ризикові оцінки:** Більшість країн не використовують дані SNRA на рівні, який очікується для оцінки національних ризиків. Рекомендація: удосконалити обов'язковість врахування SNRA у національних стратегіях.
- **Реєстри бенефіціарних власників:** Недостатня перевірка точності даних та слабке правозастосування підривають ефективність реєстрів. Рекомендація: розширити ресурси для їх адміністрування та впровадити автоматизовані системи верифікації.
- **Обмежене використання наднаціональних механізмів співпраці:** Деякі країни рідко залучають EUROPOL, EUROJUST, що знижує ефективність міжнародної взаємодії. Рекомендація: посилити тренування та заохочувати обмін практиками між країнами.
- **Відмінності у впровадженні директив AMLD:** Пряме транспонування положень директив без адаптації до національних ризиків створює розриви в відповідності вимогам FATF. Рекомендація: посилити національну

Реєстри бенефіціарних власників стали центральним елементом аналізу. MONEYVAL виявив, що більшість країн мають реєстри, але їхня ефективність обмежена через низький рівень точності та повноти даних. У багатьох випадках реєстри лише виконують функцію збору інформації, тоді як механізми перевірки, оновлення та забезпечення відповідності залишаються слабкими. У деяких країнах бракує ресурсів для управління реєстрами, що негативно впливає на їх здатність забезпечувати прозорість.

Окремо розглядається співпраця між країнами ЄС через такі механізми, як EUROPOL, EUROJUST та Європейська прокуратура (EPPO). У звітах MONEYVAL зазначається, що використання цих платформ є ефективним для розслідування складних справ, але застосовується нерівномірно. Деякі країни покладаються переважно на внутрішні механізми, що обмежує можливості для міжнародної взаємодії.

Рамкові директиви AMLD ЄС створили значну основу для гармонізації правил, однак їхня транспозиція не завжди враховує специфічні національні ризики. Наприклад, у випадках, коли країни прямо впроваджують положення директив, не адаптуючи їх до власних контекстів, це може призводити до недостатньої ефективності на практиці.

Документ також підкреслює необхідність удосконалення заходів з верифікації інформації, наявної у реєстрах бенефіціарних власників, та підвищення санкцій за недотримання правил. MONEYVAL вказує, що поточні механізми санкцій часто неефективні або непропорційні, що знижує їхню стримуючу дію.

Важливим є висновок про те, що наднаціональні механізми, такі як SNRA, реєстри БВ та платформи співпраці, мають значний потенціал для підвищення ефективності систем протидії ВК/ФТ, але потребують більшого залучення, ресурсів та адаптації до національних контекстів. MONEYVAL рекомендує країнам зміцнити інституційні можливості, інтегрувати наднаціональні інструменти в національні стратегії та забезпечити відповідність міжнародним стандартам FATF.

Роль фінансової розвідки у протидії економічним злочинам: аналіз нових стратегій і міжнародної співпраці за матеріалами *SARs in Action Issue 29*[7]

Документ є важливим виданням, спрямованим на інформування зацікавлених сторін у сфері протидії відмиванню коштів (ПВК), фінансуванню тероризму (ФТ) та іншими видами економічної злочинності. Цей випуск акцентує увагу на ролі фінансового сектору у протидії транснаціональним злочинам, торгівлі людьми, нелегальній діяльності компаній та іншим фінансовим ризикам.

Основним аспектом видання є висвітлення питань торгівлі людьми як одного з найприбутковіших і найнебезпечніших видів злочинної діяльності. Згідно з даними, понад 49,6 мільйонів людей перебувають в умовах примусової експлуатації. Торгівля людьми тісно пов'язана з економічною вигодою, що зумовлює використання як традиційних фінансових систем, так і альтернативних, наприклад криптовалют чи системи «havala». У цьому контексті фінансовий сектор відіграє критичну роль у виявленні та припиненні злочинної діяльності. Представлений посібник від Europol Financial Intelligence Public-Private Partnership (EFIPPP) надає фінансовим установам практичні інструменти, індикатори ризику та стратегії моніторингу, спрямовані на підвищення ефективності звітів про підозрілу діяльність (SARs) та протидію торгівлі людьми.

Другий важливий розділ зосереджується на аналізі створення фіктивних компаній як механізму відмивання коштів. Діяльність тимчасової групи Illicit Finance Public Private Threat Group (PPTG) дозволила визначити ключові характеристики нелегального створення компаній, включаючи ризикові ознаки, такі як використання поштових адрес, непрозорих даних про директорів та підозрілих фінансових транзакцій. Інформація зібрана для вдосконалення аналітичних інструментів і побудови ефективної моделі виявлення фіктивних структур.

Окремий акцент зроблено на діяльності «Hydroponics Cell», яка досліджує використання бізнесу з продажу систем гідропоніки для відмивання коштів, отриманих від нелегальної діяльності. Незважаючи на законність цього бізнесу, велика кількість готівкових операцій у секторі привертає увагу організованих злочинних груп. Результатом роботи групи стало створення першого галузевого «Amber Alert», який містить тематичні дослідження, індикатори ризику та рекомендації для фінансових установ. Ця

Висновки:

- **Ефективність фінансового сектору в боротьбі з торгівлею людьми:** Використання посібника EFIPPP може суттєво підвищити здатність фінансових установ виявляти та припиняти злочинні схеми.
- **Попередження створення фіктивних компаній:** Використання даних Companies House та інших інструментів моніторингу дозволяє швидко ідентифікувати ризикові компанії та їх зв'язок із відмиванням коштів.
- **Підтримка публічно-приватного партнерства:** Спільна робота державних і приватних структур (наприклад, у межах «Hydroponics Cell») підвищує ефективність розслідувань, як продемонстровано в результатах конфіскації активів на суму понад £450,000.
- **Міжнародна координація:** Участь ПФР у GFIP Summit демонструє важливість глобального обміну досвідом і розробки універсальних підходів до ідентифікації фінансових злочинів.

[7] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/737-sars-in-action-issue-29/file

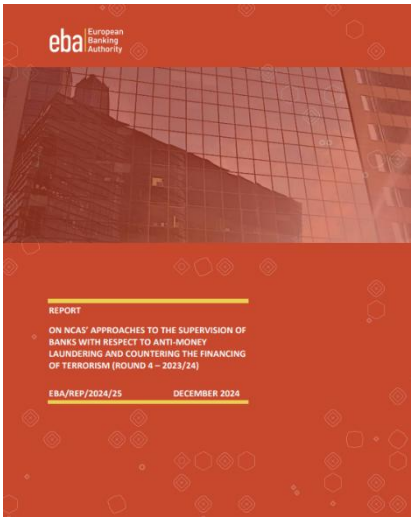
робота вже принесла конкретні результати, такі як конфіскація значних активів і порушення низки кримінальних справ.

Міжнародний контекст випуску представлено через участь ПФР Великої Британії у Global Financial Institutions Partnership (GFIP) Summit. Саміт акцентував увагу на проблемах шахрайства з використанням ідентифікаційних даних, відмивання коштів через торгівлю (TBML) та зловживання фінансовими технологіями. Учасники обговорили підходи до боротьби з цими загрозами, акцентуючи на необхідності міжнародної співпраці, обміну даними та вдосконалення системи SARs. Особливу увагу приділено використанню спільних підходів у протидії відмиванню коштів через такі інструменти, як проєкт SHADOW, спрямований на ідентифікацію доходів від онлайн-експлуатації дітей.

Заключною частиною випуску є визнання досягнень через нагородження Tackling Economic Crime Awards (TECA). Нагороди отримали представники державного та приватного секторів, які досягли значних успіхів у боротьбі з економічними злочинами. Особливо виділяються ініціативи, спрямовані на міжнародну співпрацю, вдосконалення розслідувань і розробку нових аналітичних інструментів.

Документ демонструє важливість публічно-приватного партнерства, інноваційних підходів і міжнародної координації у сфері фінансової розвідки. Він надає цінні інструменти, практичні кейси та методології, які можуть бути ефективно використані для підвищення якості розслідувань, виявлення злочинів та запобігання їм.

Оцінка ефективності нагляду за банками у сфері ПВК/ФТ: ключові виклики та досягнення за підсумками четвертого звіту ЕВА[8]



Четвертий звіт Європейського банківського органу (ЕВА) щодо підходів національних компетентних органів влади (NCA) до нагляду за банками у сфері протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ) є результатом детального аналізу 14 органів у 9 країнах-членах ЄС/ЄЕЗ у період 2023–2024 років. Цей звіт підсумовує прогрес, досягнутий з моменту попередніх раундів оцінювання, і містить оцінку ефективності підходів до ризик-орієнтованого нагляду, стратегії управління ризиками, а також координації між NCA як на національному, так і на міжнародному рівнях.

Основною метою звіту є оцінка того, як органи нагляду впроваджують ризик-орієнтований підхід, передбачений міжнародними стандартами та директивами ЄС, зокрема Директивою (ЄС) 2015/849. У документі розглядається прогрес у створенні й удосконаленні секторних та інституційних оцінок ризиків. Хоча більшість NCA запровадили нові методології оцінки ризиків, виявлено суттєві недоліки в урахуванні ризиків, пов'язаних із фінансуванням тероризму, і недостатню деталізацію процедур оцінювання. Відзначено, що деякі країни все ще використовують застарілі дані для національних оцінок ризиків, що знижує актуальність та ефективність цих оцінок.

[8] https://www.eba.europa.eu/sites/default/files/2024-12/978992b4-1b46-4b52-bb07-0d38a018c005/Report%20on%20NCAs%20approaches%20to%20the%20supervision%20of%20banks%20with%20respect%20to%20AMLCFT.pdf

Звіт наголошує на покращеннях у структурі органів нагляду. Більшість NCA створили спеціалізовані підрозділи ПВК/ФТ і збільшили ресурси, виділені на ці завдання. Проте нестача персоналу та відсутність стратегічного підходу до навчання нових і поточних співробітників залишаються значними викликами. У багатьох випадках адаптація нових працівників базується на неформальних методах, що створює ризики невідповідності стандартам.

Висновки:

- **Покращення у впровадженні ризик-орієнтованого підходу:** Більшість NCA запровадили нові методології оцінки ризиків, але деякі органи ще стикаються з викликами у врахуванні факторів ризиків тероризму та забезпеченні послідовності оцінок.
- **Недоліки в санкційній політиці:** У багатьох NCA штрафи не є ефективними через їхню недостатню величину та відсутність детального обґрунтування рішень. Це знижує стримувальний ефект санкцій.
- **Відсутність системного підходу до співпраці:** Координація між органами, що здійснюють нагляд у тій самій юрисдикції, залишається слабкою. Відсутність узгоджених підходів призводить до дублювання зусиль або прогалин у нагляді.
- **Ресурси та кадрове забезпечення:** Хоча більшість NCA створили спеціалізовані підрозділи у сфері ПВК/ФТ, виявлено нестачу персоналу, відсутність систематичних навчальних програм та слабку інтеграцію нових співробітників.

Ще однією ключовою проблемою, висвітленою у звіті, є недосконаліть санкційної політики. Виявлено, що у багатьох NCA санкції не відповідають тяжкості порушень, а процес їх визначення базується на професійних судженнях окремих співробітників без чітко задокументованих критеріїв. У результаті, штрафи часто не є достатньо стримувальними, а органи нагляду стикаються з юридичними викликами з боку банків.

Координація між NCA у межах однієї країни та на міжнародному рівні демонструє поступове покращення, але залишається обмеженою. Відсутність чітких механізмів обміну інформацією та дублювання зусиль між різними органами призводить до неефективності в нагляді за банками. У деяких випадках спостерігалися конфлікти у висновках різних NCA щодо одного й того самого банку, що створює невизначеність для підзвітних установ.

Особливу увагу звіт приділяє співпраці між органами, відповідальними за ПВК/ФТ та пруденційний нагляд. Незважаючи на те, що більшість органів усвідомлюють важливість інтеграції цих підходів, відсутність систематизованих процедур і формалізованої співпраці ускладнює обмін інформацією та своєчасне залучення експертів ПВК/ФТ до процесів оцінки банківських ризиків.

Звіт завершується рекомендаціями для NCA щодо подальшого вдосконалення їхніх підходів до ПВК/ФТ. Основний акцент зроблено на необхідності розробки чітких стратегій і процедур, посилення координації між органами, забезпечення ефективності санкційної політики, а також запровадження стратегічного підходу до навчання кадрів. У підсумку, успішне впровадження цих рекомендацій має сприяти зміцненню системи нагляду в країнах-членах ЄС/ЄЕЗ і підвищенню ефективності боротьби з ВК/ФТ.

Європейська революція регулювання криптоактивів: нові стандарти протидії відмиванняю коштів і фінансуванню тероризму[9]

Документ аналізує поточний стан і розвиток регулювання криптоактивів у Європейському Союзі, акцентуючи увагу на заходах із протидії відмиванню коштів (ПВК) і фінансуванню тероризму (ФТ). Основний зміст спрямований на вивчення регуляторного підходу до криптовалютного сектору, його слабких місць, ризиків і впроваджених інструментів для їх подолання.

Криптоактиви, попри свої інноваційні можливості, мають низку особливостей, які роблять їх привабливими для злочинців. Серед основних ризиків – анонімність користувачів, яка ускладнює ідентифікацію кінцевих бенефіціарів, та глобальний характер криптосервісів, що виходять за межі юрисдикції національних регуляторів. Відсутність належного контролю та стандартів призвела до того, що криптовалютний сектор став уразливим до відмивання коштів і фінансування тероризму.

У ЄС регулювання криптоактивів почалося з обмеженого охоплення у Директиві (ЄС) 2018/849, яка поширювалася лише на надавачів послуг зі зберігання гаманців і обміну криптовалют на фіатні валюти. Проте цей підхід не забезпечував повного охоплення сектору. У відповідь на виклики, у 2023 році був прийнятий Регламент (ЄС) 2023/1114 (MiCAR), який запроваджує єдину правову базу для регулювання криптоактивів, зокрема їхнього випуску, торгівлі та надання послуг. Паралельно зміни до Директиви 2015/849 розширили зону дії вимог ПВК/ФТ на ширший перелік суб'єктів, включаючи постачальників послуг із криптоактивами (CASPs).

Новий регуляторний режим, що набуде чинності з грудня 2024 року, вимагає від CASPs отримання авторизації для роботи в ЄС. Для цього необхідно продемонструвати наявність адекватних механізмів контролю, процедур управління ризиками та дотримання вимог ПВК/ФТ. Окрім того, особливу увагу приділено запровадженню правил для забезпечення прозорості операцій, таких як обов'язок збору і передачі інформації про відправників і отримувачів криптовалютних переказів (відомий як «Travel Rule»). Ці заходи спрямовані на підвищення відстежуваності операцій і зниження ризиків ВК/ФТ.

Висновки:

- **Розширення регуляторного охоплення:** З 2024 року регулювання ЄС поширюється на всі типи постачальників послуг із криптоактивами (CASPs), а також на токени ARTs і EMTs, запроваджуючи жорсткіші вимоги до ліцензування та моніторингу.
- **Підвищення прозорості трансакцій:** CASPs повинні збирати та передавати дані про сторони транзакцій, що значно підвищує прозорість і відстежуваність криптовалютних операцій, зменшуючи ризики ВК/ФТ.
- **Нова інфраструктура нагляду:** Європейський банківський орган передасть регуляторні функції новій агенції ЄС у сфері ПВК до кінця 2025 року, що забезпечить більшу ефективність нагляду за криптоактивами.
- **Необхідність адаптації для бізнесу:** Криптокомпанії зобов'язані розробити ефективні механізми управління ризиками, інтегрувати вимоги ПВК/ФТ у свої операційні моделі та забезпечити відповідність новим стандартам до встановлених дедлайнів.

[9] https://www.eba.europa.eu/sites/default/files/2024-12/25bb6d67-4bd1-4e54-805c-269d9657e7fb/Preventing%20ML%20TF%20in%20the%20EU%27s%20crypto%20assets%20sector.pdf

Роль Європейської банківської агенції (EBA) у цьому процесі є ключовою. Вона розробляє настанови для CASPs, ARTs (токени прив'язані до активів) і EMTs (токени електронних грошей), які регулюють питання корпоративного управління, оцінки ризиків та впровадження вимог ПВК/ФТ. EBA також координує дії наглядових органів, проводить навчання й підтримує єдиний підхід до ризик-орієнтованого нагляду в межах ЄС. Однак з кінця 2025 року ці функції буде передано новій агенції ЄС у сфері ПВК, що дозволить централізувати нагляд і посилити його ефективність.

Загалом, документ підкреслює, що нові регуляторні заходи спрямовані не лише на запобігання злочинній діяльності, але й на формування прозорого, безпечного та відповідального ринку криптоактивів у Європі.

Гармонізація нагляду за криптоактивами в ЄС: нові керівництва EBA для емітентів ARTs та EMTs відповідно до MiCAR[10]

Документи спрямовані на імплементацію єдиного підходу до звітності та нагляду за діяльністю емітентів токенів ARTs (токени прив'язані до активів) та EMTs (токени електронних грошей), відповідно до вимог Регламенту (ЄС) 2023/1114 (MiCAR). Основна мета цих настанов – забезпечити стандартизоване, ефективне та прозоре регулювання ринку криптоактивів у Європейському Союзі. Документи містять комплексні інструкції щодо звітності, шаблонів даних, критеріїв значущості токенів, а також правил для постачальників послуг із криптоактивами (CASPs).

Висновки:

- **Узгодженість даних:** Запровадження єдиних шаблонів та DPM забезпечує узгодженість звітності між емітентами та наглядовими органами, сприяючи ефективному моніторингу та уникненню дублювання запитів.
- **Поліпшення контролю:** Звітування щодо ліквідності та резервів активів дозволяє органам нагляду оцінювати ризики для фінансової стабільності та здійснювати стрес-тести ліквідності.
- **Оцінка значущості токенів:** Інформація про власників, транзакції та резерви активів необхідна для визначення системної важливості токенів і потенційного переходу нагляду до EBA.
- **Цифрова гармонізація:** Інтеграція звітності CASPs з емітентами через стандартизовані інструменти сприяє створенню прозорого та гармонізованого середовища для ринку криптоактивів.

MiCAR вимагає, щоб емітенти ARTs та EMTs дотримувалися високих стандартів управління резервами активів, ліквідності та власних коштів, забезпечуючи фінансову стабільність та захист прав власників токенів. Однією з ключових вимог є регулярне звітування емітентів про кількість власників токенів, розмір резервів активів, структуру власного капіталу, а також про транзакції з токенами. Для цього запроваджено уніфіковані шаблони звітності, які стандартизують обсяг та формат даних. Шаблони охоплюють різні аспекти, зокрема:

- структуру резервів активів із деталізацією за класами активів та термінами їхньої ліквідності;
- інформацію про транзакції, що дозволяє оцінити обсяг використання токенів як засобу обміну;
- вимоги до власного капіталу, які залежать від розміру резервів або операційних витрат емітентів.

[10] https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/asset-referenced-and-e-money-tokens-micar/guidelines-templates-assist-competent-authorities-performing-their-supervisory-duties-regarding

Інструкції деталізують, як емітенти повинні взаємодіяти з CASPs для отримання необхідних даних, таких як кількість власників токенів та обсяги транзакцій. CASPs зобов'язані надавати ці дані в уніфікованому форматі, дотримуючись вимог щодо захисту конфіденційної інформації. Для цього використовується процедура хешування персональних даних (SHA-256), що забезпечує анонімність.

Крім того, документи акцентують увагу на критерії значущості токенів. Емітенти зобов'язані надавати детальні дані про капіталізацію, транзакційну активність, а також взаємодію з іншими токенами та CASPs. Ці дані використовуються для визначення системної важливості токенів та переходу нагляду від національних регуляторів до Європейського банківського органу (EBA), якщо токен класифіковано як значущий.

Документи також регулюють питання якості даних. Запроваджується єдина модель даних (DPM), яка визначає структуру звітності, атрибути даних та логічні зв'язки між ними. Валідаційні правила забезпечують відповідність даних нормативним вимогам, перевіряють їхню узгодженість та точність.

Основною перевагою цих настанов є гармонізація регуляторних вимог у всьому ЄС. Це дозволяє уникнути дублювання зусиль, зменшує адміністративне навантаження на емітентів і CASPs, а також сприяє ефективному моніторингу фінансової стабільності. Таким чином, документи сприяють зміцненню довіри до ринку криптоактивів та створенню рівних умов для учасників.

Практичне керівництво для ВНУП: Перевірка клієнтів (CDD) як ключовий інструмент протидії фінансовим злочинам[11]

UNITED ARAB EMIRATES
MINISTRY OF ECONOMY

Документ надає комплексні рекомендації для визначених нефінансових установ чи професій (ВНУП) щодо застосування процедур перевірки клієнтів (Customer Due Diligence, CDD) у контексті протидії відмиванню коштів (ПВК), фінансуванню тероризму (ФТ) та фінансуванню розповсюдження зброї масового знищення (ФР). Його основною метою є допомога ВНУП у виконанні нормативних вимог, ефективному управлінні ризиками та запобіганні залученню до протиправних фінансових схем.

У документі зазначено, що CDD є фундаментальним інструментом для підтримання цілісності фінансової системи. Перевірка клієнтів передбачає ідентифікацію їхньої особи, розуміння мети встановлення ділових відносин, моніторинг транзакцій та підтримання актуальності даних. Ця процедура дозволяє ВНУП запобігати фінансовим злочинам, уникати репутаційних ризиків та зміцнювати довіру з боку регуляторів.

Документ описує три основні рівні CDD: спрощений (Simplified CDD), стандартний (CDD) та посилений (Enhanced CDD). Спрощений рівень застосовується до клієнтів з низьким ризиком і передбачає меншу частоту перевірок та спрощену процедуру верифікації. Стандартний рівень є базовим і включає ідентифікацію клієнта, аналіз його вигодоодержувачів та моніторинг транзакцій. Посилений рівень застосовується до клієнтів із високим ризиком, таких як політично значущі особи (PEPs), та вимагає додаткової документації, перевірок походження коштів та участі вищого керівництва у прийнятті рішень щодо співпраці.

[11] https://www.moec.gov.ae/documents/20121/0/Implementation+Guide+on+CDD.pdf/39e7e435-5206-10b2-4b13-9a2221c447bd?t=1735568337213

Значну увагу приділено ситуаціям, у яких необхідно проводити CDD. Це включає встановлення нових ділових відносин, проведення разових транзакцій на суми, що перевищують встановлені пороги, або у разі підозри щодо відмивання коштів або фінансування тероризму. У разі виникнення сумнівів щодо раніше отриманих даних клієнта або появи нових ризиків, ВНУП зобов'язані проводити додаткові перевірки.

Документ також підкреслює важливість моніторингу клієнтських транзакцій на постійній основі, особливо для клієнтів із високим ризиком. Це передбачає регулярний перегляд записів, оновлення даних та аналіз транзакцій на предмет їх відповідності профілю клієнта. ВНУП мають забезпечувати збереження всіх записів і документів, отриманих у процесі перевірки, щонайменше протягом п'яти років після завершення співпраці з клієнтом.

Особливий акцент зроблено на забезпеченні конфіденційності при підозрі на протиправну діяльність клієнта. Забороняється інформувати клієнтів про подання підозрілих звітів (Suspicious Transaction Reports, STR), оскільки це може завадити розслідуванню.

Документ наголошує, що підхід до CDD має базуватися на оцінці ризиків. ВНУП повинні адаптувати свої заходи залежно від ступеня ризику, що дозволяє ефективніше використовувати ресурси для запобігання фінансовим злочинам. Зокрема, високий ризик вимагає посиленої перевірки, тоді як низький дозволяє застосовувати спрощений підхід.

У заключній частині підкреслено важливість участі вищого керівництва у прийнятті рішень щодо співпраці з клієнтами з високим ризиком. Це гарантує дотримання внутрішньої політики управління ризиками та підвищує обізнаність керівництва про потенційні загрози.

Висновки:

- **Ризик-орієнтований підхід:** ВНУП повинні адаптувати підхід до CDD залежно від ризиків клієнта, зокрема, застосовувати посилену перевірку для клієнтів із високим ризиком та спрощену – для клієнтів із низьким.
- **Необхідність безперервного моніторингу:** Ведення постійного моніторингу клієнтських транзакцій та оновлення їхніх даних є ключовим для ефективного управління ризиками ВК/ФТ.
- **Важливість участі вищого керівництва:** У складних випадках (наприклад, клієнти з високим ризиком) рішення повинні прийматися із залученням вищого керівництва для посилення контролю та дотримання політики управління ризиками.
- **Документування та збереження інформації:** Усі дані, зібрані під час перевірки клієнтів, мають бути збережені для забезпечення відповідності законодавчим вимогам та швидкого надання інформації компетентним органам у разі потреби.

Таким чином, документ є практичним інструментом для ВНУП, який допомагає забезпечити дотримання міжнародних стандартів та нормативних вимог у сфері ПВК/ФТ, а також сприяє побудові надійних систем контролю і моніторингу фінансових ризиків.

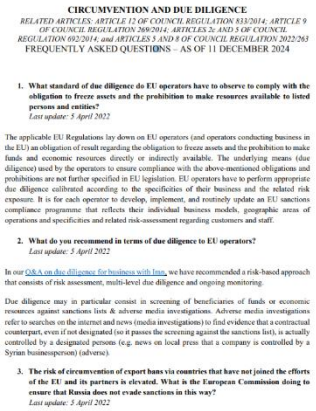
Практичні аспекти імплементації санкцій ЄС: належна перевірка та протидія обходу санкцій[12]

Документ є офіційним зведенням питань і відповідей (FAQ), яке стосується практичних аспектів імплементації санкцій, запроваджених Європейським Союзом у відповідь на військову агресію росії проти України та участь білорусі у цій агресії. Він роз'яснює норми Регламентів ЄС, що

[12] https://finance.ec.europa.eu/document/download/c2925c16-8a2b-4f17-8c4a-92355bb9d8de_en?filename=faqs-sanctions-russia-circumvention-due-diligence_en.pdf

регулюють замороження активів, запобігання наданню економічних ресурсів санкційним особам і суб'єктам, а також боротьбу з обходом санкцій.

Основна увага приділена обов'язкам європейських операторів щодо виконання вимог санкційного режиму. У документі наголошується, що операторам необхідно впроваджувати комплексні програми дотримання санкцій, які враховують специфіку їхньої діяльності, географію операцій та рівень ризику. Ці програми мають бути постійно оновлюваними та адаптованими до змін у регуляторному середовищі. Хоча законодавство ЄС не надає точних вказівок щодо методів забезпечення відповідності, оператори повинні проводити глибоку оцінку ризиків та застосовувати багаторівневу перевірку (Enhanced Due Diligence). Така перевірка включає скринінг бенефіціарів, аналіз медійних і відкритих джерел, контроль товарів та фінансових потоків.



CIRCUMVENTION AND DUE DILIGENCE

RELATED ARTICLES: ARTICLE 12 OF COUNCIL REGULATION 833/2014; ARTICLE 9 OF COUNCIL REGULATION 269/2014; ARTICLES 2c AND 5 OF COUNCIL REGULATION 692/2014; and ARTICLES 5 AND 8 OF COUNCIL REGULATION 2022/263

FREQUENTLY ASKED QUESTIONS – AS OF 11 DECEMBER 2024

1. **What standard of due diligence do EU operators have to observe to comply with the obligation to freeze assets and the prohibition to make resources available to listed persons and entities?**
Last update: 5 April 2022

The applicable EU Regulations lay down on EU operators (and operators conducting business in the EU) an obligation of result regarding the obligation to freeze assets and the prohibition to make funds and economic resources directly or indirectly available. The underlying means (due diligence) used by the operators to ensure compliance with the above-mentioned obligations and prohibitions are not further specified in EU legislation. EU operators have to perform appropriate due diligence calibrated according to the specificities of their business and the related risk exposure. It is for each operator to develop, implement, and routinely update an EU sanctions compliance programme that reflects their individual business models, geographic areas of operations and specificities and related risk-assessment regarding customers and staff.

2. **What do you recommend in terms of due diligence to EU operators?**
Last update: 5 April 2022

In our Q&A on due diligence for business with Iran, we have recommended a risk-based approach that consists of risk assessment, multi-level due diligence and ongoing monitoring.

Due diligence may in particular consist in screening of beneficiaries of funds or economic resources against sanctions lists & adverse media investigations. Adverse media investigations refer to searches on the internet and news (media investigations) to find evidence that a contractual counterpart, even if not designated (so it passes the screening against the sanctions list), is actually controlled by a designated persons (e.g. news on local press that a company is controlled by a Syrian businessperson) (adverse).

3. **The risk of circumvention of export bans via countries that have not joined the efforts of the EU and its partners is elevated. What is the European Commission doing to ensure that Russia does not evade sanctions in this way?**
Last update: 5 April 2022

Окремий акцент зроблено на проблемах запобігання обходу санкцій через треті країни, які не приєдналися до санкційних обмежень. Європейська комісія співпрацює з національними органами країн-членів для відстеження таких випадків та запровадила анонімний інструмент повідомлення про можливі порушення. Документ також уточнює, що відповідальність за імплементацію санкцій лежить насамперед на національних органах, які уповноважені виявляти та розслідувати випадки порушення.

Складність виявлення бенефіціарної власності, особливо у випадках з російськими компаніями, описана як серйозна проблема. Постачальники послуг повинні самостійно визначати структуру власності, використовуючи інформацію з доступних джерел, а також створювати механізми для ідентифікації «червоних прапорів», які можуть свідчити про ризик обходу санкцій.

Документ детально аналізує юридичні аспекти понять «навмисно» та «усвідомлено» у контексті порушень санкційного законодавства. Пояснюється, що участь у діях, які можуть мати наслідком порушення санкцій, навіть якщо це не є прямою метою, все одно може розглядатися як порушення. Особливу увагу приділено питанням захисту від відповідальності: постачальникам послуг, які не провели належну перевірку, не надається імунітет від відповідальності навіть за ненавмисні порушення. Вимоги до перевірки включають як мінімум скринінг усіх сторін транзакції, контроль товарів на предмет відповідності регуляціям подвійного призначення, а також оцінку ризиків, пов'язаних із фінансовими потоками, маршрутом доставки та кінцевим використанням продукції.

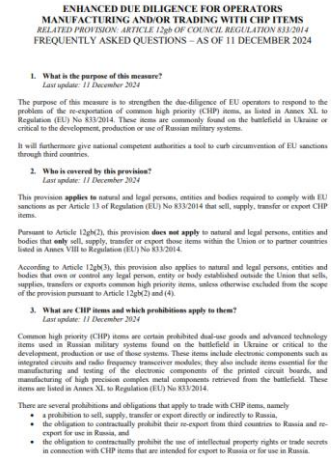
Документ є важливим ресурсом для розуміння обов'язків бізнесу в межах санкційного режиму ЄС, зокрема у контексті посиленої перевірки та запобігання обходу санкцій. Він підкреслює необхідність стратегічного підходу до оцінки ризиків та впровадження комплексних процедур комплаєнсу.

Посилена перевірка торгівлі товарами високого пріоритету: інструмент запобігання обходу санкцій ЄС[13]

Документ присвячений питанням посиленої перевірки (EDD) для постачальників послуг, які виробляють або торгують товарами високого пріоритету (CHP), у контексті санкцій

[13] https://finance.ec.europa.eu/document/download/6d765a17-b609-4282-9b99-9afef38bb545_en?filename=faqs-sanctions-russia-chp-due-diligence_en.pdf

Європейського Союзу, запроваджених у зв'язку з агресією росії проти України та залученням білорусі до цього конфлікту. Основна мета заходів, передбачених статтею 12gb Регламенту Ради (ЄС) №833/2014, полягає в посиленні контролю над експортом і торгівлею CHP-товарами, аби запобігти їх повторному експорту до росії через треті країни. Такі товари є критично важливими для російських військових систем, використовуються на полі бою або є ключовими у виробництві військової техніки.



ENHANCED DUE DILIGENCE FOR OPERATORS MANUFACTURING AND/OR TRADING WITH CHP ITEMS
RELATED PROVISION: ARTICLE 12gb OF COUNCIL REGULATION 833/2014
FREQUENTLY ASKED QUESTIONS – AS OF 11 DECEMBER 2024

1. What is the purpose of this measure?
Last update: 11 December 2024

The purpose of this measure is to strengthen the due-diligence of EU operators to respond to the problem of the re-exportation of common high priority (CHP) items, as listed in Annex XL to Regulation (EU) No 833/2014. These items are commonly found on the battlefield in Ukraine or critical to the development, production or use of Russian military systems.

It will furthermore give national competent authorities a tool to curb circumvention of EU sanctions through third countries.

2. Who is covered by this provision?
Last update: 11 December 2024

This provision **applies to** natural and legal persons, entities and bodies required to comply with EU sanctions as per Article 13 of Regulation (EU) No 833/2014 that sell, supply, transfer or export CHP items.

Pursuant to Article 12gb(2), this provision **does not apply** to natural and legal persons, entities and bodies that **only** sell, supply, transfer or export those items within the Union or to partner countries listed in Annex VIII to Regulation (EU) No 833/2014.

According to Article 12gb(3), this provision also applies to natural and legal persons, entities and bodies that own or control any legal person, entity or body established outside the Union that sells, supplies, transfers or exports common high priority items, unless otherwise excluded from the scope of the provision pursuant to Article 12gb(2) and (4).

3. What are CHP items and which prohibitions apply to them?
Last update: 11 December 2024

Common high priority (CHP) items are certain prohibited dual-use goods and advanced technology items used in Russian military systems found on the battlefield in Ukraine or critical to the development, production or use of those systems. These items include electronic components such as integrated circuits and radio frequency transceiver modules; they also include items essential for the manufacturing and testing of the electronic components of the printed circuit boards, and manufacturing of high precision complex metal components retrieved from the battlefield. These items are listed in Annex XL to Regulation (EU) No 833/2014.

There are several prohibitions and obligations that apply to trade with CHP items, namely

- a prohibition to sell, supply, transfer or export directly or indirectly to Russia,
- the obligation to contractually prohibit their re-export from third countries to Russia and re-export for use in Russia, and
- the obligation to contractually prohibit the use of intellectual property rights or trade secrets in connection with CHP items that are intended for export to Russia or for use in Russia.

Положення поширюються на осіб та організації, які підпадають під дію санкцій ЄС, включаючи суб'єктів, що прямо чи опосередковано контролюють діяльність компаній за межами ЄС, які беруть участь у торгівлі CHP-товарами. Виняток становлять лише ті постачальники послуг, які працюють виключно в межах Союзу або з країнами-партнерами, зазначеними в додатках до регламенту.

CHP-товари включають високотехнологічну продукцію, таку як електронні компоненти (мікросхеми, радіочастотні модулі), обладнання для виробництва друкованих плат і високоточні металеві деталі. Їхній експорт до росії прямо заборонений, як і використання будь-яких пов'язаних із ними інтелектуальних прав. Постачальники послуг повинні також забезпечити виконання контрактних положень, що запобігають повторному експорту таких товарів із третіх країн до росії.

Документ надає детальні рекомендації для операторів щодо впровадження ефективних процедур посиленої перевірки. Перш за все, це адаптація ризик-орієнтованого підходу, що передбачає глибоку перевірку контрагентів, кінцевих користувачів і логістичних маршрутів. Наприклад, рекомендується аналізувати історію діяльності партнерів, їхню взаємодію із санкціонованими особами, походження фінансових потоків, а також зміни у власницькій структурі після запровадження санкцій.

Серед ключових ризиків відзначено використання посередників та компаній-оболонок, участь партнерів із країн, відомих як «хаби обходу санкцій», і складні корпоративні структури, які можуть маскувати зв'язок із санкціонованими особами. Особлива увага приділяється транспортним маршрутам: наявність непрямих перевезень через такі «хаби» має розглядатися як серйозний сигнал для перевірки.

Документ також підкреслює важливість регулярного оновлення аналізу ризиків і навчання персоналу, що займається питаннями дотримання санкцій. Оператори повинні розробити внутрішні політики й процедури для моніторингу життєвого циклу товарів, ведення обліку та забезпечення відповідності. Крім того, документ заохочує залучення вищого керівництва до управління ризиками, включаючи регулярний звіт про ризики та заходи, вжиті для їх мінімізації.

Національні компетентні органи мають право перевіряти виконання цих вимог і застосовувати санкції до порушників. Якщо виявлено, що CHP-товар потрапив до росії через третю країну, це може розглядатися як порушення положень ЄС щодо EDD, навіть якщо оператор діяв через посередників. Документ рекомендує операторам звітувати про підозрілі випадки відповідним органам, зокрема фінансовим розвідкам та митним службам.

Таким чином, цей документ є детальним посібником для операторів, які торгують CHP-товарами, і містить як теоретичні положення, так і практичні інструменти для забезпечення дотримання санкцій ЄС та запобігання їх обходу.

Віртуальні IBAN: Виклики та рекомендації у контексті протидії відмиванню коштів і фінансуванню тероризму[14]

Документ містить рекомендації для підзвітних суб'єктів щодо застосування вимог протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ) під час відкриття та управління платіжними рахунками з віртуальними IBAN (vIBAN). Віртуальні IBAN – це інноваційний інструмент, який дозволяє створювати додаткові IBAN, прив'язані до одного основного рахунку (master account), і активно використовується у нових бізнес-моделях, зокрема в моделях «IBAN as a Service» (IBANaaS). Такі рішення поширюються як між фінансовими установами, так і між банками та клієнтами, забезпечуючи можливість проведення платежів і управління фінансовими потоками з більшою гнучкістю. Однак вони створюють додаткові ризики у сфері ПВК/ФТ через потенційну складність у забезпеченні прозорості, відстеженні транзакцій та ідентифікації бенефіціарів.

Документ аналізує основні ризики, пов'язані з використанням vIBAN, акцентуючи увагу на складнощах моніторингу фінансових потоків. Зокрема, віртуальні IBAN можуть ускладнювати виявлення підозрілих транзакцій, маскувати кінцевого бенефіціарного власника та створювати перешкоди для фінансових установ і регуляторів у відстеженні підозрілої активності. Враховуючи ці загрози, нові європейські нормативні акти, такі як VI Директива у сфері ПВК та Регламент у сфері ПВК (2024), включають vIBAN у перелік обов'язкових елементів для централізованих реєстрів рахунків, вимагаючи більш суворого підходу до їх моніторингу та використання.

Висновки:

- **Зміцнення контролю за фінансовими потоками:** Необхідно впроваджувати індивідуальний моніторинг vIBAN та аналізувати їхню активність окремо від головного рахунку.
- **Посилена перевірка клієнтів:** Суб'єкти зобов'язані ідентифікувати кінцевого бенефіціарного власника, особливо в контексті ОВО-операцій.
- **Гармонізація підходів до ризиків:** Інтеграція рекомендацій Європейського банківського органу (ЕВА) щодо управління ризиками vIBAN та впровадження найкращих практик.
- **Розробка спеціалізованих політик:** Банки повинні створити внутрішні політики для чіткої класифікації клієнтів та ризиків, пов'язаних із використанням vIBAN, особливо у багатонаціональних бізнес-моделях.

Документ також містить результати інспекцій, проведених у 2023 році, які виявили, що послуги vIBAN здебільшого використовуються великими корпораціями для оптимізації управління фінансовими потоками. Проте багато банків не адаптували свої політики до специфіки vIBAN, а заходи моніторингу часто обмежуються головним рахунком, не враховуючи операції, проведені через додаткові віртуальні IBAN. Це знижує ефективність виявлення ризиків відмивання коштів або фінансування тероризму.

Європейський банківський орган (ЕВА) у своєму звіті від травня 2024 року надав детальний огляд шести основних моделей бізнесу, пов'язаних із використанням vIBAN, зазначивши їх переваги та ризики. Звіт підкреслює важливість координації національних регуляторів та впровадження єдиних стандартів для управління цими ризиками.

Документ надає низку рекомендацій для

[14] https://www.bancaditalia.it/compiti/vigilanza/normativa/orientamenti-vigilanza/Comunicazione-BdI-UIF-vIBAN.pdf

суб'єктів, які пропонують послуги з використанням vIBAN. Зокрема, рекомендується посилити заходи ідентифікації та перевірки кінцевих бенефіціарів, особливо у випадках, коли vIBAN використовуються для операцій за дорученням третіх сторін («On Behalf Of» або OBO-операції). Рекомендується здійснювати моніторинг транзакцій на рівні окремих vIBAN, а не лише головного рахунку, щоб своєчасно виявляти потенційні відхилення від заявлених цілей або підозрілу активність. Також наголошується на важливості створення внутрішніх політик, які чітко визначають вимоги до клієнтів, процедур перевірки та управління ризиками.

Окремо документ зазначає про важливість кооперації між суб'єктами фінансового ринку, зокрема обмін інформацією між постачальниками платіжних послуг і банками щодо антиризикових заходів, прийнятих для клієнтів, які використовують vIBAN. Це сприятиме підвищенню прозорості та покращенню виявлення ризиків. Також підкреслюється необхідність розробки інструментів для автоматизованого визначення віртуальної природи IBAN, що може спростити моніторинг для суб'єктів.

Таким чином, документ пропонує детальний аналіз ризиків і викликів, пов'язаних із використанням віртуальних IBAN, і надає чіткі рекомендації щодо впровадження заходів з управління ризиками, щоб забезпечити ефективну протидію ВК/ФТ у цій сфері.

Регулювання

Регулювання ШІ у фінансовому секторі: останні події та основні виклики[15]

Документ досліджує сучасні тенденції та виклики регулювання штучного інтелекту (ШІ) у фінансовій сфері. Він виділяє ключові аспекти використання ШІ банками та страховими компаніями, аналізує нормативно-правові підходи різних країн і дає рекомендації для регуляторів.

ШІ вже відіграє значну роль у фінансовій сфері. Його основні кейси включають використання чат-ботів для підтримки клієнтів, виявлення шахрайства, а також андеррайтинг у банківській і страховій діяльності. Наприклад, ШІ допомагає оцінювати кредитоспроможність, автоматизувати процеси оцінки ризиків і поліпшувати клієнтський досвід. Проте зростання використання ШІ супроводжується такими ризиками, як непрозорість моделей, кіберзагрози, упередженість у даних і репутаційні ризики.

Документ наголошує на тому, що регуляторні органи переважно застосовують технологічно нейтральний підхід, інтегруючи управління ШІ в існуючі рамки регулювання. Однак існує потреба у специфічних рекомендаціях для вирішення унікальних викликів ШІ, таких як:

- Управління ризиками моделей: Відсутність пояснюваності ускладнює оцінку моделей, що може призвести до помилкових рішень.
- Прозорість і підзвітність: Необхідно забезпечити, щоб дані, на яких базуються моделі ШІ, були зрозумілими та надійними.
- Захист даних і безпека: Використання ШІ вимагає суворого дотримання норм конфіденційності та управління даними.

[15] https://www.bis.org/fsi/publ/insights63.htm

- Роль третіх сторін: Регулятори повинні впроваджувати механізми для управління залежністю фінансових установ від зовнішніх постачальників технологій.

Висновки:

- **ШІ трансформує фінансову сферу, але посилює ризики**. Необхідно покращувати моделі управління ризиками, особливо щодо прозорості, пояснюваності та захисту даних.
- **Регулятори повинні уточнити існуючі рамки регулювання.** Важливо надати чіткі рекомендації щодо використання ШІ в андеррайтингу, виявленні шахрайства та інших ключових напрямках.
- **Роль людського контролю є критичною**. У складних сценаріях необхідно забезпечувати "людину в контурі*", щоб мінімізувати негативні наслідки рішень ШІ.
- **Міжнародна співпраця та стандартизація**. Відсутність єдиного глобального визначення ШІ ускладнює регуляторну гармонізацію. Необхідна скоординована робота країн і міжнародних організацій для забезпечення сумісності нормативних актів.

** Фраза "людина в контурі" (human-in-the-loop) стосується концепції, коли у процесі роботи системи штучного інтелекту (ШІ) передбачається обов'язкова участь людини для прийняття ключових рішень або моніторингу процесу. Це забезпечує додатковий рівень контролю, знижує ризики помилок і дозволяє уникнути автоматизації критично важливих рішень без належної перевірки.*

ШІ може значно покращити ефективність і продуктивність фінансових установ, але потребує чіткої регуляторної структури для запобігання можливим негативним наслідкам, таким як дискримінація або шахрайство. Документ закликає до міжнародної співпраці для гармонізації підходів до регулювання ШІ.

Глобальне регулювання криптоактивів: тенденції, виклики та уроки з міжнародного досвіду[16]

Документ є масштабним дослідженням, яке надає глибокий аналіз сучасного регуляторного середовища криптоактивів у світі. У ньому розглядаються стратегії, підходи та практики, які різні країни та юрисдикції застосовують до регулювання цього динамічного і складного сектору. Основною метою є з'ясування, як регуляторні підходи відрізняються між собою, де вони збігаються, і які уроки можна винести для майбутньої розробки законодавчих рамок.

Дослідження починається з аналізу термінології, класифікації та таксономії криптоактивів. Автори відзначають, що навіть у глобальному масштабі немає єдиної усталеної термінології. Найпоширенішими термінами залишаються «криптоактив» та «віртуальний актив», хоча їх значення може суттєво відрізнятися залежно від юрисдикції. Документ також підкреслює важливість класифікації криптоактивів, оскільки вона визначає, які законодавчі рамки застосовуються до певного виду активів. Пропонуються два основні підходи до класифікації: функціональний, що

[16] https://www.jbs.cam.ac.uk/wp-content/uploads/2024/10/2024-2nd-global-cryptoasset-regulatory-landscape-study.pdf

базується на економічному призначенні активів, та технічний, що враховує їх технологічні особливості.

Наступний важливий аспект стосується регуляторних стратегій. Юрисдикції поділяються на три основні категорії: ті, що забороняють криптоактиви, адаптують існуюче законодавство до їх регулювання або розробляють спеціальні, так звані закоконодавчі рамки, адаптовані до конкретних потеб. Документ зазначає, що країни, що розвиваються, часто вдаються до заборон, мотивуючи це ризиками доларизації та відтоку капіталу, тоді як розвинена економіка адаптує своє законодавство для забезпечення більшої гнучкості та підтримки інновацій.

Особлива увага приділяється регулюванню стейблкоїнів, які відіграють ключову роль у криптоекосистемі завдяки своїй стабільності щодо фіатних валют. Документ аналізує, як різні країни регулюють емітентів стейблкоїнів, встановлюють вимоги до резервів і забезпечують прозорість їх діяльності. Стейблкоїни системного значення викликають особливу увагу через їх потенційний вплив на макроекономічну стабільність.

Ще одним важливим розділом є аналіз діяльності постачальників послуг криптоактивів (CASP). Різні країни запроваджують вимоги до їх авторизації, встановлюють правила для зберігання активів клієнтів, наприклад, у холодних гаманцях, та регулюють такі послуги, як стейкінг. Документ відзначає, що офшорна діяльність CASP є значним викликом для регуляторів, оскільки такі провайдери часто уникають місцевих правил.

Документ також розглядає інші важливі аспекти, такі як протидія відмиванню коштів (ПВК) і фінансуванню тероризму (ФТ), захист прав споживачів та заходи щодо обмеження доступу до ризикових фінансових продуктів для роздрібних інвесторів. Автори підкреслюють, що ефективна інтеграція міжнародних стандартів, таких як рекомендації FATF, є ключовим фактором для посилення глобальної регуляторної координації.

На завершення документ пропонує уроки, винесені з аналізу різних підходів, які можуть бути корисними для країн, що тільки розробляють свої регуляторні рамки. Зокрема, наголошується на важливості чіткої класифікації криптоактивів, поступового зняття обмежень для забезпечення макроекономічної стабільності та створення умов для інновацій через пісочниці або пільгові режими.

Загалом, дослідження є важливим джерелом для регуляторів, які прагнуть створити збалансовані рамки для криптоактивів, що забезпечуватимуть одночасно інновації, стабільність і захист інвесторів.

Висновки:

- **Необхідність гармонізації термінології та підходів до класифікації криптоактивів:** Відсутність єдиної системи ускладнює регуляторну співпрацю між країнами, особливо для визначення меж регулювання.
- **Пріоритетність регуляції стейблкоїнів та CASP:** Юрисдикції мають забезпечити відповідність активів стандартам стабільності та безпеки, зосередившись на резервних вимогах і обмеженнях офшорних операцій.
- **Глобальні стандарти FATF:** Важливо інтегрувати рекомендації FATF щодо ПВК/ФТ у національні регуляторні рамки для посилення контролю над незаконними потоками коштів.
- **Розробка спеціалізованих політик:** Банки повинні створити внутрішні політики для чіткої класифікації клієнтів та ризиків, пов’язаних із використанням vIBAN, особливо у багатонаціональних бізнес-моделях.

Інструкції щодо шаблонів для пояснень і висновків, а також стандартизованого тесту для класифікації криптоактивів відповідно до статті 97(1) Регламенту (ЄС) 2023/1114[17]

Документ, підготовлений європейськими наглядовими органами (ESAs), спрямований на впровадження єдиного підходу до класифікації криптоактивів у межах Європейського Союзу відповідно до статті 97(1) Регламенту (ЄС) 2023/1114 (MiCAR). Основною метою цих настанов є забезпечення гармонізації процесів регуляторного аналізу криптоактивів, підвищення прозорості для учасників ринку та компетентних органів, а також створення правової визначеності для всіх залучених сторін. MiCAR встановлює регулювання для публічних пропозицій криптоактивів, токенів, пов'язаних з активами (ART), токенів електронних грошей (EMT), а також інших криптоактивів, визначаючи їхню природу та зобов’язання щодо їх використання на ринку.

Настанови пропонують стандартизовані шаблони для надання пояснень та юридичних висновків, які мають бути підготовлені як внутрішніми, так і зовнішніми юридичними радниками. Ці шаблони передбачають заповнення структурованих полів із деталізованою інформацією, такою як нормативна база, що стосується активу, аргументи щодо його відповідності критеріям MiCAR, а також додаткові аспекти, які допомагають забезпечити чіткість і обґрунтованість класифікації. Це сприяє гармонізації документів, які учасники ринку подають до компетентних органів для обґрунтування свого статусу відповідно до регламенту.

У документі також описаний стандартизований тест для класифікації криптоактивів, який враховує ключові критерії MiCAR, такі як природа активу, його зв'язок із забезпеченням вартості чи прав, а також взаємозамінність. Тест надає системний підхід до оцінки активів і враховує як чинне законодавство ЄС, так і судову практику та національні нормативно-правові акти. Це дозволяє компетентним органам ефективно оцінювати активи, знижуючи ризики помилкової класифікації чи регуляторного арбітражу.

Однією з основних переваг таких рекомендацій є уніфікація процесів у межах усіх країн ЄС, що знижує потенційні розбіжності в регулюванні між юрисдикціями та створює рівні умови для учасників ринку. Це також сприяє зменшенню адміністративного

Висновки:

- **Узгодженість класифікації криптоактивів є критично важливою**. Стандартизований підхід до класифікації забезпечує однакове застосування MiCAR по всій території ЄС.
- **Шаблони спрощують процес звітності для ринкових учасників**. Деталізовані форми для пояснень і юридичних висновків зменшують непорозуміння та допомагають уникнути дублювання запитів.
- **Необхідність широкого врахування правової бази**. Для точної класифікації необхідно враховувати судову практику, нормативно-правові акти та рекомендації як на рівні ЄС, так і на національному рівні.
- **Гармонізація підвищує прозорість і довіру**. Уніфіковані підходи сприяють забезпеченню рівних умов для всіх учасників ринку та зміцненню фінансової стабільності.

[17] https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/asset-referenced-and-e-money-tokens-micar/esas-guidelines-templates-explanations-and-opinions-and-standardised-test-classification-crypto

навантаження на бізнес, адже гармонізовані шаблони дозволяють уникати дублювання запитів чи різночитань вимог. Учасники ринку отримують чітке уявлення про свої регуляторні зобов'язання, що підвищує довіру до регуляторної системи загалом.

Однак у документі також підкреслюються виклики, з якими стикаються регулятори. Зокрема, це питання інтерпретації окремих термінів, таких як "вартість" чи "право", а також складності класифікації унікальних чи гібридних активів, наприклад, NFT. Такі активи можуть мати характеристики, які одночасно відповідають декільком категоріям, що вимагає додаткової уваги та аналізу.

Ці настанови також враховують глобальні тенденції у регулюванні криптоактивів, акцентуючи на важливості міжнародної співпраці. Відсутність уніфікованого підходу на глобальному рівні може створити ризики регуляторного арбітражу між ЄС та іншими юрисдикціями, тому гармонізація регуляторної практики є ключовою умовою для ефективного розвитку цього ринку. Настанови спрямовані на те, щоб забезпечити цілісність фінансової системи та підтримати стабільність у контексті швидкого розвитку криптосфери.

Санкції

Санкції США проти Integrity Technology Group: боротьба з кібершпигунством у глобальному масштабі[18]

Публікація висвітлює санкції, запроваджені урядом США проти китайської компанії Integrity Technology Group, яка була викрита у співпраці з державним хакерським угрупованням Flax Typhoon. Це угруповання, підтримуване урядом Китаю через Міністерство державної безпеки, спеціалізується на проведенні кібератак проти критичної інфраструктури, урядових установ, телекомунікаційних компаній, університетів та медіаорганізацій, як у США, так і в інших країнах. Компанія Integrity Technology надавала технічну інфраструктуру для діяльності цих хакерських груп, що дозволило їм успішно здійснювати атаки з використанням шкідливих бот-нетів.

Виявлено, що у період із 2022 по 2023 рік Integrity Technology надавала засоби для розгортання та управління бот-нетом, що включав понад 260 тисяч інфікованих пристроїв, серед яких були пристрої, такі як камери, відеореєстратори та системи зберігання даних. Ці пристрої, заражені шкідливим програмним забезпеченням, дозволяли зловмисникам отримувати доступ до внутрішніх мереж компаній та установ, виконувати команди та розширювати атаки на нові цілі. Для управління цим бот-нетом Integrity Technology створила онлайн-додаток "KRLab", який надавав зручний інтерфейс для контролю над інфікованими пристроями.

Integrity Technology також відома у Китаї як провідний розробник "кіберполігонів" — навчальних платформ, що імітують реальні цифрові системи для тренувань у кібербезпеці. Компанія активно брала участь у підтримці національних кіберзмагань і мала значне фінансування від державних структур. Вона вважається важливим елементом у мережі приватних компаній, залучених до реалізації хакерських кампаній, організованих Китаєм.

[18] https://therecord.media/us-sanctions-chinas-integrity-cyber-company-flax-typhoon?utm_source=newsletter.illicitedge.com&utm_medium=newsletter&utm_campaign=ccp-houthis-credit-suisse-scandals-and-russian-sting

Санкції, запроваджені США, передбачають заморожування активів Integrity Technology на території країни, обмеження її фінансових операцій і заборону співпраці з американськими компаніями. Це стало черговим кроком у боротьбі з китайськими державними кібероперaціями, які становлять серйозну загрозу для безпеки США та їхніх партнерів. Окрім безпосереднього впливу на Integrity Technology, санкції мають на меті підрив економічних і технічних можливостей Китаю у сфері кібершпигунства.

Документ також акцентує увагу на необхідності міжнародної співпраці у сфері кібербезпеки для обміну інформацією про загрози, впровадження стандартів моніторингу та створення механізмів для попередження подібних атак у майбутньому. США вбачають в таких санкціях не лише спосіб захисту своїх інтересів, але й сигнал для інших країн про необхідність більш рішучих дій проти зловмисників у кіберпросторі.

Санкції США проти Ірану та Росії: Захист демократії від зовнішнього втручання у вибори 2024 року [19]

Управлінням з контролю за іноземними активами (OFAC) Міністерства фінансів США запроваджені санкційні заходи, спрямовані на протидію втручанню Ірану та Росії у президентські вибори США 2024 року. Ці заходи є частиною ширшої стратегії захисту демократичних процесів від зовнішніх загроз.

Згідно з публікацією, Іран використовував підконтрольну організацію Cognitive Design Production Center (CDPC), яка підпорядковується Ісламському революційному гвардійському корпусу (IRGC), для здійснення впливу на громадську думку в США. CDPC займався розробкою та впровадженням операцій, спрямованих на посилення соціально-політичної напруги, використовуючи методи соціальної інженерії, доступ до конфіденційної інформації ключових осіб виборчих кампаній та її подальше використання для дискредитації та маніпуляції. Раніше OFAC вже вводив санкції проти окремих представників Ірану та пов'язаних з IRGC організацій за схожі дії під час виборів 2020 року.

Росія, у свою чергу, вдалася до застосування складних механізмів дезінформації, побудованих на технологіях штучного інтелекту. Москва використовувала підконтрольний Центр геополітичної експертизи (CGE), який пов'язаний із Головним розвідувальним управлінням (GRU). CGE розробляв та поширював фейковий контент, включаючи маніпулятивні відео та фейкові відео (deepfakes), через розгалужену мережу веб-сайтів, які імітували незалежні новинні джерела. Організація створила сервер для роботи з генеративними AI-інструментами, що дозволило уникати блокувань на іноземних хостинг-платформах. Фінансування таких операцій здійснювалося безпосередньо через GRU, що також забезпечувало підтримку мережі фальшивих веб-сайтів і технічного обладнання.

Санкції, накладені OFAC, передбачають блокування всіх активів організацій і осіб, причетних до цих дій, у юрисдикції США. Забороняються будь-які фінансові операції з ними, а також

[19] https://home.treasury.gov/news/press-releases/jy2766

діяльність, яка може сприяти обходу санкцій. В документі наголошується, що такі заходи є не лише способом покарання, а й інструментом стимулювання до зміни поведінки порушників.

Документ також підкреслює важливість санкцій як інструменту захисту демократії та закликає до координації між державними і приватними суб'єктами для посилення безпеки та стійкості до кіберзагроз. Важливим є й інформування громадськості про ці заходи, оскільки це сприяє зміцненню довіри до демократичних інститутів та підвищує готовність протистояти втручанню.

Звіти окремих інституцій та експертів

Готівка у злочинному світі: чи залишається вона королевою у цифрову епоху? [20]

Документ присвячений аналізу ризиків відмивання коштів та фінансування тероризму, пов'язаних із дистанційним обслуговуванням клієнтів (Non-Face-to-Face, NFTF), а також ефективним заходам з ПВК для їхнього управління. Ризики NFTF-клієнтів виникають через відсутність фізичного контакту, що ускладнює визначення їхньої справжності, та можливість використання підроблених документів, приховування бенефіціарної власності, структурування операцій і транскордонних транзакцій. Документ детально розглядає типології ВК/ФТ, включаючи смурфінг і дроблення транзакцій, які дозволяють уникати уваги регуляторів.

У відповідь на ці виклики рекомендовано впровадження ризик-орієнтованого підходу (РОП), що передбачає оцінку ризиків залежно від типу клієнта, галузі та географічного розташування. Особливу увагу приділено впровадженню інноваційних технологій, таких як штучний інтелект, машинне навчання та блокчейн, для автоматизації ідентифікації клієнтів та моніторингу транзакцій. Важливим елементом є використання відеоконференцій для безпечного підтвердження особи клієнтів та постійний моніторинг транзакцій для виявлення аномальних шаблонів. Документ також пропонує практичні інструменти та покрокові інструкції, які сприяють зниженню ризиків ML/TF при дистанційному обслуговуванні клієнтів, забезпечуючи при цьому відповідність регуляторним вимогам.

Висновки:

- **Ризик-орієнтований підхід є ключовим**: Регульовані установи мають впроваджувати індивідуальні процедури оцінки ризиків, враховуючи тип клієнтів, географію та галузеві особливості.
- **Технології покращують AML-процедури**: Використання AI, машинного навчання та блокчейну сприяє точності ідентифікації NFTF-клієнтів та мінімізації ризиків ML/TF.
- **Роль відеоконференцій у KYC**: Запровадження відеоідентифікації дозволяє регульованим установам проводити безпечніші та ефективніші перевірки особистості клієнтів.
- **Моніторинг транзакцій як обов'язковий елемент**: Постійне відстеження транзакцій для виявлення аномальних шаблонів або поведінки є критичним для запобігання фінансовим злочинам.

[20] https://amluae.com/ebook-on-aml-strategies-to-address-ml-tf-risks-from-non-face-to-face-customers/

Глобальний звіт про відкритий банкінг і відкриті фінанси[21]

Документ є детальним дослідженням поточного стану відкритого банкінгу (Open Banking) та відкритого фінансування (Open Finance) у 95 юрисдикціях. Він аналізує підходи до впровадження цих систем, їхній вплив на фінансові ринки, політичні цілі та регуляторні виклики.

Основний акцент зроблено на двох моделях управління: регуляторно орієнтованій (regulation-led) та ринково орієнтованій (market-driven). Регуляторно орієнтована модель, яка реалізована у 54 юрисдикціях, спрямована на забезпечення широкого доступу до даних через встановлення обов'язкових стандартів і правил. Ринково орієнтована модель, яка діє у 28 юрисдикціях, покладається на комерційні домовленості між учасниками ринку.

Звіт також висвітлює розбіжності у впровадженні відкритого фінансування: лише 16 юрисдикцій прийняли відповідне законодавство, і навіть там основна увага приділяється обмеженій кількості фінансових продуктів. Серед ключових політичних цілей регуляторів виділяються підвищення конкуренції, сприяння фінансовій інклюзії, стимулювання інновацій та посилення захисту клієнтів.

Особливий інтерес викликають регіональні відмінності. У Європі, Центральній Азії та на Близькому Сході домінує регуляторний підхід, тоді як у Африці південніше Сахари та Азіатсько-Тихоокеанському регіоні переважає ринковий. Крім того, дослідження розглядає вплив цифрової інфраструктури, стандартів, технологій (наприклад, API) та довіри учасників ринку як ключових факторів успішного впровадження.

Документ включає тематичні дослідження для таких юрисдикцій, як Бразилія, Індія, ЄС, Велика Британія, США та ОАЕ, де висвітлюються практичні аспекти впровадження та досягнуті результати. У ньому також визначено основні виклики, зокрема забезпечення балансу між доступом до даних і захистом конфіденційності, а також питання адаптації регуляторних рамок до швидко змінюваних технологій.

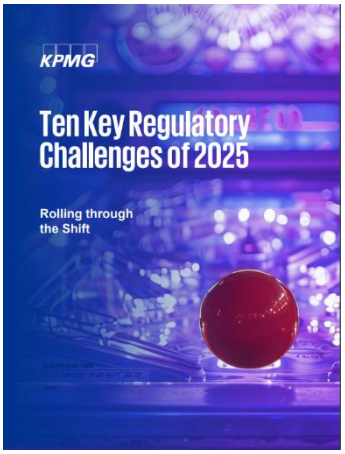
Висновки:

- **Регуляторно орієнтований підхід є більш ефективним у забезпеченні доступу до даних**, скорочуючи час впровадження на 22% у порівнянні з ринково орієнтованим підходом.
- **Цифрова інфраструктура та стандарти відіграють критичну роль** у побудові довіри між учасниками ринку, забезпечуючи взаємодію та захист даних.
- **Юрисдикції з фокусом на фінансову інклюзію (наприклад, Індія)** демонструють успішні приклади інтеграції цифрової ідентифікації та мобільних технологій у фінансові системи.
- **Обмежене розширення відкритого фінансування** свідчить про потребу вдосконалення регуляторних рамок для охоплення ширшого спектру фінансових продуктів.

[21] https://www.jbs.cam.ac.uk/wp-content/uploads/2024/11/2024-ccaf-the-global-state-of-open-banking-and-open-finance.pdf

Десять ключових регуляторних викликів 2025 року[22]

Документ KPMG аналізує основні тенденції та виклики, які визначатимуть регуляторний ландшафт у 2025 році. Ці тенденції зумовлені поєднанням технологічного прогресу, посиленням цифровізації, геополітичних змін, нових адміністративних пріоритетів і зростанням розбіжностей у регуляторних вимогах між різними юрисдикціями. У звіті підкреслюється, що організації мають бути готові до збільшення обсягів, складності та впливу нормативної бази, адаптуючи свої підходи до управління ризиками, відповідності та стійкості.



Одним із головних викликів визначено регуляторну дивергенцію, яка посилює ризики через відмінності у вимогах між глобальними, федеральними та локальними регуляціями. Це створює додаткові бар'єри для компаній, які працюють на міжнародних ринках. Очікується, що організації повинні впроваджувати динамічні підходи до адаптації, щоб зберігати відповідність у змінному правовому середовищі та мінімізувати репутаційні й операційні ризики.

Технології, зокрема штучний інтелект (ШІ), стали центральним об'єктом уваги регуляторів через ризики, пов'язані з непрозорістю алгоритмів, упередженістю даних, порушеннями приватності та кіберзагрозами. Організації повинні впроваджувати управлінські рамки, які забезпечуватимуть прозорість і надійність ШІ, включаючи регулярне тестування та аудит систем.

Кібербезпека також залишається критичним питанням, враховуючи зростання обсягів даних та їх використання третіми сторонами. Регулятори посилюють вимоги до захисту даних, управління доступом та моніторингу кіберзагроз. Організаціям слід інвестувати в передові технології для забезпечення безперервного моніторингу, виявлення вразливостей та своєчасного реагування на інциденти.

У сфері боротьби з фінансовими злочинами очікується розширення регуляторного нагляду за відмиванням коштів (AML), фінансуванням тероризму (CTF) та санкційними ризиками. У звіті наголошується на необхідності посилення процедур ідентифікації бенефіціарів, автоматизації процесів моніторингу транзакцій і залучення кваліфікованих кадрів для боротьби зі зростаючою складністю загроз.

Шахрайство та афери, у тому числі з використанням ШІ, стають серйозною

Висновки:

- **Необхідність гнучкості в умовах регуляторної дивергенції**. Організаціям слід адаптуватися до змінних вимог різних юрисдикцій, розробляючи динамічні підходи до управління ризиками та дотримання вимог.
- **Посилення контролю за ШІ та даними**. Важливо впроваджувати рамки прозорого використання ШІ, дотримуючись стандартів управління ризиками, тестування та перевірки алгоритмів.
- **Підготовка до нових викликів кібербезпеки**. Компаніям слід інвестувати у передові технології для виявлення вразливостей та посилення захисту від кібератак, включаючи управління даними.
- **Боротьба з фінансовими злочинами та шахрайством.** Інтеграція сучасних інструментів моніторингу транзакцій, вдосконалення процесів KYC/AML і посилення контролю за сторонніми контрагентами є пріоритетом.

[22] https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/ten-key-regulatory-challenges-of-2025.pdf

загрозою для компаній і споживачів. Регулятори зосереджуються на забезпеченні прозорості моделей виявлення шахрайства, посиленні автентифікації користувачів і впровадженні навчальних кампаній для підвищення обізнаності клієнтів про ризики.

Регуляторний ландшафт також вимагає підвищеної уваги до справедливості та захисту споживачів. Очікується, що на рівні штатів буде розширено ініціативи, спрямовані на захист прав споживачів, компенсацію можливих шкод і забезпечення прозорості продуктів та послуг.

Окремий акцент зроблено на фінансовій та операційній стійкості компаній. Регулятори посилять контроль за готовністю компаній до подолання кризових ситуацій, управлінням ліквідністю та забезпеченням безперервності бізнесу. Це включає проведення стрес-тестів, розробку планів реагування на інциденти та впровадження довгострокових стратегій стійкості.

Звіт також приділяє увагу управлінню сторонніми провайдерами та ризиками, які виникають через залежність від постачальників послуг. Організаціям рекомендовано впроваджувати системи моніторингу та аудиту, щоб забезпечити відповідність сторонніх провайдерів нормативним вимогам.

Усі ці виклики підкреслюють необхідність створення ефективних систем управління, прозорості та підзвітності, які відповідатимуть новим регуляторним вимогам та технологічним викликам.

Роль залишкового ризику в комплаєнсі фінансових злочинів[23]

Стаття зосереджується на значенні та управлінні залишковим ризиком у контексті боротьби з фінансовими злочинами, такими як ВК/ФТ/ФР. Залишковий ризик — це рівень ризику, що залишається після застосування всіх можливих заходів контролю та пом'якшення. Його правильне розуміння та управління є ключовими для ефективної комплаєнс-програми в будь-якій організації.

У статті зазначено, що залишковий ризик виникає через неминучі обмеження в ефективності заходів контролю, людські помилки, обмежені ресурси або складність законодавства. Автори підкреслюють, що основна мета організації полягає у зменшенні залишкового ризику до прийнятного рівня шляхом безперервного моніторингу, оцінки та вдосконалення процедур.

Також розглянуто відмінність між внутрішнім ризиком (початковий ризик, що існує до будь-яких дій) та залишковим ризиком. Ця різниця є ключовою для розуміння впливу політик та контролів на загальну ризикову ситуацію.

Автори описують процес оцінки залишкового ризику, який включає ідентифікацію ризикових сценаріїв, аналіз ефективності чинних контролів і прогнозування можливих наслідків. Особливий акцент зроблено на важливості адаптації комплаєнс-підходів до змін у законодавстві, технологіях і схемах фінансових злочинів.

У статті також наголошено на необхідності інтегрувати новітні технології, такі як автоматизація оцінки ризиків, аналіз даних і використання штучного інтелекту, для зменшення рівня залишкового ризику. Зокрема, зазначається, що використання таких інструментів дозволяє точніше визначати області високого ризику та зосереджувати ресурси на найбільш критичних аспектах.

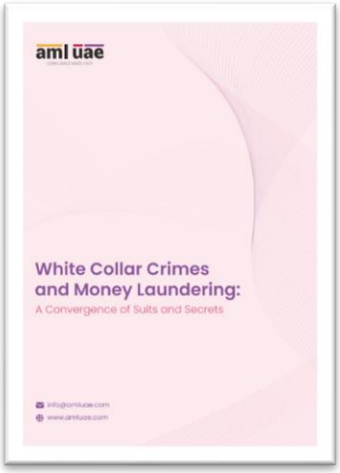
[23] https://amluae.com/the-role-of-residual-risk-in-financial-crime-compliance/

Залишковий ризик визнаний не тільки як технічний чи операційний виклик, а й як стратегічний елемент управління комплаєнсом, що впливає на репутацію організації та її здатність виконувати свої регуляторні зобов'язання.

Висновки:

- **Залишковий ризик є неминучим, але його можна зменшити**. Постійна оцінка контролів, аналіз ризиків і вдосконалення процедур дозволяють утримувати залишковий ризик на прийнятному рівні.
- **Впровадження новітніх технологій є ключовим**. Використання автоматизації, аналізу даних і ШІ дозволяє ефективніше оцінювати та пом'якшувати ризики.
- **Різниця між внутрішнім і залишковим ризиком має бути зрозумілою**. Це дозволяє краще оцінювати ефективність заходів контролю та спрямовувати зусилля на найбільш вразливі області.
- **Комплаєнс-програми мають бути адаптивними до змін**. Розвиток законодавства, технологій та схем фінансових злочинів потребує гнучкого підходу для підтримання ефективного управління ризиками.

Білі комірці та відмивання коштів: сучасні виклики та інноваційні рішення [24]



Документ детально досліджує злочини «білих комірців», їхню природу, методи реалізації, наслідки та взаємозв’язок із відмиванням коштів (ВК) і фінансуванням тероризму (ФТ). Основна ідея тексту полягає у висвітленні складності цих злочинів, їхнього глобального впливу та пропозицій щодо ефективної протидії.

Злочини білих комірців визначаються як ненасильницькі фінансово мотивовані правопорушення, які зазвичай вчиняються кваліфікованими працівниками або управлінцями. Вони використовують свій професійний досвід для маніпуляцій, обману або порушення довіри, спрямованих на особисте збагачення. Характерними рисами цих злочинів є їхній обманний характер, професійна реалізація, технологічна залежність і ретельне планування. Серед прикладів таких злочинів – шахрайство, інсайдерська торгівля, підробка, кіберзлочини, податкові махінації, екологічні злочини та інші.

Документ також підкреслює, що злочини білих комірців тісно пов’язані з відмиванням коштів і фінансуванням тероризму. Через складні багатошарові транзакції, використання підставних компаній та інноваційні методи ці злочини сприяють легалізації незаконних доходів та їх використанню для терористичної діяльності. Злочинці створюють системи для маскування джерела незаконних коштів, інтегруючи їх у легальну фінансову систему. Таким чином, ці злочини не лише шкодять окремим організаціям і економікам, але й створюють загрозу глобальній безпеці.

Окрема увага приділяється складнощам, які виникають у процесі розслідування таких злочинів. Транскордонний характер діяльності, відмінності у законодавстві різних країн,

[24] https://amluae.com/wp-content/uploads/2024/11/White-Collar-Crimes-and-Money-Laundering_A-Convergence-of-Suits-and-Secrets.pdf

технологічні інновації та маніпуляції даними ускладнюють виявлення й переслідування винних. Часто злочинці використовують впливові зв'язки для уникнення відповідальності, що створює додаткові перешкоди для правоохоронних органів.

Одним із центральних аспектів документа є розгляд технологічних інструментів, які можуть допомогти у боротьбі зі злочинами білих комірців. Машинне навчання дозволяє виявляти аномалії у поведінці клієнтів і транзакціях, аналізувати минулі дані для прогнозування потенційних ризиків і здійснювати моніторинг у реальному часі. Технології, як-от Natural Language Processing (NLP), забезпечують аналіз текстових даних, таких як електронні листи або соціальні медіа, для ідентифікації підозрілих поведінкових моделей.

Для ефективної протидії злочинам білих комірців документ рекомендує ряд заходів. До них належать розробка та впровадження ефективного корпоративного управління, навчання персоналу, посилення співпраці між юрисдикціями, створення програм захисту викривачів та використання сучасних технологій для моніторингу і розслідування. Важливим аспектом є гармонізація законодавства на міжнародному рівні, що дозволить уникнути використання правових лазівок.

Висновки:

- **Необхідність впровадження передових технологій:** Використання штучного інтелекту та машинного навчання для виявлення аномалій і аналізу великих обсягів даних є критичним для ефективної боротьби із злочинами білих комірців.
- **Гармонізація законодавства:** Важливо забезпечити узгодження правових норм між різними юрисдикціями для ефективної протидії транскордонним злочинам.
- **Роль корпоративного управління:** Запровадження етичного середовища через кодекси поведінки, прозору звітність і внутрішній аудит мінімізує ризики злочинів усередині компаній.
- **Захист викривачів:** Створення анонімних каналів звітності та програм захисту для співробітників, які повідомляють про злочини, підвищує ймовірність своєчасного виявлення підозрілої активності.

У висновку документ наголошує, що ефективна боротьба з білими комірцями можлива лише за умов тісної співпраці між урядами, бізнесом і суспільством. Підвищення обізнаності, створення прозорого середовища та використання інноваційних технологій здатні мінімізувати ризики і забезпечити більш безпечну економіку та суспільство.

Вплив "Сірого списку" FATF: Виклики, наслідки та шляхи виходу [25]

Документ глибоко аналізує роль "Сірого списку" як ключового інструменту FATF у боротьбі з відмиванням коштів (ML) та фінансуванням тероризму (TF). "Сірий список" або "Юрисдикції під посиленим моніторингом" є переліком країн, що мають стратегічні недоліки у своїх системах протидії відмиванню коштів і фінансуванню тероризму. Перебування у цьому списку означає, що країна недостатньо ефективно впроваджує стандарти FATF і піддається посиленому контролю до моменту, коли ці недоліки будуть усунені. Для країн, які потрапили до списку, FATF встановлює вимоги до вдосконалення їхніх AML/CFT режимів, що включає правові та регуляторні зміни, підвищення ефективності моніторингових органів і вдосконалення процедур контролю та звітності.

[25] https://rapidaml.com/articles/fatf-grey-list-and-its-implications-on-dnfbps-and-vasps/

Основною причиною включення країни до "Сірого списку" є її невідповідність міжнародним стандартам, встановленим FATF, що визначається через "Звіт про взаємну оцінку" (MER). Цей звіт оцінює два ключові аспекти: технічну відповідність (регуляторні рамки, процедури, міжнародну співпрацю) та ефективність (наскільки ці заходи здатні виявляти і зменшувати ризики ВК/ФТ). Невисокі оцінки за цими параметрами означають, що країна не лише має прогалини у своїх законодавчих чи адміністративних заходах, а й фактично не впроваджує їх достатньо ефективно.

Перебування у "Сірому списку" має серйозні наслідки як для самої країни, так і для суб'єктів, що працюють у її юрисдикції. Країна стикається зі значними репутаційними втратами, що можуть призвести до зменшення інвестицій та погіршення економічного клімату. Це також ускладнює міжнародну торгівлю та транзакції через підвищення вимог до перевірки з боку партнерів і фінансових установ. Негативний вплив посилюється у випадку низькорозвинених економік, де доступ до міжнародних ринків є критично важливим. У гіршому випадку, тривала бездіяльність може призвести до потрапляння до "Чорного списку," що тягне за собою ще більш серйозні санкції.

Суттєвий акцент у документі зроблено на впливі на DNFBP (визначені нефінансові установи і професії) та VASP (постачальники послуг у сфері віртуальних активів). Для цих суб'єктів включення країни до "Сірого списку" означає посилення вимог до відповідності, що включає зростання частоти звітності та витрат на процедури перевірки (CDD, KYC). Окрім фінансового тиску, DNFBP та VASP стикаються із ризиками репутації, що ускладнює співпрацю з міжнародними партнерами та доступ до глобальних фінансових послуг. Операційні витрати зростають, а бізнес-процеси стають більш ускладненими через посилений контроль з боку регуляторних органів.

Документ також окреслює шляхи виходу із "Сірого списку." Це включає вирішення стратегічних недоліків через імплементацію міжнародних стандартів FATF, посилення законодавчої бази, модернізацію регуляторних органів, зокрема фінансових розвідок (FIU), та зміцнення міжнародної співпраці. Особлива увага приділяється необхідності розробки та впровадження дієвого плану дій, що дозволить країні виправити недоліки та отримати кращу оцінку у наступному раунді оцінки FATF.

У підсумку, "Сірий список" FATF виконує роль стимулу для країн щодо вдосконалення своїх AML/CFT режимів, водночас посилаючи чіткий сигнал глобальній фінансовій спільноті бути обережними у взаємодії з такими юрисдикціями. Це механізм, що сприяє підвищенню прозорості та довіри до фінансової системи.

Роль вищого керівництва у забезпеченні дотримання вимог ПВК: виклики, недоліки та шляхи вдосконалення[26]

Стаття акцентує увагу на ключовій ролі вищого керівництва у забезпеченні дотримання вимог у сфері протидії відмиванню коштів (ПВК). У матеріалі підкреслюється, що саме керівництво відповідає за розробку та впровадження внутрішніх політик, процедур і контролю, необхідних для ефективного управління ризиками. Ключовими аспектами статті є аналіз недоліків, яких найчастіше припускається керівництво, та рекомендації щодо їхнього усунення. Автори зазначають, що основна відповідальність керівництва полягає у впровадженні ризик-орієнтованого підходу (РОП), розробці ефективних політик, постійному перегляді ризиків, особливо щодо клієнтів високого ризику, таких як політично значущі особи (PEP), та

[26] https://amlindia.in/aml-lapses-by-senior-management-staying-cautious-to-foster-aml-compliance/

моніторингу їхньої діяльності. Наголошується, що недоліки, пов'язані з низьким рівнем обізнаності про законодавчі вимоги, недостатньою підготовкою персоналу, відсутністю належних ресурсів для програм у сфері ПВК або неефективністю внутрішнього контролю, можуть призвести до серйозних наслідків. Серед таких наслідків – регуляторні санкції, зростання ризиків відмивання коштів, шкода репутації компанії.

Особливу увагу приділено важливості навчання персоналу та керівництва. Автори вказують, що недостатня підготовка співробітників і керівників у сфері комплаєнсу є однією з головних причин системних недоліків. Крім того, в статті підкреслюється необхідність регулярного оновлення знань про зміни в законодавстві та впровадження новітніх технологій для моніторингу транзакцій. Таблиця, наведена у статті, чітко окреслює три основні категорії проблем, з якими може стикатися керівництво: недоліки в управлінні ризиками, наслідки таких помилок для компанії та рекомендації щодо їх вирішення. Зокрема, у таблиці йдеться про відсутність належного перегляду політик ПВК, недостатнє управління клієнтами високого ризику та слабку інтеграцію процедур ПВК у бізнес-процеси. Як наслідки таких порушень згадуються штрафні санкції, репутаційні ризики та зростання ймовірності фінансових злочинів.

Автори наголошують на необхідності незалежних внутрішніх і зовнішніх аудитів, які дозволяють своєчасно виявляти прогалини у системах ПВК. Керівництво повинно активно підтримувати культуру комплаєнсу, інтегруючи вимоги ПВК у всі бізнес-операції, забезпечуючи належні ресурси, зокрема фінансування та навчання персоналу. Також підкреслюється важливість впровадження автоматизованих аналітичних систем, здатних ідентифікувати ризикові операції, та створення систем раннього попередження.

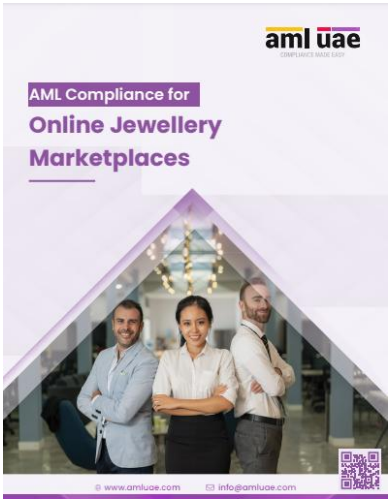
Загальний висновок статті полягає в тому, що ефективність програм ПВК залежить від залученості керівництва, яке має бути першою лінією захисту в боротьбі з фінансовими злочинами. Нульова толерантність до випадків відмивання коштів, інтеграція політик у сфері ПВК у щоденну діяльність компанії та постійний моніторинг ефективності впроваджених заходів є необхідними умовами для зниження ризиків та забезпечення відповідності регуляторним вимогам.

Ефективне впровадження системи ПВК/ФТ на онлайн-ринках ювелірних виробів: виклики, ризики та практичні рішення[27]

Документ аналізує проблемні питання у сфері протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ) у контексті онлайн-ринків торгівлі ювелірними виробами. Ці платформи, які є частиною глобального сектора електронної комерції, з одного боку, створюють значні можливості для розвитку міжнародної торгівлі дорогоцінними металами та камінням, а з іншого — стають привабливим середовищем для зловмисників через низку вразливостей. Анонімність учасників, легкість проведення транскордонних операцій та розбіжності у регуляторних підходах між різними країнами створюють умови для таких

[27] https://amluae.com/wp-content/uploads/2024/11/eBook-on-AML-Compliance-for-Online-Jewellery-Marketplace.pdf

ризиків, як структуризація транзакцій, фальсифікація інвойсів, маніпуляції з документацією та використання підставних осіб.



У вступній частині документ окреслює загальну проблему: висока вартість ювелірних виробів та їхня популярність на міжнародних ринках роблять ці активи вразливими до відмивання доходів, отриманих злочинним шляхом. Особлива увага приділяється тому, як ювелірні ринки можуть бути використані для фінансування тероризму (ФТ) або розповсюдження зброї масового знищення (ФР). Онлайн-платформи, що сприяють купівлі-продажу дорогоцінних металів і каміння, відзначаються високим рівнем анонімності, що ускладнює виявлення зловмисників і створює ризики для операторів цих платформ.

Документ детально розглядає нормативно-правову базу, яка регулює діяльність онлайн-ринків у цій сфері. Основна увага приділена законодавству Об'єднаних Арабських Еміратів (ОАЕ), зокрема Федеральному декрету-закону №20 від 2018 року у сфері протидії відмиванню коштів, а також рекомендаціям FATF, що є міжнародним стандартом у сфері ПВК/ФТ. Визначено, що платформи повинні дотримуватися таких вимог, як реєстрація на порталі goAML, регулярне звітування про підозрілі транзакції (STR/SAR) та проведення заходів з ідентифікації та перевірки клієнтів (KYC/CDD).

Висновки:

- **Онлайн-ринок ювелірних виробів особливо вразливий до ВК/ФТ через анонімність та високу цінність товарів.** Платформи повинні запровадити строгі механізми перевірки користувачів та транзакцій для мінімізації ризиків.
- **Ризик-орієнтований підхід є ключовим елементом стратегії у сфері ПВК.** Онлайн-платформи повинні оцінювати ризики транзакцій за географічними, продуктовими та клієнтськими критеріями.
- **Важливість дотримання міжнародних стандартів FATF.** Рекомендації FATF мають бути інтегровані в політики платформи, включаючи реєстрацію на порталі goAML та звітність про підозрілі операції.
- **Необхідність постійного моніторингу та навчання персоналу.** Постійна оцінка ризиків та підвищення кваліфікації співробітників є критичними для забезпечення відповідності вимогам ПВК/ФТ.

Окремий розділ присвячено практичним заходам, які повинні бути впроваджені операторами онлайн-ринків. Серед них — застосування ризик-орієнтованого підходу (РОП), що передбачає оцінку ризиків кожної транзакції залежно від географічного розташування, вартості товару, репутації клієнта та інших факторів. Документ наголошує на важливості проведення посиленої перевірки клієнтів (EDD) у випадках, коли ризики є високими. Крім того, платформи повинні забезпечити моніторинг усіх транзакцій у реальному часі для виявлення підозрілих операцій і запобігання їх проведенню.

Описано, як оператори платформ мають організувати внутрішню інфраструктуру у сфері ПВК. Це включає призначення відповідального з питань ПВК, впровадження технологій для аналізу транзакцій, розробку політик відповідності та регулярне навчання персоналу. Додатково, акцентується на важливості партнерської роботи з постачальниками, які також повинні впроваджувати відповідні процедури у сфері ПВК та забезпечувати прозорість своїх операцій.

Документ також детально розглядає питання відповідності санкційним режимам. Онлайн-ринкам рекомендовано розробляти програми санкційної відповідності, що включають скринінг клієнтів та постачальників на основі актуальних санкційних списків. Важливу роль відіграє ведення детальних записів усіх транзакцій, що дозволяє у разі потреби швидко надати необхідні дані регуляторам.

Таким чином, документ не лише описує існуючі ризики, а й надає комплексні рекомендації для мінімізації цих загроз, забезпечуючи безпеку платформ та довіру їхніх користувачів. У центрі уваги — інтеграція міжнародних стандартів, побудова ефективних внутрішніх систем контролю та співпраця з регуляторними органами.

Рекомендовані матеріали

Міжнародні зобов'язання щодо протидії фінансуванню розповсюдження[28]

Відео аналізує проблему фінансування розповсюдження зброї масового знищення (ЗМЗ) як ключову, але часто недооцінену загрозу глобальній безпеці. Воно охоплює історію виникнення цієї проблеми, зусилля міжнародного співтовариства щодо її вирішення, а також основні виклики та необхідні кроки для покращення регулювання.

Основний зміст:

1. Що таке фінансування розповсюдження (ФР):
   - Фінансування розповсюдження охоплює діяльність з генерації доходів, переміщення коштів, забезпечення доступу до фінансів для розробки та розповсюдження зброї масового знищення.
   - FATF пропонує дві робочі дефініції ФР, які акцентують увагу на наданні фінансів, фінансових послуг та переміщенні коштів.
2. Історичні етапи боротьби з ФР:
   - Початок уваги до проблеми ФР бере свій початок з Договору про нерозповсюдження ядерної зброї (NPT) у 1960-х.
   - Після терористичних атак 9/11 та діяльності мережі AQ Khan у 2000-х прийнято Резолюцію 1540 Ради Безпеки ООН (2004 р.), яка вимагає від країн впроваджувати ефективні закони для боротьби з фінансуванням ЗМЗ.
   - Санкції проти Північної Кореї розпочалися з Резолюції 1718 (2006 р.), що поступово розширювалися.
3. Роль FATF:
   - У 2012 році FATF включила боротьбу з ФР до своїх стандартів, зокрема вимогу імплементувати цільові фінансові санкції (ЦФС).
   - Країни зобов’язані заморожувати активи підсанкційних осіб та суб'єктів і впроваджувати національні заходи для оцінки та зменшення ризиків ФР.
4. Проблеми імплементації санкцій:
   - Не всі країни ефективно впроваджують санкції через брак знань або національної координації.
   - Список санкцій ООН проти Північної Кореї включає лише 80 фізичних осіб і 75 організацій, тоді як звіти експертів ООН вказують на понад 7000 потенційно причетних суб'єктів.
5. Необхідність ширшого підходу:

[28] https://www.youtube.com/watch?v=p8S_zIamdJs

- Використання мережевого аналізу для виявлення зв'язків поза вузькими межами санкційних списків.
- Залучення до аналізу інших країн, які можуть бути залучені до ФР, зокрема росії, Китаю, Пакистану, Індії та Сирії.

6. Ключові висновки:
   - Країнам необхідно інтегрувати міжнародні стандарти FATF у свої закони, особливо у контексті Рекомендації 7.
   - Зусилля з протидії ФР мають виходити за межі списків санкцій ООН, враховуючи ризики, які створюють непрямі зв'язки.
   - Міжнародна співпраця залишається ключовою для забезпечення глобальної безпеки, враховуючи масштабність фінансових мереж, які підтримують ЗМЗ.

Ефективна боротьба з фінансуванням розповсюдження вимагає глобальних зусиль, які включають жорстке виконання санкцій, активну співпрацю країн, застосування інноваційних методів аналізу фінансових зв'язків та виявлення слабких місць у національних і міжнародних системах контролю.

Інші новини

Огляд ключових новин 2024 року [29]

Стаття містить аналіз ключових подій, пов'язаних із ПВК/ФТ та санкційними ризиками у 2024 році. Основна увага зосереджена на висвітленні глобальних тенденцій, нових регуляторних ініціатив, а також практичних викликів, з якими стикалися фінансові установи та регулятори.

Основні аспекти змісту:

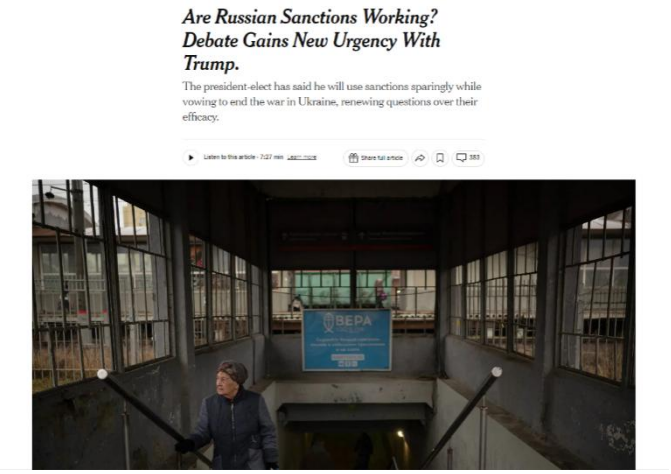
1. Ключові заголовки: У документі наведено перелік важливих новин та подій, що стосуються KYC, AML і санкційного законодавства, які були опубліковані на платформі LinkedIn протягом року. Вони висвітлюють як регуляторні зміни, так і великі скандали, пов'язані з фінансовими порушеннями.
2. Регуляторні ініціативи: Проаналізовано впровадження нових механізмів боротьби з фінансовими злочинами у різних юрисдикціях. Документ звертає увагу на важливі нормативно-правові зміни, такі як оновлення законодавства, що стосується обов'язкових перевірок клієнтів (KYC) та процедури належної перевірки (CDD).
3. Санкційні ризики: Велику увагу приділено санкційним програмам, їхньому впливу на фінансовий сектор, а також викликам для дотримання нових вимог. Особливо акцентується на випадках обходу санкцій та їхньому виявленні.
4. Аналіз тенденцій: Представлено загальні тенденції 2024 року у сфері ПВК/ФТ, включаючи інновації в технологіях (штучний інтелект, автоматизація процесів) та їхнє застосування для підвищення ефективності комплаєнс-процедур.

Стаття надає структурований огляд подій та досягнень року, орієнтуючи читача на найбільш актуальні питання у сфері ПВК/ФТ/санкцій. Він може слугувати практичним довідником для спеціалістів, які працюють у галузі комплаєнсу та фінансового моніторингу.

[29] https://www.linkedin.com/pulse/2024-review-74-kycamlsanctions-relevant-headlines-ion-radu-emnsf/?trackingId=6VeD%2BXT8SRemMFlc71a3Kw%3D%3D

Чи діють російські санкції?[30]

Стаття в The New York Times від 2 січня 2025 року аналізує вплив міжнародних санкцій, запроваджених проти росії у відповідь на її вторгнення в Україну, на російську економіку та глобальні ринки.



Основні аспекти статті:

- **Економічний вплив санкцій**: Санкції призвели до значного скорочення російських валютних резервів, обмеживши здатність країни підтримувати стабільність рубля та фінансувати військові операції. Зокрема, було заморожено близько $300 мільярдів резервів центрального банку росії, що становить приблизно половину загальних резервів країни.
- **Енергетичний сектор**: Обмеження на експорт російської нафти та газу, включаючи запровадження цінових обмежень країнами G7, суттєво знизили доходи росії від енергоресурсів. У першому кварталі 2023 року доходи від нафти та газу склали лише $19,61 мільярда, що значно нижче запланованих показників.
- **Пошук альтернативних ринків**: росія намагалася переорієнтувати експорт енергоресурсів на країни, які не приєдналися до санкцій, такі як Китай та Індія. Однак логістичні труднощі та знижки, необхідні для залучення нових покупців, зменшили ефективність цих зусиль.
- **Вплив на глобальні ринки**: Санкції проти росії спричинили зростання цін на енергоносії та продовольство, що вплинуло на інфляцію в багатьох країнах. Особливо постраждали країни, залежні від імпорту російських енергоресурсів та зерна.
- **Адаптація російської економіки**: Попри санкції, росія вжила заходів для стабілізації економіки, включаючи підвищення процентних ставок та контроль за капіталом. Однак довгострокові перспективи залишаються невизначеними через обмежений доступ до західних технологій та інвестицій.

Глобальна битва за довіру: Як APP-шахрайства змінюють фінансову екосистему у 2024 році[31]

Стаття, опублікована на платформі Global Initiative Against Transnational Organized Crime, пропонує глибокий аналіз очікуваних викликів та змін, які можуть вплинути на боротьбу з транснаціональною організованою злочинністю у 2025 році. Автори досліджують, як геополітичні події, збройні конфлікти та соціально-економічні зміни сприяють еволюції злочинних мереж. Особливу увагу приділено конфлікту в Україні, який може призвести до зростання нелегальної торгівлі зброєю у випадку деескалації або активізації злочинних структур росією для гібридної агресії у разі продовження

[30] https://www.nytimes.com/2025/01/02/business/economy/russia-sanctions-ukraine.html?unlocked_article_code=1.mU4.JpQj.o4KHLso6Wvx3&smid=url-share&utm_source=newsletter.illicitedge.com&utm_medium=newsletter&utm_campaign=ccp-houthis-credit-suisse-scandals-and-russian-sting

[31] https://globalinitiative.net/analysis/the-telescope-what-to-watch-for-in-2025/

конфлікту. У Північній Африці та Сахелі конфлікти в Малі, Буркіна-Фасо, Нігері та Судані створюють кримінальні екосистеми, що забезпечують нелегальні ринки зброї, золота, пального та найманців, а також стимулюють міграційні потоки, що загрожують стабільності й демократії у регіоні. Гаїті висвітлюється як епіцентр гуманітарної кризи, де поширення злочинних угруповань і зростання насильства створюють значні виклики для міжнародної спільноти, яка має реагувати на ці загрози шляхом миротворчих місій та економічної допомоги. Важливою подією 2025 року стане 25-та річниця Палермської конвенції, яка може слугувати платформою для перегляду міжнародних зобов'язань у боротьбі з транснаціональною злочинністю. Автори наголошують на необхідності адаптації цієї конвенції до сучасних реалій, враховуючи зростання кіберзлочинності, використання криптовалют для відмивання коштів та екологічні злочини. Також у статті зазначається, що інновації у сфері фінансових технологій та цифровізації створюють додаткові виклики, полегшуючи діяльність злочинних мереж через глобальні ланцюги поставок. Загалом, стаття підкреслює складність сучасних загроз, які поєднують традиційні форми злочинності з новими технологіями та соціальними викликами, закликаючи до посилення міжнародної координації, модернізації інструментів боротьби із злочинністю та впровадження гнучких підходів до цих викликів. Це дослідження є важливим закликом до дій, підкреслюючи, що майбутні виклики потребують негайної уваги урядів, міжнародних організацій і громадянського суспільства.

Інновації та виклики у сфері ПВК/ФТ: ключові законодавчі зміни від ЕВА у 2024 році[32]

Документ є випуском за 2024 рік Європейського банківського органу (ЕВА), що висвітлює ключові події, досягнення та рекомендації у сфері протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ). Основною темою є зміни у законодавчому середовищі Європейського Союзу, спрямовані на посилення прозорості та ефективності фінансової системи, а також адаптація до нових викликів у сфері криптоактивів, санкцій та ризиків фінансових злочинів.

У документі детально розглянуто впровадження регуляторної бази для ринків криптоактивів відповідно до Регламенту про ринки криптоактивів (MiCAR), який набуває чинності з 30 грудня 2024 року. Нові настанови регламентують плани викупу активів для токенів, забезпечених активами (ARTs), та електронних грошових токенів (EMTs). Це охоплює процеси ліквідації резервних активів, управління ризиками та перевірку власників токенів через процедури належної перевірки (CDD). Важливим аспектом є вимога до емітентів, які не підпадають під зобов'язання ПВК/ФТ, залучати посередників, які є підзвітними суб'єктами відповідно до Директиви ЄС про ПВК.

Також акцент зроблено на новій структурі ПВК/ФТ у ЄС, що включає гармонізоване регулювання, єдину нормативну базу та створення нового органу – Європейської AMLA. В рамках цього процесу ЕВА залучив понад 150 представників приватного сектору до круглого столу, щоб отримати зворотний зв'язок щодо впровадження нових норм. Це свідчить про відкритий підхід до співпраці з зацікавленими сторонами.

У документі представлені рекомендації щодо внутрішніх політик фінансових установ для дотримання санкційних заходів на рівні ЄС та національному рівні. Два комплекти настанов

[32] https://www.eba.europa.eu/sites/default/files/2024-12/b4f373bc-1dcc-4cc1-b675-1b681cac0df4/eba_aml_cft_newsletter_issue_14_-_2024.pdf

вперше запроваджують єдині стандарти, що охоплюють заходи щодо управління ризиками порушення санкцій, а також специфічні дії для постачальників платіжних послуг (PSPs) та постачальників послуг криптоактивів (CASPs).

Важливе місце займає щорічна оцінка ризиків європейської банківської системи, яка виявила, що ризики, пов'язані з фінансовими злочинами, залишаються значними. Зокрема, ризики ВК/ФТ та ризики, пов'язані з санкціями через російську агресію, є пріоритетними для банків. Водночас зростає значущість ризиків, пов'язаних з відмиванням доходів від шахрайства.

Сектор криптоактивів отримує окрему увагу, оскільки він став підзвітним суб'єктом для цілей ПВК/ФТ. У документі висвітлено вплив MiCAR на регулювання CASPs, зокрема введення вимог щодо централізованих контактних пунктів для забезпечення дотримання місцевих норм у сфері ПВК/ФТ.

База даних EuReCA стала важливим інструментом для моніторингу ризиків. У 2024 році до бази було подано 787 звітів про серйозні недоліки у процедурах CDD, серед яких переважали проблеми, пов'язані з неправильним використанням технологій. Документ також повідомляє про зростання кількості штрафів та інших заходів впливу, включаючи відкликання ліцензій.

Також у документі аналізуються перспективи токенізованих депозитів, їхні потенційні переваги, такі як програмованість та автоматизація, а також виклики, включаючи ризики для захисту споживачів та дотримання вимог у сфері ПВК/ФТ.

Завершальний блок містить огляд роботи коледжів у сфері ПВК/ФТ, які продовжують покращувати свої функції. Однак є потреба в подальшій адаптації до ризиків ВК/ФТ та узгодженні спільних підходів між компетентними органами.

Документ завершується анонсом майбутніх звітів та ініціатив EBA, спрямованих на покращення нагляду за криптоактивами та боротьбу з фінансовими злочинами.

Для загального розвитку

Передплачені картки: палиця з двома кінцями у відмиванні коштів

Передплачені картки використовуються на кожному етапі процесу відмивання грошей, починаючи від розміщення й закінчуючи розшаруванням та інтеграцією.

Як передплачені картки використовуються для відмивання грошей:

1. Розміщення:
   - Незаконні кошти використовуються для купівлі передплачених карт оптом.
   - Ці картки перевозяться через кордони, щоб уникнути перевірки.
   - Грошові мули використовуються для купівлі/продажу карток, переміщення незаконних грошей у фінансову систему.
2. Розшарування:
   - Передплачені картки використовуються для купівлі цінних товарів (наприклад, електроніки).
   - Ці предмети перепродуються кілька разів, щоб приховати походження коштів.
3. Інтеграція:
   - Злочинці використовують незаконні кошти на передплачених картках для купівлі законних товарів і послуг (наприклад, предметів розкоші, компонентів ліків або страхових продуктів).

Чому передплачені картки вразливі?

- ✓ Анонімність: обмежена належна перевірка клієнта дозволяє злочинцям використовувати передплачені картки для незаконної діяльності.
- ✓ Глобальне охоплення: передплачені картки можна використовувати будь-де, що дає змогу транскордонно відмивати гроші.
- ✓ Портативність: маленький і простий у транспортуванні, що спрощує міжнародне переміщення грошей.
- ✓ Доступне фінансування: джерело коштів, завантажених на передплачені картки, можна приховати за допомогою онлайн-банкінгу або телефонного банкінгу.

Червоні прапорці в операціях з передплаченими картками

- Надмірна кількість карток у одного клієнта.
- Небажання надавати необхідні документи або дані.
- Картки відправляються за межі країни.
- Часті невеликі зняття з наступними великими депозитами в іноземній валюті.
- Незвичні або повторювані моделі транзакцій у штатах або країнах.
- Кілька транзакцій трохи нижче порогових значень.
- Підозріла купівельна поведінка або незрозумілі транзакції.

Уряди та фінансові установи повинні посилити заходи з ПВК/ФТ, зокрема:

- ✓ Відстеження масових покупок або великих транзакцій за передплаченими картками.
- ✓ Розслідування частого фінансування третьою стороною або ненормальних моделей використання.
- ✓ Позначення частих поповнень карток, негайних переказів коштів або зняття лише готівки.

У відповідь на ці ризики глобальні правила посилюються. Наприклад, 5-та Директива ЄС щодо боротьби з відмиванням коштів зменшила ліміти транзакцій для передплачених карток.

Злочинці використовують передплачені картки, щоб використовувати лазівки у фінансовій системі. Але, визначаючи червоні прапорці та запроваджуючи суворіші правила протидії відмиванню коштів та фінансуванню тероризму, ми можемо спільно боротися з цією зростаючою загрозою.

Що таке фінансування розповсюдження?

Відмивання коштів і фінансування тероризму часто домінують у розмовах щодо відповідності вимогам. Але чи помітили ви, що останнім часом уряди дуже стурбовані фінансуванням розповсюдження?

Фінансування розповсюдження стосується фінансової підтримки, що надається окремим особам, організаціям або діяльності, залученої до розробки, виробництва чи доставки зброї масового знищення (ЗМЗ). Ці кошти можуть проходити через законні комерційні канали або незаконні мережі.

Незважаючи на те, що Рекомендації FATF охоплюють відмивання коштів, фінансування тероризму та фінансування розповсюдження, останньому часто приділяється менше уваги як країн, так і підзвітних установ.

Вимоги FATF Щодо Фінансування Розповсюдження

Рекомендація 7 підкреслює її важливість, вимагаючи від країн виконання санкцій Ради Безпеки ООН. Це передбачає заморожування активів і запобігання передачі коштів особам або організаціям, причетним до розповсюдження ЗМЗ.

Що мають робити підзвітні установи?

Організації, включно з фінансовими установами, ВНУП та постачальниками послуг віртуальних активів, повинні розглянути заходи в контексті фінансування розповсюдження, які включають:

↳ **Виявлення та оцінка ризиків**: Зрозуміти свою схильність до ризику фінансування розповсюдження. Це включає в себе аналіз клієнтської бази, країн, у яких вони працюють, продуктів і послуг, які вони пропонують, а також сили їх внутрішнього контролю.

=> Задокументуйте свої оцінки.

↳ **Скринінг**: Встановити комплексні системи перевірки санкцій, щоб перевіряти клієнтів на відповідність санкційним спискам ООН. Забезпечити своєчасне оновлення цих списків і вносити зміни у свої процеси скринінгу.

=> Розгляньте інструменти, які використовують машинне навчання для підвищення ефективності перевірки.

↳ **Належна перевірка**: Запровадити надійні процедури KYC для ідентифікації та перевірки клієнтів. Проводити посилену належну перевірку, якщо це необхідно, особливо для клієнтів, які працюють у секторах високого ризику або тих, хто демонструє підозрілу діяльність.

=> Зрозумійте бенефіціарну власність компаній і ретельно досліджуйте складні структури.

↳ **Моніторинг транзакцій**: Запровадити системи моніторингу транзакцій для виявлення незвичних або підозрілих дій, які можуть вказувати на ухилення від санкцій. Звертати пильну увагу на транзакції, пов'язані з юрисдикціями високого ризику, товарами подвійного призначення, підставними компаніями та складними фінансовими потоками.

Зловживання кредитними картками: як злочинці використовують платіжні системи для відмивання коштів [33]

Публікація висвітлює ключову проблему сучасної фінансової системи – зловживання кредитними картками для здійснення фінансових злочинів, зокрема відмивання коштів. Автор розкриває різні методи, які використовують злочинці для маніпуляції системами, з метою "очищення" незаконно отриманих грошей, надаючи їм легальний вигляд.

Основний акцент зроблено на трьох тактиках, що широко застосовуються в таких схемах. По-перше, це використання "брудних" грошей для погашення рахунків кредитних карток. Ця тактика дозволяє створити видимість, що гроші, які надходять до фінансової системи, є легітимними, оскільки вони використовуються для оплати заборгованостей. По-друге, злочинці часто здійснюють великі покупки дорогих товарів, таких як розкішні годинники, електроніка або ювелірні вироби, за допомогою кредитних карток. Ці товари потім перепродаються за готівку, яка виглядає як "чисті" кошти. По-третє,

[33] https://www.linkedin.com/pulse/understanding-credit-card-misuse-financial-crime-anand-rajpurohit-wzkbc/

застосовується метод переплат, коли клієнт навмисно платить більше, ніж належить за рахунком, а потім запитує повернення надлишкової суми. У результаті ці повернені гроші вважаються "чистими", оскільки вони проходять через фінансову систему як частина законної операції.

Публікація наголошує на масштабності цієї проблеми та підкреслює необхідність активної боротьби з такими схемами. Банки та фінансові установи, згідно з автором, мають бути надзвичайно пильними у виявленні подібних підозрілих операцій. Пильність має супроводжуватися впровадженням сучасних автоматизованих систем моніторингу та аналізу транзакцій, які можуть швидко виявляти аномальні активності, що свідчать про можливе відмивання коштів.

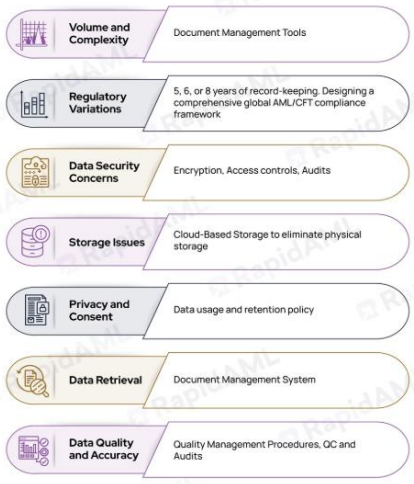
Крім того, документ акцентує увагу на необхідності посилення політик "Знай свого клієнта" (KYC) для запобігання зловживанням кредитними картками. Фінансові установи повинні ретельно перевіряти джерела доходів клієнтів, особливо у випадках великих витрат, які не відповідають звичайній поведінці власника рахунку. Освітня робота серед споживачів також відіграє важливу роль у запобіганні злочинним схемам. Клієнти мають знати про ризики, розуміти, як виявляти підозрілі транзакції, і бути готовими повідомляти про них.

Окремо підкреслюється важливість співпраці фінансових установ із правоохоронними органами. Швидкий обмін інформацією та доступність необхідних даних для розслідування є критичними для ефективного виявлення та запобігання фінансовим злочинам. Автор закликає до скоординованої роботи всіх учасників фінансової системи для захисту її від кримінальних зловживань.

Загалом, документ представляє всебічний огляд проблеми зловживання кредитними картками у контексті відмивання коштів і пропонує низку стратегій для її вирішення.

Виклики та рішення у веденні записів у сфері ПВК: Як подолати бар’єри та забезпечити відповідність[34]

Інфографіка розкриває глибокі проблеми, з якими стикаються організації у сфері ведення облікових записів відповідно до стандартів у сфері протидії відмиванню коштів (ПВК). Основний акцент зроблено на ключових аспектах цієї діяльності, що включає дотримання нормативних вимог, управління даними та використання технологій для підвищення ефективності. У документі йдеться про те, що ведення записів є критично важливим для виконання обов’язків фінансових установ щодо запобігання ВК/ФТ, але разом із цим залишається однією з найскладніших сфер для реалізації на практиці.



Зокрема, підкреслюється, що однією з головних проблем є складність у забезпеченні точності, доступності та актуальності даних у реальному часі. Організації часто стикаються з труднощами інтеграції даних із різних джерел, що особливо гостро проявляється у глобальному масштабі, де регуляторні вимоги різних юрисдикцій мають значні відмінності. Окремо виділяється питання відповідності регуляторним стандартам, яке передбачає не

[34] https://rapidaml.com/infographics/aml-record-keeping-challenges-and-solutions/

тільки зберігання великих обсягів інформації, але й здатність швидко аналізувати та надавати її на запит регуляторів. Це створює додатковий адміністративний та фінансовий тягар для компаній.

Інфографіка також акцентує увагу на технологічних викликах, серед яких використання застарілих систем, недостатня інтеграція між платформами та велика залежність від ручного введення даних. Це призводить до високих ризиків людських помилок, затримок у процесах і зниження загальної ефективності. Крім того, у матеріалі зазначено, що забезпечення відповідності вимогам потребує значних фінансових інвестицій у технічну підтримку, навчання персоналу та постійне оновлення інфраструктури. Організації також стикаються з труднощами у створенні централізованої бази даних, яка б відповідала всім нормативним вимогам та забезпечувала прозорість процесів.

Для вирішення цих викликів пропонуються інноваційні підходи, що базуються на використанні сучасних технологій. Основну увагу приділено автоматизації процесів, що дозволяє зменшити навантаження на персонал та мінімізувати ризики помилок. Хмарні технології та рішення на основі штучного інтелекту відіграють ключову роль у забезпеченні доступу до інформації у режимі реального часу та аналізу великих обсягів даних. Також підкреслено важливість інтеграції всіх систем у межах однієї платформи для підвищення ефективності та прозорості.

Крім технологій, у документі наголошується на важливості людського фактора. Регулярне навчання співробітників, підвищення їхньої обізнаності про ризики, пов’язані з ВК/ФТ, та розвиток культури комплаєнсу є ключовими аспектами успішного впровадження рішень у сфері ПВК. Підкреслюється необхідність поєднання технічних інновацій із чітким стратегічним плануванням для створення стійких систем управління обліковими записами.

Остання частина інфографіки присвячена перспективам глобальної гармонізації нормативних вимог. Зазначено, що для ефективної боротьби з ВК/ФТ необхідна співпраця між різними юрисдикціями, яка б сприяла обміну інформацією та уніфікації стандартів. У підсумку наголошується, що впровадження технологічних інновацій, стратегічного планування та розвитку навичок персоналу є основними інструментами для подолання сучасних викликів у сфері ПВК. Інфографіка пропонує комплексний підхід, який допоможе організаціям адаптуватися до швидко змінюваних умов регуляторного середовища, забезпечити ефективність процесів і знизити ризики, пов’язані з порушенням нормативних вимог.

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-2025-02

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].