



Серійний номер: ДСФМУ-ДК-2024-036
Грудень 2024

Методологічний Бюлетень

Мета

Методологічний Бюлетень видається Держфінмоніторингом на регулярній основі починаючи з квітня 2024 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.

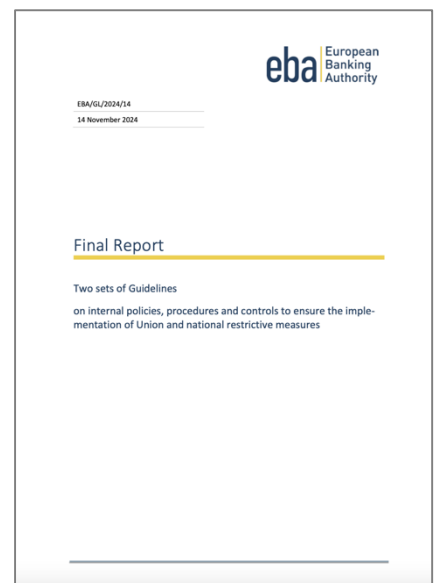
Включає актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

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

Керівництво Європейського органу банківського нагляду (ЕВА) щодо внутрішньої політики, процедур і засобів контролю для забезпечення впровадження обмежувальних заходів на рівні ЄС та окремих країн¹

Документ є ключовим кроком у гармонізації підходів до виконання санкційних заходів у фінансовому секторі ЄС. Керівництва були створені у відповідь на розбіжності в підходах національних компетентних органів до впровадження санкцій, які раніше створювали значні труднощі для фінансових установ у досягненні відповідності правовим вимогам. Основна мета документа – встановити єдині стандарти внутрішніх політик, процедур та механізмів контролю, які забезпечують ефективне впровадження



¹ <https://www.eba.europa.eu/sites/default/files/2024-11/eaeae49d-81a5-4154-8af9-5014f6ee8881/Final%20Report%20Guidelines%20restrictive%20measures%20.pdf>

обмежувальних заходів, запобігають ризикам їх порушення, а також підвищують стабільність і прозорість фінансової системи ЄС.

Документ складається з двох наборів рекомендацій. Перший адресовано всім фінансовим установам під юрисдикцією ЕВА і визначає загальні вимоги до управлінських структур, політик і систем управління ризиками, необхідних для забезпечення дотримання санкцій. Другий набір рекомендацій орієнтований на постачальників платіжних послуг (PSPs) і постачальників послуг з криптоактивів (CASPs) і містить спеціалізовані інструкції щодо виконання санкційних заходів у сфері транзакцій з грошовими коштами та криптоактивами.

Ключовою частиною документа є рекомендації щодо оцінки вразливості до санкційних ризиків. Вони зобов'язують фінансові установи регулярно аналізувати свої операції, клієнтську базу, географічне охоплення та канали постачання послуг для виявлення потенційних вразливостей. Цей аналіз є основою для адаптації внутрішніх політик і процедур, що відповідають розміру, складності та специфіці діяльності кожної установи. Документ також містить вказівки щодо інтеграції таких заходів, як скринінг клієнтів і транзакцій, моніторинг відповідності санкційним вимогам, а також використання сучасних технологій, включаючи автоматизовані системи моніторингу та "fuzzy matching" для підвищення точності ідентифікації ризиків.

Важлива роль у реалізації цих рекомендацій відведена керівним органам фінансових установ, які повинні затверджувати стратегії дотримання санкцій, забезпечувати ресурси для їх впровадження, а також регулярно оцінювати ефективність виконання. Особлива увага приділена навчальним програмам для персоналу, які мають забезпечити розуміння санкційних режимів і процедур їх дотримання.

Висновки:

- Уніфіковані стандарти ЕВА зменшують вразливість фінансових установ до санкційних ризиків, усуваючи розбіжності між підходами країн ЄС.
- Оцінка вразливості до санкційних ризиків дозволяє фінансовим установам ідентифікувати транзакції та клієнтів, що можуть підпадати під санкції.
- Спеціалізовані рекомендації для PSPs і CASPs покращують моніторинг криптоактивів і міжнародних платежів, забезпечуючи дотримання санкційних режимів.
- Зобов'язання керівництва щорічно оцінювати ефективність політик сприяє більшій відповідності установ до санкційних вимог.

Крім того, документ визначає стандарти для PSPs і CASPs у сфері криптоактивів, включаючи вимоги до скринінгу клієнтів, перевірки транзакцій та оцінки ризиків обходу санкцій. Приділено увагу ролі блокчейн-аналізу для виявлення підозрілих транзакцій та підвищення прозорості операцій.

Очікується, що впровадження цих рекомендацій допоможе уникнути необґрунтованих обмежень для добросовісних клієнтів, мінімізувати ризики порушення санкційних вимог, а також сприятиме зміцненню міжнародного іміджу ЄС як надійного фінансового регулятора. Документ є значним кроком у гармонізації санкційної політики, підтримуючи цілі збереження міжнародного миру, прав людини та верховенства права.

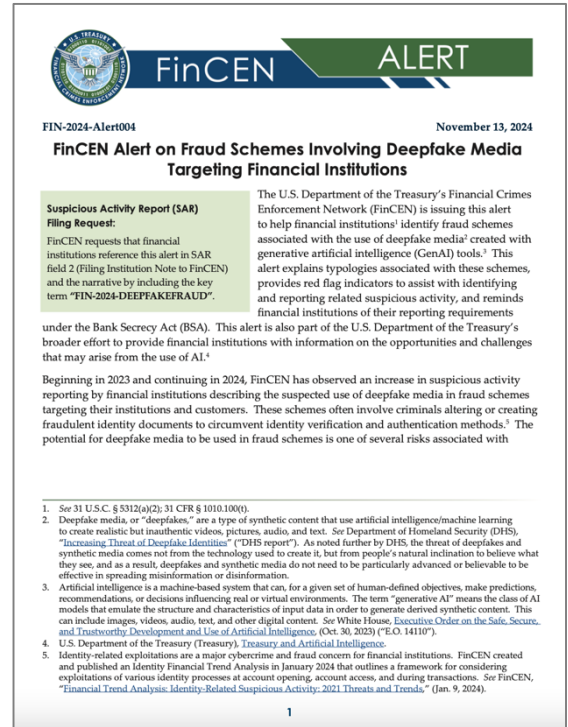
Попередження Мережі по боротьбі з фінансовими злочинами Міністерства фінансів США (Financial Crimes Enforcement Network, FinCEN) щодо шахрайських схем із залученням Deepfake, націлених на фінансові установи²

Документ представляє собою офіційне попередження для фінансових установ, яке описує загрози, пов'язані з використанням медіа deepfake, створених за допомогою генеративного штучного інтелекту (GenAI). Головна мета — допомогти фінансовим організаціям виявляти шахрайські схеми, пов'язані з deepfake, і реагувати на них відповідно до вимог законодавства. Документ наголошує, що deepfake не обов'язково повинні бути високотехнологічними чи реалістичними, щоб бути ефективними. Часто простих маніпуляцій вистачає для поширення дезінформації та обходу систем верифікації.

FinCEN звертає увагу на те, що з 2023 р. було зафіксовано зростання підозрілих транзакцій, які фінансові установи пов'язують із використанням deepfake. Такі медіа часто використовуються для створення підроблених ідентифікаційних документів, які дозволяють зловмисникам обходити процедури перевірки клієнтів, відкривати рахунки та здійснювати транзакції, пов'язані з шахрайством. Шахраї також використовують технології GenAI для створення синтетичних осіб, які поєднують справжні і фальшиві персональні дані. Такі синтетичні особи використовуються для схем, пов'язаних із

Висновки:

- Розвиток технологій deepfake збільшує ризик шахрайства у фінансовому секторі, особливо у сфері ідентифікації клієнтів та соціальної інженерії.
- Використання інструментів розпізнавання deepfake та запровадження багатофакторної автентифікації є ключовими методами зменшення цих ризиків.
- Навчання співробітників фінансових установ та оновлення внутрішніх процедур є необхідними для ефективної протидії сучасним схемам шахрайства.
- Включення у SAR специфічних індикаторів ризику забезпечує ефективну комунікацію між установами та FinCEN для покращення моніторингу та аналізу ризиків.



кредитами, шахрайством із чеками, онлайн-шахрайством та схемами відмивання коштів. Особливу небезпеку становлять funnel accounts — рахунки, які відкриваються для збору та переказу коштів у рамках мережі зловмисників.

Документ також наголошує на використанні deepfake у схемах соціальної інженерії, таких як бізнесовий компроміс електронної пошти (BEC), романтичні шахрайства, експлуатація довіри літніх людей або шахрайство під виглядом інвестицій. Наприклад, deepfake-відео чи аудіо використовуються для імітації голосів або обличчя керівників компаній, членів

² <https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf>

родини чи інших довірених осіб, щоб виманювати гроші чи доступ до чутливих даних. Такі схеми створюють ризики для співробітників фінансових установ і їхніх клієнтів.

FinCEN надає рекомендації для фінансових установ, які включають впровадження багатофакторної автентифікації, перевірок у реальному часі (через відео чи аудіо), використання програм для розпізнавання deepfake, реверсивного пошуку зображень і моніторингу транзакцій на предмет підозрілих патернів. Інституціям також рекомендується підвищувати обізнаність персоналу про ризики, пов'язані з deepfake, та оновлювати політики щодо належної перевірки клієнтів.

FinCEN закликає фінансові установи включати позначку «FIN-2024-DEEPFAKEFRAUD» у звіти про підозрілі транзакції (SAR), щоб сигналізувати про шахрайство, пов'язане з deepfake, і покращити аналіз таких випадків. У документі наголошується, що об'єднання зусиль фінансових установ, розробників технологій і регуляторів є критично важливим для запобігання зловживанням GenAI і захисту фінансової системи від нових ризиків.

Інструкції Управління впровадження фінансових санкцій (OFSI) щодо фінансових санкцій для учасників ринків високовартісних товарів та мистецтва³

Документ «Financial Sanctions Guidance for High Value Dealers & Art Market Participants» підготовлено як практичний посібник для учасників ринків високовартісних товарів та мистецтва, які працюють у Великій Британії. Мета цього документа – допомогти бізнесу дотримуватися режимів фінансових санкцій, розроблених для досягнення зовнішньополітичних та безпекових цілей Великої Британії, а також захисту її фінансової системи.

Guidance

Financial sanctions guidance for High Value Dealers & Art Market Participants

Published 14 November 2024

Фінансові санкції визначаються як один із ключових інструментів боротьби з тероризмом, внутрішніми репресіями, порушенням прав людини та іншими глобальними загрозами. Вони охоплюють географічні та тематичні режими, спрямовані на певні країни, регіони чи категорії осіб і організацій. Документ підкреслює, що навіть якщо суб'єкт працює в юрисдикції, яка не підпадає під географічний режим санкцій, йому слід враховувати ризики тематичних режимів.

Документ наводить поширені методи обходу санкцій, зокрема використання підставних осіб і компаній, переміщення активів через офшорні рахунки, маніпуляції з цифровими активами, включаючи криптовалюти та NFT. Ці схеми дозволяють санкціонованим особам приховувати свої активи або уникати обмежень. Особливо підкреслюється ризик для дилерів мистецтва та предметів розкоші, оскільки їхній ринок характеризується високим рівнем анонімності, можливістю маніпуляцій із цінами та складністю відстеження руху товарів.

У відповідь на ці ризики документ рекомендує бізнесу впроваджувати системи посиленої належної перевірки (EDD). Це включає перевірку клієнтів, контрагентів, кінцевих бенефіціарів та транзакцій за участю підозрілих юрисдикцій. Учасникам ринку пропонується регулярно перевіряти списки санкцій OFSI, зокрема консолідований список, і забезпечувати, щоб бізнес-процеси відповідали вимогам фінансового моніторингу.

³ <https://www.gov.uk/government/publications/high-value-dealers-art-market-participants-guidance/financial-sanctions-guidance-for-high-value-dealers-art-market-participants>

Документ також наголошує на важливості програм дотримання санкцій. Бізнесу рекомендується розробляти внутрішні політики, проводити навчання персоналу, здійснювати зовнішні аудити та створювати механізми для конфіденційного повідомлення про підозрілі дії. Серед ключових вимог є необхідність негайно припинити будь-які транзакції з санкціонованими особами, заморозувати їхні активи та повідомляти про підозри до OFSI.

Висновки:

- З травня 2025 року учасники ринків високовартісних товарів та мистецтва зобов'язані повідомляти про підозрілі транзакції та осіб зі списків санкцій до OFSI.
- Рекомендується впровадження системи перевірки клієнтів і транзакцій, зокрема з використанням актуальних списків OFSI, для запобігання співпраці з санкціонованими особами.
- Популярні схеми, такі як використання підставних компаній, офшорів та цифрових активів, вимагають посиленого моніторингу з боку бізнесу.
- Недотримання вимог санкційного режиму може призвести до значних штрафів (до 1 млн фунтів стерлінгів або 50% суми порушення) чи тюремного ув'язнення до 7 років.

Важливу роль у забезпеченні дотримання санкцій відіграє звітування. Від 14 травня 2025 р. дилери високовартісних товарів та учасники арт-ринку будуть зобов'язані інформувати OFSI про будь-які підозрілі транзакції або осіб, які можуть бути пов'язані зі списками санкцій. Недотримання цих вимог вважається серйозним кримінальним правопорушенням, за яке передбачені значні штрафи та, навіть, позбавлення волі.

Особливу увагу приділено важливості ідентифікації структур власності та контролю, оскільки навіть непрямий контроль може підпадати під обмеження. Документ також пояснює взаємозв'язок між фінансовими та торговельними санкціями, що накладає додаткові зобов'язання для бізнесу, який здійснює міжнародну торгівлю.

Таким чином, посібник є комплексним

ресурсом, що надає практичні рекомендації для бізнесу в секторах високовартісних товарів і мистецтва, спрямовані на зміцнення санкційної відповідності, мінімізацію ризиків та уникнення юридичної відповідальності.

Європол попереджає про організовані злочинні групи, які вербують неповнолітніх⁴

Документ розглядає проблему залучення організованими злочинними угрупованнями неповнолітніх до злочинної діяльності на території Європи, акцентуючи увагу на стрімкому зростанні цього явища. Europol у своєму звіті зазначає, що приблизно 70% злочинної діяльності тією чи іншою мірою включає використання неповнолітніх. Це є частиною свідомої стратегії злочинних організацій, які прагнуть знизити ризики для себе, одночасно експлуатуючи вразливу групу населення.



⁴ https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The-recruitment-of-young-perpetrators-for-criminal-networks.pdf



Залучення молоді стає вигідною тактикою, оскільки неповнолітні не мають кримінальних досьє, що ускладнює їхнє переслідування правоохоронними органами. Крім того, ці особи зазвичай ізольовані від верхніх ешелонів злочинної ієрархії, що зводить до мінімуму їхню обізнаність про структуру і діяльність угруповання. Такий підхід створює буфер між лідерами мережі й виконавцями злочинів, ускладнюючи доведення вини керівників та організаторів.

Особливою загрозою є зростання залучення неповнолітніх у наркоторгівлю, зокрема в сегменті ринку кокаїну.

Висновки:

- **Масштаб залучення молоді:** Неповнолітні беруть участь у 70% злочинної діяльності, виконуючи низькорівневі та ризиковані завдання, включаючи насильницькі злочини та наркоторгівлю.
- **Стратегії вербування:** Соціальні медіа стали основним інструментом для рекрутингу, де злочинці використовують емоційні маніпуляції для залучення вразливих підлітків.
- **Вигоди для злочинних угруповань:** Молодь ізольована від лідерів організацій, має низький рівень ризику для арешту і не здатна розкрити інформацію про ієрархію угруповання.

Методи вербування неповнолітніх значно еволюціонували. Сучасні злочинні угруповання активно використовують соціальні медіа для пошуку потенційних "співробітників". Соціальні платформи дозволяють їм швидко виявляти молодь, яка потребує емоційної підтримки, відчуває себе ізольованою або шукає приналежності до певної спільноти. Рекрутери часто використовують маніпулятивну мову, що викликає довіру та формує у жертви почуття лояльності та вдячності. У багатьох випадках це дозволяє злочинцям майже безперешкодно залучати молодих людей до виконання кримінальних завдань.

Документ підкреслює, що така діяльність поширена у багатьох європейських країнах і має тенденцію до подальшого розширення.

Europol закликає до активізації міжнародної співпраці, зміцнення превентивних заходів і посилення просвітницьких кампаній, спрямованих на попередження злочинної експлуатації молоді.

Національна стратегія Сінгапуру 2024: Нові горизонти у протидії відмиванню коштів⁵

Документ є всебічним планом, спрямованим на боротьбу з ризиками, пов'язаними з відмиванням коштів (ПВК), у глобально інтегрованій фінансовій системі Сінгапуру. Стратегія розглядає ключові виклики, пов'язані з геополітичними змінами, технологічним прогресом і складністю сучасних злочинних схем, що становлять загрозу фінансовій безпеці та репутації країни. Документ оновлює попередні підходи, деталізовані у 2016 році, і зосереджується на впровадженні ризик-орієнтованих, пропорційних та ефективних заходів у сфері ПВК.

NATIONAL ANTI-MONEY LAUNDERING STRATEGY
SINGAPORE
2024

⁵ <https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/amld/2024/singapore-national-aml-strategy.pdf>



У документі наголошується на необхідності застосування міжсекторального підходу "всім суспільством", де уряд, приватний сектор та громадянське суспільство працюють разом, щоб забезпечити ефективну протидію злочинним діям. Ключові механізми, такі як система обміну даними NAVIGATE та робочі групи з аналізу ризиків, спрямовані на посилення співпраці між державними органами. Публічно-приватні партнерства, зокрема через ініціативи на кшталт ACIP, активно розвиваються для обміну передовими практиками, підвищення обізнаності про ризики та розробки галузевих рекомендацій.

Юридична та регуляторна база, що підтримує стратегію, постійно вдосконалюється відповідно до змін ризиків і типологій злочинів. Зокрема, внесено зміни до Закону про конфіскацію доходів від злочинної діяльності (CDSA), що передбачають нові злочини та посилення відповідальності. Удосконалюється регулювання секторів, схильних до високих ризиків, таких як цифрові платіжні послуги, трасти, оператори нерухомості та постачальники корпоративних послуг. Підвищено прозорість бенефіціарної власності завдяки створенню централізованого реєстру та новим вимогам щодо розкриття інформації.

Стратегія також акцентує увагу на міжнародному співробітництві як ключовому елементі боротьби з транснаціональними злочинами. Сінгапур активно залучений до роботи таких організацій, як FATF, Egmont Group та ARIN-AP, що сприяє розробці міжнародних стандартів і обміну інформацією. Внесено законодавчі зміни для вдосконалення механізмів правової

допомоги та екстрадиції, а також для полегшення спільних розслідувань із міжнародними партнерами.

Суттєвий акцент зроблено на технологічних інноваціях для виявлення підозрілих дій. Платформи COSMIC і NAVIGATE дозволяють ефективно аналізувати дані та виявляти підозрілі транзакції. У рамках цього підходу впроваджуються сучасні методи аналітики даних, що дозволяють урядовим і приватним структурам виявляти ризики у реальному часі. Встановлення спеціальних платформ обміну інформацією між банками сприяє швидшому виявленню та нейтралізації ризикових операцій.

Документ також підкреслює важливість ефективного виконання та застосування штрафних санкцій для посилення стримуючого ефекту. Пріоритет надається розслідуванню складних транснаціональних справ і конфіскації злочинних доходів як ключового засобу

Висновки:

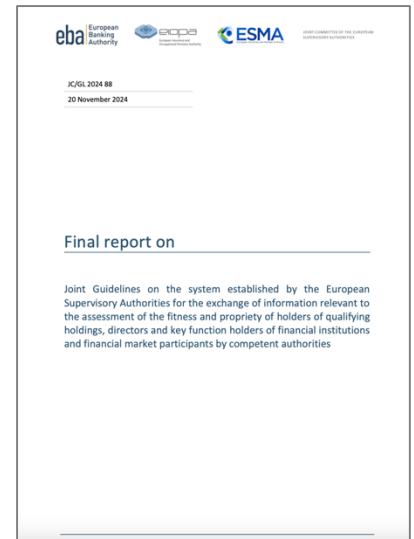
- **Ризик-орієнтований підхід:** Запровадження персоналізованих вимог до секторів із високими ризиками, таких як цифрові платіжні послуги, нерухомість та трасти, підвищує ефективність заходів AML.
- **Сучасні технології у виявленні:** Використання платформ COSMIC та NAVIGATE демонструє ефективність технологічних рішень у виявленні складних схем відмивання коштів.
- **Прозорість бенефіціарної власності:** Законодавчі зміни сприяють прозорості, зменшуючи ризики використання компаній та трастів для незаконної діяльності.
- **Міжнародна координація:** Посилення міжнародного співробітництва через участь у FATF, Egmont Group та ARIN-AP значно збільшує можливості виявлення та боротьби з транснаціональними злочинами.

позбавлення злочинців фінансового стимулу. У цьому контексті підвищено штрафи та покарання за порушення вимог з ПВК у високоризикових секторах.

На завершення стратегія визначає цілі щодо зміцнення інтегрованого та ризик-орієнтованого підходу до ПВК, де важливу роль відіграє постійна адаптація до сучасних викликів. Це забезпечує стійкість Сінгапуру до злочинних дій, підтримуючи його статус як надійного міжнародного фінансового центру.

Система обміну інформацією для оцінки придатності та доброчесності⁶

Документ є фінальним звітом щодо спільних настанов, розроблених Європейськими наглядовими органами (ЕВА, ЕІОРА, ЕСМА), для впровадження системи обміну інформацією між компетентними органами, яка забезпечує оцінку придатності та доброчесності осіб, що займають ключові посади у фінансових установах або володіють контрольними частками. Основною метою є підвищення ефективності нагляду та забезпечення узгоджених підходів у регулюванні фінансового сектору, що сприяє прозорості й стабільності ринку. Настанови базуються на Регламентах ЄС, які вимагають створення інструменту для обміну інформацією щодо осіб, що оцінюються.



Розроблена система ESAs Information System є

міжсекторальною базою даних, яка дозволяє компетентним органам визначати інші органи, що мають релевантну інформацію про особу, яка проходить оцінку. Система зберігає обмежений обсяг даних про таких осіб, зокрема основні ідентифікаційні дані, але без

деталізації результатів оцінок. Дані можуть бути доступні лише за принципом "необхідності знання", з метою забезпечення конфіденційності та відповідності нормам захисту даних ЄС. Сам обмін деталями між органами здійснюється поза системою, на двосторонній основі.

Настанови передбачають, що органи повинні вносити дані до системи протягом двох тижнів після отримання повідомлення або заявки на оцінку. Включаються як завершені, так і поточні

Висновки:

- Система ESAs Information System спрощує і прискорює обмін інформацією між компетентними органами, підвищуючи ефективність оцінок придатності та доброчесності осіб.
- Запровадження спільних настанов забезпечує гармонізацію практик регулювання, сприяючи стабільності фінансового сектору та зменшенню ризиків шахрайства.
- Дотримання норм захисту даних та обмежений доступ до системи мінімізують ризики неправомірного використання персональної інформації.
- Потреба у внесенні історичних даних (за останні 5 років для фізичних осіб та 2 роки для юридичних осіб) дозволяє забезпечити повноту бази даних і її ефективність із першого дня впровадження.

⁶ <https://www.eba.europa.eu/sites/default/files/2024-11/43114fbe-9a5a-412e-b461-955f86848ac3/Guidelines%20on%20ESAs%20system%20for%20exchange%20of%20information%20on%20fit%20and%20proper%20assessment.pdf>

оцінки, а також ті, що завершилися без остаточного рішення, наприклад, через відкликання заявки. Передбачено, що органи можуть надсилати запити на інформацію через систему, а відповіді мають надаватися у двотижневий термін, якщо це дозволяють правові норми. Усі дані зберігаються до 15 років, після чого автоматично видаляються, щоб уникнути надлишкового зберігання інформації про осіб, які більше не беруть участі у фінансовій системі.

Документ наголошує, що, хоча система значно спрощує обмін інформацією, остаточна відповідальність за проведення оцінки придатності та доброчесності залишається за компетентними органами. Кожна оцінка враховує контекст і нормативні вимоги, а результати можуть відрізнятися залежно від обставин. Настанови також враховують правові обмеження, пов'язані із захистом даних, і були узгоджені з Європейським інспектором із захисту даних.

Цей звіт підсумовує результати публічних консультацій, проведених із залученням компетентних органів. У процесі обговорення було враховано зауваження щодо необхідності захисту персональних даних, забезпечення прозорості процедур і зменшення адміністративного навантаження. Загальна оцінка підкреслює важливість цих настанов для підвищення ефективності нагляду та підтримання стабільності фінансового ринку.

Санкції

Великобританія розправляється з брудними грошима новими санкціями ⁷

21 листопада 2024 р. уряд Великої Британії запровадив санкції проти трьох відомих клептократів та їхніх спільників, які привласнювали багатства своїх країн для особистої вигоди. Ці заходи включають заборону на в'їзд та замороження активів і є першим кроком у новій кампанії міністра закордонних справ щодо боротьби з корупцією та незаконними фінансами.



Санкції були накладені на:

- Дмитра Фірташа — українського олігарха, який через корупцію та контроль над газорозподільчою системою вивіз з України сотні мільйонів фунтів стерлінгів. Частина цих незаконно отриманих коштів була інвестована в нерухомість у Великій Британії. Також під санкції потрапили його дружина Лада Фірташ, яка володіє активами у Великій Британії від його імені, та Денис Горбуненко, фінансовий махінатор, що сприяв корупційним схемам Фірташа.
- Ізабель душ Сантуш — доньку колишнього президента Анголи, яка зловживала своїми посадами в державних компаніях, привласнивши щонайменше 350 мільйонів фунтів стерлінгів, позбавляючи Анголу необхідних ресурсів для розвитку. Разом з нею санкції накладено на її подругу та бізнес-партнерку Паулу Олівейру та фінансового директора Сарджу Райкундалію, які допомагали виводити національні багатства Анголи для особистої вигоди душ Сантуш.

⁷ <https://www.gov.uk/government/news/uk-cracks-down-on-dirty-money-with-fresh-sanctions>

- Айварса Лембергса — одного з найбагатших людей Латвії, який використовував своє політичне становище для особистого збагачення. Його син, Анрійс Лембергс, також потрапив під санкції за сприяння корупційним діям батька.

Міністр закордонних справ Великої Британії Девід Леммі заявив, що ці санкції демонструють рішучість країни боротися з корупцією та захищати демократію, а також підтримувати економічне зростання. Він підкреслив, що "золота ера" відмивання грошей закінчується, і Великобританія більше не буде безпечним притулком для корумпованих осіб.

Ці заходи є частиною ширшої урядової стратегії, спрямованої на захист громадськості, зміцнення демократії та стимулювання економічного розвитку, протидіючи корупції та незаконним фінансам як на національному, так і на міжнародному рівнях.

Звіти окремих інституцій та експертів

Досвід країн щодо перевірки інформації про бенефіціарну власність⁸

Документ є оглядовою запискою, яка узагальнює основні аспекти вебінару «Досвід країн у перевірці інформації про кінцевих бенефіціарних власників» (КБВ). Вебінар, проведений 10 липня 2024 р., став продовженням триденного регіонального форуму, що відбувся в Буенос-Айресі у листопаді 2023 р., та був організований проектом ЄС Global Facility, GAFILAT та Інтер-Американським банком розвитку. У ньому взяли участь понад 150 експертів із 13 країн Латинської Америки, які представляли органи державної влади та міжнародні інституції.

Метою заходу було представлення найкращих практик і механізмів перевірки КБВ для забезпечення точності, актуальності та повноти даних перед новим раундом взаємних оцінок FATF. Основна увага приділялась системам верифікації у Бельгії, Австрії, Словаччині та практикам використання великих даних у Великій Британії.



Основні моменти:

Бельгія:

- Впроваджено механізм повідомлення про невідповідності, який дозволяє фінансовим установам та іншим компетентним органам повідомляти про невідповідності у даних про КБВ.
- Застосовуються профілактичні заходи, включаючи попереднє заповнення даних із державних реєстрів, перевірки на узгодженість і авторизацію даних КБВ.
- Активно проводиться інформаційна робота для підвищення обізнаності серед населення.

Австрія:

⁸ https://www.global-amlcft.eu/wp-content/uploads/2024/10/18.9.24-EUGF-GAFILAT-IDB_BO_compressed.pdf

- Використовується високий рівень автоматизації та взаємозв'язку баз даних. Інформація про КБВ попередньо заповнюється з інших державних реєстрів, що мінімізує ризик невідповідностей.

Висновки:

- **Бельгія продемонструвала ефективність механізму повідомлення про невідповідність**, який дозволяє швидко виправляти невідповідності у даних КБВ через взаємодію з компетентними органами та фінансовими установами.
- **Австрія забезпечила автоматизацію процесу верифікації КБВ**, що значно скоротило ручні перевірки та підвищило ефективність управління ризиками.
- **Словацьчина запровадила новаторський механізм перевірки КБВ через громадський контроль і відповідальність суб'єктів**, які отримують державне фінансування.
- **Велика Британія використовує аналітичні інструменти великих даних**, що дозволяють виявляти ризики на етапі реєстрації компаній, що є корисною практикою для юрисдикцій із високими ризиками незаконної діяльності.

- Здійснюється автоматичний моніторинг ризиків із використанням національної оцінки ризиків, що дозволяє ідентифікувати червоні прапорці.

Словацьчина:

- Унікальний механізм перевірки КБВ застосовується до суб'єктів, які отримують державне фінансування. Процес верифікації здійснюють «уповноважені особи», які несуть відповідальність за точність поданих даних.
- Система дозволяє громадськості подавати зауваження щодо даних КБВ, причому тягар доведення коректності даних лягає на зареєстрований суб'єкт.

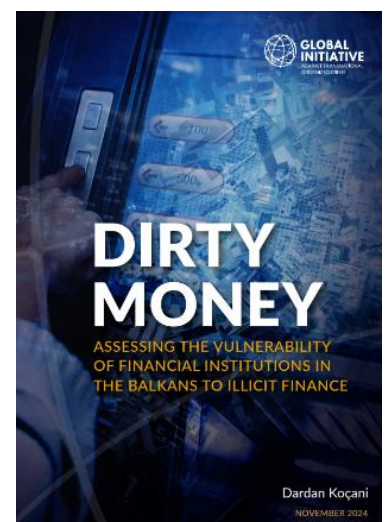
Велика Британія:

- Використовується система аналізу великих даних для виявлення підозрілих патернів під час реєстрації компаній, таких як незвичайні адреси чи повторювані елементи у назвах.

Захід закінчився обговоренням перспектив упровадження представлених механізмів у інших країнах, а також планами на організацію подальших навчальних заходів.

Брудні гроші: оцінка вразливості фінансових установ на Балканах до незаконного фінансування⁹

Документ досліджує ризики, пов'язані з відмиванням коштів та фінансуванням злочинної діяльності у фінансовій системі Західних Балкан. У центрі уваги — роль фінансових установ у сприянні злочинним фінансовим потокам та їхній потенціал для запобігання цим загрозам. Дослідження базується на даних, отриманих через інтерв'ю, офіційні документи та польові дослідження, і охоплює шість країн: Албанію, Боснію і Герцеговину, Косово, Чорногорію, Північну Македонію та Сербію.



⁹ <https://globalinitiative.net/wp-content/uploads/2024/11/Dardan-Kocani-Dirty-money-Assessing-the-vulnerability-of-financial-institutions-in-the-Balkans-to-illicit-finance-GI-TOC-November-2024.pdf>



Фінансові установи, особливо банки, залишаються ключовими об'єктами зловживань для злочинних мереж, які використовують їх на всіх етапах відмивання коштів: розміщення, розпорошення та інтеграція. Наприклад, банки надають доступ до глобальних фінансових ринків, але водночас демонструють серйозну вразливість через корупцію, слабкий нагляд і складні трансакції. Окрім банків, також аналізуються ризики, пов'язані з іншими фінансовими послугами, такими як обмін валют, мікрофінансування, криптовалюти та швидкі перекази.

Особливу увагу приділено криптовалютам і віртуальним активам, які сприяють анонімності фінансових потоків. У більшості країн регіону недостатньо регулювання криптовалютних послуг, що створює можливості для зловживань, таких як фінансування тероризму та відмивання коштів. Крім того, аналізуються проблеми з визначенням кінцевих бенефіціарів і використанням фіктивних осіб для приховування власності.

У документі наголошується, що хоча банки демонструють сильніші політики комплаєнсу

Висновки:

- **Фінансові установи Західних Балкан залишаються вразливими** до відмивання коштів через корупцію, слабкий нагляд і недостатню регуляцію криптовалют.
- **Недостатня інформація про кінцевих бенефіціарних власників** та використання фіктивних осіб створюють значні ризики для фінансової системи.
- **Ефективність підрозділів фінансової розвідки обмежується** недостатнім обміном інформацією з фінансовими установами та правоохоронними органами.
- **Необхідні кращі регуляторні рамки для криптовалютного сектору** та посилення комплаєнсу в усіх типах фінансових установ.

порівняно з іншими установами, їх ефективність обмежується недостатнім обміном інформацією з підрозділами фінансової розвідки та низьким рівнем знань у правоохоронців щодо боротьби з фінансовими злочинами.

Рекомендації включають:

- посилення співпраці між банками, ПФР та правоохоронними органами;
- запровадження технологій для аналізу трансакцій, включаючи інструменти розпізнавання ризиків;
- регуляція криптовалютного ринку з підвищенням вимог до провайдерів послуг віртуальних активів (VASPs);
- навчання співробітників фінансових установ для підвищення їхньої обізнаності щодо нових типологій фінансових злочинів.

Криптовалютна зрілість 2024: Покроковий шлях інтеграції цифрових активів у традиційні фінанси ¹⁰

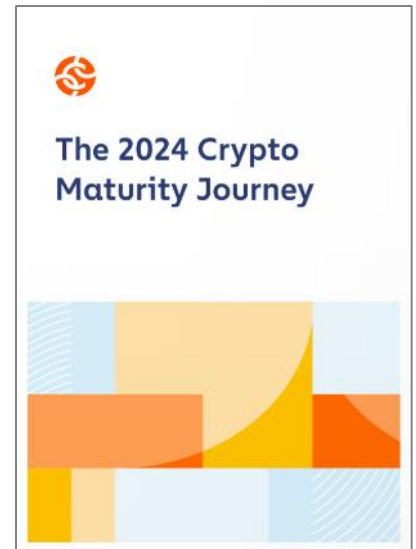
Документ є стратегічним посібником для фінансових установ, які прагнуть інтегрувати криптовалюту в свої бізнес-процеси. Він висвітлює, як фінансові організації можуть поступово впроваджувати криптовалютні продукти, зберігаючи при цьому баланс між інноваціями, регуляторною відповідністю та управлінням ризиками. Основна ідея документа полягає у створенні покрокового плану, який дозволяє установам адаптувати свої операційні процеси та продуктову лінійку до умов цифрової економіки.

¹⁰ <https://go.chainalysis.com/2024-crypto-maturity-journey.html>

Розглядаючи поступове впровадження криптовалют, автори визначають п'ять рівнів зрілості: від початкового етапу освіти та планування до складної інтеграції продуктів децентралізованих фінансів (DeFi) і розрахунків стейблкоїнами. Кожен рівень є логічним продовженням попереднього, що дозволяє мінімізувати ризики та поступово збільшувати залучення до криптоекосистеми.

На першому етапі (Рівень 0), фінансовим установам пропонується розпочати з формування команди ключових зацікавлених сторін, до якої входять експерти з інвестицій, корпоративного банкінгу, ризик-менеджменту та комплаєнсу. Основна увага зосереджена на вивченні базових принципів роботи криптовалют, використанні інструментів аналізу блокчейн-даних, таких як Chainalysis KYT, та оцінці поточного впливу криптовалют на діяльність установи. На цьому рівні важливо визначити ризик-апетит установи, а також заповнити прогалини в знаннях команди щодо специфіки криптоактивів.

На наступному рівні (Рівень 1) фінансові установи починають працювати з криптовалютними бізнесами, пропонуючи їм базові фінансові послуги. Це включає інтеграцію інструментів аналізу ризиків для оцінки клієнтів, що працюють у криптосекторі. Такі банки, як BankProv, демонструють приклад створення спеціалізованих послуг для криптокомпаній, включаючи рахунки у фіатній валюті та конверсію криптовалют у традиційні валюти. Успішна реалізація цього етапу потребує залучення досвідчених експертів, які розуміють специфіку криптоіндустрії.



Висновки:

- Підхід із п'яти рівнів дозволяє фінансовим установам мінімізувати ризики та забезпечувати поступову адаптацію до ринку криптовалют.
- Інтеграція криптовалютних сервісів потребує кооперації з технологічними партнерами, такими як Fireblocks або Chainalysis, для зменшення складності та підвищення ефективності.
- Регуляторні та аналітичні інструменти типу Chainalysis KYT та Address Screening сприяють ефективному управлінню ризиками та забезпеченню відповідності вимогам з ПВК/ФТ.
- Залучення криптовалют дозволяє традиційним фінансовим установам задовольняти запити клієнтів, пропонуючи нові інвестиційні продукти та рішення для управління цифровими активами.

На третьому рівні (Рівень 2) установи можуть пропонувати своїм клієнтам синтетичні криптовалютні продукти, які не передбачають зберігання криптоактивів. Прикладом таких продуктів є біржові торгові фонди (ETFs), створені компаніями BlackRock і Fidelity, які дозволяють інвесторам отримувати прибутки від зростання криптовалютного ринку без необхідності безпосередньо володіти активами. Такий підхід знижує ризики для установ і спрощує інтеграцію криптопродуктів у традиційну фінансову систему.

Рівень 3 передбачає безпосередню інтеграцію криптовалютних депозитів у продуктивний портфель банків. На цьому етапі клієнтам дозволяється зберігати цифрові активи у банку, що створює нові можливості для бізнесу. Партнерство з

криптокомпаніями, такими як Fireblocks, допомагає фінансовим установам подолати технічні складнощі впровадження. У цьому контексті важливо забезпечити надійність інфраструктури та відповідність регуляторним вимогам.

Нарешті, Рівень 4 присвячений розширенню послуг за межі депозитів. На цьому етапі установи впроваджують складні фінансові продукти, наприклад, DeFi-рішення для кредитування під заставу криптовалют або стейблкоїнові розрахунки. Компанії, як-от Fidelity, використовують криптоактиви як заставу для кредитів, а Visa інтегрує можливості розрахунків у стейблкоїнах, що свідчить про зростаючу адаптацію криптоекосистеми в глобальному фінансовому секторі.

Документ наголошує на важливості партнерств із криптокомпаніями, таких як Chainalysis, що надають інструменти для моніторингу транзакцій і управління ризиками. Впровадження інноваційних технологій дозволяє не лише покращити клієнтський досвід, але й забезпечити ефективну відповідність вимогам з ПВК/ФТ. У підсумку, документ закликає фінансові установи використовувати поетапний підхід до інтеграції криптовалют, зберігаючи прозорість і зосередженість на довгострокових стратегічних цілях.

Рекомендовані матеріали

Китайські компанії в податкових гаванях ¹¹

Нове дослідження показує, як китайські технологічні гіганти грають у податкову гру, відмінну від їхніх західних колег, і чому це важливо для глобальної конкуренції.

Революційне дослідження Noked і Wang проаналізувало 79 найбільших китайських технологічних компаній, які торгуються на американських біржах, і виявило вражаючу закономірність: УСІ вони стверджують, що вони є «підприємствами-нерезидентами» для податкових цілей Китаю, незважаючи на те, що вони мають більшість операцій, управління та активів у Китаї.

Чому це важливо:

- Китайські технологічні компанії отримують значну конкурентну перевагу над західними суперниками, які стикаються з вищими ефективними податковими ставками;
- Це може допомогти пояснити їхню швидку глобальну експансію та домінування на ринку;
- Незважаючи на посилення глобальних податкових правил, китайські компанії знайшли надійний спосіб зберегти податкові переваги;
- Структура знижує податки як на корпоративному рівні, так і на рівні акціонерів.

Китайська влада, схоже, знає та приймає цю практику, припускаючи, що це частина навмисної стратегії підвищення конкурентоспроможності китайських технологій у всьому



¹¹ <https://academic.oup.com/jiel/article/27/3/521/7778422>

світі. На відміну від США, у Китаї немає правил проти інверсії, щоб перешкоджати таким структурам.

Це дослідження допомагає пояснити, як китайським технологічним компаніям вдалося так швидко розвиватися і чому вони можуть зберегти переваги навіть у разі зміни глобальних податкових правил. Оскільки ці компанії виходять на міжнародний рівень, розуміння цих структурних переваг стає вирішальним для інвесторів, конкурентів і політиків.

Висновки:

- **Велика картина:** Такі компанії, як Alibaba, Baidu та Pinduoduo, можуть значно зменшити свій податковий тягар, реєструючи материнські компанії в таких місцях, як Кайманові острови, працюючи в Китаї. Це не помилка – це особливість податкової системи Китаю, розроблена для підвищення конкурентоспроможності.
- **Як це працює:** Хоча китайське законодавство передбачає, що компанії, керовані з Китаю, повинні сплачувати китайські податки, існує розумний обхідний шлях. Компанії можуть уникнути статусу «резидента», просто ведучи свою бухгалтерію та записи в офшорах і маючи деяких некитайських директорів, навіть якщо всі реальні операції здійснюються в Китаї. Ця структура дозволяє їм накопичувати неоподатковуваний прибуток у податкових гаванях.
- **Цифри:** З найбільших досліджуваних компаній, які представляють 93% ринкової капіталізації китайських фірм на американських біржах, кожна повідомила, що є «нерезидентом». Це включає гігантів у сфері технологій, побутових послуг, охорони здоров'я та фінансів. Ці компанії відкрито визнають у своїх річних звітах, що такий статус забезпечує істотну економію податків.
- **Глобальний вплив:** Навіть новий глобальний мінімальний податок у розмірі 15% (рівень 2) може не повністю закрити цю перевагу. Китайські компанії все ще можуть користуватися різними винятками та підтримувати нижчі податкові ставки, ніж якби вони були резидентами Китаю (що означало б 25% податку). Крім того, доходи багатьох компаній нижчі за ці нові правила.

Катастрофа TD Bank і як її виправити ¹²

Відео з каналу "Designated" з Яя Джата Фанусі детально аналізує роль TD Bank у фінансових скандалах, пов'язаних із відмиванням коштів та сприянням незаконній діяльності. У розмові з експертом із банківської справи та боротьби з фінансовими злочинами Джимом Річардсом обговорюються недоліки банківського контролю та їхні наслідки.



Особливу увагу приділено справі про зв'язки TD Bank із фінансуванням злочинних схем, включно з забезпеченням іпотек для лідера мафії в Торонто, Анджело Фільомені, навіть після його арешту в рамках найбільшого розслідування мафії у Канаді. Це викликає питання про ефективність внутрішнього контролю банку, який, за офіційними звинуваченнями, зазнав

¹² <https://www.youtube.com/watch?v=5dco8vE7Aco>

краху через керівників найвищого рівня, які допустили порушення норм Закону про банківську таємницю.

У відео також розглядається нещодавня справа, в якій TD Bank визнав свою провину у відмиванні коштів і сплатив рекордні \$3,1 млрд штрафу. Обговорюються наслідки таких дій для суспільства, руйнування довіри клієнтів та репутації банківського сектора.

Глядачі отримають:

- Розуміння, як великі банки можуть ставати каналами для відмивання коштів.
- Інсайти від Джима Річардса щодо реформ, які можуть посилити системи боротьби з фінансовими злочинами.
- Практичні рекомендації, як можна зменшити ризики подібних скандалів у майбутньому.

Відео дає змогу подивитися на сучасні виклики у фінансовій системі та важливість підвищення прозорості й підзвітності банківських установ.

Інші новини

В Україні започатковано Робочу групу з публічно-приватного партнерства у протидії фінансовим злочинам ¹³



15 листопада 2024 р. за підтримки Федерального міністерства закордонних справ Німеччини (Auswärtiges Amt), було офіційно започатковано Робочу групу з публічно-приватного партнерства у протидії фінансовим злочинам в Україні. Ініціатива співкерується Центром фінансів та безпеки (CFS) при RUSI та Центром фінансової доброчесності.

У Варшаві відбулась перша зустріч, яка об'єднала 40 представників публічного та приватного секторів з України, а також міжнародних експертів. Основна тема обговорення – побудова довіри як ключової основи для ефективної співпраці в протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ФТ). Довіра формується через взаємний обмін інформацією, зворотній зв'язок і партнерство.

Основні результати дискусії:

- Поточний прогрес: Ініціативи, такі як E-Cabinet українського ПФР та Digital Finance Ukraine Hub, є перспективними, проте потребують залучення ширшого спектра секторів, зокрема ВНУП і правоохоронних органів.
- Стратегічний фокус: Запровадження національної стратегії публічно-приватного партнерства може зробити співпрацю стандартною практикою, змінюючи культуру

¹³ <https://rusi.org/explore-our-research/projects/taskforce-public-private-partnership-fighting-financial-crime-ukraine>

фінансового моніторингу в Україні. Це також допоможе підвищити ефективність системи ПВК/ФТ у контексті майбутньої оцінки MONEYVAL.

- Віртуальні активи: Публічно-приватне партнерство має значний потенціал для сприяння кращому розумінню викликів і можливостей, пов'язаних із регулюванням віртуальних активів в Україні.
- Глобальні уроки: Моделі, такі як Спільна група з розвідки у сфері відмивання коштів у Великій Британії (UK Joint Money Laundering Intelligence Taskforce), Центр досконалості у сфері ПВК у Литві (AML Center of Excellence), і польська модель публічно-приватного партнерства демонструють, як цілеспрямований обмін інформацією скорочує обсяг нерелевантної звітності до ПФР та підвищує ефективність системи.

Робоча група з публічно-приватного партнерства у протидії фінансовим злочинам стане платформою для інновацій та співпраці, сприяючи посиленню фінансової доброчесності в Україні в умовах викликів сьогодення.

Футбольний скандал: як тренера ФК «Цюрих» запідозрили у відмиванні 2,2 мільйона євро¹⁴

Стаття розповідає про скандал навколо Ромео Кастелена, колишнього футболіста з Нідерландів, який займав посаду тренера талантів у футбольному клубі «Цюрих». Кастелен, відомий своєю кар'єрою в таких країнах, як Нідерланди, Німеччина, Австралія та Китай, був найнятий клубом на початку жовтня 2024 року. Його робота отримала схвальні відгуки, однак через місяць контракт із ним було розірвано з його ініціативи, посилаючись на «приватні причини». Насправді, це стало наслідком розслідування, що триває в Нідерландах, де Кастелена звинувачують у причетності до відмивання грошей.

Згідно з даними нідерландських ЗМІ, розслідування охоплює період у п'ять років, і прокуратура підозрює, що Кастелен брав участь у схемі відмивання близько 2,2 мільйона євро. Гроші, ймовірно, отримані злочинним шляхом, були переведені з Нідерландів до Китаю. Особливу увагу слідства привернув випадок, коли Кастелен був затриманий в аеропорту Схіпгол в Амстердамі з 139 000 євро готівкою, які він збирався перевезти до Китаю. Прокурори також стверджують, що Кастелен використовував фальшиві контракти одного з китайських футбольних клубів для створення враження, що гроші були отримані законним шляхом.

У розслідуванні фігурує ще один підозрюваний – футбольний агент. Однак Кастелен і його адвокат відкидають усі звинувачення. Вони стверджують, що великі суми грошей є звичайною практикою у світі професійного футболу. Адвокат також пояснює, що кошти мають



¹⁴ https://www.blick.ch/fr/sport/football/super_league/un-petit-mois-et-sen-va-accuse-de-blanchiment-dargent-romeo-castelen-a-quitte-zurich-id20313417.html

законне походження, зокрема від заробітної плати, комісійних за діяльність агента, вигравів у казино та продажу дорогих годинників. У свою чергу, деякі працівники казино підтверджують, що Кастелен був успішним гравцем, який регулярно вигравав значні суми.

Незважаючи на тяжкість звинувачень, на цей момент Кастелен не був особисто присутній на слуханнях у суді міста Зволле, де розглядається справа. Його адвокат активно захищає позицію свого клієнта, акцентуючи на відсутності доказів злочинного походження коштів.

Ця справа демонструє складність виявлення та переслідування схем відмивання грошей у світі спорту. Висвітлюючи деталі розслідування, стаття також підкреслює ризики, з якими стикаються організації, що не проводять належної перевірки співробітників. Скандал завдав репутаційної шкоди ФК «Цюрих», який не знав про розслідування, коли наймав Кастелена. Судовий процес триває, і обвинувачений наразі зберігає презумпцію невинуватості.

Для загального розвитку

Цільовий підхід до розслідувань криптовалюти¹⁵

Стаття описує цільовий підхід до розслідувань, пов'язаних із криптовалютами, що фокусується на глибокому аналізі ключових суб'єктів злочинної діяльності, а не лише на окремих транзакціях. Цей підхід передбачає використання сучасних інструментів для аналізу та візуалізації даних, таких як GraphSense або Chainalysis, що дозволяє створювати комплексні графічні моделі зв'язків і потоків фінансів. Особлива увага приділяється інтеграції різних джерел даних, включаючи соціальні мережі та комунікаційні дані, щоб виявляти структури злочинних схем і визначати їхніх ключових учасників. Такий підхід забезпечує кращу адаптацію до складних умов розслідувань у криптопросторі, підвищує точність і ефективність роботи, а також сприяє формуванню доказової бази, яка може бути використана в судових процесах. Основним акцентом є створення повної картини злочинної діяльності, яка допомагає зрозуміти мотивацію злочинців і їхні методи роботи.



Відмивання грошей у торгівлі: короткий огляд

Відмивання коштів у торгівлі (TBML) – це метод, який використовують злочинці для маскуванню незаконних коштів через міжнародні торгові операції. Ця форма відмивання коштів використовує законні торговельні практики, такі як маніпуляції з рахунками-фактурами або фальсифікація торгових документів, щоб приховати справжнє походження та призначення незаконних грошей. Оскільки глобальна торгівля зростає, TBML став серйозною

¹⁵ <https://www.linkedin.com/pulse/target-centric-approach-cryptocurrency-investigations-brennan-long-3e5ze/?trackingId=qz%2ByvIN6Qp2%2BZ0emcj5TAA%3D%3D>



проблемою для органів влади, оскільки його важко виявити та часто включає складні багатонаціональні мережі.

Як працює ТВМЛ

ТВМЛ використовує кілька методів для переміщення незаконних грошей через кордони, не привертаючи уваги. Деякі з найпоширеніших методів включають:

1. Завищення та заниження рахунків-фактур:

- Завищене виставлення рахунків: завищення ціни на товари, щоб перемістити більше грошей, ніж фактична вартість товарів.
- Виставлення занижених рахунків: декларування вартості товарів нижчої від їх фактичної вартості, що дозволяє переказувати незаконні кошти за нижчою ціною.

2. Фальшива документація:

- Злочинці можуть використовувати підроблені рахунки-фактури, коносаменти та митні документи, щоб приховати справжній характер операцій.

3. Кілька рахунків-фактур для однієї транзакції:

- Створення кількох рахунків-фактур для тих самих товарів може приховати фактичну вартість угоди.

4. Зловживання зонами вільної торгівлі:

- Зони вільної торгівлі з пом'якшеними митними правилами можуть бути використані для переміщення незаконних коштів під виглядом законних операцій.

5. Використання підставних компаній:

- Злочинці часто створюють фальшиві компанії, які не займаються реальним бізнесом, а використовуються для здійснення шахрайських торгових операцій.

Проблеми у виявленні ТВМЛ

Виявлення ТВМЛ складно, оскільки торгівля за своєю суттю є законною та передбачає великі обсяги транскордонних операцій. Деякі виклики включають:

- Обсяг торгівлі: величезний масштаб міжнародної торгівлі ускладнює моніторинг кожної операції.
- Складність транзакцій: численні посередники, підставні компанії та непрозорі структури власності ускладнюють виявлення незаконних потоків.

Наслідки ТВМЛ

ТВМЛ створює серйозні ризики як для фінансової системи, так і для світової торгівлі:

- Підриває фінансову чесність: ТВМЛ дозволяє злочинним підприємствам відмивати гроші, спотворюючи ринки та фінансуючи подальшу незаконну діяльність.
- Втрата податкових надходжень: шахрайське виставлення рахунків-фактур і заниження звітності може призвести до втрати митних зборів і податків.
- Спотворює торгівлю: ТВМЛ може створити недобросовісну конкуренцію, збільшити витрати бізнесу та зашкодити законній торговій практиці.



Боротьба з TBML

Для боротьби з TBML вживаються різні заходи:

1. Посилена належна перевірка: Фінансові установи все частіше зобов'язані перевіряти транскордонні операції та перевіряти торгові документи.
2. Міжнародне співробітництво: Обмін даними про торгівлю та транскордонне співробітництво допомагає владі виявляти підозрілі моделі.
3. Інструменти аналізу даних: Фінансові установи використовують машинне навчання та автоматизовані інструменти для виявлення аномалій у торговельних операціях.

Контакуйте щодо цього документу з Держфінмоніторингом:

- Email: bulletin@fiu.gov.ua
- Поштова адреса: Державна служба фінансового моніторингу України, Україна, 04050 м. Київ, вул. Білоруська, 24
- Ідентифікація контакту: стосовно Методологічного Бюлетеня № ДСФМУ-ДК-2024-036

Бюлетень є волонтерською розробкою методологічної команди Державної служби фінансового моніторингу України відповідно до пункту 18 частини 2 статті 25 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 Держфінмоніторингу].