Серійний номер: ДСФМУ-ДК-2024-005
Квітень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Публічні консультації щодо проєкту змін до Р.16 та ПЗР.16

Вольфсберзька Група надає коментар FATF щодо запропонованих змін до Рекомендації 16 та Пояснювальної Записки до неї. Платіжна індустрія значно розвинулася з моменту публікації цих інструкцій, і Вольфсберзька Група вітає ініціативу щодо їх оновлення. Вона вважає, що «платіж є платіж» і що будь-яка організація, незалежно від того, як вона описується або як себе називає, повинна підпадати під дію Р.16 відповідно до принципу «однакова діяльність, однаковий ризик, однакове правило». У своїй відповіді Група підкреслює важливість майбутньої перевірки Рекомендації шляхом прийняття термінології ISO20022, життєво важливої ролі, яку мають відігравати оператори інфраструктури платіжного ринку (PMI), тому що якщо обов'язкова інформація не може вміститись у повідомлення, то або PMI має розвинути спроможність працювати з інформацією, або вони не повинні дозволяти діяльність, яка потребує використання такої інформації. Відповідь Вольфсберзької Групи також підкреслюється важливість використання правильного інструменту для поточної роботи, а не намагання використовувати Р.16 для засобів контролю, які більш доцільно було б розглянути в Р.10 про належну перевірку клієнта.

https://bit.ly/4bckCgs

Проект ЕВА щодо нових видів платіжного шахрайства та можливих пом'якшувальних заходів

📣 29 квітня 2024 р. оновлення PSD3 і PSR. Європейське банківське управління (EBA) опублікувало проєкт висновку, в якому воно оцінює дані про шахрайство з платежами, які нещодавно стали доступними для EBA, визначає нові типи та моделі шахрайства з платежами та розробляє пропозиції щодо їх пом'якшення. Ключові моменти:

▶ Миттєві платежі мають вищі показники шахрайства, ніж традиційні кредитні перекази, що значно впливає на клієнтів.

▶ Незважаючи на надійну автентифікацію клієнтів, з'явилися нові складні типи шахрайства, зокрема через соціальну інженерію.

▶ EBA пропонує додаткові заходи для PSD3/PSR, включаючи посилену безпеку постачальників платіжних послуг, структуру управління ризиками шахрайства, змінені правила відповідальності, посилений нагляд та уніфіковану платформу ЄС для виявлення шахрайства.

Отже:

✓ Постачальники платіжних послуг повинні стежити за подальшими змінами в рамках PSD3 і PSR щодо структури боротьби з шахрайством.

✓ Постачальники платіжних послуг повинні переглянути або запровадити систему управління ризиками шахрайства.

✓ Постачальники платіжних послуг повинні проводити періодичну оцінку ризиків шахрайства.

https://bit.ly/44pZEZd

Оновлення керівництва з фінансових злочинів

Керівництво з фінансових злочинів і FCA: Управління з питань фінансової поведінки Великобританії (FCA) пропонує оновлення свого Посібника з фінансових злочинів (FC Guide) щодо санкцій, фінансування розповсюдження та моніторингу транзакцій.

FCA також пропонує додати посилання на криптоактиви та споживчий збір, а також відповідні зміни в посібнику FCA.

Завдяки цим змінам FCA має намір:

- допомогти фірмам зрозуміти, чого очікує FCA;

- допомогти фірмам оцінити належність їхніх систем фінансових злочинів і засобів контролю;

- усунути недоліки.

https://www.fca.org.uk/publication/consultation/cp24-9.pdf

Наглядовий звіт з ПВК/ФТ за 2022-2023 фіскальний рік

Скарбниця Його Величності опублікувала свій одинадцятий щорічний звіт про політику ПВК/ФТ, що охоплює 2022-2023 фінансовий рік.

У звіті детально описано зусилля Великобританії у боротьбі з фінансовими злочинами шляхом ефективного регулювання та нагляду. Це підкреслює важливість співпраці між Скарбницею і наглядовими органами, такими як Управління з питань фінансової поведінки, Податкове та митне управління Його Величності та Комісія з азартних ігор. Ці інституції відіграють ключову роль у забезпеченні того, щоб регульовані підприємства дотримувалися нормативних актів шляхом перевірок, оновлень ризиків і коригувальних заходів.

У документі також наголошується на покращеннях після перегляду нормативних актів щодо протидії відмиванню коштів та фінансуванню тероризму у 2022 році, включаючи запровадження нової системи ефективності для оцінки впливу нагляду та реформ, спрямованих на посилення цих заходів. Ризик-орієнтований підхід, прийнятий у наглядовій діяльності, має важливе значення для розподілу ресурсів у сферах високого ризику та ефективної боротьби із загрозами відмивання коштів і фінансування тероризму.

https://bit.ly/4dq6S3u

Річний звіт ПФР Швейцарії

У звіті надається докладний огляд діяльності, стратегічних розвитків та статистичних аналізів, пов'язаних із протидією відмиванню коштів та фінансування тероризму в Швейцарії. Він включає оцінку несподіваного зростання кількості Повідомлень про підозрілу діяльність (SARs), що відображає суворіші заходи щодо дотримання вимог, покращені технології моніторингу та зміни у законодавстві. Звіт також висвітлює розвиток у регулюванні та комплаєнсі, включаючи адаптації до ризик-орієнтованого підходу до моніторингу, вплив нових законів та міжнародних санкцій, особливо стосовно Росії та Хамасу. Подальші деталі присвячені використанню криптовалют і віртуальних активів, опису ризиків та регуляторних відповідей, а також посиленню спроможностей з протидії відмиванню коштів через публічно-приватне партнерство. Значну увагу приділено статистичним даним, які надають уявлення про характер видів діяльності щодо яких надходять повідомлення. Загалом, звіт підкреслює складність і масштаби зусиль, необхідних для управління та мінімізації ризиків, пов'язаних з відмиванням коштів та фінансуванням тероризму, відображаючи як виклики, так і прогрес у стратегіях регулювання та правозастосування в Швейцарії.

https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/jb.html

Детальна оцінка ризиків у сфері ПВК/ФТ Британських Віргінських Островів

Цей звіт підсумовує заходи з протидії відмиванню коштів/фінансуванню тероризму (ПВК/ФТ), що діють на Віргінських Островах (ВО) станом на дату виїзного візиту 15-30 березня 2023 року. У ньому аналізується рівень дотримання 40 Рекомендацій Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) та рівень ефективності системи ПВК/БФТ ВО, а також надаються рекомендації щодо того, як можна посилити цю систему.

https://bit.ly/4dnIBLs

ЗВІТ ПРО РОЛЬ ПФР У БОРОТЬБІ З ВИКОРИСТАННЯМ НПО ДЛЯ ФІНАНСУВАННЯ ТЕРОРИЗМУ

Егмонтська група об'єднуючи 174 підрозділи по всьому світу, випустила ґрунтовний звіт, підготовлений Робочою групою з обміну інформацією. Цей ключовий документ під назвою "Роль ПФР у боротьбі із зловживаннями некомерційними організаціями для фінансування тероризму" висвітлює стратегічні та операційні ролі, які відіграють підрозділи фінансової розвідки (ПФР) у протидії незаконному використанню неприбуткових організацій (НПО) для фінансування тероризму (ФТ).

Звіт окреслює складність та масштаби цього виклику, зазначаючи, що некомерційний сектор, який часто діє на міжнародному рівні в районах конфліктів, залишається уразливим до експлуатації з метою фінансування тероризму. Ця вразливість посилюється присутністю НПО в середовищі, де вони працюють поруч або близько до терористичних угруповань. Визнаючи це, Група Егмонт прагнула покращити розуміння типологій зловживань НПО та посилити глобальну протидію цим загрозам.

Внески від багатьох ПФР, зокрема з Ізраїлю, Нігерії, Австралії, Канади, Фінляндії, Греції, Маврикію, Нідерландів, Південної Африки та Великобританії, були ключовими для підготовки звіту. Їх дані показують, що терористичні організації адаптували свої механізми фінансування у відповідь на глобальні заходи з протидії фінансуванню тероризму, все частіше використовуючи новітні методи, такі як децентралізовані фінанси (DeFi), віртуальні активи та фінтех-платформи.

Документ наголошує на критичній важливості міжнародної співпраці та ефективного обміну інформацією між ПФР для запобігання та припинення експлуатації НКО терористами. Також розглядається необхідний баланс між впровадженням жорстких заходів для запобігання зловживанням і забезпеченням того, щоб законна гуманітарна діяльність не була надмірно обмежена.

Цей звіт Егмонтської групи є не лише свідченням постійних зусиль із захисту цілісності глобальної фінансової системи, а й закликом до подальшої пильності та співпраці між міжнародними спільнотами фінансової розвідки.

Метою звіту є підтримка постійних зусиль у боротьбі проти зловживання НПО для ФТ. Це досягається шляхом виявлення, оновлення та розширення наявної інформації для розробки нових знань про типології та фінансові загрози. Крім того, звіт має на меті надати огляд того, як ПФР максимально ефективно використовують міжнародну співпрацю, обмінюючись фінансовою інформацією та розвідданими для покращення виявлення та досягнення кращих результатів у припиненні зловживання НПО для фінансування тероризму.

https://bit.ly/3UJDJck

ФІНАНСУВАННЯ КРАЙНІХ ПРАВИХ ЕКСТРЕМІСТСЬКИХ УГРУПУВАНЬ

Егмонтська група випустила свій останній звіт під назвою "Фінансування тероризму екстремістських правих груп Фаза II". Цей документ, продовження їхнього початкового звіту 2022 року, досліджує фінансування екстремістських правих терористичних груп, з фокусом на покращенні розуміння та виявленні таких активностей у всесвітньому масштабі. У цьому другому звіті визначаються основні обмеження та виклики на основі початкових висновків, пропонуються поліпшення та розширюється обсяг з білатеральних на мультилатеральні заходи боротьби з загрозами. Детальний аналіз охоплює оновлення щодо загроз фінансування екстремістського правого тероризму, випробування конкретних показників XRWTF та операційний аналіз основних екстремістських груп.

Звіт також надає висновки з спільних операційних аналізів та використовує новостворений зразок спільних зусиль. Важливим висновком з звіту є те, що екстремістські праві групи мають розпливчаті зв'язки на всесвітньому рівні, позбавлені єдиної, спланованої ідеології, що ускладнює виявлення та реагування з боку ПФР та правоохоронних органів.

https://bit.ly/3y14eRD

Викриття імперативу прозорості військових витрат

Звіт "Trojan Horse Tactics: Unmasking the imperative for transparency in military spending" від Transparency International обговорює збільшення витрат на оборону на тлі глобальних конфліктів та підкреслює зв'язок між витратами на оборону і корупцією. Використовуючи дані Індексу прозорості уряду та Стокгольмського міжнародного інституту досліджень миру, документ аналізує, як відсутність прозорості може сприяти корупції в оборонних витратах, і наголошує на необхідності посилення інституційної стійкості до корупційних ризиків.

https://ti-defence.org/publications/trojan-horse-tactics-transparency-military-spending-corruption-risk/

РЕГУЛЮВАННЯ

Санкції США

Президент Сполучених Штатів підписав HR 815. Законопроект складається зі 133 сторінок і охоплює безліч тем, зокрема ПВК та Санкції. Наслідки досить далекосяжні...

У двох словах, ось оновлення санкцій у HR 815:

☼Збільшено термін давності за порушення санкцій з 5 до 10 років

☼Законопроект Прагне гармонізувати санкції США щодо Росії з санкціями Великобританії та ЄС

☼Передбачаються санкції проти іранської нафти та ракетної програми Ірану

☼Націленість на китайські організації за їх роль в ухиленні від іранських нафтових санкцій

☼Розширено правило про прямі іноземні товари стосовно певних товарів, призначених до Ірану.

https://bit.ly/4bg4OZY

Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) і Державний департамент США вжили заходів проти здатності Росії продовжувати війну проти України, націлюючись на компанії, фізичних осіб та іноземних партнерів, які підтримують військово-промисловий комплекс Росії. Зокрема, OFAC і Держдеп санкціонували цілі, пов'язані з російськими програмами БПЛА, біологічної та хімічної зброї.

Крім того, Казначейство та держава націлилися на закупівельні мережі та міжнародних партнерів, у тому числі компанії, розташовані в Китаї, які «надають важливий внесок у військово-промислову базу Росії».

На додаток до 80 юридичних та фізичних осіб OFAC включив криптовалютні адреси, пов'язані з російською компанією «Конструкторське бюро «Око», яка розробляє дешеві багатофункціональні безпілотні літальні апарати (БПЛА). Oko design збирав пожертви в криптовалюті через канал Telegram. Однак адреси отримали незначну суму коштів - менше 1000 доларів США - і, здається, неактивні.

Директива щодо визначення кримінальних злочинів і покарань за порушення обмежувальних заходів Союзу

Щойно ЄС видав нову директиву про криміналізацію порушення санкцій, згідно з якою кожен випадок порушення санкцій ЄС тепер буде розглядатися як злочин. Нова Директива має на меті узгодити визначення кримінальних правопорушень, види та рівень покарань, акцентує увагу на питаннях заморожування та конфіскації (своєрідне поєднання з директивою ЄС щодо повернення активів) тощо. Звичайно, гуманітарна допомога та діяльність правників є винятками, відповідно до нової Директиви.

Усі країни-члени мають прийняти Директиву до 20 травня 2024 року.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401226

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Стійкість і цілісність фінансової системи України

Опубліковано звіт CFS про зусилля з протидії відмиванню коштів в Україні!

Звіт ґрунтується на онлайн-семінарі CFS, проведеному в лютому – два роки після повномасштабного вторгнення Росії в Україну – на якому обговорювалися стійкість і цілісність фінансової системи України.

Семінар зібрав представників ключових українських фінансових установ та відповідних органів влади, щоб обговорити технічну відповідність країни стандартам Financial Action Task Force (FATF) та ефективність реагування на фінансові злочини.

У звіті, який написали Оксана Ігнатенко та Арзу Аббасова представлено підсумки дискусії, зосереджені на чотирьох основних напрямках:

- розвиток законодавства про віртуальні активи;
- шлях до створення єдиного реєстру банківських рахунків фізичних та юридичних осіб;
- державно-приватне партнерство;
- повернення доходів, одержаних злочинним шляхом.

https://bit.ly/4aGZJtM

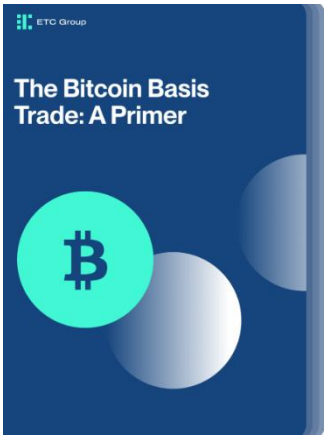
Про DeFi та On-Chain CeFi: як (не) регулювати децентралізовані фінанси

У статті пропонується структура для оцінки фактичної децентралізації фінансової інфраструктури на основі блокчейну, яку зазвичай називають «децентралізованими фінансами» (DeFi). У ній розглядаються різні вектори централізації вздовж рівнів архітектури DeFi з технологічної та юридичної точок зору. Розрізняючи ендогенну та успадковану централізацію, показано важливість оцінки децентралізації для регуляторів. По-перше, вектори централізації є вагомим свідченням того, що проект DeFi може мати (деякі) кастодіальні властивості, які вимагають регулювання. По-друге, вектори централізації розкривають шляхи контролю в проектах, вказуючи на відповідні регуляторні гачки. Стаття є міждисциплінарним вступом, який аналізує фінансову інфраструктуру на основі блокчейну та надає політикам і регуляторам інструмент для визначення відмінностей між справді незалежною, нейтральною інфраструктурою та фальшивою децентралізацією. У ньому зроблено висновок, що перша може мати дуже корисні властивості та може сприяти створенню більш відкритої та прозорої фінансової системи, тоді як друга є формою фінансового посередництва на основі блокчейну та має регулюватися як така.

https://academic.oup.com/jfr/advance-article/doi/10.1093/jfr/fjad014/7606986

Інвестиційне обґрунтування біткойна

Документ, підготовлений ETC Group, надає аналіз інвестиційного потенціалу Bitcoin та його основного значення на перетині передових технологій та фінансів. Цей звіт висвітлює



фундаментальні аспекти Bitcoin, як ключового активу у сфері інвестицій, зокрема для професійних інвесторів, які прагнуть диверсифікації та стійкості своїх портфелів.

Основний акцент у звіті зроблено на притаманній дефляції Bitcoin, зумовлену такими механізмами, як події зменшення винагороди за блок (halving) та алгоритм консенсусу proof-of-work. Видання також підкреслює, як глобальні тенденції масового прийняття та ефекти мережі зміцнюють його статус як надійного засобу зберігання вартості та засобу обміну на тлі зростаючих світових фінансових невизначеностей.

Розглядаються різні моделі оцінювання Bitcoin, включно з аналізом блокчейну. В звіті наголошено на історичній ефективності Bitcoin та його ролі як інноваційного технологічного активу, який перетворився з експериментальної цифрової валюти на визнаний глобально фінансовий актив.

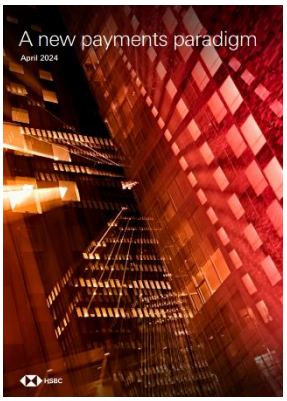
https://etc-group.com/blog/special-reports/the-investment-case-for-bitcoin/

Як Lazarus Group відмила 200 мільйонів доларів від 25+ крипто-зломів у фіат у 2020–2023 роках

Для того аби зрозуміти, як Північна Корея відмиває вкрадені від зламів кошти, прочитайте 15-місячне розслідування ZachXBT, проведене за допомогою TRM Labs для відстеження потоків коштів. У звіті описано 25 експлойтів і використовується TRM для відстеження коштів через міксери та різні блокчейни.

https://zora.co/collect/base:0xb445b5c8deadb38458b857a96cb8b74305a903cd/1

Нова парадигма платежів



Документ "A new payments paradigm", опублікований у квітні 2024 року, розглядає адаптацію корпоративних казначеїв до швидкозмінних тенденцій у платіжних технологіях. У цьому контексті, документ охоплює широкий спектр сучасних платіжних рішень, включаючи реальні платежі, цифрові гаманці, криптовалюти, стейблкоїни та цифрові валюти центральних банків (CBDC). Він підкреслює виклики та можливості, пов'язані з цими технологіями, зокрема у сферах безпеки, регулювання та управління ліквідністю. Особливу увагу приділено застосуванню блокчейну та технології розподілених реєстрів (DLT) для оптимізації платіжних процесів і підвищення ефективності казначейств, а також новітнім методам автентифікації, включно з біометричними технологіями, які покращують безпеку транзакцій. Документ також акцентує на необхідності стратегічних партнерств і інтеграції передових технологій для ефективної адаптації до нових платіжних моделей, що є ключовими для підготовки корпоративних казначеїв до майбутнього платіжного ландшафту.

https://www.gbm.hsbc.com/-/media/media/gbm-global/pdf/articles/a-new-payments-paradigm-report.pdf

Ризики відмивання коштів у сфері комерційної нерухомості: аналіз 25 кейсів

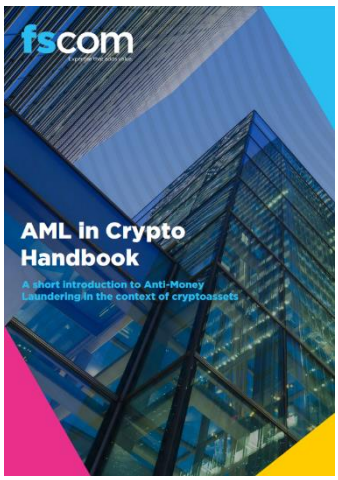
У звіті Global Financial Integrity ідентифіковано 25 випадків, коли незаконні, ймовірно незаконні або підозрілі кошти були спрямовані в комерційну власність у

Сполучених Штатах приблизно за останні 20 років. Із загальною вартістю власності, що перевищує 2,6 мільярда доларів, Каліфорнія, Флорида та Нью-Йорк є одними з найбільш сприятливих місць для цих незаконних інвестицій, але злочинці ховали гроші приблизно у 20 різних штатах.

«Кошти, використані для купівлі комерційної нерухомості в Сполучених Штатах, надходили з 14 різних країн, включаючи Росію (4 випадки), Мексику (4 випадки), Китай, Малайзію, Іран і Казахстан».

https://bit.ly/4a8ljGx

Довідник з ПВК у Крипті: Короткий вступ до боротьби з відмиванням коштів у контексті криптоактивів



Даний посібник пояснює, що таке блокчейн, розподілені реєстри (DLT), гаманці, адреси та хеші транзакцій у криптовалютах. Далі йде огляд основних видів криптоактивів, таких як біткоїн, ефіріум, стейблкоїни, DeFi та NFT.

Посібник також розглядає відповідні нормативні акти та керівництва, зокрема рекомендації FATF, 5-ту Директиву ЄС з боротьби з відмиванням коштів та секторальне керівництво JMLSG для постачальників послуг віртуальних активів.

Детально описуються ризики, пов'язані з криптовалютами, такі як шахрайство, відмивання коштів, фінансування тероризму та санкційні ризики. Наводяться приклади відповідних типологій.

Окремий розділ присвячений елементам системи протидії відмиванню коштів для крипто-компаній: оцінці ризиків, належній перевірці, моніторингу блокчейну, розслідуванням, звітності та навчанню персоналу. Надаються практичні поради щодо їх впровадження.

https://bit.ly/49YjlbW

Виклики для протидії фінансуванню розповсюдження та санкційного контролю в банківській сфері

У зв'язку із все більш складним ландшафтом санкцій, необхідні заходи для посилення фінансової системи проти фінансування розповсюдження зброї масового знищення (ФР) та ухилення від санкцій. Хоча уряди відіграють роль у встановленні нормативно-правового ландшафту для боротьби з ФР та збереження цілісності глобальної фінансової системи, вони покладаються на глобальну співпрацю фінансового сектору для досягнення ефективної боротьби з ФР та імплементації санкцій.

Цей звіт підтримує фінансовий сектор, визначаючи проблеми, з якими стикаються фінансові установи при впровадженні заходів боротьби з ФР та санкційного контролю, та надаючи рекомендації щодо вирішення таких проблем. Згідно оптуванням авторів з експертами, чотири ключові проблеми ефективної боротьби з ФР та виконання санкцій:

- Розрив між нормативними очікуваннями та практичною реалізацією.
- Обмежена якість та цілісність даних.
- Обмежена експертиза у предметній області.

- Розбіжності у банківському секторі щодо оцінки ризиків ФР та санкцій.

Для вирішення цих проблем автори наводять рекомендації для компетентних органів та банківського сектору, такі як публікація керівних настанов, організація круглих столів між юрисдикціями, покращення якості даних тощо.

https://bit.ly/3UGfPyu

Майбутнє фінтеху Великобританії – 2015-2035

Звіт під назвою "Майбутнє фінтеху в Великобританії: 2015 – 2035" презентовано під час Тижня фінтеху у Великобританії 2024 року. Він включає огляди від лідерів індустрії і досліджує тенденції та майбутні інновації у сфері фінансових технологій. Звіт аналізує вплив фінтеху на фінансові послуги, розвиток нових технологій та споживчий ринок у Великобританії. Хоча звіт не зосереджується безпосередньо на темі відмивання грошей. Цей документ детально розглядає тенденції і перспективи розвитку фінансових технологій в Великобританії, включно з інноваціями у сфері банківських послуг і новітніми технологічними рішеннями.

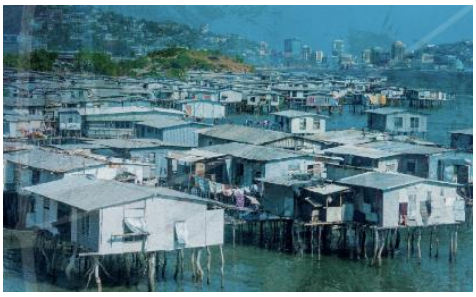
https://bit.ly/3UJctuA

Величезний новий набір даних може посилити «полювання» ШІ на відмивання коштів у криптовалюті

Стаття описує новий підхід Elliptic спільно з MIT та IBM у виявленні відмивання грошей через блокчейн Bitcoin, використовуючи штучний інтелект. Вони розробили AI-модель, яка аналізує патерни транзакцій, щоб виявляти потенційно підозрілу діяльність. Дослідники зібрали дані з 200 мільйонів транзакцій, виокремивши 122,000 субграфів, які містять відомі схеми відмивання грошей. Ефективність AI було перевірено на реальних даних, що вказує на потенціал інструменту у значному зменшенні часу, необхідного для виявлення підозрілої активності у фінансовій сфері.

https://www.elliptic.co/blog/our-new-research-enhancing-blockchain-analytics-through-ai

Транснаціональна організована злочинність і острови Тихого океану

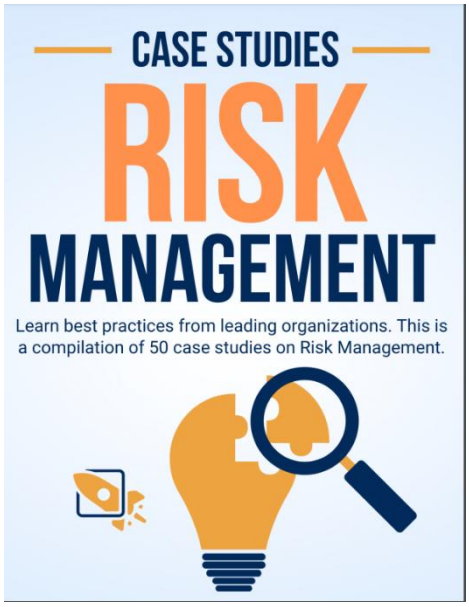


Звіт Global Initiative аналізує, як транснаціональна організована злочинність впливає на Тихоокеанські острови, висвітлюючи злочинні мережі, що використовують цей регіон як транзитний пункт для незаконного перевезення наркотиків, людей, а також для незаконного рибальства. Дослідження підкреслює роль місцевих та іноземних злочинних угруповань, що використовують слабкі урядові структури та високий рівень корупції для своїх цілей, водночас вказуючи на стратегії та рекомендації для посилення правопорядку та міжнародної співпраці для боротьби з цими викликами.

https://globalinitiative.net/analysis/transnational-organized-crime-and-the-pacific-islands/

РЕКОМЕНДОВАНІ КНИГИ

«50 прикладів з управління ризиками»



Документ "Flevy Management Insights" є збіркою кейсів, що розглядають різноманітні аспекти управління ризиками в багатьох індустріях. Книга зосереджується на стратегічних викликах і рішеннях, які використовуються великими компаніями для забезпечення безпечного і ефективного бізнес-процесу в умовах ризику. Вона включає ретельні аналізи ситуацій, що виникають у таких секторах, як фінанси, технології, роздрібна торгівля, виробництво та охорона здоров'я.

Кожен кейс у книзі надає детальний опис викликів, з якими стикаються організації, а також стратегій, що були розроблені та впроваджені відомими консультативними фірмами, такими як McKinsey, BCG, Bain, Deloitte та Accenture, для вирішення цих проблем. Основні моменти включають розробку системи управління ризиком, управління кібербезпекою, фінансовий ризик-менеджмент і рамки управління ризиками для інфраструктурних проєктів у великих урбанізованих системах.

Книга розрахована на виконавчих директорів, управлінців та практиків, які прагнуть поглибити свої знання в оцінці ризиків, стратегіях їх мінімізації та процесах управління ризиками. Читачі зможуть не тільки ознайомитися з теоретичними аспектами управління ризиками, але й вивчити реальні приклади їх застосування, що дозволить значно підвищити рівень стратегічного мислення і готовності до ризиків в сучасному бізнес-середовищі.

https://www.rvoicmai.in/e-book/50-case-Studies-on-Risk-Management-wl95IxBToR0ssk

ІНШІ НОВИНИ

Створення Управління ЄС з протидії відмиванню коштів (AMLA)

Нове Управління ЄС з протидії відмиванню коштів (AMLA) планує розпочати більшу частину своєї діяльності до середини 2025 року. Орган об'єднає зусилля для нагляду за фінансовими установами з високим ризиком і підтримки підрозділів фінансової розвідки (ПФР) у всьому Європейському Союзі.

Основні функції AMLA:

1. AMLA здійснюватиме нагляд за суб'єктами фінансового сектору, які здійснюють транскордонну діяльність принаймні в шести державах-членах і піддаються значним ризикам ВК/ФТ.
2. Це допоможе ПФР у ЄС зміцнити співпрацю та підвищувати ефективність обміну інформацією.
3. AMLA має на меті сприяти конвергенції нагляду та розвивати спільну культуру нагляду між національними органами.

Персонал і менеджмент:

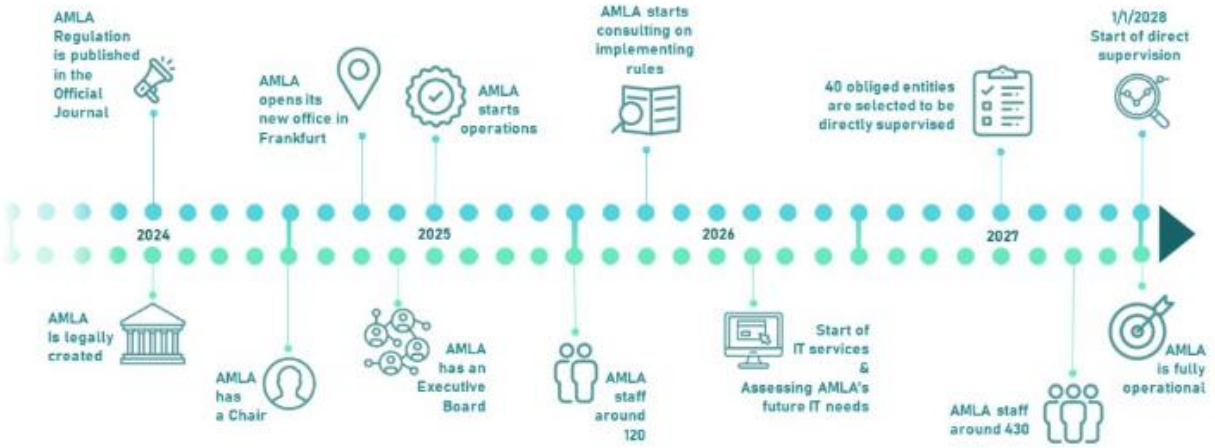
- AMLA буде поступово розширювати свій штат, досягнувши понад 430 членів до 2027 року.
- Ним керуватимуть Виконавча рада та Генеральна рада, до складу яких входитимуть представники національних наглядових органів та ПФР.

Місцезнаходження:

- Штаб-квартира AMLA буде розташована у Франкфурті-на-Майні, Німеччина.

Початок роботи та обсяг:

- Управління має розпочати роботу до 2025 року, а безпосередній нагляд за вибраними організаціями розпочнеться у 2028 році.
- AMLA не замінить національні наглядові органи, але тісно співпрацюватиме з ними, щоб покращити систему правозастосування ПВК/ФТ у ЄС.



Попередження про компанії, що надають грошові послуги в криптовалюті

🏛 ФБР випустило попередження для громадян США, щоб вони остерігалися криптосервісів, які не відповідають федеральним нормам. Порада особливо застерігає від ведення бізнесу з компаніями, які не зареєстровані як грошово-кредитні компанії (MSBs) і не дотримуються протоколів протидії відмиванню коштів, включаючи процедури KYC.

https://www.ic3.gov/Media/Y2024/PSA240425

Прийнято визначні європейські закони з ПВК, ОАЕ та Гібралтар залишаються в сірому списку ЄС принаймні до вересня, та останні дані щодо заробітної плати в FCC – новини від AML Intelligence

Європейський парламент ухвалив нові закони про протидію відмиванню коштів, які включають створення єдиної правової бази та нового органу AMLA для кращого контролю над фінансовими операціями в ЄС. Це зменшить можливості для відмивання коштів у Європі. Водночас ОАЕ та Гібралтар зберігаються в "сірому списку" ЄС, незважаючи на їхнє виключення з аналогічного списку FATF. Також обговорюються підняття зарплат для менеджерів з питань комплаєнсу та невирішені питання щодо нових правил AML, які не завжди ясно регулюють складні аспекти сучасних операцій.

https://bit.ly/3UDD7ot

Локалізація криптовалют відповідно до Швейцарського Федерального Закону «Private International Law»

Окружний суд Цюриха виніс рішення, яке цікаве тим, що воно роз'яснює, як криптовалюти мають бути локалізовані в контексті статей 167 і далі. В яких випадках криптовалюти можна вважати такими, що знаходяться в юрисдикції суду, таким чином встановлюючи юрисдикцію для визнання іноземного рішення про банкрутство та застосування запобіжних заходів. У ньому розглядаються технічні основи криптовалют та їх юридична кваліфікація.

У цьому рішенні також розглядаються цікаві питання доступу до приватного ключа, ролі ключа адміністратора, токенів управління, контролю над протоколом, посередництва смарт-контрактів, програми винагород за знайдені баги, оновлень протоколу та інших аспектів, пов'язаних з управлінням цифровими активами.

Кілька основних моментів:

🔻Нематеріальні активи, такі як клейми чи платіжні токени, не можуть бути фізично, а лише нормативно — фіктивно — локалізовані.
🔻Метою статті 167 є встановлення юрисдикції у швейцарському суді, якщо можна отримати доступ до активів, які мають бути передані до іноземного банкрота (…).
🔻Для визначення локалізації платіжних токенів (принаймні в контексті статті 167(1) IPRG) фактичний доступ є вирішальним.
🔻Потрібно продемонструвати, що криптовалюти у вужчому сенсі (платіжні токени) знаходяться в юрисдикції суду, якщо існує певна форма фактичного доступу до них.

https://bit.ly/4dok5Kc

Штрафні санкції проти TD Bank

Розслідування Міністерства юстиції США щодо TD Bank зосереджено на тому, як китайські торговці наркотиками використовували другого за величиною кредитора Канади для відмивання коштів від продажу фентанілу.

Зараз повідомляється про повний масштаб звинувачень, зокрема щодо фентанілу, і які змусили TD виділити 450 мільйонів доларів цього тижня.

Тим часом раніше в четвер канадський ПФР FINTRAC наклав на банк найбільший штраф у своїй історії у розмірі 6,7 млн доларів США за шокуючу серію збоїв у процесі з ПВК.

https://fintrac-canafe.canada.ca/pen/amps/pen-2024-05-02-eng

Добірка ключових новин у світі криптовалюти від TRM Labs

https://bit.ly/44oQQ66

Як відстежується відмивання крипто-грошей для офчейн злочинів

Стаття Chainalysis описує випадок відмивання грошей через криптовалюти в Японії. Вона розкриває співпрацю між поліцією, банками та криптовалютними біржами за допомогою інструментів Chainalysis для виявлення і відслідковування підозрілих транзакцій. Застосування аналітичних інструментів Chainalysis допомогло правоохоронним органам виявити і відстежити транзакції, пов'язані з кримінальною діяльністю. За допомогою співпраці з банками та криптовалютними біржами, дослідники ідентифікували і проаналізували ланцюги транзакцій, що дозволило встановити джерела та призначення незаконних коштів.

https://www.chainalysis.com/blog/japan-cryptocurrency-money-laundering-case-study/

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Вимоги KYC для фінтех компаній

У швидкоплинному світі фінансових технологій фінтех-компаніям необхідно мати надійний процес «Знай свого клієнта» (KYC), щоб відповідати нормативним вимогам і зменшити ризики фінансових злочинів. Фінтех-компанії повинні відповідати особливим вимогам KYC, щоб забезпечити ефективну ідентифікацію та перевірку своїх клієнтів, оцінку ризиків і дотримання правил.

⚠ 1: належна перевірка клієнта (CDD)

CDD – це процес ідентифікації та перевірки особистості клієнтів та оцінки ризиків, пов'язаних з їх діяльністю. Фінтех-компанії повинні проводити CDD щодо всіх клієнтів, включаючи фізичних та юридичних осіб, і повинні враховувати характер діяльності клієнта та рівень його ризику.

⚠2: Перевірка особи

Перевірка особи є критично важливим аспектом KYC, і фінтех-компанії повинні мати надійні процедури для перевірки особи своїх клієнтів. Це може включати використання біометричної автентифікації, як-от розпізнавання обличчя, або інших автоматизованих інструментів для перевірки автентичності документів, що посвідчують особу. Важливо перевірити особу фізичної чи юридичної особи, яка проводить транзакцію, а не лише особу фізичної чи юридичної особи, яка є суб'єктом транзакції.

⚠3: Оцінка ризику

Фінтех-компанії повинні проводити оцінку ризиків своїх клієнтів, щоб визначити та зменшити потенційні ризики. Ця оцінка повинна включати оцінку фінансової історії клієнта, географічного розташування та інших відповідних факторів, які можуть становити загрозу. Рівень ризику визначатиме ступінь необхідної CDD для клієнта.

⚠4: Електронні підписи

Електронні підписи можуть бути цінним інструментом для фінтех-компаній, щоб оптимізувати процес KYC і покращити взаємодію з клієнтами. Однак важливо переконатися, що електронні підписи відповідають нормативним вимогам і є такими ж надійними та безпечними, як і традиційні підписи. Фінтех-компанії повинні розглянути юридичну силу електронних підписів у юрисдикціях, у яких вони працюють, і запровадити відповідні процедури для забезпечення їх автентичності.

⚠5: Конфіденційність даних

Фінтех-компанії повинні дотримуватися правил конфіденційності даних, таких як Регламент із загального захисту даних (GDPR) у Європейському Союзі, під час збору та обробки даних клієнтів. Це включає отримання згоди клієнтів на збір і використання їхніх даних, забезпечення безпеки даних і надання клієнтам доступу до своїх даних за запитом.

Фінтех-компанії повинні відповідати особливим вимогам KYC, щоб запобігти фінансовим злочинам і відповідати нормам. Проводячи CDD, перевіряючи особу клієнтів, проводячи оцінку

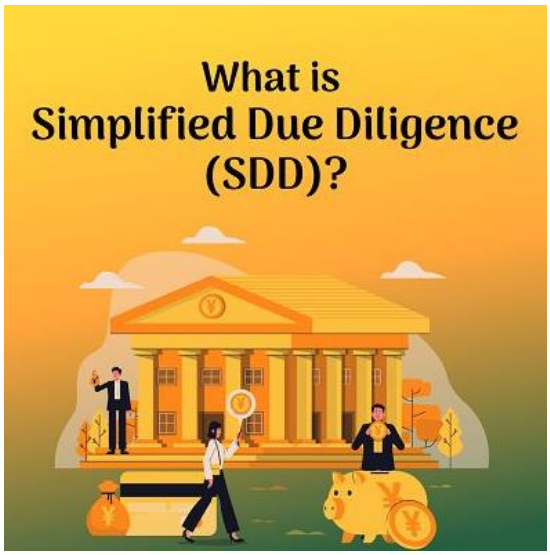
ризиків, запроваджуючи електронні підписи та дотримуючись правил конфіденційності даних, фінтех-компанії можуть запровадити програму KYC, яка відповідає нормативним вимогам і захищає їхній бізнес і клієнтів.

Схеми фінансування тероризму

Insight Monitor безкоштовний ресурс із описом схеми фінансування тероризму: як терористи збирають, використовують, переміщують, зберігають, управляють і приховують свої кошти.

https://newsletter.insightthreatintel.com/p/the-terrorist-financing-blueprint

Спрощена Належна Перевірка (SDD)



Спрощена Due Diligence – це економічний та ефективний підхід до належної перевірки. Це в основному використовується в ситуаціях, коли ділові відносини або транзакція представляють низький ризик фінансових злочинів, таких як відмивання коштів або фінансування тероризму. SDD характеризується зменшеним обсягом перевірок, що, як наслідок, призводить до більш прискореного процесу порівняно з аналогами.

По суті, SDD — це варіант належної перевірки клієнта, спеціально розроблений для сценаріїв з низьким рівнем ризику. Це дозволяє фінансовим установам та іншим секторам проводити необхідні оцінки клієнтів, не занурюючись у вичерпні перевірки, тим самим підвищуючи операційну ефективність.

Коли необхідна спрощена належна перевірка?

SDD вступає в дію за певних обставин, коли ризик фінансових злочинів вважається низьким. Приклади таких ситуацій:

- Обробка транзакцій невеликої вартості

- Пропозиція послуг або продуктів з низьким ризиком відмивання коштів

Важливо відзначити, що застосування SDD може відрізнятися в різних юрисдикціях через різну правову та нормативну базу. Отже, компанії повинні добре розуміти конкретні закони, які регулюють належну перевірку в усіх юрисдикціях, у яких вони працюють.

Етапи процесу SDD

Впровадження SDD передбачає ряд систематичних кроків:

- Оцінка ризику: початковий крок передбачає оцінку ризику, пов’язаного з клієнтом або транзакцією. Ця оцінка допомагає визначити, чи можна застосовувати SDD.

- Ідентифікація клієнта: після встановлення характеру клієнта або транзакції з низьким рівнем ризику, компанії повинні зібрати основну інформацію про клієнта.

- Профілювання ризиків: після встановлення особи клієнта створюється профіль ризиків. Цей профіль допомагає визначити необхідний рівень належної обачності.

❗Постійний моніторинг: незважаючи на спрощену природу SDD, дуже важливо постійно відстежувати діяльність клієнтів і транзакції, щоб виявити будь-які зміни в статусі ризику.

Переваги SDD

Впровадження SDD пропонує значні переваги, зокрема:

✅Ефективність: оптимізуючи процес належної перевірки, SDD дозволяє компаніям пришвидшити перевірку клієнтів, тим самим підвищуючи операційну ефективність.

✅Економічність: SDD зменшує потребу в розширених процедурах перевірки, що зрештою призводить до економії коштів.

✅Задоволеність клієнтів: за допомогою простого та швидкого процесу перевірки компанії можуть покращити взаємодію з клієнтами, тим самим покращуючи задоволеність та лояльність клієнтів.

Які етапи спрощеної належної перевірки?

SDD складається з трьох етапів:

1. Визначте відповідність вимогам

2. Зберіть базову інформацію

3. Постійний моніторинг

KYC та ПВК в онлайн казино

У контексті KYC і AML в азартних онлайн-іграх це передбачає перевірку особи гравців, які використовують платформу. Цей процес включає збір і перевірку особистої інформації, такої як документи, що посвідчують особу, і підтверджують місце проживання. Основна мета KYC в азартних іграх онлайн – запобігання шахрайству, грі неповнолітніх та іншим незаконним діям.

Сайти онлайн-казино можуть забезпечити відповідність нормам ПВК, запровадивши комплексну програму відповідності ПВК. Ця програма повинна включати такі елементи:

1: Оцінка ризику

Оцінка ризиків включає виявлення та оцінку ризиків відмивання грошей і фінансування тероризму, пов’язаних з різними типами клієнтів, продуктами, послугами та географічним розташуванням. Це дозволяє ігровим платформам запроваджувати відповідні засоби контролю для ефективного управління цими ризиками.

2: належна перевірка клієнта (CDD)

CDD передбачає перевірку особи клієнтів і розуміння їхньої звичайної поведінки у транзакціях. Він також включає постійний моніторинг транзакцій клієнтів для виявлення будь-яких відхилень від норми, які можуть вказувати на підозрілу активність.

3: Повідомлення про підозрілу діяльність

Якщо гральна платформа виявить будь-яку підозрілу діяльність, яка може свідчити про відмивання грошей або фінансування тероризму, вона зобов’язана повідомити про це відповідні органи. Зазвичай це робиться за допомогою звіту про підозрілу активність (SAR).

4: Ведення документації

Гральні платформи зобов’язані зберігати записи про всі транзакції клієнтів, підтвердження особи та звіти про підозрілу діяльність протягом певного періоду.

KYC в азартних іграх: процес і вимоги

Ось що це зазвичай включає:

1: Ідентифікація клієнта

Це перший крок у процесі KYC і AML у азартних онлайн-іграх. Він передбачає збір основної інформації про клієнта, такої як його повне ім’я, дата народження та адреса. Ця інформація зазвичай збирається, коли клієнт реєструє обліковий запис на платформі онлайн-казино.

2: Підтвердження особи

Після того, як інформацію про клієнта зібрано, наступним кроком є перевірка точності цієї інформації. Зазвичай для цього клієнта просять надати копію офіційного посвідчення особи, як-от паспорта чи водійських прав, а також останній рахунок за комунальні послуги чи виписку з банківського рахунку як підтвердження адреси.

3: Постійний моніторинг

Навіть після підтвердження особи клієнта процес KYC не завершується. Платформи азартних онлайн-ігор зобов’язані відстежувати транзакції клієнтів, щоб постійно виявляти будь-які підозрілі дії. Це включає пошук моделей, які можуть вказувати на відмивання грошей, таких як великі депозити або ставки, часте зняття коштів або незвичайні зміни моделей ставок.

4: Посилена належна перевірка (EDD)

Для клієнтів із підвищеним ризиком, наприклад із країн із високим ризиком, політично значущих осіб (PEPs) або клієнтів, які здійснюють великі транзакції, платформам азартних онлайн-ігор може знадобитися проведення розширеної належної перевірки (EDD).

Статистика відмивання коштів у різних країнах

Важливо вивчити статистичні дані з різних регіонів, щоб отримати повне розуміння тенденцій відмивання грошей. Ці статистичні дані дають важливе уявлення про масштаби діяльності з відмивання грошей та ефективність заходів, вжитих для боротьби з ними.

1: Сполучені Штати

У Сполучених Штатах відмивання грошей продовжує викликати серйозне занепокоєння. Міністерство фінансів США опублікувало Національну оцінку ризиків відмивання грошей, фінансування тероризму та фінансування розповсюдження зброї масового знищення за 2024 рік, висвітлюючи найбільш значні загрози незаконного фінансування, вразливі місця та ризики, з якими стикається країна.

Ці звіти підтверджують і оновлюють ключові проблеми незаконного фінансування у відповідь на зміну середовища загроз і ризиків. Сполучені Штати очолюють список країн з найвищим рівнем подій з протидії відмиванню коштів на душу населення. З понад 11 472 подіями, це майже 3,5 події на кожні 100 000 людей.

Крім того, у 2022 році влада США наклала штрафи на суму 14 мільярдів доларів у зв'язку з порушеннями ПВК у 2022 році, підкреслюючи значні фінансові ризики, пов'язані з недотриманням правил ПВК.

2: Великобританія

У Сполученому Королівстві спостерігається зростання діяльності з відмивання грошей, причому відмивання грошей є найпоширенішою подією, яка становить 27,5% від усіх подій ПВК. Для боротьби з цією проблемою Сполучене Королівство запровадило надійні заходи протидії відмиванню коштів, зосереджуючись на розумінні та перевірці КБВ (кінцевих бенефіціарних власників).

Велика Британія є другою країною з найбільшою кількістю правопорушень, із 1664 зареєстрованими випадками ПВК – майже 2,5 події на кожні 100 000 осіб. У Великій Британії понад три чверті подій стосуються саме відмивання коштів, що свідчить про те, що країні ще потрібно пройти довгий шлях у викоріненні цього.

3: Австралія

В Австралії торгівля наркотиками була визначена як найпоширеніша подія, що становить майже 40,9% від усіх подій ПВК. У країні вживаються активні заходи щодо боротьби з відмиванням коштів.

4: Канада

У Канаді також спостерігалося зростання діяльності з відмивання коштів, причому відсутність належного комплаєнсу склала 23,9% від усіх випадків ПВК. Країна запровадила потужні заходи щодо протидії відмиванню коштів, зосереджуючись на розумінні та перевірці КБВ.

У Канаді зросла кількість випадків відмивання коштів, пов'язаних з операціями з нерухомістю та криптовалютою. Враховуючи ці тенденції, Канада посилила свою систему боротьби з відмиванням коштів, особливо зосередившись на операціях з нерухомістю та цифрових валютах.

5: Сінгапур

Згідно зі звітом у газеті Singapore Business Times, активи, конфісковані в рамках найбільшої в країні справи про відмивання грошей, зросли з 2,8 мільярда сінгапурських доларів у жовтні до понад 3 мільярдів сінгапурських доларів (2,24 мільярда доларів).

За даними Business Times, поліція видала розпорядження про обмеження утилізації 55 нових будинків і 15 автомобілів. Разом з ордерами на арешт були видані червоні повідомлення Інтерполу, які просять правоохоронні органи по всьому світу знайти та затримати двох осіб.