Серійний номер: ДСФМУ-ДК-2024-013
Липень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Вплив включення до сірого списку на потоки капіталу: аналіз за допомогою машинного навчання

Цей документ є дослідженням, що аналізує вплив включення країн до сірого списку FATF на їхні потоки капіталу.

Сірий список FATF включає країни, які мають стратегічні недоліки в режимах ПВК/ФТ і активно працюють з FATF для їх усунення. Наразі в сірому списку перебуває 21 країна, включаючи Болгарію, Камерун, Хорватію, Ямайку, Нігерію, ПАР та інші. Основна мета дослідження — оцінити величину впливу включення до сірого списку на капітальні потоки за допомогою машинного навчання.

Дослідження використовує методику лассо (Lasso) для аналізу даних про капітальні потоки з 89 країн, що розвиваються, в період з 2000 по 2017 рік. Основний висновок полягає в тому, що включення до сірого списку призводить до значного скорочення капітальних вливань в середньому на 7,6% від ВВП. Це скорочення включає зменшення прямих іноземних інвестицій (FDI) на 3,0% від ВВП, портфельних інвестицій на 2,9% від ВВП і інших інвестицій на 3,6% від ВВП. Всі ці результати є статистично значущими.

Документ також включає розділи, присвячені методології дослідження, опису моделі, даним, та результатам аналізу. Крім того, розглядаються різні фактори, що можуть впливати на результати, та проводяться додаткові перевірки надійності висновків.

Це дослідження є важливим внеском у розуміння того, як міжнародні заходи з боротьби з відмиванням грошей та фінансуванням тероризму можуть впливати на економіку країн, що розвиваються, та їхню здатність залучати капітал.

http://surl.li/ustoj

Аналіз ринків наркотиків

Документ "EU Drug Markets Analysis 2024" від Europol пропонує комплексний аналіз ринку наркотиків у Європейському Союзі. У ньому розглядаються основні тенденції, зміни та виклики, пов'язані з обігом наркотиків, включаючи виробництво, контрабанду та розповсюдження. Особлива увага приділяється новим синтетичним наркотикам та їхньому впливу на здоров'я громадян. Документ також аналізує діяльність кримінальних організацій, які контролюють наркотичні ринки, та заходи правоохоронних органів щодо протидії цим загрозам. Звіт містить рекомендації для посилення міжнародного співробітництва та стратегій боротьби з наркотиками.

http://surl.li/moqowl

Результати EMPACT 2023. Інформаційні довідки

EMPACT (Європейська мультидисциплінарна платформа проти кримінальних загроз) – це ініціатива в галузі безпеки, запроваджена державами-членами ЄС для виявлення, визначення пріоритетів та усунення загроз, які становлять організована та серйозна міжнародна злочинність.

Документ "EMPACT 2023 Results. Factsheets" підсумовує результати оперативних дій EMPACT у 2023 році. У ньому представлені результати щодо 15 пріоритетних напрямків, включаючи контрабанду мігрантів, торгівлю людьми, екологічні злочини, шахрайство з акцизами, незаконний обіг вогнепальної зброї, наркотиків, синтетичних наркотиків та нових психоактивних речовин, онлайн-шахрайства, кіберзлочинів, відмивання коштів, організованих злочинних мереж, інтелектуальної власності та підробок.

Основні досягнення включають:

- 13,871 арештів
- 796,821,792 € вилучених коштів та активів
- Ініціація 15,644 розслідувань
- 197 тонн вилучених наркотиків
- 155 високовартісних цілей (HVT) ідентифіковано

Документ підкреслює успіхи в міжнародній співпраці та комплексному підході до боротьби з організованою злочинністю через спільні оперативні дні, навчання та аналітичну підтримку.

https://www.consilium.europa.eu/media/3ulegcm5/empact-factsheets-2023.pdf

Керівні настанови щодо CDD

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO
Reserve Bank of New Zealand
Te Pūtea Matua
Te Tari Taiwhenua
Internal Affairs

Міністерство внутрішніх справ разом з Управлінням фінансових ринків і Резервним банком Нової Зеландії опублікували оновлені керівні настанови щодо CDD, щоб допомогти фінансовим установам виконати нові нормативні вимоги, які набудуть чинності з червня 2024 року. Це включає в себе конкретні вказівки для компаній, трастів і обмежених партнерств

https://www.dia.govt.nz/AML-CFT-Updated-guidelines-related-to-customer-due-diligence

Національна оцінка ризиків ФТ у ПАР

Оцінка ризиків фінансування тероризму (TF NRA) 2024 р. пропонує оновлене дослідження загроз, вразливостей та можливого впливу фінансування тероризму на ПАР.

Що таке фінансування тероризму?

Фінансування тероризму включає збір, переміщення, зберігання та використання коштів і активів для підтримки терористичної діяльності. Оцінка ризику складається з трьох елементів: загроз, вразливостей та наслідків.

Загрози тероризму

ПАР стикається з міжнародними та внутрішніми терористичними загрозами. Основні міжнародні загрози походять від Ісламської Держави (IS) та її афілійованих осіб, зокрема в Демократичній Республіці Конго та північному Мозамбіку. Внутрішні загрози включають політично мотивоване насильство, екстремізм правого крила та зв'язки з транснаціональною організованою злочинністю.

Вразливості

ПАР має ряд вразливостей, що сприяють фінансуванню тероризму, включаючи:

- Ненадійність кордонів та зловживання системою біженців та притулків.
- Велика частка готівкової та неформальної економіки.
- Велика кількість переказів коштів з діаспорних спільнот.
- Недостатній нагляд за неприбутковими організаціями (НПО).
- Розвиваюча екосистема фінтех та криптоактивів.

Ризики

Ризик фінансування тероризму в ПАР оцінюється як високий через вразливості та загрози. Використання коштів для фінансування тероризму пов'язане з внутрішнім екстремізмом та підтримкою активностей IS.

ПАР активно вживає заходів для боротьби з фінансуванням тероризму, включаючи законодавчі, інституційні та оперативні заходи. Оцінка ризиків фінансування тероризму є безперервним процесом, що потребує ефективного міжвідомчого обміну інформацією та спільного розуміння загроз і вразливостей для належного реагування.

http://surl.li/sydyca

Національна стратегія Сінгапуру з повернення активів

Сінгапур запустив комплексну національну стратегію повернення активів, спрямовану на повернення незаконних коштів і активів у злочинців, про що оголосив прем'єр-міністр і міністр фінансів Лоуренс Вонг на пленарному засіданні FATF. Ця стратегія є частиною постійних зусиль Сінгапуру щодо зміцнення режиму ПВК/ФТ.

Діяльність з відмивання коштів у всьому світі стає все більш витонченою, часто включає великі суми незаконних коштів, що перетинають юрисдикції. У Сінгапурі багато випадків відмивання грошей є транснаціональними, пов'язаними з іноземними злочинами та складними методами приховування коштів.

Повернення активів займає центральне місце в зусиллях Сінгапуру щодо боротьби з відмиванням коштів, спрямованих на запобігання

незаконному потоку активів, одночасно підтримуючи законний бізнес. У період із січня 2019 року по червень 2024 року Сінгапур вилучив 6 мільярдів сінгапурських доларів, пов’язаних зі злочинністю, повернувши 416 мільйонів сінгапурських доларів жертвам і конфіскувавши 1 мільярд сінгапурських доларів на користь держави.

Стратегія зосереджена на чотирьох стовпах: виявлення підозрілої діяльності, вилучення та конфіскація злочинних доходів, максимальне повернення активів жертвам і стримування злочинців від використання Сінгапуру для приховування активів. Реалізація включає превентивні заходи та співпрацю з міжнародними партнерами та партнерами з приватного сектору. Примітно, що нещодавня ініціатива поліції Сінгапуру та місцевих банків дозволила подолати понад 3000 шахрайств і запобігти збиткам на суму понад 100 мільйонів сингапурських доларів.

http://surl.li/cbzicl

Повідомлення про шахрайські заяви, пов'язані з відстеженням і відшкодуванням електронних переказів із закордонних банків на рахунки в нігерійських банках

Підрозділ фінансової розвідки Нігерії опублікував новий консультаційний документ щодо шахрайства з авансовими зборами через підроблені документи електронного переказу. У цій схемі неправдиво стверджують, що значні кошти були перераховані на банківський рахунок одержувача з іноземної юрисдикції. Консультаційний документ містить тематичні дослідження та резюме типологій, закликаючи ключових зацікавлені сторони проявити додаткову належну обачність.

По суті, основна типологія, описана в документі, включає шахраїв, які вимагають кошти за допомогою підроблених документів, часто обіцяючи майбутні платежі або частину повернутих коштів.

https://bit.ly/3L3T4Pf

РЕГУЛЮВАННЯ

14-й пакет санкцій ЄС бореться з обходом і вживає енергетичних заходів

ЄС запровадив нові економічні санкції проти режиму Путіна та тих, хто продовжує його незаконну, неспровоковану та невиправдану агресивну війну проти України. Ці заходи:

📌 націлені на важливі сектори російської економіки, такі як енергетика, фінанси, транспорт і торгівля

📌 ускладнюють обхід санкцій

Крім того, політичні партії, фонди та громадські організації більше не зможуть отримувати фінансування з Росії. ЄС також запровадив санкції проти 116 фізичних та юридичних осіб.

http://surl.li/tcytqv

Що потрібно аби бути миттєвим

У березні цього року в ЄС було прийнято Регламент 2024/886, який оновлює нормативну базу для миттєвих кредитних платежів (ICT)

У ЄС платіж, щоб називатися миттєвим повинен:

- оброблятися менше ніж за 10 секунд та направлятися безпосередньо на банківський рахунок отримувача
- бути безкоштовним для фізичних осіб і коштувати 0,20 євро для компаній (як правило, норматив передбачає, що комісії за миттєві платежі SEPA мають бути такими ж, як і для звичайних кредитних переказів SEPA)
- бути доступний 24 години на добу, 7 днів на тиждень, 365 днів на рік
- мати обмеження у 100 000 євро за переказ

Трохи більше ніж через 6 місяців, до 9 січня 2025 року, завдяки цьому Регламенту про миттєві платежі постачальники платіжних послуг (PSP) у регіоні ЄС SEPA мають надавати можливість надсилати й отримувати миттєві платежі в євро.☎️.

Основна мета цього регламенту – значно збільшити впровадження миттєвих платежів у Єдиній зоні платежів у євро (SEPA)📈. Що, враховуючи їх квазіміттєвий характер і низьку вартість, є (здебільшого) гарною новиною для споживачів (як фізичних осіб, так і компаній).

https://eur-lex.europa.eu/eli/reg/2024/886/oj

Визначення Північного Руху Опору як терористичної організації та його трьох лідерів як терористів

📣 Нові терористичні визначення США щодо ультраправої організації

⏺ США визнали Північний рух опору (NRM) і трьох його членів спеціально визначеними глобальними терористами (SDGT).

NRM є найбільшою неонацистською групою у Швеції, має філії в Данії, Ісландії, Фінляндії та Норвегії. Група влаштовувала напади із застосуванням сили та намагалася зібрати зброю та вибухові матеріали.

Це лише другий випадок, коли США визнають терористичною організацію, яка сповідує ідеологію білого супермасизму.

Першою ультраправою групою, визначеною США, був Російський імперський рух (PIM) у 2020 році. Тоді США вже визнавали зв'язки між PIM і NRM.

Ці групи внесено до списку глобальних терористів (SDGT), а не до іноземних терористичних організацій (FTO). Ці списки відрізняються кількома елементами. Визначення SDGT спрямовані на обмеження доступу групи до США та міжнародної фінансової системи, тоді як визначення FTO виходять за рамки цього:

- FTO та їхнім членам заборонено в'їзд до США, але це не стосується SDGT.

- Надання фінансування або матеріальної підтримки FTO є кримінальним злочином, тоді як у випадку SDGT це потребує доказів «навмисного» наміру.

- Жертви терористичних атак FTO можуть подавати позови проти них, але не проти SDGT.

Заслуговує на увагу екстериторіальне застосування визначення FTO та повноваження США переслідувати іноземних осіб, які підтримують FTO, на відміну від випадку SDGT, де для переслідування терористичні дії мають бути вчинені в США або громадянином США.

https://www.state.gov/terrorist-designations-of-nordic-resistance-movement-and-three-leaders/

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Методика зниження можливостей зброї Російської Федерації

Незважаючи на міжнародні зусилля щодо скорочення російського оборонного виробництва, Росія продовжувала отримувати доступ до критично важливих компонентів з-за кордону, що дозволяє продовжувати зростання виробництва основної зброї та підвищувати рівень складності деяких ключових можливостей.

Росія дуже залежить від доступу до сировини та компонентів для виробництва зброї, які часто надходять від міжнародних партнерів України.

Тож чому західним урядам не вдалося ефективно перервати російське військове виробництво? У новому звіті описано кілька основних причин, зокрема:

- Бути надто реактивним, а не проактивним, у підриві російських мереж закупівель.
- Виконання відповідної роботи з надто високим рівнем секретності, що створює проблеми з обміном даними, необхідними для застосування санкцій.
- Повільне надання дозволів на втручання, які разом могли б змінити ситуацію, оскільки багато чиновників і політиків зберігали нереалістичні очікування щодо того, як виміряти ефект.

Однак у звіті підкреслюється, що залежність Росії від міжнародних ланцюгів постачання робить її вразливою до збоїв, і пропонується більш ефективна методологія роззброєння Росії:

- Забезпечення того, щоб різні залучені органи мали детальне розуміння цілі та того, як вона функціонує.
- Ефекти синхронізації та нашарування, що охоплюють багатонаціональні відкриті дії, міні-сторонні таємні дії та односторонні таємні дії, щоб максимально порушити оборонну промисловість Росії.
- Використання збору розвідувальних даних для оцінки впливу, а потім агрегування зібраних даних, щоб зменшити чутливість їхніх висновків, дозволяючи ними ділитися для вдосконалення цільового процесу.

https://static.rusi.org/methodology-degrading-russian-arms-rusi-op-june-2024.pdf

Нові ризики та можливості генеративного ШІ для банків

Цей документ, підготовлений консорціумом MindForge досліджує можливості та ризики використання генеративного штучного інтелекту (ГШІ) в банківському секторі. ГШІ, заснований на великих мовних моделях (LLMs) і фундаментальних моделях (FMs), обіцяє значні переваги в обслуговуванні клієнтів, продуктивності співробітників та прийнятті рішень. Водночас, він створює суттєві ризики, такі як упередженість, етичні проблеми, питання відповідальності та прозорості, юридичні та регуляторні виклики, кібербезпека та стабільність системи.

Документ починається з передмови, де наголошується на значному потенціалі ГШІ для банківського сектору та потребі у відповідальному підході до його використання.

У вступі розглядається історія розвитку ГШІ та його значення для сучасної банківської індустрії. Далі йде огляд можливостей і ризиків ГШІ, де детально розглядаються ключові ризики, пов'язані з використанням цієї технології. Наводиться рамкова модель ризиків, яка охоплює такі аспекти, як

справедливість, етика, підзвітність, прозорість, юридичні питання, моніторинг та стабільність, а також кібербезпека.

Документ також містить оцінку відповідності принципів FEAT (Fairness, Ethics, Accountability, Transparency) у контексті ГШІ, з рекомендаціями щодо їх оновлення та доповнення. Описуються приклади галузевих випадків використання, таких як Compliance Co-Pilot, який допомагає фінансовим установам ефективніше управляти нормативними вимогами за допомогою ГШІ.

Завершується документ розглядом наступних кроків для розширення застосування ГШІ в інших галузях фінансових послуг і розробкою стратегії зниження ризиків. У додатку наводиться глосарій термінів, розширений розділ для практиків з деталізацією ризиків і методології Veritas, а також оцінка викликів для банків, які працюють в різних юрисдикціях.

Загалом, документ підкреслює, що генеративний штучний інтелект має потенціал для революційних змін у банківському секторі, але його впровадження повинно супроводжуватися ретельним управлінням ризиками та дотриманням етичних стандартів.

http://surl.li/kgnxyj

Як регулятори можуть виявляти та досліджувати незареєстровані VASP за допомогою Blockchain Intelligence

Документ "Detect and Investigate Unregistered VASPs Using Blockchain Intelligence" є практичним керівництвом для регуляторів, яке пояснює методи виявлення та розслідування незареєстрованих постачальників послуг віртуальних активів (VASPs) за допомогою інструментів блокчейн-розвідки.

Основна мета документа – підтримка правоохоронних дій проти незареєстрованих VASPs та відповідальних осіб. У ньому детально описуються чотири основні категорії незареєстрованих VASPs:

- Незнання - компанії, які не знають або неправильно трактують регуляторні вимоги.
- Умисне порушення - компанії, які навмисно ігнорують вимоги реєстрації для надання послуг без процедури KYC.
- Невдала заявка - компанії, які подали заявку на ліцензію, але не отримали її.
- Відкликана ліцензія - компанії, які втратили ліцензію після її отримання.

Для виявлення таких VASPs регуляторам пропонуються наступні методи:

- Аналіз даних про місцезнаходження - використання блокчейн-розвідки для визначення VASPs, які можуть працювати без реєстрації в конкретній юрисдикції.
- Аналіз даних про фіатні валюти - вивчення валют, з якими працюють VASPs, що може вказати на юрисдикції їх діяльності.
- Виявлення вкладених сервісів - визначення VASPs, що використовують архітектуру та ліквідність інших, зареєстрованих сервісів, часто без їх відома або згоди.

Також у документі розглядаються методи подальшого розслідування незареєстрованих VASPs, включаючи ідентифікацію постачальників ліквідності, аналіз третіх сторін, та часовий аналіз транзакцій.

Документ підкреслює важливість блокчейн-розвідки для надання детальної картини взаємозв'язків між VASPs та іншими учасниками, що допомагає регуляторам проводити ефективні розслідування та вживати відповідних заходів.

http://surl.li/kgnxyj

Стан цифрових активів у Європі

Звіт про стан цифрових активів у Європі (DAIE) зосереджується на шести ключових сферах галузі, включаючи економічний вплив розвитку цифрових активів; інновації в секторі; останні нормативні розробки; роль криптовалюти в регіональних і глобальних конфліктах; а також освіти і культури.

Очікуваний вплив Регламенту MiCA, перспективи токенізації активів реального світу та інновації цифрових активів (або їх відсутність) у Європі є одними з багатьох тем, які розглядаються. Від дедалі більшої конкуренції на ринку праці до зростаючого апетиту до ризику серед європейських інвесторів, звіт надає 360-градусний огляд галузі, що швидко вибудовується і розвивається.

Опитані експерти включають Джона Шиндлера, генерального секретаря Ради з фінансової стабільності, Євгенія Панченка, керівника відділу оперативного аналізу Департаменту кіберполіції Національної поліції України, та експерта з питань регулювання Марка Фостера, керівника політики ЄС у Crypto Council for Innovation.

Експерти з приватного сектора, зокрема Лоран Бенаюн, генеральний директор Acheron Trading, і співзасновники Taurus SA Ламін Брахімі та Дж. П. Аумассон також представлені у цьому дослідженні.

https://assets.dlnews.com/dlresearch/the-state-of-digital-assets-in-europe-research.pdf

Вісь військових технологій Іран/Росія: Росія демонструє Ірану нові та передові військові технології

Базуючись на чотиристорінковому документі з набору файлів, зламаних мережею PRANA, документ показує ширшу зацікавленість Ірану в придбанні російських військових товарів і технологій у Technodinamika. Інтереси Ірану включають реактивні гранатомети (РПГ), авіаційні деталі, виробництво безпілотних літальних апаратів (БПЛА), виробництво ракетних установок, включаючи реактивні системи залпового вогню (РСЗВ), і транспортні засоби ППО. Частини цього документа обговорювалися в статті Washington Post від 15 квітня 2024 року, до якої долучився Інститут Науки та Міжнародної Безпеки. Представлений ними звіт обговорює документ більш детально.

У звіті йдеться про візит іранської делегації у складі 17 осіб до Росії з 5 по 13 березня 2023 року з метою ознайомлення з «науково-технічним потенціалом і виробничими можливостями АТ «Технодинаміка». Ця компанія включає понад 100 підприємств і є частиною більшої групи «Ростех», яка називається російським державним оборонним конгломератом, який зосереджений на просуванні розробки, виробництва та експорту високотехнологічної продукції.

Хоча «Технодинаміка» публічно сприяє розробці, виробництву та експорту високотехнологічної продукції для ринків цивільної авіації, її холдинги виробляють різноманітну військову продукцію та товари подвійного призначення. Її дії щодо постачання товарів збройним силам Росії призвели до того, що вона потрапила під санкції ряду країн, зокрема США, Європейського Союзу та Швейцарії.

http://surl.li/gqzhih

Четверта транснаціональна кримінальна хвиля: нові додаткові регіональні суб'єкти та зміна ринків трансформують незаконну економіку Латинської Америки та транснаціональні організовані злочинні альянси

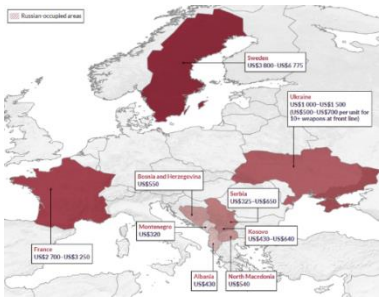
Транснаціональні злочинні організації (ТЗО) у Латинській Америці зазнають значних трансформацій, які створюються новими альянсами з позарегіональними гравцями та підтримуються ідеологічно гнучкими авторитарними урядами. Ці зміни становлять серйозну загрозу демократичному врядуванню та верховенству права.

Поява нових акторів, ринків і продуктів спричиняє фрагментацію серед традиційних груп, водночас консолідуючи кримінальні економіки через альянси з такими організаціями, як італійська Ндрангета, албанські клани торгівлі людьми та турецькі злочинні синдикати.

У цьому звіті, створеному Міжнародною коаліцією проти незаконної економіки (ICAIE) / ICAIE Labs, розглядається еволюція транснаціональної злочинної екосистеми в Латинській Америці, підкреслюється створення нових ринків і центрів конвергенції для позарегіональних гравців. Диверсифікація кримінальної діяльності призводить до нестабільної зміни порядку злочинної економіки та відносин між ТЗО, що має довгострокові стратегічні наслідки.

https://digitalcommons.fiu.edu/jgi_research/64/

Дим на горизонті: тенденції торгівлі зброєю внаслідок конфлікту в Україні



Звіт Global Initiative досліджує зростання незаконного обігу зброї внаслідок конфлікту в Україні після російського вторгнення у лютому 2022 року. Після вторгнення, велика кількість зброї надійшла до України, на додачу до значного арсеналу, який вже був накопичений з 2014 року. Це викликає занепокоєння через потенційне потрапляння зброї до рук злочинців у Європі.

Україна та її західні партнери впровадили суворі механізми контролю для відстеження постачання зброї, щоб запобігти її розповсюдженню. Національна поліція України, зазначає, що всі втрачені та викрадені одиниці зброї, яких наразі нараховується 593 000, обліковуються, і європейські партнери поінформовані про них.

Проект "Моніторинг" був створений Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC) у 2023 році для відстеження потоків зброї з України до Європи. Основним завданням проекту був збір даних про чорний ринок зброї в Україні та Європі, включаючи ціни на різні види зброї. Дані були зібрані від підпільних джерел і правоохоронних органів різних країн. Інтерв'ю з підпільними джерелами, правоохоронцями, журналістами та активістами допомогли доповнити картину щодо попиту на зброю серед злочинців та факторів такого ризику.

Звіт підсумовує перший рік роботи проекту (2023 та початок 2024 року) та виявляє, що незаконне переміщення зброї наразі обмежене територією України, без підтверджених випадків організованого перевезення зброї до країн ЄС. Проте, висновки вказують на необхідність продовження моніторингу та співпраці між країнами для запобігання потенційному розповсюдженню зброї у майбутньому.

https://globalinitiative.net/analysis/trends-arms-trafficking-conflict-ukraine-russia-monitor/

Придушення відмивання: використання FATF як фігового листка для боротьби з громадянським суспільством

У дослідженні "Suppression Laundering" від RUSI розглядається, як стандарти FATF з протидії відмиванню грошей та фінансуванню тероризму використовуються авторитарними режимами для переслідування громадянського суспільства. Зокрема, Рекомендація 8, призначена для запобігання зловживанню некомерційними організаціями, але часто використовується для придушення журналістів, активістів та політичних опонентів.

Звіт підкреслює, що різні режими, включаючи демократичні та авторитарні, зловживають цими стандартами для досягнення власних цілей, таких як обмеження свободи зібрань та вираження думок. Наприклад, Рекомендація 29, яка вимагає створення підрозділів фінансової розвідки, часто використовується для збору інформації про політичних опонентів без належних підстав.

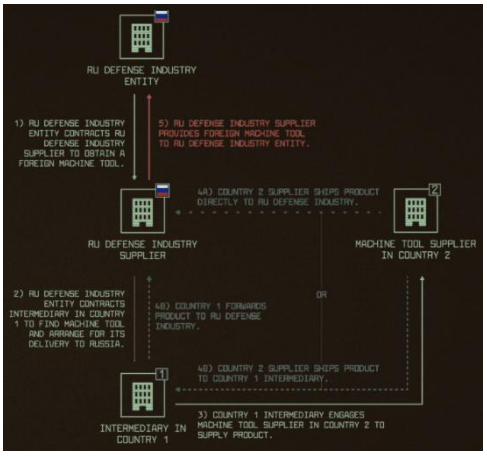
Звіт містить приклади з різних країн, де такі зловживання призвели до серйозних обмежень на діяльність некомерційних організацій. Наприклад, в Росії, Індії та Туреччині влада використовує закони проти відмивання грошей для переслідування НУО, які виступають проти урядових політик або підтримують права людини.

Звіт закликає до покращення механізмів зворотного зв’язку між FATF та громадянським суспільством, включаючи формалізацію комунікаційних каналів та посилення незалежності підрозділів фінансової розвідки. Також пропонується змінити методологію FATF для оцінки випадків зловживань стандартами. Крім цього, наголошується на необхідності забезпечення прозорості та підзвітності у використанні стандартів FATF, щоб запобігти їх використанню як інструменту політичного тиску. Для цього потрібна тісніша співпраця між міжнародними організаціями, урядами та громадянським суспільством.

http://surl.li/whuxed

WAR MACHINE: мережі, що постачають і підтримують російський арсенал прецизійних верстатів

Дослідження C4ADS аналізує, як Росія продовжує отримувати високоточні верстати з числовим програмним управлінням (CNC) для своєї оборонної промисловості, попри глобальні санкції та обмеження на торгівлю. Ці верстати критично важливі для виробництва оборонної техніки, такої як високоточні боєприпаси та авіаційні деталі. Звіт підкреслює, що Росія використовує посередників з "третіх країн" (Китаю, Гонконгу, Туреччини, ОАЕ) для обходу санкцій, імпортуючи як нові, так і вживані верстати. Це демонструє слабкість у режимах контролю за експортом і санкціях.



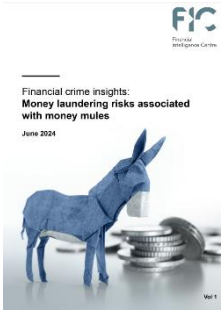
У дослідженні виявлено дві основні тактики ухилення від санкцій: "ухилення через дочірні компанії", коли російські філії іноземних компаній продовжують отримувати продукцію від материнських компаній, і "ухилення через дистриб'юторів", коли незалежні російські дистриб'ютори імпортують нові та вживані CNC верстати.

Звіт включає п'ять кейсів, в яких деякі компанії вже під санкціями, а інші – ні. Наприклад, у кейсі "Діабло" описано, як російська компанія зуміла отримати доступ до передових технологій через мережу підставних компаній у Гонконгу та ОАЕ, що ускладнює контроль за експортом.

Дослідження також вказує на те, що обмежені ресурси для нагляду, недостатні штрафи за порушення і відсутність міжнародної координації ускладнюють ефективне стримування Росії від доступу до необхідних технологій. Автори звіту рекомендують посилити наглядові ресурси, запровадити жорсткіші штрафи за порушення та поліпшити міжнародну співпрацю для обмеження торгівлі з посередниками "третіх країн".

https://c4ads.org/wp-content/uploads/2024/06/War-Machine-C4ADS-Report.pdf

Ризики відмивання коштів, пов’язані з грошовими мулами



Центр фінансової розвідки (FIC) випустив свою першу публікацію «Financial Crime Insights», присвячену ризикам відмивання коштів, пов'язаним з діяльністю грошових мулів у Південній Африці. У звіті, що охоплює дані з серпня 2016 року по липень 2023 року, проаналізовано звіти про підозрілі операції та діяльність з метою виявлення моделей і тенденцій загроз.

Основні висновки включають збірку індикаторів відмивання коштів, які допоможуть правоохоронним органам та бізнесу вжити превентивних заходів. У звіті представлений профіль потенційних злочинців, які займаються відмиванням коштів, місця проведення транзакцій та залучені галузі. Публікація має на меті покращити виявлення та запобігання відмиванню коштів.

Пітер Сміт, в.о. директора FIC, підкреслив роль звіту в розумінні діяльності грошових мулів та її зв'язку з іншими злочинами, такими як шахрайство. Аналіз виявив 58 випадків і витягнув дані зі 153 регуляторних звітів, що свідчить про широке використання підставних компаній і поширеність залучення місцевого населення, особливо в провінціях Гаутенг і Західна Капська провінція.

https://www.fic.gov.za/wp-content/uploads/2024/06/Financial-Crime-Insights-Money-mules.pdf

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Мафія та банки

Документальний фільм "Mafia & Banks" є трисерійним дослідженням зв'язків між організованою злочинністю та банківським сектором. Режисером виступив Крістоф Буке, а прем’єра відбулася у 2023 році.

Основні теми фільму:

- Початок взаємодії (The Time of Pioneers): Перша серія описує, як після вибухового зростання наркоторгівлі мафіозні угруповання знайшли посередників у банківському секторі. Це призвело до великого банківського краху.
- Відстеження грошей (Follow The Money): Друга серія фокусується на проблемі надлишку грошей у кримінальних організаціях та розвитку сучасних технік відмивання грошей у 1980-х роках. Держави вперше спробували простежити фінансові потоки, щоб знищити кримінальні організації.
- Міжнародна злочинність (International Crime): Третя серія розповідає про те, як із падінням Берлінської стіни та глобалізацією капіталізму злочинні мережі стали ще сильнішими. Банки, які повинні були контролювати систему, часто ставали співучасниками мафії.

Документальний фільм доступний на таких платформах, як Apple TV та Tubi TV, і розкриває мало відомі історії про взаємодію мафії з банками у різних місцях світу, включаючи Гавану, Нью-Йорк, Шанхай, Лондон, Москву та Кіпр.

https://tv.apple.com/us/show/mafia-banks/umc.cmc.6ihx5u8xw4rboqdhhhirbay8r

Китайські брокери відмивають сотні мільйонів для глобальних злочинних груп

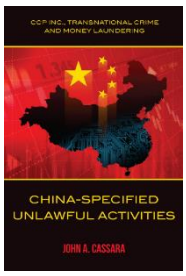
📽 Документальний фільм, опублікований Financial Times, із серії «Брудні гроші, картелі та підпільні банки».

У відео розповідається про те, як китайські відмивачі грошей сприяють епідемії фентанілу і допомагають міжнародним торгівцям наркотиками, наприклад мексиканським картелям та італійській мафії, відмивати доходи, отримані злочинним шляхом.

Розслідування FT вивчає зв'язок між втечею капіталу з Китаю та глобальною організованою злочинністю.

https://www.youtube.com/watch?v=EjGIp7kdS6E

Незаконна діяльність Китаю



Комуністичний Китай є ідеологічним, військовим, економічним, технічним, комерційним, розвідувальним і дипломатичним суперником США та Заходу. Китай має зростаючу експлуататорську присутність у країнах, що розвиваються. Хоча ці загрози відомі, участь Комуністичної партії Китаю (КПК) у співпраці з великим бізнесом або – КПК Інк. – у транснаціональній злочинності та відмиванні грошей невідома. Колишній офіцер розвідки ЦРУ і спеціальний агент Казначейства Джон Кассара першим розглядає КПК Інк. з всеосяжної точки зору правоохоронних органів. **"China - Specified Unlawful Activities: CCP Inc.,

Transnational Crime and Money Laundering"** є важливою, своєчасною і відвертою книгою. У своїй останній книзі Джон продовжує говорити правду. Використовуючи свій дуже читабельний ненауковий стиль, він досліджує 12 категорій злочинної діяльності КПК Інк. Він викриває методології відмивання грошей та сприяючих осіб з "китайськими характеристиками". Він пояснює сучасний китайський меркантилізм, корозійний капітал і різних шкідливих посібників. Джон все об'єднує і пояснює конвергенцію. Загальна сума транснаціональної злочинності та відмивання грошей КПК Інк. є по-справжньому приголомшливою. І це впливає на всіх нас.

https://www.amazon.com/China-Specified-Activities-Transnational-Laundering/dp/B0BW2S2SKN

ІНШІ НОВИНИ

Основні криптоновини минулого тижня

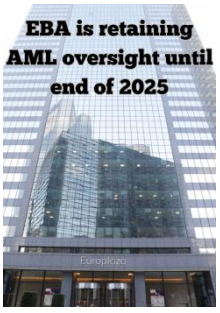
1. Ripple анонсувала новий стейблкоїн Real USD (RLUSD), прив'язаний до долара США. Він буде доступний на платформах XRP Ledger і Ethereum. RLUSD спрямований на стабілізацію транзакцій і розширення аудиторії. Ripple також співпрацює з центральними банками десяти країн щодо цифрових валют і бере участь у пілотних проектах у кількох країнах.
2. Президент Китаю Сі Цзіньпін похвалив вченого Ендрю Чі-Жі Яо з мережі Conflux за його внесок у освіту та інновації. Conflux, єдиний публічний блокчейн Китаю, який відповідає нормативним вимогам, представив нову платформу для ініціативи «Один пояс, один шлях», підкреслюючи її важливість у світовій економіці.
3. 1inch і Blockaid представили систему 1inch Shield для покращення безпеки в DeFi. Система виявляє шахрайські токени та використовує машинне навчання для виявлення підозрілих транзакцій. Інтеграція з TRM Labs дозволяє аналізувати ризики та перевіряти адреси на відповідність нормам AML.
4. Платформа ZettaBlock і Stellar Development Foundation об'єдналися, щоб спростити розробку блокчейн-додатків. Ця співпраця надасть розробникам інструменти для створення та розгортання децентралізованих додатків швидше та ефективніше завдяки використанню можливостей аналітики даних ZettaBlock.
5. Мережа BNB активувала хардфорк BEP 336 Haber, який знижує транзакційні витрати для рішень L2 на 90%. Впровадження BLOB покращує продуктивність мережі та знижує транзакційні витрати приблизно до $0,0001, особливо для користувачів opBNB.

Дорожня карта стійкості: як банки можуть використовувати ШІ для посилення можливостей з ПВК

Стаття "A Roadmap to Resilience: How Banks Can Leverage AI to Advance AML Capabilities" розглядає використання штучного інтелекту (AI) для покращення заходів протидії відмиванню коштів у банках. Вона підкреслює важливість якісних даних, збагачення контексту даних, різноманітності моделей AI та забезпечення прозорості та зрозумілості моделей. Банки можуть підвищити ефективність AML, впроваджуючи рішення, що враховують більше даних та зв'язків, що дозволяє точніше виявляти незаконні фінансові операції. Стаття також наголошує на необхідності міжнародного співробітництва та гармонізації регуляторних вимог.

http://surl.li/pzppuk

EBA залишається наглядовим органом з ПВК до кінця 2025 року



Європейське банківське управління (EBA) продовжуватиме виконувати свою роль ключового агентства з контролю за ПВК, перш ніж передати свої повноваження та ресурси AMLA до кінця 2025 року.

«EBA збереже свої повноваження та мандати у сфері ПВК/ФТ до грудня 2025 року, щоб мінімізувати збої та забезпечити безперервність, а також продовжить тісно співпрацювати з AMLA у майбутньому», — йдеться в офіційній заяві.

«Зокрема, після передачі повноважень, які стосуються ПВК/ФТ, до AMLA, EBA залишатиметься відповідальним за усунення ризиків відмивання коштів та фінансування тероризму в рамках своєї пруденційної компетенції».

Тим часом ЕВА визначила кілька ключових пріоритетів у сфері ПВК/ФТ, на яких вона зосереджуватиметься з цього моменту до кінця 2025 року. Ними будуть:

- Розробка методології відбору фінансових установ для здійснення прямого нагляду за ПВК/ФТ на рівні ЄС.
- Розробка загальної методології оцінки ризиків.
- Збір інформації, необхідної для проведення належної перевірки клієнта.
- Встановлення критеріїв для визначення серйозності порушення положень ПВК/ФТ.

http://surl.li/thquyg

Вилучення крипто: коли повернення активів стане цифровим

Стаття обговорює складнощі вилучення криптовалютних активів. Автори підкреслюють важливість спеціалізованих навичок, регуляторних рамок і міжнародної співпраці. Використовуючи приклад у Великобританії, де було конфісковано £2 мільярди в біткоїнах, вони пояснюють необхідність доступу до приватних ключів або співпраці з централізованими біржами. Також розглядаються виклики, такі як юридичні прогалини та складнощі збирання доказів для підтримки кримінальних переслідувань.

http://surl.li/orhiyt

Федеральне обвинувачення звинувачує альянс між картелем Сіналоа та відмивачами грошей, пов'язаними з китайським підпільним банкінгом

Office of Public Affairs
U.S. Department of Justice

Основні методи відмивання коштів, перелічені в обвинувальному акті:

• Відмивання коштів засноване на торгівлі (TBML) 🏭

- Приховування брудних грошей у законній торгівлі

• Китайський підпільний банкінг 🏦

- Обхід суворого валютного контролю Китаю

• Криптовалютні транзакції 💻

- Використання цифрових валют для стирання грошових слідів

• Структурування депозитів 💳

- Кілька невеликих депозитів, щоб уникнути виявлення

• Розкішні покупки 🚗🏠

- Перетворення готівки на товари високої вартості

Шокуючі подробиці:

- Комісії в розмірі 0,5%-2% за послуги відмивання
- Переміщено мільйони доларів
- Складна мережа залучених брокерів і підприємств

Ключові висновки:

- Висвітлює характер транснаціональної організованої злочинності, що розвивається
- Викриває творчі методи, які використовуються для відмивання незаконних доходів
- Демонструє виклики для фінансових установ і правоохоронних органів

http://surl.li/trwgae

Нова мережа відмивання грошей розпалює фентанілову кризу

CN MX 🔎 🔄 🔄. Розслідування почалося в січні 2021 року, коли Управління США по боротьбі з наркотиками (DEA) помітило, як чоловік доставляв значні суми готівки в, здавалося б, невинних пакетах, таких як пакет із написом «З днем народження» та коробка з пластівцями. Ці грошові надходження, які спочатку вважалися пов'язаними виключно з продажем фентанілу, були визнані частиною більшої незаконної фінансової мережі.

🔻У знаковому обвинувальному акті прокуратура звинуватила Едгара Мартінеса-Рейєса та дев'ятьох громадян Китаю у відмиванні 50 мільйонів доларів США для картелю Сіналоа. Цей випадок підкреслив розвиток і заплутаність методів відмивання грошей, оскільки китайські організовані злочинні групи стали центральними у цьому процесі. Ці групи, що працюють через програми із зашифрованими додатками, такі як Weixin/WeChat, створюють систему, у якій гроші рідко перетинають кордони фізично. Натомість вони використовують такі методи, як дзеркальні перекази та продаж доларів заможним китайцям, які прагнуть обійти контроль над капіталом.

🔻DEA та інші правоохоронні органи висловили тривогу щодо цього альянсу, відзначаючи його ефективність у швидкому та недорогому переміщенні великих сум грошей. Співпраця між китайськими відмивачами грошей і мексиканськими картелями не тільки підтримує торгівлю фентанілом, але й безперешкодно інтегрується в законну економіку, при цьому відмиті кошти використовуються для купівлі люксових товарів та майна.

🗝 **Ключові висновки**🗣

💡Продумана мережа

🔑Китайські підпільні банки та мексиканські картелі створили складну мережу відмивання грошей, уникаючи традиційних методів спостереження

💡Глобальне охоплення

🔑Мережа охоплює кілька країн, включаючи США, Китай і Мексику, сприяючи міжнародному відтоку капіталу та фінансуванню наркотиків

💡Ефективність і секретність

🔑Використання зашифрованих комунікацій і дзеркальних переказів дозволяє здійснювати швидкі та секретні транзакції, значно знижуючи витрати та ризики, зазвичай пов'язані з відмиванням грошей

💡Вплив на правоохоронні органи

🔑Поява цієї мережі створює серйозні проблеми для правоохоронних органів, ускладнюючи зусилля з відстеження та припинення операцій з незаконного обігу наркотиків

💡Економічна інтеграція

🔑Відмиті гроші реінтегруються в економіку через законні покупки, що ускладнює відстеження та боротьбу з ними

https://www.ft.com/content/acaf6a57-4c3b-4f1c-89c4-c70d683a6619?countryCode=SGP

Демонтаж Глобальної Системи Фінансової Таємниці

У статті Global Financial Integrity (GFI) обговорюється глобальна "система фінансової секретності", яка дозволяє приховувати багатства, уникати податків і сприяє корупції. Ця система, що охоплює понад 70 юрисдикцій, утримує більше $50 трильйонів. Вона дозволяє елітам уникати відповідальності, розширюючи нерівність у доходах та майні, і підриває довіру до демократичних інституцій. Також фінансова секретність ускладнює здатність урядів виконувати закони, сприяє корупції та економічній нерівності.

Система фінансової секретності дозволяє широкомасштабне ухилення від сплати податків, що зменшує податкову базу, знижує доходи для державних послуг та перекладає податковий тягар на середній та робітничий класи. Це посилює соціальну нерівність і підриває довіру до демократичних інституцій, адже громадяни бачать, що еліти ухиляються від сплати податків, користуючись при цьому державними послугами.

Фінансова секретність підриває соціальний контракт, на якому будуються демократичні суспільства, і посилює недовіру та обурення щодо демократичних інституцій. Це відкриває можливості для популістських демагогів, які використовують недовіру для підриву демократичних норм. Також секретність у фінансовій сфері ускладнює урядам здатність виконувати свої закони, оскільки, наприклад, російські олігархи приховують свої активи за непрозорими трастами, а китайські компанії використовують фіктивні компанії для обходу санкцій.

Для розв'язання проблеми необхідно розібрати чотири основні стовпи системи фінансової секретності:

(i) припинення анонімності компаній,
(ii) ліквідація інструментів фінансової секретності,
(iii) притягнення до відповідальності тих, хто сприяє корупції,
(iv) захист фінансової системи від юрисдикцій, що надають секретність.

Стаття закликає до глобальних зусиль у ліквідації фінансової секретності, включаючи міжнародне співробітництво, розробку нових стандартів прозорості та забезпечення підзвітності всіх учасників фінансової системи. Підкреслюється, що лише спільними зусиллями можна побороти глобальну систему фінансової секретності та забезпечити економічну справедливість.

https://gfintegrity.org/dismantle-the-global-financial-secrecy-system/

Як прибуткова торгівля Північної Кореї людським волоссям допомагає їй уникнути впливу санкцій

Стаття The Guardian аналізує експорт людського волосся з Північної Кореї, що використовується для виробництва перук і накладних вій. Як не дивно, ця сфера торгівлі забезпечує значний потік валютних надходжень для північнокорейського режиму, що допомагає обходити міжнародні санкції. Волосся, зібране в Північній Кореї, обробляється і переробляється у вироби, які потім експортуються через приховані канали та підставні компанії, переважно у Китай. Це дозволяє Північній Кореї підтримувати свою економіку і фінансувати різні державні програми.

Незважаючи на суворі міжнародні санкції, що спрямовані на обмеження фінансових потоків до Північної Кореї, режим Кім Чен Ина знаходить способи обходу цих обмежень через торгівлю людським волоссям. Ця діяльність викликає занепокоєння у міжнародної спільноти через можливі порушення прав людини, оскільки є підозри, що волосся може збиратися примусово у в'язницях та трудових таборах.

Експорт перук і накладних вій з людського волосся приносить значні прибутки, що дозволяє Північній Кореї фінансувати свою політичну та військову діяльність. Більшість продукції проходить через китайські компанії, які забезпечують її вихід на світові ринки. Вироби з північнокорейського волосся продаються в Європі, Північній Америці та інших регіонах, де користуються попитом.

Міжнародна спільнота намагається посилити контроль над цією торгівлею, однак через складність відстеження походження волосся та використання підставних компаній це залишається важким завданням. Незважаючи на це, Північна Корея продовжує успішно використовувати торгівлю людським волоссям для забезпечення обходу санкцій та фінансової стабільності свого режиму.

http://surl.li/rrszau

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Анонімність і конфіденційність у DeFi: міфи та реальність

Стаття присвячена дослідженню питань анонімності та конфіденційності у децентралізованих фінансових системах (DeFi). Вона розглядає рівні анонімності, які забезпечують DeFi-платформи, надає приклади платформ з високими стандартами конфіденційності та аналізує пов'язані з цим ризики та переваги.

DeFi-платформи, такі як Ethereum, пропонують псевдонімність замість повної анонімності, де транзакції здійснюються під публічними адресами замість реальних імен. Це дозволяє приховати особистість користувача, хоча самі транзакції є публічними та можуть бути відстежені.

Сучасні DeFi-платформи використовують передові криптографічні методи для покращення конфіденційності. Одним з таких методів є zk-SNARKs (неінтерактивний аргумент знань із нульовим розголошенням), які дозволяють приховувати інформацію про транзакції, зберігаючи при цьому їхню безпеку.

Однією з провідних платформ, що забезпечують високий рівень анонімності, є Tornado Cash. Вона використовує zk-SNARKs для приховування походження та цілей транзакцій, змішуючи депозити та зняття коштів, роблячи їх практично невідстежуваними. Інша платформа, Railgun, також забезпечує високий рівень конфіденційності для користувачів DeFi, використовуючи zk-SNARKs для захисту даних транзакцій.

Переваги анонімності у DeFi включають захист особистих даних від несанкціонованого доступу та шахрайства, свободу фінансових транзакцій без розкриття особистості та захист від стеження з боку третіх осіб, включаючи державні органи та корпорації. Однак високий рівень анонімності також несе ризики, такі як привабливість для злочинців, що використовують DeFi для відмивання грошей та інших незаконних дій, технічні вразливості криптографічних технологій, які можуть бути використані хакерами, та можливі регуляторні проблеми, що можуть призвести до посилення контролю та закриття анонімних платформ.

Загалом, питання анонімності та конфіденційності у DeFi залишаються актуальними та дискусійними. Майбутнє DeFi буде залежати від знаходження балансу між анонімністю та регулюванням, створення правової та технологічної бази, що враховуватиме інтереси всіх сторін, забезпечуючи стале розвиток екосистеми DeFi.

http://surl.li/nwlkrw

Як повідомляти про підозрілу діяльність

➢ Повідомлення про підозрілу діяльність включає спеціальні процедури, визначені фінансовими установами та контролюючими органами. Ось важливі кроки:

- Ідентифікація: розпізнавайте незвичні або підозрілі транзакції за допомогою автоматизованих систем або моніторингу з боку людини.
- Внутрішні процедури: фінансові установи часто мають відповідальних працівників або групи, відповідальні за розслідування та документування підозрілої діяльності.
- Документація: Зберіть необхідну інформацію — деталі транзакції, залучених осіб, дати та будь-які підтверджуючі докази.

- Подання SAR: заповніть форму звіту про підозрілу діяльність із детальною інформацією та надішліть її до відповідного органу протягом зазначеного періоду часу.

➢ Основа та мета подання SAR

Фінансові установи відіграють ключову роль у процесі подання SAR. Коли фінансова установа виявляє незвичайну або підозрілу діяльність на рахунку, вона повинна негайно надіслати SAR до ПФР. Основна мета подання звітів про підозрілу діяльність — розпочати розслідування позначеного інциденту.

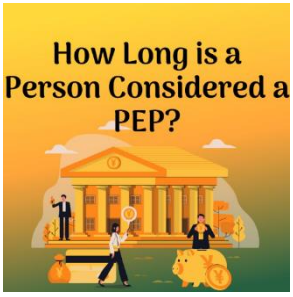
За даними FinCEN, найбільшою причиною подання SAR є відмивання грошей. Фінансова установа зобов'язана повідомити спеціально уповноважений орган про підозрілу діяльність негайно, але не пізніше ніж протягом одного робочого дня з моменту виявлення таких фактів або обставин. Важливо, що подання звітів про підозрілу діяльність не потребує доказів злочину, і власник рахунку не знає про подання звіту.

➢ Ключові елементи подання SAR

Готуючи SAR, фінансові установи повинні надати важливу інформацію, окреслюючи п'ять основних елементів:

- Особи, які здійснюють підозрілу діяльність.
- Інструменти, що використовуються в транзакціях.
- Період часу, протягом якого виникла підозріла діяльність.
- Місце, де відбулася діяльність.
- Причина сприйняття діяльності як підозрілої.

Як довго особу можуть вважати PEPом



Немає універсально узгоджених часових рамок, протягом яких особа має вважатися публічним діячем після звільнення з публічної посади. Ризик, пов'язаний з PEP, тісно пов'язаний з політичною ситуацією в їхній країні, властивим ризиком корупції, посадою чи функцією, яку вони обіймали, і впливом, пов'язаним із цією посадою.

Незважаючи на те, що їхній вплив може суттєво зменшитися, як тільки вони залишають посаду, політично значуща особа, могла придбати свої статки незаконним шляхом, що вимагає ретельного контролю навіть після того, як вона залишила посаду.

Відповідно до Вольфсберзької Групи, асоціації тринадцяти глобальних банків, яка прагне розробити рамки та вказівки для управління ризиками фінансових злочинів, підхід «одного разу PEP, завжди PEP» суперечить підходу, що ґрунтується на оцінці ризику.

Група пропонує, щоб при розгляді декласифікації політично значущої особи установи повинні враховувати такі фактори, як рівень притаманного корупційного ризику в їхній країні політичного впливу, займану посаду та її вразливість до корупції, а також правдоподібність заявленого профілю клієнта та його статків.

Як використовувати футбольний клуб для відмивання коштів

Спортивна індустрія протягом тривалого часу була благодатним ґрунтом для корупції, такої як відмивання грошей та ухилення від сплати податків.

Річні витрати на спортивну корупцію в усьому світі зараз становлять приблизно 90 мільярдів євро 💶, причому багатий на гроші футбольний сектор Європи привертає особливу увагу організованих злочинних угруповань.

В останні роки національна поліція та Європол успішно припиняли операції з відмивання грошей як у клубах з нижчих ліг, так і у великих футбольних клубах.

Вони також тісно співпрацюють з індустрією азартних ігор і регуляторними органами, щоб боротися з підозрілими ставками, пов'язаними з договірними матчами. 🔍

Проте органи кримінальної юстиції визнають, що вони ледве подолали ці загрози цілісності найпопулярнішого та все більш заможного виду спорту у світі.

⛽ Одним із класичних методів відмивання готівки через футбол є захоплення злочинцями фінансово нестабільних клубів, а потім перекачування їх незаконними коштами.

Ці заходи можуть включати:

- змішування законних коштів із незаконними через касові чеки
- завищення зарплат персоналу або гравців 📈
- завищена або занижена вартість трансферу гравця ⤴ ⤵
- платежі агентам або третім особам 💰
- спонсорство клубу ™
- Угоди про телевізійні права 🖥
- позики директорів або власників клубу 🏦

🚌 Але інші методи відмивання грошей і корупції поєднують фінансову вразливість футболу з дедалі витонченішими спробами націлитися на індустрію азартних ігор через договірні матчі.

Минулого року ESSA – загальноєвропейський орган спортивної доброчесності, який представляє великі букмекерські фірми – заявив, що виявив 52 підозрілі моделі ставок на футбол.

Цікавий приклад, «Операція «Російські матрьошки» □, була зірвана Європолом у Португалії у 2016 році.

Клуб із фінансовими труднощами вперше отримав значні пожертви від благодійників. Потім ті самі донори, діючи як підставні особи, сприяли купівлі клубу непрозорою та складною мережею холдингових компаній, що належать підставним компаніям, розташованим в офшорних податкових гаванях. 🏝 Кінцевий бенефіціарний власник компаній, які стоять за покупкою клубу, міг залишитися невідомим, але розслідування виявили зв'язки з організованою злочинністю в Австрії, Естонії, Німеччині, Латвії, Молдові та Великобританії 🏴 🛰

Види політично значущих осіб

PEP можна класифікувати на кілька різних типів залежно від сфери їхнього впливу та характеру їхніх стосунків. Давайте заглибимося в різні категорії:

✅ Національні публічні діячі

Це особи, які займають або займали визначну державну посаду чи функцію у своїй країні. Це може включати такі ролі, як глави держави чи уряду, міністри уряду, вищі державні службовці, високопоставлені військовослужбовці або топ-менеджери державних підприємств.

✅ Іноземні публічні діячі

Ці політично значущі особи – це особи, які обіймають або займали важливі державні посади в інших країнах. Серед них можуть бути глави іноземних держав чи урядів, високопоставлені політики, судові чи військові чиновники або керівники державних корпорацій в інших країнах.

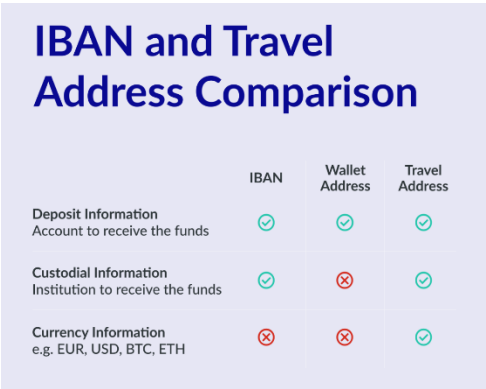
✅ PEP Міжнародних Організацій

Міжнародна організація, як-от Організація Об’єднаних Націй, Світовий банк або Міжнародний валютний фонд, довірила цим особам важливу функцію. Ця категорія зазвичай включає членів вищого керівництва, директорів, заступників директорів і членів правління.

✅ Члени сім'ї та пов'язані особи

Ця категорія стосується осіб, які пов’язані з публічним діячем або мають тісний особистий чи професійний зв’язок. Члени сім’ї можуть включати подружжя, дітей, батьків, братів і сестер. Пов'язані особи можуть охоплювати осіб, про яких відомо, що вони мають спільне бенефіціарне володіння юридичними особами, або тих, хто має тісні ділові стосунки з публічним діячем.

Crypto IBAN



Як визначити VASP на іншій стороні транзакції? Або ще важливіше: як відхилити перекази від тіньового VASP? ✋

У відповідності з Travel Rule, перш ніж здійснювати транзакцію з коштами, ви повинні:

😊 знати, що ви справді здійснюєте транзакції з VASP (інакше під час транзакцій із приватним гаманцем застосовуватимуться простіші зобов’язання)

🏭 знати, з яким VASP ви здійснюєте операції

▶ провести належну перевірку цього VASP і дізнатися, як він оброблятиме дані вашого клієнта

надіслати необхідну інформацію про відправника та отримувача

Щоб зробити це, ви можете спробувати централізований спосіб – бути частиною централізованої мережі VASP – або децентралізований спосіб – підтримуючи глобально відкритий протокол Travel Rule (TRP, наприклад).

Коли ви є частиною централізованої мережі VASP, ви:

☹ не може контролювати, які VASP надсилають вам кошти, тому вам доводиться створювати політики для обробки відхилених коштів

🔎 не можете знати до переказу, чи зберігається адреса гаманця в VASP, або навіть чи цей VASP доступний у вашій мережі, що спричиняє затримки переказу

🔓 передаєте на аутсорс до мережі будь-який захист даних, ліцензування та перевірку ВК/ФТ - це не відповідає правилам ЄС і Travel Rule ☺

Завдяки Crypto IBAN, також відомому як Travel Address, ви маєте повний контроль, оскільки можете:

✅ знати завчасно та напевно, що переказ залучає контрагента VASP, а не особовий гаманець

✅ дозволити вхідні перекази лише ПІСЛЯ отримання необхідних даних відповідно до Travel Rule

✅ блокувати перекази від VASP, які неодноразово не надсилають вам необхідні дані відповідно до Travel Rule

✅ гарантувати, що ваш контрагент має належний захист даних для отримання конфіденційної ідентифікаційної інформації вашого клієнта та що лише він отримає вашу інформацію, а не ваш централізований постачальник.

✅ надсилати дані, необхідні відповідно до Travel Rule, безпосередньо своєму контрагенту VASP на одноранговій основі, без жодного постачальника, який бачить ваш трафік

Що таке перевірка за допомогою списків спостереження

Списки спостереження - це електронні записи, в яких зібрана інформація та профілі осіб з країн з високим рівнем ризику, політично значущих осіб (PEP), осіб щодо яких є негативні згадки у ЗМІ, злочинців, які відмивають кошти, та кіберзлочинців. Таким чином, коли компанії та групи хочуть вести бізнес з особами з групи ризику, вони можуть перевірити ці списки, щоб дізнатися, чи є вони в них. Люди та компанії з чорного списку, як правило, вважаються особами високого ризику, оскільки вони беруть участь у незаконній діяльності або мають зв'язки з терористичними угрупованнями, відмиванням коштів або іншою незаконною діяльністю.

Як працює перевірка за допомогою контрольних списків?

Глобальна перевірка за списками спостереження необхідна фінансовим установам для виявлення та запобігання фінансовим злочинам, таким як відмивання коштів, підтримка тероризму та шахрайство. Програма протидії відмиванню коштів у фінансовій установі використовує інформацію з різних джерел для ретельної перевірки клієнтів.

Ці контрольні списки містять інформацію про людей або компанії, яким заборонено працювати в певних сферах, таких як банківська справа, охорона здоров'я та сільське господарство. Першим кроком у процесі скринінгу є перевірка імені особи за допомогою точної інформації з кількох джерел.

Після того, як ім'я особи або організації підтверджено, система перевіряє особу або об'єкт за різними списками, включаючи глобальні та урядові. Банківська компанія отримує повідомлення, коли виявляється збіг з одним із контрольних списків. Це дозволяє компаніям з'ясувати ступінь небезпеки і те, які послуги клієнт отримає або не отримає.

Що таке джерела контрольних списків?

Фінансові установи використовують рішення з перевірки ПВК для отримання точних даних, що зберігаються в різних джерелах, ось деякі з яких:

- Список санкцій, консолідований OFAC та Європейським Союзом (ЄС)

- Список заборонених осіб - список політично значущих осіб (PEPs) по всьому світу.
- Бази даних Інтерполу, міжурядових та державних органів.
- Сірі та чорні списки країн, які не співпрацюють з FATF та сумнозвісні за відмиванням коштів.
- Інформація, яку надають SEC та FINMA - вищі органи влади та незалежні регуляторні органи.