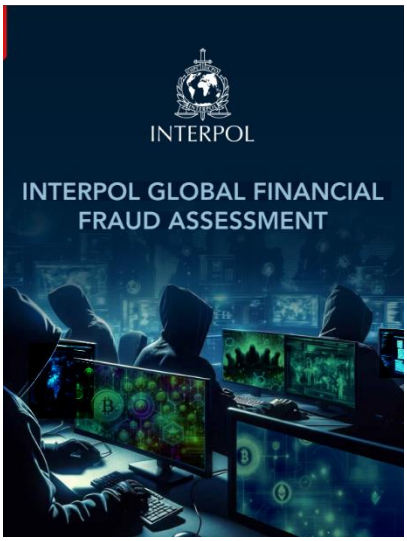
Серійний номер: ДСФМУ-ДК-2024-008
Травень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

ІНТЕРПОЛ: ГЛОБАЛЬНА ОЦІНКА ФІНАНСОВОГО ШАХРАЙСТВА



🕵 Глобальна оцінка фінансового шахрайства Інтерполу пропонує поглиблений аналіз фінансових злочинів, які впливають на окремих осіб і компанії в усьому світі. 🌍🔍

Основна інформація:

- **Великі випадки шахрайства**: шахрайство з інвестиціями, шахрайство з передоплатою, романтичні схеми та компрометація ділової електронної пошти очолюють список у всьому світі. 📉💔
- **Роль технологій**: шахрайські операції все більше залежать від глобальних інформаційних і комунікаційних технологій, що робить їх транснаціональними. 🌐🛡
- **Просунутий обман**: використання штучного інтелекту та дипфейків зловмисниками стає все більш поширеним для обману жертв і приховування своєї особистості. 🤖😨
- **Центри шахрайства**: у Південно-Східній Азії, Африці, Східній Європі та Латинській Америці спостерігається зростання кількості шахрайських центрів, пов'язаних із торгівлею людьми для примусових злочинів. 🏢🌏
- **Схема "Pig-Butchering"**: метод шахрайства, який поєднує романтику та інвестиційне шахрайство, часто з використанням криптовалют. 🐖💰
- **Організована злочинність**: фінансове шахрайство зазвичай залучає певне коло співучасників, від добре структурованих до слабко організованих груп. 🤖🕵
- **Конвергенція злочинності**: кіберзлочини як послуга та відмивання коштів як послуга відіграють значну роль у розширенні можливостей шахраїв. 🔗⚠

ІНТЕРПОЛ продовжує підтримувати глобальні зусилля проти фінансового шахрайства шляхом збору даних, аналізу та оперативної підтримки. Це дослідження є частиною поточної ініціативи Інтерполу з оцінки та реагування на нові загрози злочинності, результати якого внесуть внесок у майбутню Глобальну оцінку загрози злочинності в листопаді 2024 року.

https://bit.ly/4asd3S3

Попередження крайнє правого екстремізму в силах безпеки Великобританії

Документ "Defending Our Defenders" від Королівського інституту об'єднаних служб (RUSI) присвячений аналізу сучасних загроз і викликів, з якими стикаються захисники прав людини, особливо в умовах збройних конфліктів. У ньому досліджуються методи захисту і підтримки цих осіб, включаючи правові, дипломатичні та громадські стратегії. Також розглядаються приклади успішних ініціатив та надаються рекомендації для урядів і міжнародних організацій з метою покращення умов роботи захисників прав людини.

https://static.rusi.org/defending-our-defenders-final-proof.pdf

Національна оцінка загрози від наркотиків 2024

DEA опублікувало Національну оцінку загроз від наркотиків на 2024 рік (NDTA), в якій описано поточні загрози, пов'язані з незаконними наркотиками в США. Оцінка підкреслює критичну небезпеку синтетичних наркотиків, таких як фентаніл і метамфетамін, які продовжують бути головними причинами смертей від передозувань.

Соціальні медіа та шифровані месенджери дозволяють картелям розширювати свій вплив, використовуючи нові способи реклами та продажу наркотиків. Цифрова ера дозволяє драгдилерам продавати наркотики без необхідності особистих зустрічей, що ускладнює роботу правоохоронних органів. Вони також застосовують криптовалюту для відмивання коштів. DEA відзначає важливість міжнародного співробітництва для протидії цим фінансовим схемам, а також збільшення ресурсів для моніторингу та блокування незаконних фінансових потоків, пов'язаних з наркотрафіком.

https://www.dea.gov/sites/default/files/2024-05/NDTA_2024.pdf

Національна стратегія боротьби з тероризмом та іншим незаконним фінансуванням

Міністерство фінансів США оприлюднило Національну стратегію боротьби з тероризмом та іншими незаконним фінансуванням. У цьому комплексному плані викладено підхід уряду США до припинення та запобігання незаконній фінансовій діяльності, яка загрожує національній безпеці та економічній стабільності.

Стратегія 2024 відповідає висновкам останньої Національної оцінки ризиків і спирається на нещодавні реформи, спрямовані на модернізацію систем ПВК/ФТ. У ній виділено чотири пріоритетні напрями, зокрема усунення лазівок у нормативних актах, удосконалення нормативної бази, орієнтованої на ризики, підвищення операційної ефективності та застосування технологічних інновацій для протидії загрозам .

Основні загрози включають великомасштабне шахрайство, програми-вимагачі та фінансування тероризму з боку таких груп, як ХАМАС, і державних структур, таких як Росія. Заступник міністра Браян Е. Нельсон наголосив на важливості закриття шляхів,

якими користуються незаконні учасники, заявивши: «Нам потрібно продовжувати закривати шляхи, які незаконні учасники намагаються використати для своїх схем».

Стратегія детально описує 15 допоміжних дій із значним наголосом на введенні в дію інформації про бенефіціарну власність та розробці нових технологій для покращення комплаєнсу та правозастосування.

https://home.treasury.gov/news/press-releases/jy2346

РЕГУЛЮВАННЯ

Федеральна рада Швейцарії ухвалила депешу про посилення системи з протидії відмиванню коштів

Федеральна рада Швейцарії схвалила пропозицію щодо посилення правил країни щодо протидії відмиванню коштів.

Запропонований закон, спрямований на посилення Швейцарії як безпечного та конкурентоспроможного фінансового центру, включає запровадження федерального реєстру бенефіціарних власників і посилених процедур належної перевірки для високоризикової юридичної консультативної діяльності. Заходи, які відповідають світовим стандартам, спрямовані на запобігання вразливості до відмивання коштів, фінансування тероризму та ухилення від санкцій.

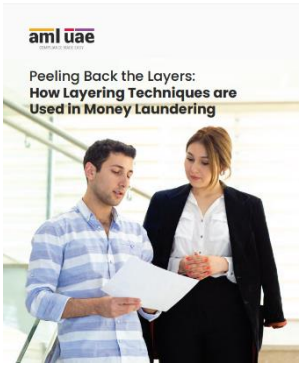
Примітно, що реєстр сприятиме швидшій і точнішій ідентифікації справжніх бенефіціарів, що стоять за юридичними структурами, і буде управлятися Федеральним департаментом юстиції та поліції.

Законодавство, яке було схвалено на етапі консультацій, буде розглянуто парламентом і, за прогнозами, буде прийнято не раніше 2026 року.

https://bit.ly/3wNxZ8k

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Як методи розшарування використовуються у відмиванні коштів



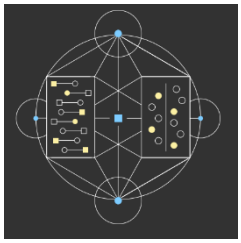
Відмивання коштів – це складний процес, який злочинці використовують для обробки грошей, отриманих від незаконної діяльності, і надання їм вигляду чистих або законних.

Розшарування є другим етапом процесу відмивання коштів. На цьому етапі незаконно отримані кошти направляються через складні шари транзакцій, щоб віддалити їх від злочинного джерела, що ускладнює виявлення походження незаконних коштів.

У цій брошурі пояснюється як працює розшарування, і розглядається кожен із його аспектів.

https://bit.ly/4bqPWsu

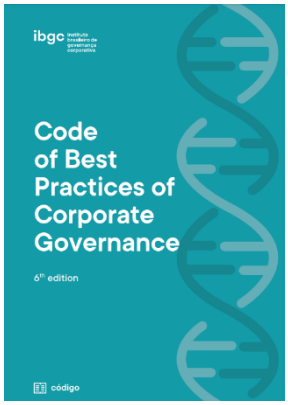
Звіт про інституційні венчурні та хедж-фонди за 1 квартал 2024 року



Документ "Q1 2024 Institutional Crypto Hedge Fund & Venture Report" підготовлений VisionTrack і Galaxy, представляє детальний аналіз ринку крипто-хедж-фондів і венчурних інвестицій за перший квартал 2024 року. Основні висновки включають зростання загальної вартості ринку крипто-хедж-фондів до $21.0 млрд, збільшення кількості нових інвесторів в pre-seed/seed раундах, а також зростання ринку криптовалют до $2.75 трлн. Документ також аналізує перформанс хедж-фондів, збір коштів венчурними фірмами та основні географічні тенденції у прийнятті криптовалют.

https://visiontrack.galaxy.com/q1-2024-institutional-crypto-hedge-fund-and-venture-report/

Кодекс найкращих практик корпоративного управління



З метою матеріалізації принципу доброчесності комплаєнс — це постійний пошук узгодженості між тим, що очікується від організації — повагою до правил, мети, цінностей і принципів, які становлять її ідентичність — і тим, що вона фактично практикує щодня.

Програма відповідності організації повинна включати набір механізмів і процедур, політик, інструкцій, кодексу поведінки, каналу викривачів та інших інструментів з метою запобігання, виявлення та виправлення відхилень у поведінці, шахрайства, корупції, відмивання коштів, незаконних дій тощо. Крім того, вона має узгоджувати діяльність кожного в організації з її принципами, цінностями та метою, одночасно сприяючи культурі доброчесності.

■ Рада директорів і виконавче керівництво повинні взяти на себе зобов’язання та підтримувати розвиток етичної культури та зміцнення програми комплаєнсу в організації;

■Рада директорів і виконавче керівництво повинні явно й публічно заявляти про важливість цінностей і політики, які складають програму комплаєнсу організації, завжди діючи недвозначно та послідовно тому, що вони проповідують;

■ Рада директорів і виконавче керівництво повинні переконатися, що відділ, відповідальний за програму комплаєнсу організації, має засоби для її реалізації на практиці, забезпечуючи виділення необхідних фінансових, матеріальних і людських ресурсів;

■ Керівники повинні сприяти постійному вдосконаленню етичної культури організації, щоб її дії завжди узгоджувалися з принципами, цінностями, законами та правилами.

На додаток до дотримання законів і нормативних актів, організація повинна визначити організаційну політику, застосовну до реальних умов її діяльності.

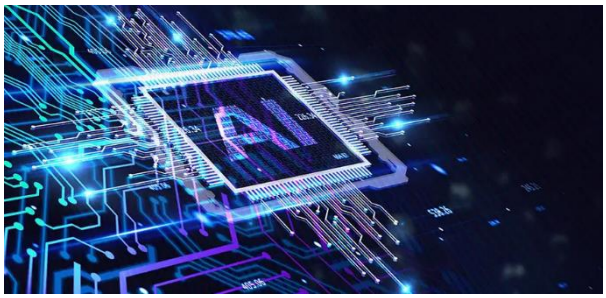
Політика має відображати стратегічні вказівки та ґрунтуватися на цінностях, принципах і меті організації.

Незважаючи на те, що вони можуть відрізнятися залежно від структури, галузі, юридичної природи чи зрілості управління, можна згадати деякі з найпоширеніших політик для бразильських організацій:

- таких як режим ієрархії;
- ризик-менеджмент; комунікація;
- антикризове управління;
- операції між пов'язаними особами;
- внески та пожертвування;
- різноманітність, справедливість та інклюзивність;
- розподіл результатів;
- попередження та виявлення протиправних діянь;
- протидія корупції;
- біржова торгівля;
- розкриття інформації;
- позааудиторські послуги.

https://bit.ly/4axOlQm

Використання штучного інтелекту в контексті розвідки. Майбутній сценарій



Документ "Using AI in an Intelligence Context: Future Scenario Workshop" від Королівського інституту об'єднаних служб (RUSI) обговорює використання штучного інтелекту (ШІ) в розвідувальній діяльності до 2040 року. На основі гіпотетичного сценарію, де технічно розвинена держава Роланд конфліктує з сусідньою острівною державою Ісламі, учасники досліджують переваги та ризики інтеграції ШІ в військових і розвідувальних структурах. Висновки включають необхідність високоякісних даних, гнучких процедур закупівель, розуміння культурного контексту і ефективного управління даними для забезпечення стратегічних переваг та підвищення готовності Великої Британії до майбутніх викликів.

Документ висвітлює три основні фази сценарію: передвторгнення, повномасштабне вторгнення та встановлення цивільної влади, і пропонує рекомендації для покращення підготовки та стратегії в умовах використання ШІ.

https://static.rusi.org/AI-Intelligence-Workshop-Report-web-final.pdf

Дослідження тенденцій та розвитку децентралізованої фінансової системи: розширення можливостей фінансового світу

DeFi (Decentralized Finance) є глобальним рухом, спрямованим на створення децентралізованих фінансових додатків і інструментів на основі блокчейн-технологій. Ця концепція переосмислює

традиційні фінансові системи і відкриває нові можливості для фінансової участі мільйонів людей у всьому світі. Одним з ключових аспектів розвитку DeFi є швидке зростання і вдосконалення протоколів, таких як Yearn Finance, MakerDAO, Uniswap та Compound, які пропонують інструменти для обміну, кредитування, стейкінгу та інших операцій з криптовалютами і цифровими активами. Ці протоколи постійно підвищують свою ефективність, безпеку та зручність використання.

Інтеграція DeFi з іншими блокчейн-платформами, такими як Polkadot, забезпечує розширення екосистеми і підвищує її стійкість і масштабованість. Polkadot, наприклад, пропонує крос-чейн можливості для створення мостів між різними блокчейнами, що сприяє інтеграції різних проектів DeFi.

DeFi стимулює розробку інноваційних фінансових продуктів, таких як DeFi-індексні фонди, децентралізовані оракули та NFT-колекції. Ці продукти відкривають нові можливості для диверсифікації портфелів і отримання доходу з цифрових активів. Розвиток DeFi має значний вплив на глобальну економіку, забезпечуючи доступ до фінансових послуг для мільйонів людей, які раніше не мали доступу до традиційних банківських сервісів. Крім того, DeFi може стати інструментом для боротьби з гіперінфляцією і фінансовими кризами в нестабільних економіках.

Очікується подальше зростання і розвиток DeFi, однак для досягнення повної зрілості необхідно вирішити питання масштабованості, безпеки і регулювання. Розробка стандартів і найкращих практик у сфері безпеки і управління ризиками стане пріоритетом. Також важливо підвищувати фінансову грамотність серед користувачів DeFi. DeFi представляє еволюційний крок у розвитку фінансових технологій, створюючи більш демократичний і доступний фінансовий ландшафт. Тренди та інновації в DeFi роблять його одним із найперспективніших напрямків сучасних фінансових технологій.

https://bit.ly/3Xbz7O3

Правила та найкращі практики моніторингу транзакцій в контексті протидії відмиванню коштів

⚖️ На днях фінансовий регулятор Німеччини BaFin оголосив, що оштрафував N26, німецький необанк, на 9,2 мільйона євро.

DE BaFin виявила, що компанія, яка базується в Берліні, систематично запізнювалася з поданням звітів про підозру у відмиванні коштів протягом 2022 року.

💬 Коментуючи покарання, N26 зазначив, що з того часу вжив численні заходи для покращення процесів звітності.

⬆️ Ефективна подача звітів про підозрілу діяльність (SAR) до місцевих підрозділів фінансової розвідки є ключовим аспектом правил моніторингу транзакцій ПВК і найкращих практик.

https://bit.ly/3KeRda4

Транснаціональна злочинність у Південно-Східній Азії: зростаюча загроза глобальному миру та безпеці

Дослідження United States Institute of Peace обговорює зростання транскордонної злочинності в Південно-Східній Азії, яка загрожує глобальному миру і безпеці. Основні злочинні мережі, що виникають переважно з Китаю, використовують слабке управління та корупцію в регіоні для проведення незаконних азартних ігор і онлайн-шахрайств. Ці операції зумовлюють значні фінансові втрати у всьому світі, поширюють насильство і конфлікти. Обговорюється, як міжнародна співпраця і скоординовані дії можуть допомогти в боротьбі з цим явищем.

https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf

Консолідовані важливі примітки щодо AML KYC і запитання та відповіді

Документ є детальним посібником з процесу "Знай свого клієнта" (KYC), який використовується для ідентифікації та перевірки особистості клієнтів з метою запобігання відмиванню коштів, фінансуванню тероризму та шахрайству. Основна мета KYC полягає у зменшенні ризику шахрайства та забезпеченні того, що фінансові установи мають точну інформацію про своїх клієнтів. Це включає збір та перевірку базової інформації, такої як імена, адреси, дати народження та реєстраційні документи компаній.

KYC є важливим інструментом у сфері ПВК/ФТ. Процес KYC включає кілька етапів: початкову перевірку (IDD), належну перевірку клієнта (CDD) та посилену перевірку (EDD) для клієнтів з високим рівнем ризику і спрощену перевірку (SDD) для клієнтів з низьким рівнем ризику. Для цього процесу необхідно збирати різні документи, такі як реєстраційні витяги, фінансові звіти податкову інформацію тощо.

Основні учасники процесу KYC включають аналітиків, відділи забезпечення якості, відділи комплаєнсу та менеджерів з відносин. Ці команди працюють разом, щоб забезпечити точність і повноту зібраних даних.

Документ також підкреслює важливість використання як первинних джерел інформації (реєстраційні витяги, річні звіти), так і вторинних (Bloomberg, Thompson Reuters), щоб забезпечити комплексну перевірку клієнтів.

Процес KYC не закінчується після здійснення перевірки клієнта. Він включає постійний моніторинг транзакцій та регулярне оновлення даних, щоб виявляти будь-які зміни у профілі ризику клієнта. Фінансові установи повинні проводити регулярні перевірки клієнтів, щоб запобігти можливим шахрайським діям і забезпечити відповідність нормативним вимогам.

Документ містить приклади, що ілюструють недоліки у реалізації процесів KYC та AML, які призвели до шахрайства. Також надаються рекомендації щодо покращення цих процесів, включаючи необхідність навчання персоналу, впровадження автоматизованих систем для зменшення людських помилок та посилення контролю за виконанням процедур KYC та AML.

https://bit.ly/452Fe9e

РЕКОМЕНДОВАНІ КНИГИ та ФІЛЬМИ

Викриття Хезболли - Епізод 3 - В ім'я держави

Цей документальний серіал заглиблюється в таємні операції та механізми фінансування Хезболли, зосереджуючись на «Проекті Кассандра», ініціативі США, започаткованій у 2008 році, щоб викрити причетність організації до торгівлі наркотиками та відмивання коштів для підтримки своєї армії та терористичної діяльності.

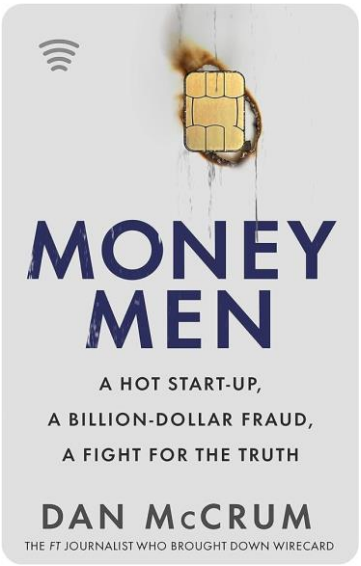
У документальному фільмі висвітлюється, як Хезболла використовувала доходи від торгівлі наркотиками для фінансування своїх операцій, і обговорюється притулок бойовиків у Франції з 2010 року, чому сприяла велика ліванська громада та свобода пересування європейською територією.

Крім того, серіал проливає світло на співпрацю між американським DEA та французькою поліцією, що призвело до «Операції «Кедр», спрямованої проти відмивання коштів, отриманих від торгівлі кокаїном, з Парижем як ключовим центром цієї діяльності.

Цей документальний фільм є чудовим ресурсом для тих, хто хоче краще зрозуміти динаміку міжнародної безпеки та зусилля по боротьбі з глобальною злочинністю і тероризмом.

https://www.youtube.com/watch?v=nrltqY3xDHg

Money Man



"Money Men" – це захоплююча і водночас тривожна історія про один з найбільших фінансових скандалів у сучасній історії. Автор, Ден МакКрам, журналіст Financial Times, розповідає про своє розслідування, яке розкрило багатомільярдну шахрайську схему, створену компанією Wirecard.

Wirecard, німецька фінтех-компанія, що займалася онлайн-платежами, здавалася одним з найуспішніших стартапів у Європі. З моменту свого заснування компанія стрімко зростала, приваблюючи інвесторів та партнерів з усього світу. Wirecard позиціонувалася як лідер у сфері цифрових фінансових послуг, але за цим успішним фасадом приховувалася грандіозна махінація.

МакКрам, слідуючи за підозрілими фінансовими звітами та аномальними транзакціями, виявив складну мережу підставних компаній, фальшивих банківських рахунків та підроблених бухгалтерських документів. Керівництво Wirecard використовувало ці методи, щоб приховати фактичний фінансовий стан компанії і вводити в оману інвесторів, аудиторів та регуляторів.

Книга розкриває деталі розслідування, яке велося в умовах постійного тиску та загроз з боку тих, хто прагнув приховати правду. МакКрам стикається з численними перешкодами, але його наполегливість та відданість справі зрештою призводять до викриття масштабного шахрайства.

"Money Men" не лише висвітлює драматичну історію падіння Wirecard, але й піднімає важливі питання про роль регуляторів, аудиторів та засобів масової інформації у виявленні та запобіганні корпоративних шахрайств. Книга є вагомим нагадуванням про те, наскільки важливими є прозорість та підзвітність у бізнесі.

ІНШІ НОВИНИ

Справа про пограбування криптовалюти: заарештовано братів Перейре-Буено!

Влада заарештувала братів Перейре-Буено у зв'язку з великою крадіжкою криптовалюти. Брати вкрали мільйони у криптовалюті за допомогою складної схеми злому. Справа підкреслює поточні виклики кібербезпеки в криптопросторі.

https://regtechtimes.com/crypto-heist-case-peraire-bueno-brothers/

Як російські військові літаки отримують свій «мозковий потенціал» із Заходу, незважаючи на санкції

Стаття Радіо Свободи розповідає про те, як російські військові літаки, такі як Су-27, Су-30, Су-34, Су-35 і Су-57, використовують електронні компоненти від західних виробників, незважаючи на санкції. Українська розвідка виявила, що компоненти, зокрема від японської Murata, американських Texas Instruments і Analog Devices, та тайванської Kemet, потрапляють до Росії. Ці компоненти постачаються через посередників у Європі, зокрема з Японії, США та Тайваню. Вони використовуються для навігації, радіоелектронної боротьби та зв'язку. Розслідування показує, як складно запобігти постачанню військових технологій через глобальні ланцюги постачання.

https://www.rferl.org/a/ukraine-russia-warplanes-sukhoi-sanctions-west-investigation/32939831.html

Витік документів показує, що Абрамович все ще пов'язаний з футбольним клубом Vitesse

Стаття від The Bureau of Investigative Journalism розповідає про витік документів, які виявили тривалу фінансову підтримку голландського футбольного клубу "Вітесс" з боку Романа Абрамовича. Незважаючи на санкції, накладені на нього Великою Британією та Європейським Союзом після вторгнення Росії в Україну, Абрамович продовжує фінансувати клуб через офшорні компанії.

Документи показують, що Абрамович використовує складну мережу компаній для перекачування коштів у "Вітесс", що дозволяє йому зберігати контроль над клубом. Основним посередником у цій схемі є Валерій Ойф, давній бізнес-партнер Абрамовича. Саме він офіційно значиться власником клубу, хоча фактично контроль та фінансування здійснюються через структури, пов'язані з Абрамовичем.

Ця схема викликає питання щодо ефективності міжнародних санкцій, спрямованих на обмеження фінансових можливостей російських олігархів. Виявлені документи свідчать про те, що Абрамович досі має можливість впливати на європейський футбол і використовувати свої ресурси для обходу накладених на нього санкцій. Це ставить під сумнів здатність міжнародної спільноти ефективно стримувати олігархів від використання їхніх багатств для підтримки режиму Путіна.

Крім того, у статті піднімається питання про моральну відповідальність футбольних клубів та організацій, які приймають кошти від осіб, що знаходяться під санкціями. Автори закликають до посилення контролю та прозорості у фінансуванні спортивних організацій, щоб запобігти подібним випадкам у майбутньому.

https://bit.ly/4dSrxgS

США викрили спробу ухилення від санкцій, пов'язану з російським олігархом

Стаття на сайті Міністерства фінансів США повідомляє про викриття схеми обходу санкцій, пов'язаної з російським олігархом Олегом Дерипаскою. Управління з контролю за іноземними активами (OFAC) виявило, що Дерипаска намагався розморозити понад 1,5 мільярда доларів своїх акцій через мережу підставних компаній і фінансових посередників. В схемі брали участь російський підприємець Дмитро Бєлоглазов та три російські компанії. OFAC заблокував всі активи, що належать цим особам і компаніям.

Це розслідування підкреслює складність і витонченість методів, які використовують олігархи для обходу санкцій, накладених Заходом. Сполучені Штати продовжують зміцнювати свої санкційні заходи для забезпечення їх ефективності та запобігання подібним спробам у майбутньому.

https://home.treasury.gov/news/press-releases/jy2337

Близько 40% брудних грошей відмиваються в Британії та на територіях, що підпадають під її юрисдикцію.

За словами заступника міністра закордонних справ Великої Британії Ендрю Мітчелла, майже 40% світових брудних коштів відмивається через Лондон і коронні володіння. Він закликав такі регіони, як Кайманові острови та Британські Віргінські острови, дотримуватися законів Великобританії, які вимагають публічних реєстрів бенефіціарної власності для підвищення прозорості.

З моменту ухвалення законодавства в Палаті громад у 2016 році заморські території чинили опір запровадженню цих державних реєстрів. Мітчелл наголосив на важливості боротьби з відмиванням коштів, зазначивши, що значна частина незаконних коштів проходить через Лондон і заморські території.

Мітчелл наголосив на зобов’язанні Сполученого Королівства гарантувати, що брудні гроші не можуть надходити в ці регіони та виходити з них, заявивши, що коронні володіння та заморські території повинні прийняти цінності Великобританії. Під час головування Великобританії у Великій вісімці у 2016 році основна увага була приділена боротьбі з брудними грошима та просуванню відкритих реєстрів бенефіціарної власності.

Незважаючи на початковий імпульс, зусилля по боротьбі з корупцією на заморських територіях зменшилися після відставки прем’єр-міністра Девіда Кемерона в 2016 році. Однак у 2018 році було прийнято закон, який вимагає впровадження реєстрів бенефіціарних власників до 2020 року.

Британські Віргінські Острови і Кайманові острови ще не запровадили публічні реєстри, і наразі посилаються на рішення Європейського суду (ECJ) щодо обмеження доступу. Раніше міністр фінансових послуг БВО висловив стурбованість порушенням прав людини через рішення Суду ЄС.

Уряд Кайманових островів заявив, що вони працюють над наданням доступу тим, хто відповідає «тесту законного інтересу» в контексті ПВК/ФТ. Вони очікують, що цю вдосконалену структуру буде представлено не пізніше кінця 2024 року.

https://bit.ly/3Kd6icj

Тижневий огляд від TRM Labs

TRM Labs — це компанія, що займається питаннями пошуку інформації у блокчейнах, яка допомагає фінансовим установам, криптобізнесу та державним установам виявляти та розслідувати пов'язані з криптовалютою фінансові злочини та шахрайство. Щодня вони вирішують завдання в галузі обробки даних, data science та аналізу загроз.

Цього тижня вони більш детально розглянули наступні питання:

- Влада Аргентини ліквідовує мережі кіберзлочинців за допомогою блокчейн-розвідки
- Міністерство фінансів США випускає щорічну стратегію протидії незаконному фінансуванню з акцентом на криптовалюту
- Корейська поліція розправляється з криптографічною наркогрупою
- Сара Хаммер з Wharton приєднується до TRM Talks
- Міністерство юстиції США заарештувало двох громадян Китаю за відмивання криптовалютних доходів від шахрайства
- Перехід до цифрового ID в Австралії та Великобританії
- FIOD проводить арешти та конфіскації у розслідуванні ZKasino

https://www.linkedin.com/pulse/trm-weekly-roundup-may-23-2024-trmlabs-jcqbe/

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Що таке eKYC?

«eKYC» — це абревіатура від «electronic Know Your Customer» — цифрова процедура, яка використовується для віддаленої перевірки ідентифікаційних даних осіб.

Рішення KYC — це цифрова система, яка дозволяє компаніям електронно перевіряти особу своїх клієнтів. Оскільки це усуває потребу в громіздкій фізичній документації та присутності, процес можна пришвидшити та зробити його зручнішим як для клієнтів, так і для залучених компаній.

Процес електронного KYC

1: Перевірка клієнта

Компанії повинні використовувати електронну систему «Знай свого клієнта», яка добре працює з їхніми додатками, веб-сайтами та іншими інструментами для роботи з клієнтами. Це покращує досвід для всіх. Клієнт повинен буде пред'явити посвідчення особи, щоб підтвердити, що він є тим, за кого себе видає.

Зазвичай це передбачає запис зображення водійського посвідчення або паспорта особи, яке згодом завантажується як документ, що посвідчує особу. Рішення eKYC використовує оптичне розпізнавання символів, щоб отримати особисту інформацію, наприклад ім'я та адресу, з пристрою користувача та миттєво заповнити форму заявки.

2: Біометрична автентифікація

Бувають випадки, коли клієнтам також може знадобитися пройти біометричну ідентифікацію. Для цього потрібна перевірка біометричної інформації, зокрема фотографії, відбитка пальця або сканування сітківки ока.

Більшість рішень просять клієнтів надіслати своє фото, яке потім перевіряється програмним забезпеченням для розпізнавання обличчя, щоб переконатися, що воно справжнє. Для більшості людей це найпростіший варіант, оскільки більшість із них мають смартфони з хорошими камерами.

3: Жвавість обличчя

Клієнт повинен надати докази того, що він є особою, вказаною в його документах. Для цього вони можуть записати коротке відео про себе в прямому ефірі, зробити селфі, яке можна порівняти із зображенням на їх посвідченні особи, або, якщо документи мають відбитки пальців, покласти палець на пристрій для зчитування відбитків пальців на своєму ноутбуці чи телефоні.

Типи eKYC

Існують різні типи рішень eKYC, кожне з яких задовольняє конкретні потреби та нормативне середовище. Серед поширених типів:

Автентифікація на основі знань (KBA): використання попередньо встановлених запитань, як-от дівоче прізвище матері чи адреса дитинства.

eKYC на основі документів: використовує перевірку цифрових документів і перевірку даних державних записів і державних посвідчень, як-от паспорта, соціального страхування, рахунків за комунальні послуги тощо.

Біометричний eKYC: використовує біометричні функції, які вже є в електронних пристроях, наприклад розпізнавання обличчя або сканування відбитків пальців.

Гібридний eKYC: поєднує різні доступні методи для більш комплексного підходу до перевірки.

Типи санкційних списків

Санкційний скринінг передбачає перехресну перевірку транзакцій, клієнтів або бізнес-партнерів на відповідність санкційним спискам уряду з метою виявлення будь-яких потенційних ризиків та забезпечення дотримання відповідних нормативних актів.

1. Санкційний список ООН:

Рада Безпеки Організації Об'єднаних Націй веде цей список, щоб накладати санкції на країни, організації та окремих осіб, причетних до дій, що загрожують глобальному миру та безпеці. Санкції включають такі заходи, як заборона на в'їзд, заморожування активів та торгові обмеження.

2. Список спеціально визначених громадян (SDN) Міністерства фінансів США:

Виданий урядом США, цей список націлений на сторони, причетні до незаконної діяльності, такої як тероризм, торгівля наркотиками та ухилення від санкцій. Заморожує активи та забороняє фінансові операції з фізичними, юридичними особами та урядами, внесеними до списку.

3. Санкційний список ЄС:

Цей список, запроваджений Європейським Союзом, зосереджується на тих, хто причетний до порушень прав людини, конфліктних зон та різних порушень. Він включає такі санкції, як заборона на в'їзд, заморожування активів і торгові обмеження з метою сприяння дотриманню міжнародних норм.

4. Санкційний список OFAC (Управління з контролю за іноземними активами):

Цей список, який адмініструється Міністерством фінансів США, націлений на сторони, що діють проти інтересів зовнішньої політики та національної безпеки США. Він передбачає такі заходи, як заморожування активів, торгові обмеження та заборони на в'їзд.

5. Національні списки санкцій:

Окремі країни ведуть ці списки, щоб накладати санкції на сторони, які становлять загрозу національній безпеці або порушують національне законодавство. санкції можуть включати заморожування активів, заборону на в'їзд і торговельні обмеження, залежно від інтересів кожної країни.

6. Чорний список FATF:

FATF - це міжнародна організація, яка визначає країни, що не вживають належних заходів проти фінансових злочинів, таких як відмивання коштів та фінансування тероризму. Перебування в цьому списку може призвести до міжнародної фінансової ізоляції та підвищеної уваги.

7. Неурядові санкційні списки:

Ці списки, які ведуться приватними організаціями та правозахисними групами, націлені на фізичних та юридичних осіб, причетних до суперечливих видів діяльності, таких як корупція або екологічні порушення. Вони слугують для підвищення обізнаності та можуть впливати на громадську думку і бізнес-рішення.

Що таке Звіт про підозрілу операцію/діяльність (STR/SAR)

STR/SAR, також відомі як Subject Matter Report (SMR), — це офіційне повідомлення, яке подається до підрозділу фінансової розвідки (ПФР) країни фінансовими установами (або іншими

регульованими організаціями), коли вони виявляють транзакцію чи діяльність, яка викликає підозри в контексті відмивання коштів або іншої незаконної діяльності.

Чи це є обов'язком?

Абсолютно!

Фінансові установи та інші регульовані організації мають юридичне зобов’язання повідомляти про підозрілу діяльність відповідно до норм ПВК/ФТ.

Юридична відповідальність = Неповідомлення про підозрілу операцію чи діяльність може призвести до значних штрафів для установи.

Що таке підозріла операція чи діяльність?

Зазвичай це відноситься до операцій, які:

☞ Співпадають з кримінальною типологією – відомі паттерни, які використовують злочинці для відмивання коштів або фінансування незаконної діяльності.

☞ Не відповідають профілю клієнта.

☞ Породжують занепокоєння щодо законності залучених коштів.

Як виявляються підозрілі операції?

Процедури STR/SAR зазвичай включають:

- Персонал на першій лінії, навчений виявляти підозрілу активність на основі червоних прапорців і профілів клієнтів.
- Співробітник першої лінії досліджує транзакцію, щоб зрозуміти її характер і контекст.
- Якщо є підстави для підозри, працівник повідомляє про операцію чи діяльність співробітнику з ПВК.
- Співробітник з ПВК проводить подальше розслідування та вирішує, чи подавати SAR до ПФР через спеціальні канали.

Неповідомлення про підозрілі транзакції є порушенням законодавства про ПВК/ФТ і може призвести до юридичних і фінансових наслідків.

Ось вагомий недавній реальний приклад: Валютно-фінансове управління Сінгапуру (MAS) нещодавно оштрафувало компанію Swiss-Asia Financial Services на 2,5 мільйона сінгапурських доларів (1,8 мільйона доларів США) за численні порушення вимог протидії відмиванню коштів та фінансуванню тероризму, включно з ненаданням звітів про підозрілі операції.

Репутаційний ризик

Репутаційний ризик є одним із найважливіших аспектів управління ризиками, з яким стикаються сучасні організації. Він впливає на здатність компанії підтримувати існуючі відносини та встановлювати нові. Цей ризик присутній у всіх підрозділах організації та зачіпає всіх зацікавлених осіб, включаючи клієнтів, партнерів, інвесторів та регуляторів. Неналежне управління репутаційним

ризиком може призвести до значних фінансових втрат та збільшення кількості судових позовів.

Атрибути репутаційного ризику включають кілька ключових аспектів:

1. Він впливає на здатність організації продовжувати обслуговувати існуючі відносини. Будь-які негативні події або скандали можуть призвести до втрати довіри з боку клієнтів та партнерів.
2. Репутаційний ризик може кристалізуватися у збільшену кількість судових позовів, що значно ускладнює правову та фінансову ситуацію компанії.
3. Якщо репутаційний ризик не управляється належним чином, це може призвести до збільшення фінансових втрат.
4. Він також впливає на здатність встановлювати нові відносини, оскільки потенційні партнери та клієнти будуть обережнішими у співпраці з компанією з поганою репутацією.
5. Репутаційний ризик зачіпає всіх зацікавлених осіб, що робить його критично важливим для всіх рівнів організації.
6. Він присутній по всій організації, що означає, що всі підрозділи повинні бути залучені до управління цим ризиком.

Впливи репутаційного ризику можуть бути різної інтенсивності. На низькому рівні він може обмежитися локальними скаргами з мінімальними змінами в довірі зацікавлених осіб, а його вплив триватиме менше одного місяця. Помірний рівень включає локальне висвітлення в ЗМІ та помірні зміни в довірі зацікавлених осіб з впливом, що триває від одного до трьох місяців. Високий рівень характеризується національним медійним висвітленням та значними змінами в довірі, які тривають понад три місяці і привертають увагу регуляторів. Дуже високий рівень включає міжнародне медійне висвітлення, драматичні зміни в довірі зацікавлених осіб та вплив, що може тривати понад 12 місяців, з публічним осудженням регуляторами.

Управління репутаційним ризиком є критично важливим для збереження довіри зацікавлених осіб і забезпечення стабільного функціонування організації. Це вимагає ретельного моніторингу всіх аспектів діяльності компанії, прозорої комунікації з громадськістю та готовності швидко реагувати на будь-які негативні події.

Процес фінансування тероризму

Процес фінансування тероризму складається з кількох етапів, кожен з яких відіграє критичну роль у забезпеченні ресурсами терористичних організацій. Давайте розглянемо цей процес детальніше, використовуючи прикріплене зображення.

1. Збір коштів (Collecting)

Перший етап – це збір коштів, метою якого є накопичення фінансових ресурсів для подальших операцій. Кошти можуть бути зібрані з різних джерел, включаючи благодійні та неприбуткові організації (НПО), пожертвування від фізичних осіб, а також фінансування від держав, які підтримують тероризм. На цьому етапі важливо маскувати джерела коштів, щоб уникнути підозр з боку регуляторних органів.

2. Зберігання коштів (Storing)

Після збору кошти необхідно безпечно зберігати, щоб уникнути їх втрати або виявлення. На цьому етапі терористичні організації можуть використовувати різні способи для зберігання фінансів, такі

як купівля антикваріату чи творів мистецтва, інвестування в криптовалюти, або розміщення коштів на банківських та фінансових рахунках. Використання цих методів допомагає приховати справжню природу та призначення коштів.

3. Переміщення коштів (Moving)

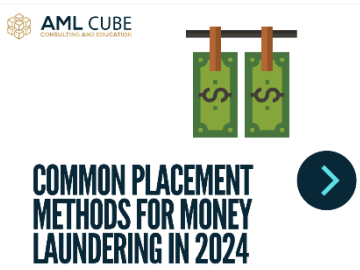
Третій етап включає переміщення коштів з метою їх подальшого використання. Терористи можуть використовувати різні методи для переміщення грошей, такі як система "хавала" (неформальна система передачі грошей), криптовалюти, перевезення готівки у великих обсягах, перекази тіньового банкінгу. Ці методи дозволяють обійти традиційні банківські системи та зменшити ризик виявлення.

4. Використання коштів (Using)

Останній етап процесу – це використання зібраних і переміщених коштів. Ці гроші використовуються для різних цілей, таких як організація комунікації, закупівля зброї та матеріалів, рекрутинг нових членів, проведення тренувань, а також покриття адміністративних та інших витрат. Важливо, щоб ці витрати залишалися непомітними, щоб уникнути підозр і подальших розслідувань.

Процес фінансування тероризму є складним і багатоступеневим, що вимагає ретельного моніторингу та вжиття заходів для його запобігання. Розуміння кожного з цих етапів допомагає правоохоронним органам та фінансовим установам ефективніше протидіяти фінансуванню тероризму та забезпечувати безпеку.

Методи розміщення коштів у 2024 році



Готівка є найбільш переважним способом розрахунків під час кримінальних дій. 💰

Чому?

Оскільки готівка:

🔎 Є анонімною і

🔎 не залишає слідів.

Однак цю готівку необхідно ввести або «розмістити» у фінансовій системі, не викликаючи підозри щодо її незаконного походження.

Відмивачі коштів традиційно використовують кілька методів «розміщення», що є першим етапом схеми відмивання коштів.

До них належать, серед іншого:

☞ Структурування / смурфінг

☞ Кредити готівкою

☞ Контрабанда готівки

☞ Придбання цінних речей

☞ Операції з нерухомістю

☞ Казино

☞ Дорогоцінні метали та каміння

https://bit.ly/3UTvNUH