Серійний номер: ДСФМУ-ДК-2024-012
Липень 2024

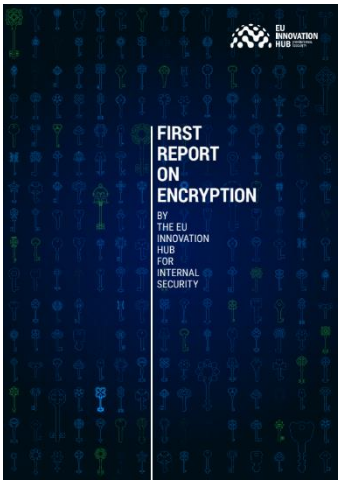
ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Розширення переваг генеративного ШІ: роль фіскальної політики

НОВЕ ДОСЛІДЖЕННЯ МВФ: фіскальна політика відіграє важливу роль у збільшенні переваг людства від генеративного штучного інтелекту. Нова доповідь МВФ містить аналіз і рекомендації для тих, хто створює політики і має справу з цією трансформаційною технологією.

https://bit.ly/3XupdXK

Перший звіт про використання зашифрованого зв'язку в кримінальних розслідуваннях



Було опубліковано новий звіт Європейського інноваційного центру внутрішньої безпеки щодо використання шифрування у кримінальних справах. Звіт підкреслює необхідність балансу між забезпеченням приватності комунікацій та можливістю проведення розслідувань і переслідувань організованої злочинності, включаючи відмивання коштів. Шифрувальні інструменти, такі як EncroChat і SkyECC, використовуються злочинними мережами для приховування своїх дій, зокрема відмивання грошей, торгівлі наркотиками та зброєю.

Звіт аналізує юридичні, технічні та політичні аспекти шифрування, а також проблеми, з якими стикаються правоохоронні органи у доступі до зашифрованих даних. Наголошується на необхідності створення правових рамок, які б забезпечували законний доступ до зашифрованих комунікацій без підриву кібербезпеки та приватності. У звіті також розглядаються судові процеси і рішення, які встановлюють прецеденти використання зашифрованих даних у судових справах.

Звіт включає технічну інформацію про нові розробки та інструменти, такі як квантові обчислення, криптовалюти, біометричні дані, телекомунікаційні технології та штучний інтелект. Представлені як виклики, так і можливості, які вони створюють для судових і правоохоронних органів. Особлива увага приділяється тому, як криптовалюти використовуються для відмивання злочинних доходів, і підкреслюється необхідність міжнародного співробітництва для боротьби з цими явищами.

У звіті рекомендується продовжувати дослідження і моніторинг технологій криптографії, співпраця з академічними колами та приватним сектором, а також розробка нових інструментів для кримінальних розслідувань.

https://www.eurojust.europa.eu/sites/default/files/assets/eu-innovation-hub-first-report-on-encryption.pdf

Цифрова криміналістика та структура реагування на інциденти для операційних технологій

Документ опублікований Національним інститутом стандартів і технологій (NIST) США у 2022 році, розглядає питання захисту конфіденційності під час використання відкритих даних. У ньому детально описуються методи забезпечення конфіденційності, зокрема диференційовану приватність, та інші технічні підходи. Описуються також приклади застосування цих методів у різних галузях, таких як охорона здоров'я, соціальні науки та економіка. Документ надає рекомендації для організацій щодо впровадження політик та практик, що мінімізують ризики розкриття приватної інформації при оприлюдненні даних.

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8428.pdf

Звіт про оцінку ризиків ВК у Сінгапурі, 2024

Сінгапур випустив національну оцінку ризиків відмивання коштів у рамках поточних зусиль щодо підтримки ефективного режиму з ПВК.

Звіт, заснований як на якісних, так і на кількісних даних, висвітлює основні загрози, включаючи кібершахрайство, організовану злочинність, корупцію та податкові злочини.

Банківський сектор, включаючи управління капіталом, і постачальники корпоративних послуг визначені як сфери найвищого ризику.

Інші сектори високого ризику включають постачальників послуг цифрових платіжних токенів, постачальників послуг транскордонних грошових переказів, ліцензовані трастові компанії, сектор нерухомості та торговців дорогоцінним камінням і металами.

Отримані результати скеровують фінансові установи і визначені нефінансові установи та професії (ВНУП) для виявлення, адаптації до нових ризиків, впровадження відповідних превентивних заходів і посилення контролю для протидії незаконній діяльності.

http://surl.li/urfjd

РЕГУЛЮВАННЯ

Консультація щодо підвищення ефективності законодавства про відмивання коштів

Wolfsberg Group подала свою відповідь на консультацію з Міністерством фінансів Великобританії щодо підвищення ефективності Положення про відмивання коштів 2017 (MLR). Ця консультація є частиною ширшої ініціативи в рамках Плану боротьби з економічною злочинністю на 2023-2026 роки. Відповідь стосується двох основних тем консультації: підвищення пропорційності та ефективності належної перевірки клієнта та посилення системної координації.

http://surl.li/uqlds

Пакет ЄС з ПВК було опубліковано

Пакет ЄС з ПВК було опубліковано в офіційному журналі Європейського Союзу 19 червня 2024 року і через 20 днів після цієї дати вони наберуть чинності. Втім, повноцінно вони почнуть діяти лише через 3 роки, а держави-члени протягом цього періоду повинні відповідним чином відкоригувати свої правила.

📖 Регламент ПВК (єдиний звід правил)

☞ https://lnkd.in/erTRMAe7

⚙ 6-та Директива щодо ПВК (інституційна основа)

☞ https://lnkd.in/eNkQUK4c

🏛 Регламент AMLA (загальноєвропейський орган з нагляду, координації та гармонізації)

☞ https://lnkd.in/eWcyM-xb

Боротьба з корупцією: Рада ЄС ухвалила позицію щодо закону

14 червня 2024 року Рада Європейського Союзу прийняла свою позицію щодо нового закону про боротьбу з корупцією. Метою цього закону є встановлення мінімальних стандартів для визначення та санкціонування корупційних правопорушень, впровадження запобіжних заходів, а також правил для більш ефективного розслідування та переслідування корупційних діянь.

Основні нововведення цього закону включають:

- Вперше на рівні ЄС буде встановлено загальні мінімальні правила щодо корупційних правопорушень.
- Розширено визначення корупційних правопорушень, включаючи не тільки класичне хабарництво, але й такі злочини як зловживання функціями, торгівля впливом, перешкоджання правосуддю та незаконне збагачення, пов’язане з корупційними злочинами.
- Введено мінімальні кримінальні санкції та покарання для різних видів правопорушень, щоб забезпечити рівні умови у всіх державах-членах.
- Подовжено терміни давності для судового переслідування корупції.

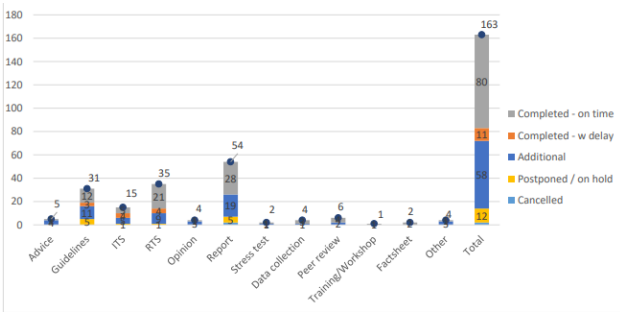
- Забезпечено наявність відповідних інструментів та ресурсів для правоохоронних органів та прокурорів для боротьби з корупцією.

Ця ініціатива спрямована на модернізацію поточної роздробленої антикорупційної рамки ЄС, що існувала до Лісабонського договору, і на виконання міжнародних зобов'язань згідно з Конвенцією ООН проти корупції (UNCAC).

https://data.consilium.europa.eu/doc/document/ST-10247-2024-INIT/en/pdf

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Річний звіт Європейського Банківського Наглядового Органу (EBA)



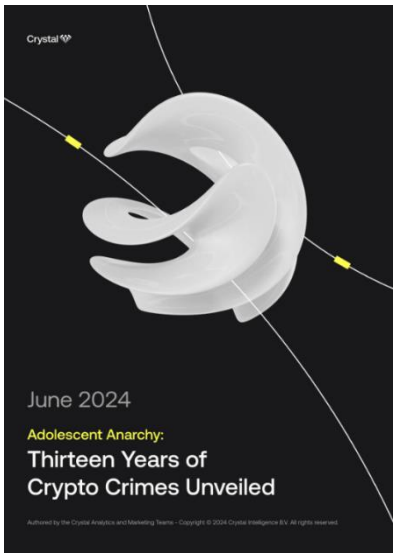
EBA щойно опублікувало свій річний звіт за 2023 рік, у якому окреслено основні досягнення та заходи, здійснені за минулий рік. У звіті підкреслюється, як EBA сприяв стабільності та ефективності європейської фінансової системи через просте, послідовне, прозоре та справедливе регулювання, а також нагляд, який приносить користь усім громадянам ЄС.

Незважаючи на глобальні виклики, такі як триваюча війна в Україні, потрясіння в банківській системі США, висока інфляція та процентні ставки, а також тривалі наслідки пандемії COVID19, EBA виконала понад 95% покладених на нього завдань. Основні досягнення в 2023 році включають завершення впровадження Basel III в ЄС, проведення розширеного загальноєвропейського стрес-тесту та просування цифрових фінансів і ринків у рамках мандатів MiCAR/DORA.

Крім того, EBA зміцнила свій потенціал у боротьбі з відмиванням коштів і фінансуванням тероризму в ЄС, запровадила екологічну, соціальну та державну дорожню карту (ESG) і провела оцінки ризиків. Інші сфери уваги включали платіжні послуги, захист споживачів і вкладників, еквівалентність, та наглядову незалежність і конвергенцію

http://surl.li/uqmum

Підліткова анархія: тринадцять років крипто-злочинів



Оскільки ринок цифрових валют продовжує розвиватися, змінюються і тактики кіберзлочинців. Цього року Crystal Intelligence пропонує поглиблений аналіз, критичні висновки та дієві рекомендації, які допоможуть захистити фінансову екосистему.

Ключові моменти:

⚙ Найбільшою шахрайською криптосхемою у 2023/24 роках була інвестиційна афера з JPEX у Гонконзі 13 вересня 2023 року, під час якої було викрадено 194,3 мільйона доларів у кількох валютах.

⚙ За той самий період найбільшим хакерським випадком із DeFi став інцидент із EulerFinance, який почався у Великобританії 13 березня 2023 року, вартістю 197 мільйонів доларів в ETH.

⚙ Топ-5 регіонів, які найбільше атакували у період 2011-2024: США - $984 млн, Гонконг - $1,2 млрд, Південна Корея - $380 млн, Великобританія - $618 млн та Сінгапур - $133 млн.

⚙ Злочинні організації з січня 2020 року по лютий 2024 року перемістили на криптовалютні біржі приблизно 75,3 мільярда доларів США, пов'язаних зі схемами pigbutchering. 15,2 мільярда доларів із цієї суми припадало на біржі, популярні серед американських інвесторів.

Цей звіт є обов'язковим до прочитання, щоб безпечно орієнтуватися у світі цифрових валют. 🌎

https://crystalintelligence.com/resources/adolescent-anarchy-thirteen-years-of-crypto-crimes-unveiled/

Моніторинг незаконної торгівлі дикими тваринами

Дослідження розглядає загрозу незаконної торгівлі дикими тваринами (IWT), що активно перемістилася в онлайн-простір. Ця торгівля охоплює продаж живих тварин, частин тіл і продуктів дикої природи на e-commerce сайтах, в соціальних мережах та месенджерах. Онлайн-IWT загрожує не лише біорізноманіттю, але й підвищує ризик виникнення зоонозних хвороб, що можуть передаватися від тварин до людей.

Основною проблемою є відсутність достатніх даних для ефективного контролю. Проект ECO-SOLVE запровадив Глобальну систему моніторингу для збору і аналізу даних про онлайн-IWT, підтримуючи правоохоронні органи та інформуючи політиків.

У дослідженні підкреслюється необхідність покращення збору та аналізу даних, міжнародного співробітництва, навчання і забезпечення ресурсами правоохоронних органів. Також наголошується на важливості кращої координації між неурядовими організаціями та правоохоронцями. Завдяки комплексному підходу, що включає зусилля міжнародних організацій, урядів і приватного сектору, можливо досягти значного прогресу в боротьбі з онлайн-IWT.

Проект ECO-SOLVE, очолюваний Global Initiative, активно використовує дані для підтримки правоохоронних органів у припиненні незаконних потоків тварин і формуванні ефективних політик. Вони прагнуть перетворити дані у реальні дії, підтримуючи правоохоронні органи у виявленні та припиненні незаконних операцій. Зокрема, важливою є робота з виявлення схем торгівлі та ідентифікація ключових гравців на ринку.

Ефективний моніторинг онлайн-IWT вимагає великої кількості даних та їх ретельного аналізу. Спільні зусилля на міжнародному рівні дозволяють покращити координацію і підвищити ефективність боротьби з екологічними злочинами.

https://globalinitiative.net/analysis/monitoring-online-illegal-wildlife-trade/

Контрабанда та торгівля людьми в Північній Африці та Сахелі. Частина 2 - Марокко

У другому дослідженні циклу "Human smuggling and trafficking in North Africa and the Sahel" описуються тенденції нелегальної міграції з Марокко до Європи у 2023 році.

Дослідження підкреслює значне зростання кількості мігрантів, які прямують до Іспанії через Альборанське море і Гібралтарську протоку. За даними Frontex, кількість марокканців, які прибули до материкової Іспанії, зросла з 4307 у 2022 році до 7910 у 2023 році.

Попри посилені заходи безпеки, які були впроваджені як Марокко, так і Іспанією, мігранти продовжують шукати способи досягти Європи. Зусилля влади Марокко щодо обмеження нелегальної міграції включають депортацію нелегальних мігрантів з північних прибережних районів до внутрішніх міст та посилення контролю на кордонах. Зменшення кількості мігрантів пов'язано з посиленими операціями безпеки, в результаті яких кількість мігрантів знизилася на 75%.

У той же час, відзначається деяке зростання кількості мігрантів, які прибувають на Канарські острови, особливо з інших країн, таких як Мавританія та Сенегал. Це частково пояснюється тим, що мігранти сприймають цей маршрут як менш небезпечний, хоча він залишається дорогим і ризикованим. У дослідженні також підкреслюється роль організованих мереж контрабандистів, які використовують різні маршрути і методи для обходу заходів безпеки, включаючи корупційні зв'язки з посадовцями.

Додатково, у звіті наголошується на складній економічній ситуації в Марокко, яка стимулює міграцію. Незважаючи на економічне відновлення після серії криз, включаючи посуху та зростання цін на товари, багато марокканців продовжують стикатися з труднощами, що підштовхують їх до пошуку кращих можливостей за кордоном. Це підкріплюється висновками опитувань, що вказують на погіршення якості життя та зростання незадоволеності серед населення.

https://bit.ly/45wx5Ka

Побудова екосистеми цінних паперів цифрових активів

Документ під назвою "Будівництво екосистеми цінних паперів цифрових активів" є всебічною білою книгою, створеною спільно DTCC, Clearstream та Euroclear за підтримки BCG. Головна мета полягає у створенні надійної основи для впровадження та регулювання цінних паперів цифрових активів (DAS), використовуючи технологію розподіленого реєстру (DLT). У документі викладені Принципи контролю цінних паперів цифрових активів (DASCP), які служать керівництвом для управління ризиками, забезпечення дотримання нормативних вимог та сприяння впровадженню DAS на ринку.

Біла книга починається з листа від генеральних директорів трьох основних фінансових ринкових інфраструктур (FMI), які підкреслюють важливість співпраці та необхідність стратегічного підходу для інтеграції цифрових технологій у глобальну фінансову екосистему. В резюме висвітлюється трансформаційний потенціал DLT у сфері цінних паперів цифрових активів і необхідність загальноіндустрійної системи управління ризиками та контролю для подолання пов'язаних з цим викликів.

Рамка DASCP розроблена так, щоб бути нейтральною як щодо класу активів, так і щодо технологій, що робить її адаптованою до різних операційних вимог. Ключові принципи цієї рамки включають забезпечення дотримання нормативних вимог, управління специфічними ризиками, пов'язаними з DAS, сприяння інтероперабельності та створення довіри серед учасників ринку.

Документ також детально описує процес спільної розробки DASCP, що включає всебічний аналіз нормативних документів, обговорення з експертами та інтерв'ю з учасниками ринку та постачальниками технологій. Мета полягає у створенні стандартизованої, стійкої та безпечної екосистеми для цінних паперів цифрових активів, яка може адаптуватися до технологічних досягнень і потреб ринку.

Принципи в межах DASCP зосереджені на кількох основних аспектах:

- Юридична визначеність і дотримання нормативних вимог для підтримання цілісності ринку
- Управління ризиками для підвищення стабільності та безпеки ринку.
- Впровадження на ринку через чіткі керівні принципи, що знижують бар'єри для нових учасників.
- Інтероперабельність та ефективність для підтримки безперешкодних транзакцій на різних платформах.
- Створення довіри серед емітентів, інвесторів, регуляторів та учасників ринку.

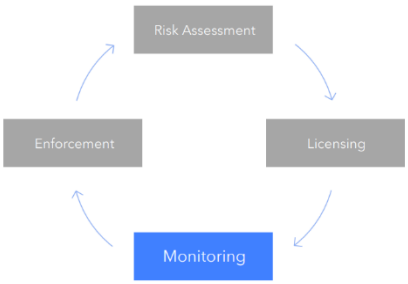
У документі також наведено докладне дослідження випадку, яке демонструє практичне застосування рамки DASCP у реальних сценаріях. Воно ілюструє, як принципи та контрольні заходи можуть бути інтегровані у життєвий цикл транзакцій з цифровими активами, наголошуючи на автоматизації та управлінні ризиками.

Нарешті, документ підкреслює важливість безперервного залучення галузі та співпраці для вдосконалення та розширення рамки DASCP. Він закликає передати керівництво цими принципами нейтральній галузевій асоціації, щоб забезпечити їх актуальність та ефективність.

Загалом, біла книга представляє візійний підхід до створення безпечної, ефективної та інклюзивної екосистеми цінних паперів цифрових активів, закликаючи до спільних дій у галузі для використання переваг цифрової трансформації у глобальних фінансах.

https://www.dtcc.com/-/media/DASCPWhitePaper.pdf

Новий посібник: посилення поточного нагляду з ПВК



Документ "Elevating Ongoing AML Supervision" від TRM Labs обговорює використання блокчейн-інтелекту для вдосконалення процесів моніторингу та звітності віртуальних сервісів з активами (VASPs) у рамках протидії відмиванню грошей (AML). Він підкреслює важливість аналізу транзакційних даних та попереджень про фінансові злочини для ефективного ризик-орієнтованого нагляду.

Основні аспекти включають використання інструментів блокчейн-інтелекту для моніторингу та оцінки ризиків VASPs, а також управління відповідністю. Документ описує різні типи ризиків, такі як ризик володіння, ризик контрагента та непрямий ризик, і їх значення для нагляду. Він також пояснює, як ці інструменти можуть допомогти в перевірці надійності VASPs через регулярні звіти та випадкові запити.

Інструкція включає кейси, такі як оцінка ризиків VASP, порівняння діяльності локальних і групових структур, реагування на санкції, розслідування повідомлень правоохоронних органів та виявлення незареєстрованих VASPs. Кожен кейс ілюструє, як блокчейн-інтелект може бути використаний для розкриття підозрілих транзакцій та оцінки відповідних ризиків.

Висновок документа підкреслює, що для ефективного нагляду за VASPs необхідно мати надійні інструменти для аналізу даних, які допоможуть регуляторам впевнено розподіляти свої ресурси. TRM Labs пропонує рішення для попередження, виявлення та розслідування криптовалютних шахрайств і фінансових злочинів, що допомагає фінансовим установам і державним органам підвищити ефективність своєї діяльності.

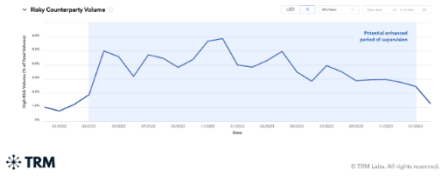
https://www.trmlabs.com/post/new-guide-elevating-ongoing-aml-supervision

Поширені типології маніпулювання ринком у криптовалюті та як їх виявити

Стаття від TRM Labs описує основні типи маніпуляцій на ринку криптовалют і способи їх виявлення. Основні типи включають "wash trading" (помилкове створення активності на ринку шляхом купівлі та продажу активів між пов'язаними сторонами), маніпуляції оракулами (маніпуляція даними, які визначають вартість токенів), інсайдерську торгівлю (використання непублічної інформації для торгівлі), та схеми "pump and dump" (штучне підвищення ціни активу з наступним продажем). Важливим аспектом боротьби з цими маніпуляціями є співпраця між VASP, аналітичними компаніями та державними установами.

https://www.trmlabs.com/post/common-market-manipulation-typologies-in-crypto-and-how-to-spot-them

Покращення ліцензування і нагляду за віртуальними активами за допомогою Blockchain Intelligence



Стаття від TRM Labs описує використання Blockchain Intelligence для покращення ліцензування та нагляду за віртуальними активами (VASPs). Вона підкреслює важливість поєднання даних з блокчейну та позаблокчейнової інформації для виявлення ризиків і підтвердження достовірності інформації, поданої VASPs. Окрім цього, розглядається використання блокчейн-інтелекту для постійного нагляду і впровадження санкцій, що дозволяє регуляторам здійснювати детальний і заснований на даних нагляд за фінансовими злочинами. Стаття демонструє, як ці інструменти можуть допомогти у різних аспектах регуляторної діяльності.

https://bit.ly/45x6DQR

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Нельма Кодама: Королева брудних коштів

Цей документальний фільм розповідає про життя Нельми Кодама, однієї з найвідоміших бразильських торговців валютою на чорному ринку. У ньому досліджується її причетність до значних корупційних скандалів, включаючи сумнозвісну справу LavaJato, і детально описано її 18-річний термін ув'язнення за різні фінансові злочини.

Вийшовши з в’язниці, Кодама ділиться своєю історією, надаючи захоплюючий погляд у світ підпільної торгівлі валютою та корупції.

https://www.netflix.com/ua/title/81641767

Вебінар: Шахрайство з ідентифікацією та роль ШІ

Найновіша інформація про ризики шахрайства, спричинені штучним інтелектом, для фахівців з комплаєнсу та фінансів. Фахівці, які працюють у сфері ризиків, протидії відмиванню коштів, інформаційної безпеки та фінансів, зможуть дізнатися нові подробиці про загрозу, яку представляє штучний інтелект, від деяких провідних експертів сектору ризиків та інформаційної безпеки з США та Європи.

Безкоштовний вебінар відбудеться 27 червня і організований ID-Pal спільно з AMLintelligence.com.

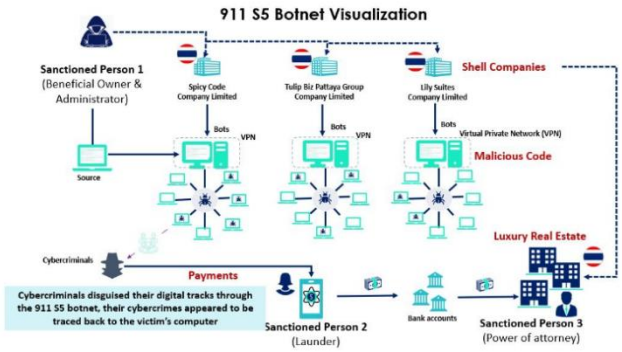
На вебінарі, доповідачі досліджуватимуть «реальні тематичні дослідження, які висвітлюють можливості ШІ та нові ризики - розповідає CEO ID-Pal Колум Лайонс.

«Ви зможете ознайомитися з перевіреними стратегіями підвищення кібербезпеки та комплаєнсу, а також ефективними підходами до боротьби з шахрайством із ідентифікаційною інформацією», — сказав він.

https://www.amlintelligence.com/2024/06/exclusive-webinar-hear-latest-insights-on-ai-driven-fraud-risks/

ІНШІ НОВИНИ

Міністерство фінансів США наклало санкції на мережу кіберзлочинців, пов'язану з ботнетом 911 S5



Наприкінці травня Управління з контролю за іноземними активами (OFAC) Міністерства фінансів США наклало санкції на трьох осіб і три компанії-оболонки, пов'язані з ботнетом 911 S5. Цей ботнет зламав 19 мільйонів IP-адрес, сприяючи масовому кібершахрайству.

⚠ Схема, керована цими трьома особами, дозволила різним кіберзлочинцям здійснювати широкомасштабне шахрайство, використовуючи скомпрометовані комп'ютери жертв з домашніми IP-адресами.

⚠Це дозволило подати десятки тисяч шахрайських заявок, пов'язаних із Законом про допомогу та економічну безпеку внаслідок коронавірусу, що призвело до втрат уряду США на мільярди доларів.

⚠Сервіс 911 S5 допомагав злочинцям маскувати свою присутність, скомпрометувавши IP-адреси жертв.

⚠Spicy Code Company Limited, Tulip Biz Pattaya Group Company Limited і Lily Suites Company Limited потрапили під санкції. Ці санкції спрямовані на перешкоджання кіберзлочинцям, які використовують технологію для отримання незаконної вигоди.

⚠Сервіс 911 S5 використав технологію, щоб зробити фінансові злочини ефективнішими та дешевшими. Замаскувавши свої цифрові сліди через ботнет 911 S5, кіберзлочинці створили враження, що їхні злочини ведуть до комп'ютера жертви.

https://home.treasury.gov/news/press-releases/jy2375

Ukraine Recovery Conference

Минулого тижня ключові діячі зібралися на Конференції з відновлення України (URC) у Берліні, щоб обговорити відбудову України, при цьому звертаючи увагу на антикорупційні зусилля, які залишаються на порядку денному.

На заході, організованому German Marshall Fund of the United States, наголошували на необхідності прозорого залучення політиків, особливо у світлі нещодавньої відставки Голови Державного агентства відновлення та розвитку інфраструктури.

Хоча обговорення цього питання є важливим, приділено більш широку системну увагу цілісності фінансової системи та боротьбі з відмиванням коштів. Зусилля з відбудови є локальними, і Україна має забезпечити прозорість та ефективність правоохоронних органів на всіх рівнях. Україна повинна вжити активних заходів для запобігання таким проблемам, як фінансові злочини, а не лише розглядати їх як наслідки.

Учасники дійшли згоди щодо важливості протидії корупційному наративу на Заході та забезпечення ефективної імплементації реформ в Україні.

На заході The Clingendael Institute, присвяченому перспективам економіки України, було підкреслено нагальну необхідність зосередитися на цілісності фінансової системи та проведенні

відповідних реформ. Це важливо для залучення інвестицій приватного сектору та запевнення міжнародних донорів у її стійкості.

https://www.urc-international.com/

Розуміння використання ШІ та машинного навчання в боротьбі з фінансовими злочинами

У статті, окрім іншого, розглядається використання штучного інтелекту (ШІ) та машинного навчання (МН) для боротьби з фінансовими злочинами, такими як шахрайство та відмивання грошей. Згідно з даними Федеральної торгової комісії, у 2023 році втрати від шахрайства досягли 10 мільярдів доларів, що на мільярд більше порівняно з попереднім роком. Це свідчить про зростаючу складність та ефективність методів шахраїв. ШІ та МН пропонують ефективні рішення для протидії цим загрозам, забезпечуючи можливість швидкої обробки великих обсягів даних та виявлення підозрілих активностей, які можуть бути непомітними для людей. ШІ відноситься до комп'ютерних систем, що виконують завдання, які зазвичай потребують людського інтелекту, тоді як МН дозволяє комп'ютерам навчатися на основі даних, виявляючи нові схеми шахрайства. Традиційні методи виявлення шахрайства, що базуються на фіксованих правилах, не здатні адаптуватися до нових тактик злочинців, тоді як ШІ та МН безперервно вчаться та еволюціонують, що робить їх більш ефективними. В реальних умовах ці технології використовуються для виявлення аномалій у поведінці користувачів, розпізнавання шаблонів у транзакціях та прогнозування можливих шахрайських дій на основі історичних даних. Застосування ШІ та МН дозволяє фінансовим установам негайно виявляти та реагувати на підозрілі транзакції. Для впровадження цих технологій необхідно провести оцінку ризиків, обрати відповідні інструменти, зібрати якісні дані для навчання моделей та інтегрувати їх у наявні системи. Важливо також забезпечити безперервний моніторинг та оновлення моделей ШІ/МН. Таким чином, використання ШІ та МН значно покращує здатність виявляти та запобігати фінансовим злочинам, забезпечуючи більш ефективний захист для фінансових установ та їх клієнтів.

https://bit.ly/4cv9prU

Вогнепальна зброя західного виробництва надходить до Росії попри санкції: AOAV досліджує масштаби проблеми

Дослідження AOAV докладно демонструє, як західна зброя продовжує потрапляти до Росії, незважаючи на міжнародні санкції, введені через війну в Україні. Росія використовує мережу посередників і паралельний імпорт через країни Євразійського економічного союзу (включаючи Вірменію, Білорусь, Казахстан і Киргизстан), Туреччину та Об'єднані Арабські Емірати для обходу санкційних обмежень.

У статті згадуються кілька західних компаній, зокрема Barrett, SIG Sauer та Beretta, які продовжують експортувати зброю до Росії. Зброя часто потрапляє до Росії через треті країни, де вона перекуповується посередниками, що спеціалізуються на обході санкцій. Розслідування виявило конкретні приклади великих партій зброї, що експортуються до Росії. Наприклад, високоточні снайперські гвинтівки Barrett були виявлені в руках російських військових на сході України. Ці гвинтівки потрапили до Росії через фіктивні компанії та підставних покупців у Туреччині та ОАЕ.

У статті наголошується на необхідності посилення міжнародного контролю за експортом зброї та підвищення рівня співпраці між країнами для виявлення та припинення незаконних поставок.

Пропонується введення більш жорстких заходів щодо фіктивних компаній та підставних покупців, а також посилення санкцій щодо країн, які допомагають обходити існуючі обмеження.

https://bit.ly/3XsDhkF

У листі Національного агентства боротьби зі злочинністю [Великобританії] висвітлюються проблеми з режимом контролю за фінансуванням політичних партій Великобританії

Стаття від Spotlight on Corruption досліджує проблеми дотримання законодавства щодо фінансування політичних партій у Великій Британії та роль відмивання коштів у цьому процесі.

Національне агентство боротьби зі злочинністю (NCA) у своїй відповіді на запит про покращення контролю за політичним фінансуванням висвітлює кілька основних проблем. Однією з головних проблем є відсутність центрального органу, який би відповідав за кримінальні переслідування у випадках порушення фінансових законів. Виборча комісія більше не має права ініціювати кримінальні провадження, а Спеціалізований підрозділ поліції Лондона зосереджується лише на шахрайстві у виборчому процесі.

Друге питання вказує на серйозні прогалини в чинному законодавстві, яке не забороняє використання іноземних коштів для пожертв, якщо донор є допустимим у Великій Британії. Це дозволяє злочинцям використовувати політичні пожертви для відмивання коштів. NCA наголошує на необхідності посилення перевірок джерел фінансування, особливо політичних пожертв, для запобігання використанню політичних партій як інструментів для відмивання грошей.

NCA пропонує кілька реформ для покращення ситуації. По-перше, необхідно переглянути законодавство для усунення регуляторних прогалин і забезпечення більш ефективного контролю за політичними пожертвами. Це включає обов'язкові перевірки джерел пожертв від політичних партій та депутатів для виявлення справжніх джерел фінансування. Крім того, підвищення ролі NCA у координації зусиль по контролю за політичним фінансуванням може бути досягнуто шляхом створення спеціалізованого підрозділу з необхідними ресурсами.

Незважаючи на виклики, NCA вважає, що усунення цих проблем можливе за рахунок надання додаткових ресурсів та посилення співпраці між політичними партіями та регуляторами. Політичні партії повинні внести пропозиції щодо покращення законів про політичне фінансування та впровадити надійні політики "знай свого донора". Після виборів необхідно провести оцінку впливу нових правил і забезпечити захист демократії.

https://www.spotlightcorruption.org/nca-political-finance-enforcement/

Розробка проекту для відкритої, вільної та надійної цифрової економіки

Стаття "Designing a blueprint for open, free and trustworthy digital economies" від Atlantic Council обговорює, як політика формує цифровий світ і підкреслює необхідність балансу між свободою та безпекою в цифрових інфраструктурах. Вона аналізує ключові аспекти цифрової економіки, такі як інфраструктура, дані та ідентифікація, та наголошує на важливості відповідальності та безпеки. Стаття закликає до співпраці між урядом, індустрією та

громадянським суспільством для створення відкритої, безпечної та довірчої цифрової економіки.

http://surl.li/urabz

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:

- Головний комплаєнс спеціаліст Binance Ноа Перлман приєднується до TRM Talks
- Влада Німеччини затримала організатора збору коштів ISKP напередодні Чемпіонату Європи з футболу
- «Криптовибори»
- Результати в опитуванні BIS 2023 CBDC
- Що далі для Ради з фінансової стабільності щодо цифрових активів?
- Це все про цю «Base»: TRM підтримує блокчейн Coinbase Base
- Правові акти щодо протидії відмиванню коштів опубліковано в журналі ЄС

http://surl.li/uramn

Рішення для боротьби з відмиванням грошей. Аналіз розміру та частки ринку в 2024-2031 рр

Звіт про ринок рішень для боротьби з відмиванням грошей (Anti-Money Laundering Solution Market) за 2024-2031 роки аналізує розміри ринку, сегментацію, типи продуктів та їх застосування, а також регіональні перспективи. Основні типи програмного забезпечення включають моніторинг транзакцій, звітність про валютні операції, управління ідентичністю клієнтів та управління відповідністю. Звіт призначений для зацікавлених сторін, постачальників і учасників галузі, охоплює 220 сторінок і прогнозує значний річний ріст (CAGR) протягом зазначеного періоду.

Визначено найбільших виробників на світовому ринку, серед яких Oracle, Thomson Reuters, Fiserv, SAS та інші. Очікується, що ринок в Північній Америці, особливо в США, продовжить відігравати важливу роль у зростанні ринку через високу впровадженість передових технологій і присутність великих гравців. Європа також демонструє значний ріст протягом прогнозного періоду.

Незважаючи на високу конкуренцію, інвестори залишаються оптимістичними щодо цього сегмента, і передбачається збільшення нових інвестицій у цю галузь у майбутньому. Звіт зосереджується на розмірах ринку, сегментах за типом продукту та застосуванням, конкурентному ландшафті, поточному стані та тенденціях розвитку. Технологічні інновації та прогрес сприятимуть оптимізації продуктивності продуктів, що призведе до ширшого використання у різних галузях. Аналіз поведінки споживачів і динаміка ринку (водії, стримуючі фактори, можливості) забезпечують важливу інформацію для розуміння ринку рішень для боротьби з відмиванням грошей.

https://bit.ly/3RBnjki

Глобальний звіт про фінансування тероризму: Вибірка новин за травень

Стаття "Global Terrorist Financing Report" від Insight Threat Intelligence розглядає сучасні методи фінансування терористичних організацій по всьому світу. В ній наведено приклади та випадки з різних регіонів, які ілюструють, як терористичні групи використовують різноманітні методи для збору коштів і приховування своїх фінансових потоків.

Основні регіональні приклади:

- Північна Америка: В США, підлітка з Айдахо заарештували за планування атаки на церкву від імені ІДІЛ, фінансованої через криптовалюту. У Канаді, крадіжки автомобілів підозрюються у фінансуванні тероризму.
- Африка: ISWAP в Нігерії збільшив податки та збори з місцевого населення, що викликає невдоволення. Деякі лідери Jama'at Nusrat al-Islam wal-Muslimin у Малі та Буркіна-Фасо займаються викраденням людей для викупу.
- Європа: В Італії заарештовано підозрюваного у зв'язках з ІДІЛ, у Великобританії триває судовий процес над особою, яка фінансувала терористичні групи через перекази.
- Близький Схід: Ізраїль заморозив рахунки партії Ra'am через підозри у зв'язках з ХАМАС, а в Лівані застрелили особу, підозрювану у фінансуванні ХАМАС.
- Центральна та Південно-Східна Азія: В Індії та Пакистані терористичні групи використовують підроблені документи та криптовалюту для фінансування своїх операцій.

Основні методи:

- Використання криптовалют та анонімних транзакцій для приховування фінансових потоків.
- Перекази через традиційні фінансові установи з використанням підставних осіб або компаній.
- Оподаткування та інші форми вимагання коштів від місцевих громад.

Рекомендації:

- Підвищення співпраці між державними установами та приватним сектором для обміну інформацією.
- Використання розширеного фінансового аналізу для виявлення підозрілих транзакцій.
- Посилення заходів з боротьби з використанням криптовалют у фінансуванні тероризму.

https://newsletter.insightthreatintel.com/p/global-terrorist-financing-report-e8d

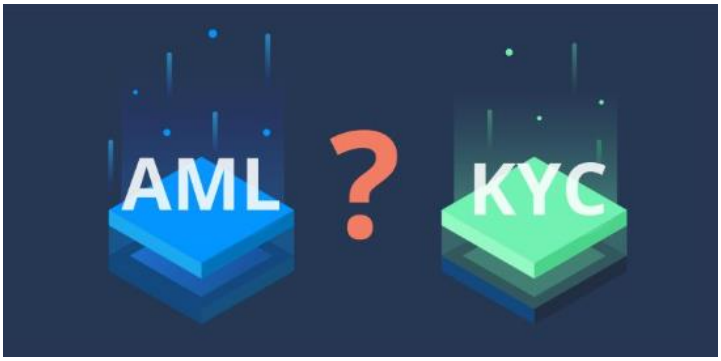
Вибори до ЄС 2024: прокриптопартії отримують місця на фоні втрат Зелених

🌍 На виборах до ЄС 2024 року партії, які прихильники криптовалюти, отримали місця, тоді як Зелені програли. Ключові партії, такі як Християнські демократи та Renew Europe, наполягають на жорсткому регулюванні криптовалют і розробці цифрового євро. Європейська народна партія підтримує MiCA, виступаючи за збалансоване регулювання криптовалют. Соціал-демократи зосереджуються на суворих правилах, щоб запобігти зловживанням. Renew Europe бореться за інновації та цифрову ідентичність. Цей різноманітний політичний ландшафт сформує європейське криптовалютне майбутнє. 🚀🔐

https://cointelegraph.com/news/eu-elections-2024-crypto-law-europe?es_id=3991439939

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Регулювання AML/KYC



Останні зміни в нормативних актах щодо KYC і ПВК змінюють ландшафт відповідності в усьому світі, відображаючи узгоджені зусилля щодо зміцнення фінансової цілісності та боротьби з незаконною діяльністю. Ось детальний огляд ключових регуляторних змін та їх наслідків:

Шоста директива ЄС з ПВК (6AMLD)

Починаючи з червня 2024 року, 6AMLD ЄС розширює регулятивний нагляд, включаючи віртуальні активи та постачальників крипто-послуг. Ця директива передбачає більш суворі заходи належної перевірки клієнта та вимагає передачу інформації про відправника та одержувача для криптовалютних транзакцій на суму понад 1000 євро. Охоплюючи цифрові валюти, ЄС прагне закрити лазівки та підвищити прозорість у криптосекторі, що швидко розвивається.

Закон про корпоративну прозорість (CTA) у США

Запроваджений із січня 2024 року CTA зобов'язує американські компанії розкривати інформацію про бенефіціарну власність FinCEN (Мережі боротьби з фінансовими злочинами). Ця ініціатива спрямована на підставні компанії, які часто використовують для відмивання коштів та інших фінансових злочинів, з метою підвищення прозорості та підзвітності в корпоративних структурах.

План боротьби з економічною злочинністю Великобританії 2 (ECP2)

Запроваджений у 2023 році ECP2 у Великій Британії зосереджується на зміцненні можливостей правоохоронних органів, посиленні повернення активів і боротьбі з різними фінансовими злочинами, зокрема відмиванням коштів та ухиленням від санкцій.

Покращення законодавства в азійсько-тихоокеанському регіоні та Латинській Америці

Країни азійсько-тихоокеанського регіону, такі як Сінгапур і Австралія, посилюють правила AML/KYC, зокрема у відповідь на інновації цифрових платежів і криптовалюти. Подібним чином країни Латинської Америки, такі як Бразилія та Мексика, зміцнюють свої системи з ПВК, щоб протистояти зростаючим загрозам фінансових злочинів.

Міжнародне співробітництво та ризик-орієнтований підхід

Такі глобальні організації, як FATF і Egmont Group, наголошують на важливості міжнародної співпраці та обміну інформацією для ефективної протидії транскордонним фінансовим злочинам.

Регулювання посиленої належної перевірки та криптовалют

Регулятори в усьому світі підвищують вимоги до належної перевірки, особливо в секторах, які вважаються високоризиковими. Криптовалюти залишаються в центрі уваги, і органи влади посилюють контроль, щоб запобігти їх використанню для відмивання коштів і незаконної фінансової діяльності.

Адаптація стратегій відповідності

Ці нормативні зміни підкреслюють динамічний характер вимог AML/KYC і необхідність швидкої адаптації фінансових установ. Щоб ефективно орієнтуватися в цьому мінливому ландшафті, організації повинні пріоритезувати комплексні стратегії відповідності, які включають надійну належну перевірку, технологічні досягнення та проактивні заходи для зменшення ризиків.

CBDC і DeFi: взаємодія та перспективи

Цифрові валюти центральних банків (CBDC) привертають все більше уваги, оскільки вони можуть покращити ефективність фінансових систем і контроль над грошовою масою. Водночас, сектор децентралізованих фінансів (DeFi) розвивається, пропонуючи нові фінансові моделі без участі традиційних установ. Взаємодія між CBDC та DeFi відкриває нові можливості та виклики.

CBDC можуть забезпечити стабільність та довіру, зменшивши волатильність криптовалют та залучаючи нових користувачів. Вони можуть служити надійними активами для DeFi-протоколів, сприяючи зростанню обох ринків через взаємодію активів. Однак інтеграція CBDC в DeFi вимагає нових регуляторних рамок, що може збільшити прозорість і безпеку операцій, але обмежити анонімність та децентралізацію.

Інтеграція CBDC в DeFi може стати важливим кроком у розвитку глобальної фінансової системи, підвищуючи стабільність та прозорість фінансових транзакцій. Успіх цієї інтеграції залежить від співпраці між центральними банками, розробниками блокчейн і регуляторами, спрямованої на створення ефективних регуляторних рамок, забезпечення взаємодії між системами та захист конфіденційності та безпеки користувачів.

http://surl.li/uqnbw

Ігрові валюти

Розглянемо деякі з найбільш поширених ігор, їхні внутрішньоігрові валюти, способи оплати та потенційні ризики відмивання коштів.

1. Fortnite

- Внутрішньоігрова валюта: V-Bucks

- Використовується для: Купівля косметичних предметів, бойових пропусків та іншого ігрового контенту

- Фіатний обмін: V-Bucks можна придбати безпосередньо за реальні гроші, використовуючи кредитні/дебетові картки, PayPal або подарункові картки

- Задіяні фінтех-компанії: PayPal, Stripe, Xsolla

- Ризики відмивання коштів: V-Bucks можна купувати і продавати на сторонніх ринках, що потенційно уможливлює відмивання коштів через купівлю та перепродаж ігрових предметів

2. Roblox

- Внутрішньоігрова валюта: Robux

- Використовуються для: Купівля внутрішньоігрових предметів, покращення та досвід, створені іншими користувачами

- Фіатний обмін: Robux можна придбати за реальні гроші за допомогою кредитних/дебетових карток, PayPal або подарункових карток Roblox

- Задіяні фінтех-компанії: PayPal, Stripe, Apple Pay, Google Pay

- Ризики відмивання коштів: Ринок контенту, створеного користувачами Roblox, і можливість конвертувати Robux назад у реальні гроші можуть створювати можливості для відмивання коштів

3. Minecraft

- Внутрішньоігрова валюта: Монети Minecraft (Minecoins)

- Використовується для: Купівля скінів, пакетів текстур та інший внутрішньоігровий контент на Minecraft Marketplace

- Фіатний обмін: Minecoins можна придбати за реальні гроші за допомогою кредитних/дебетових карток, PayPal або подарункових карток

- Задіяні фінтех-компанії: PayPal, Stripe, Xsolla

- Ризики відмивання коштів: Хоча самі Minecoins не є предметом торгівлі, купівля-продаж акаунтів Minecraft з цінними ігровими предметами може бути потенційним шляхом для відмивання коштів.

4. PUBG Corporation

- Внутрішньоігрова валюта: Невідома готівка (UC)

- Використовується для: Купівля ігрових предметів, скінів та бойових пропусків

- Фіатний обмін: UC можна купити за реальні гроші, використовуючи кредитні/дебетові картки, PayPal або мобільні платіжні системи

- Задіяні фінтех-компанії: PayPal, Stripe, Xsolla, Codashop

- Ризики відмивання коштів: Торгівля цінними ігровими предметами та акаунтами на сторонніх ринках може потенційно сприяти відмиванню коштів

5. Call of Duty

- Внутрішньоігрова валюта: Бали COD

- Використовується для: Купівля бойових пропусків, косметичних предметів та іншого ігрового контенту

- Фіатний обмін: COD Points можна придбати за реальні гроші за допомогою кредитних/дебетових карток, PayPal або подарункових карток

- Задіяні фінтех-платформи: PayPal, Stripe, Xsolla

- Ризики відмивання коштів: Купівля та продаж акаунтів COD з рідкісними ігровими предметами на сторонніх ринках може бути потенційним методом відмивання коштів

Спільною рисою цих популярних ігор є наявність внутрішньоігрових валют, які можна придбати за реальні гроші та використовувати для придбання віртуальних предметів або апгрейдів. Залучення таких фінтех-компаній, як PayPal і Stripe, спрощує процес оплати, але також створює потенційні можливості для відмивання коштів, особливо в поєднанні зі сторонніми майданчиками для торгівлі ігровими предметами та акаунтами.

Ухилення від санкцій: прихована загроза відмивання коштів у відеоіграх

Оскільки світ ігор продовжує розвиватися, зростає ризик відмивання коштів та ухилення від санкцій. Використання віртуальних валют і внутрішньоігрових предметів як альтернативних методів оплати створило нові можливості для суб'єктів, які перебувають під санкціями, щоб обійти традиційні фінансові канали та отримати доступ до глобальної фінансової системи.

Як це працює?

1. Підсанкційні особи або організації купують цифрові активи за незаконні кошти та продають їх на вторинних ринках за чисті гроші.
2. Підставні компанії або посередники в ігровій індустрії можуть бути використані для відмивання коштів і уникнення виявлення.
3. Регуляторні прогалини та слабке правозастосування в деяких країнах можуть бути використані для відмивання коштів за допомогою відеоігор.

Глобальний вплив

Використання відмивання коштів у відеоіграх для ухилення від санкцій може мати серйозні наслідки, підриваючи ефективність режимів міжнародних санкцій і сприяючи потоку незаконних коштів для підтримки злочинної діяльності або порушень прав людини.

Що можна зробити?

1. Посилити правила протидії відмиванню коштів та фінансуванню тероризму в індустрії відеоігор і забезпечити послідовне їх дотримання в усіх юрисдикціях.
2. Заохочуйте більшу співпрацю та обмін інформацією між гральними компаніями, фінансовими установами та правоохоронними органами.
3. Розробити нові інструменти та технології для відстеження потоків віртуальних валют і внутрішньоігрових предметів.
4. Сприяти обізнаності та освіті громадськості щодо ризиків відмивання коштів у відеоіграх та ухилення від санкцій.

Заклик до дії

Вкрай важливо, щоб уряди, міжнародні організації та ігрова індустрія працювали разом, щоб протистояти цій новій загрозі.

Дослідження вторинного ринку: торгівля, обмін і продаж токенів і предметів у грі

Після того, як гравці використали фіатну валюту для придбання ігрових токенів або предметів, є кілька способів обміну або монетизації цих цифрових активів в ігровій екосистемі.

1. Внутрішньоігрова торгівля

Багато ігор, особливо MMORPG, мають вбудовані системи, які дозволяють гравцям торгувати предметами або валютою безпосередньо один з одним. Ці операції часто відбуваються на спеціальних ігрових ринках або через взаємодію між гравцями.

2. Офіційні ігрові ринки

Деякі ігри мають офіційні ринки, де гравці можуть купувати, продавати або обмінювати ігрові предмети та валюту, використовуючи власну валюту гри або реальні гроші. Ці ринки, як правило, контролюються і регулюються розробниками ігор.

3. Сторонні маркетплейси

Існує безліч сторонніх веб-сайтів і платформ, які полегшують купівлю, продаж і торгівлю внутрішньоігровими предметами та акаунтами. Ці ринки часто працюють незалежно від розробників ігор і можуть не мати такого ж рівня нагляду чи регулювання. Одним із прикладів є G2G.com, популярна платформа, де гравці можуть купувати та продавати ігрові предмети, валюту та акаунти для різних ігор, таких як Fortnite, Roblox та World of Warcraft.

4. Пірингова торгівля

Гравці також можуть брати участь у прямій піринговій торгівлі, використовуючи чати, форуми або соціальні мережі для пошуку потенційних торгових партнерів. Ці транзакції часто відбуваються поза ігровим середовищем і можуть включати використання сторонніх платіжних систем або навіть криптовалюти.

5. Подарункові картки та коди

Деякі ігри дозволяють гравцям купувати подарункові картки або коди, які можна обміняти на ігрові предмети або валюту. Ці картки можна купувати і продавати на вторинних ринках, забезпечуючи ще один шлях для обміну цифровими активами.

Ризики вторинних ринків

Хоча ці методи пропонують гравцям гнучкість і можливість монетизувати свої внутрішньоігрові активи, вони також створюють потенційні шляхи для відмивання коштів та іншої незаконної діяльності. Відсутність регулювання та нагляду на деяких з цих вторинних ринків, таких як G2G.com, може ускладнити відстеження та запобігання підозрілим транзакціям.

Боротьба з ризиками

Для боротьби з цими ризиками розробники ігор, власники платформ і регулятори повинні працювати разом:

- Впроваджувати надійні заходи боротьби з відмиванням коштів

- Контролювати вторинні ринки

- Інформувати гравців про небезпеку участі в несанкціонованих операціях

Інструкції США щодо протидії відмиванню коштів та відмиванню коштів у відеоіграх: моніторинг, проблеми та вдосконалення

Згідно з чинними вказівками США щодо AML/BSA, існує кілька аспектів ігрової індустрії, які можна контролювати, щоб виявити та запобігти відмиванню грошей. Однак існують також значні проблеми та сфери, які потрібно вдосконалити.

1. 🕵 Можливості моніторингу

- Фінансові установи, які обробляють платежі для компаній, що займаються відеоіграми, повинні проводити належну перевірку та повідомляти про підозрілу діяльність.
- Розробники ігор і оператори платформ можуть впроваджувати процедури KYC (Знай свого клієнта) і відстежувати транзакції в грі на наявність незвичних шаблонів.
- Офіційні ігрові ринки можуть відстежувати та повідомляти про великі або часті транзакції.

2. ⊘ Проблеми та обмеження

- Сторонні торгові майданчики та однорангову торгівлю важко контролювати, оскільки вони часто працюють поза юрисдикцією влади США.
- Відсутність узгодженого регулювання в ігровій індустрії ускладнює одноманітне дотримання правил AML/BSA.
- Природа відеоігор і віртуальної економіки, що постійно розвивається, ускладнює регуляцію, щоб йти в ногу з новими методами відмивання грошей.
- Обмежені ресурси та досвід у регуляторних органах можуть перешкоджати ефективному моніторингу та застосуванню.

3. 💡 Потенційні покращення

- Розширення правил боротьби з відмиванням коштів/BSA, щоб вони охоплювали відеоігри та віртуальні валюти, забезпечуючи ясність і послідовність для галузі.
- Заохочувати міжнародну співпрацю для вирішення проблеми глобального характеру відмивання відеоігор і використання офшорних ринків.
- Вимагати від сторонніх ринків впроваджувати заходи протидії відмиванню коштів та обмінюватися інформацією з органами влади, подібно до вимог до традиційних фінансових установ.
- Інвестуйте в навчання та ресурси для регуляторних органів, щоб краще розуміти та контролювати складний світ економіки відеоігор.
- Сприяти співпраці між розробниками ігор, операторами платформ і правоохоронними органами для обміну інформацією та передовими методами виявлення та запобігання відмиванню грошей.
- Впроваджуйте більш надійні системи перевірки ідентифікації та моніторингу транзакцій в іграх і на ігрових платформах.
- Навчайте гравців про ризики відмивання грошей і важливість використання законних, регульованих ринків.

Як запобігти шахрайству?

Кілька важливих порад щодо стратегії запобігання шахрайству для повсякденної безпеки:

Бережіть свої паролі: Ставтеся до своїх паролів як до цінних ключів. Уникайте передбачуваних варіантів, таких як дні народження або клички домашніх тварин, натомість обирайте складні комбінації букв, цифр і символів. Не використовуйте їх повторно на різних платформах і подумайте про використання менеджера паролів, щоб надійно їх зберігати.

Слідкуйте за дзвінками: Остерігайтеся небажаних дзвінків, електронних листів і текстів, особливо тих, що пропонують "занадто хороші, щоб бути правдою" пропозиції. Фішингові схеми є поширеним явищем, тому подумайте двічі, перш ніж переходити за посиланнями або ділитися особистою інформацією. Якщо це здається підозрілим, так воно і є!

Захистіть свою систему: Регулярно оновлюйте своє програмне забезпечення, від операційної системи до додатків. Ці оновлення часто виправляють вразливості в системі безпеки, що робить ваші цифрові стіни складнішими для злому. Інвестуйте в антивірусний захист і постійно оновлюйте його для додаткового рівня захисту.

Щомісячна звірка банківських рахунків: Вимагайте проведення звірки незалежною особою, яка не є бухгалтером або особою, відповідальною за підписання чеків, або забезпечте контроль з боку наглядових органів.

Будьте пильні, але не лякайтеся: Знання - це сила! Будьте в курсі поширених тактик шахрайства та афер, що циркулюють в Інтернеті. Поінформованість дає вам змогу виявити підозрілу діяльність та не стати жертвою.

Довіряй, але перевіряй: здійснюючи покупки в Інтернеті, обирайте надійні вебсайти з перевіреними відгуками. Шукайте значки безпеки та протоколи шифрування, які вказують на безпеку транзакцій. Якщо щось не так, не соромтеся геть.

Блокуйте свої фінанси: Регулярно перевіряйте свої банківські рахунки та кредитні звіти. Раннє виявлення несанкціонованої діяльності може допомогти мінімізувати збитки та запобігти подальшим втратам. Використовуйте безпечні способи оплати, особливо для онлайн-транзакцій, і уникайте публічних Wi-Fi для проведення чутливих фінансових операцій.

ПВК у секторі страхування

Хоча страховий сектор пропонує фінансову безпеку для багатьох людей, він не захищений від тактики кмітливих злочинців. Ці підлі актори виявляють та використовують різні страхові продукти, плетучи складні мережі для відмивання незаконних доходів.

Наприклад, ануїтетні поліси стали популярними інструментами, особливо з високими регулярними преміями. Злочинці вливають шахрайські кошти як премії, а натомість отримують постійний потік «чистого» доходу. Але на цьому їх винахідливість не закінчується. Деякі маневрують системою, купуючи поліси та передаючи право власності третім особам, залученим у відмивання коштів, фактично перетворюючи незаконні кошти на законні виплати.

Крім того, політика єдиної премії та поповнення дають можливість непомітно переходити великим сумам з рук в руки. Інвестуючи в поліси єдиної премії або здійснюючи додаткові платежі, відмивачі знаходять шляхи для скидання великих шматків брудних грошей під виглядом справжніх транзакцій.

Навіть механізми, покликані надати страхувальникам гнучкість, як-от періоди обмірковувань, не позбавлені ризику. Відмивачі грошей іноді навмисно переплачують премії або маніпулюють системою, щоб отримати відшкодування, успішно відмиваючи значні суми. Крім того, хитре використання позик, коли грошова вартість полісу страхування життя використовується за кредитом, дозволяє цим злочинцям циркулювати незаконні кошти, залишаючись поза увагою.

Основні заходи відповідності

Страховий ландшафт — це не лише розробка найкращих полісів для клієнтів; це також пильність проти прихованих фінансових загроз. Оскільки злочинці все частіше плетуть складні змови, щоб використовувати страхові рішення для відмивання коштів, компанії знаходяться під тиском, для посилення свого захисту.

1. Знай свого клієнта (KYC)
2. Перевірка санкцій
3. Пильний моніторинг транзакцій
4. Правозастосування через нагляд
5. Нюанси належної перевірки

Поширені методи відмивання грошей

✅Відмивання на основі торгівлі:

Відмивання грошей у торгівлі передбачає виставлення завищених або занижених рахунків за товари та послуги для переміщення грошей через кордон. Відмивачі узгоджують свій облік з незаконними грошима, маніпулюючи ціною, кількістю або якістю товару чи послуги.

✅Компанії-оболонки та трасти:

Це неактивні компанії або юридичні особи, які використовуються як засіб фінансових маневрів, що допомагає приховати справжнє походження грошей. Вони часто існують лише на папері і не мають фізичної присутності чи працівників.

✅Офшорні рахунки:

Злочинці часто використовують рахунки в країнах із суворими законами про банківську таємницю, щоб приховати гроші та їх походження. Ці юрисдикції часто мають м'яке законодавство з ПВК, що полегшує приховування великих сум грошей.

✅Цифрові валюти:

З розвитком криптовалют цифрові транзакції стали новим рубежом для відмивання грошей. Анонімність, яку забезпечують криптовалюти, ускладнює відстеження транзакцій.

✅Смурфінг:

Смурфінг передбачає розбиття великої транзакції на кілька менших, щоб уникнути підозр. Ці менші транзакції потім вносяться на один або кілька банківських рахунків або використовуються для придбання активів.

✅Оборот коштів:

У цьому випадку фізичні особи вносять гроші в регульовану іноземну корпорацію, розташовану в офшорах, в ідеалі в податковій гавані з мінімальним обліком. Потім вони повертають гроші як прямі іноземні інвестиції, які зазвичай звільняються від податків.

✅Казино:

Людина може купити фішки за незаконну готівку, зіграти лише на невелику суму, а потім обміняти решту на чек у казино. Це створює враження, ніби заробіток є законним виграшем в азартних іграх.

Розкриття прихованих ризиків: уразливості казино від відмивання коштів

Казино – це не просто місця розваг; вони також є потенційними гарячими точками для відмивання грошей. Складні транзакції та високий грошовий потік у казино створюють унікальні вразливості, якими можуть скористатися злочинці.

Розуміння цих ризиків має вирішальне значення для захисту цілісності ігрової індустрії та забезпечення відповідності законодавству з ПВК.

🔍 Основні вразливості:⬇

✅Високий обсяг готівкових операцій: обсяг готівкових операцій може приховати незаконну діяльність.

✅Чіпи та токени: конвертацію готівки в фішки та назад можна використовувати для відмивання грошей.

✅Структурування: Розбиття великих сум на менші, менш підозрілі операції.

✅Транскордонний рух: міжнародні клієнти та транзакції підвищують ускладнення.

✅Програми для VIP-персон: транзакції з високою вартістю, здійснені VIP-персонами, можуть менше перевірятися.

🔒 Стратегії пом'якшення:

🎯Впровадження надійних процедур KYC.

🎯Постійний моніторинг транзакцій за допомогою розширеної аналітики.

🎯Навчання персоналу розпізнавати підозрілу діяльність і повідомляти про неї.

🎯Співпраця з регуляторними органами, щоб випереджати нові загрози.

👉Управління з питань азартних ігор Швеції, Spelinspektionen, отримало дозвіл на збільшення штрафів за порушення, пов’язані з ПВК, починаючи з квітня 2024 року. Ця зміна спрямована на посилення захисту споживачів і боротьбу зі злочинністю в ігровому секторі шляхом застосування вищих штрафів за невідповідність Закону про відмивання грошей.

Оскільки ми все глибше заглиблюємося в епоху цифрових технологій, дуже важливо адаптувати та вдосконалювати наші системи протидії відмиванню коштів для боротьби з цими складними схемами. Разом ми можемо гарантувати, що захоплення від гри не будуть заплямовані незаконними діями.

5 кроків для визначення високих ризиків ВК/ФТ у вашому бізнесі

Фінансові правила вимагають від усіх підзвітних організацій бути уважними щодо ВК/ФТ.

Ось 5 ключових кроків, які допоможуть визначити зони високого ризику у вашому бізнесі:

1. **Перевірте клієнтів: санкції та негативні згадки у ЗМІ**

Перш ніж встановлювати ділові відносини з будь-яким клієнтом, проведіть ретельну перевірку на відповідність санкційним списками та негативному висвітленню в ЗМІ. Це допомагає ідентифікувати осіб або підприємства, пов’язані з незаконною діяльністю.

2. **Визначте політично значущих осіб (PEPs)**

Чиновники, члени сімей та їхнє близьке оточення становлять більший ризик через свій потенційний вплив. Визначте всіх публічних діячів серед ваших наявних і потенційних клієнтів, щоб застосувати посилені заходи належної перевірки.

3. **Звертайте увагу на зв’язки з країнами високого ризику**

Відомо, що деякі країни мають слабший контроль за протидією відмивання коштів. Будьте особливо обережні, коли маєте справу з клієнтами або транзакціями, що відбуваються з юрисдикцій із високим ризиком.

4. **Визначайте складні або незвичайні транзакції**

Транзакції, які є надто складними, передбачають надзвичайно великі суми або не мають чіткої комерційної мети, повинні викликати подальше розслідування. Шукайте невідповідності типовій фінансовій діяльності або економічному профілю клієнта.

5. **Не ігноруйте незрозумілі дії**

Будь-яка операція, яка не має сенсу або не відповідає встановленому фінансовому профілю клієнта. Ретельно розслідуйте та, якщо все ще є підозри, повідомте про підозру до відповідних органів.

Як моніторинг транзакцій виявляє шахрайство?

У 2024 році моніторинг транзакцій як ніколи важливий. Фінансові злочини, як-от відмивання грошей і шахрайство, стають дедалі складнішими, що вимагає передових заходів виявлення та запобігання.

https://www.zigram.tech/blog/how-does-transaction-monitoring-detect-fraud/