Серійний номер: ДСФМУ-ДК-2024-020
Серпень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Децентралізовані автономні організації (DAO)

Документ представляє собою оглядову роботу, присвячену децентралізованим автономним організаціям (DAOs). У ньому розглядається концепція DAOs, їх ключові риси, юридичний статус, практичні аспекти їх впровадження та можливі напрямки правових реформ для підтримки розвитку таких організацій у Великій Британії.

Основні теми включають **філософію DAOs, яка базується на ідеях прозорості, демократичності та рівноправності через використання технологій розподілених реєстрів (DLT) та смарт-контрактів**. Документ також обговорює різноманітні варіанти організації DAOs, включаючи чисті DAOs, гібридні моделі та цифрові юридичні особи.

Юридичний статус DAOs розглядається як важливий аспект, оскільки від цього залежить багато питань, таких як відповідальність учасників, можливість укладення контрактів, володіння майном та податкові зобов'язання. Особлива увага приділяється викликам, пов'язаним з відсутністю визначеного правового статусу та залежності DAOs від технологій.

Ключові висновки:

1. **Різноманітність DAOs та їх правовий статус:** DAOs являють собою широкий спектр організаційних структур, які можуть включати "чисті" DAOs, гібридні структури та цифрові юридичні особи. **"Чисті" DAOs** уникають використання юридичних форм, покладаючись на технології, такі як смарт-контракти та розподілені реєстри. **Гібридні DAOs**, навпаки, інтегрують юридичні особи для захисту учасників від відповідальності та полегшення взаємодії з офлайн світом. **Цифрові юридичні особи** - це юридичні компанії, які використовують технології для своїх операцій і управління.
2. **Юридичні виклики та ризики:** Визначення правового статусу DAOs є критично важливим через потенційні ризики відповідальності. У випадку відсутності формальної юридичної структури, учасники DAOs можуть бути визнані загальним партнерством або незареєстрованою асоціацією, що накладає на них особисту відповідальність за зобов'язання

організації. Визначення, хто є відповідальним у разі правопорушення або збитків, стає складним питанням, особливо для "чистих" DAOs.

3. **Юрисдикція та міжнародні аспекти:** DAOs часто функціонують у глобальному масштабі, що створює виклики для визначення юрисдикції. Децентралізований характер DAOs та їхня діяльність через розподілені реєстри ускладнюють прив'язку до конкретного географічного розташування. Це може призводити до труднощів у визначенні, які закони застосовуються до організації та її учасників, що, в свою чергу, ускладнює питання оподаткування та регулювання.
4. **Вплив на регулювання та законодавство:** Документ підкреслює, що необхідності в створенні спеціальної юридичної форми для DAOs в Англії та Уельсі на даний момент немає. Більшість існуючих юридичних структур достатньо гнучкі, щоб включати елементи DAOs. Однак, необхідність перегляду деяких аспектів законодавства, зокрема в області корпоративного права та боротьби з відмиванням грошей, є очевидною. Такі зміни можуть полегшити використання технологій розподілених реєстрів у рамках існуючих юридичних форм.
5. **Можливі сценарії правового розвитку:** Документ пропонує кілька напрямків для подальшого вивчення та можливих реформ, включаючи перегляд законодавства про трасти та можливість створення нових правових форм, таких як неприбуткові асоціації з обмеженою відповідальністю. Також пропонується переглянути законодавство з ПВК/ФТ, щоб забезпечити його сумісність з новими технологіями.
6. **Аспекти управління та децентралізації:** DAOs прагнуть до децентралізованого управління, де рішення приймаються через голосування спільноти, а не через централізований орган управління. Це може створювати певні виклики в ефективності прийняття рішень, особливо на ранніх стадіях розвитку DAOs, коли рішення часто залишаються в руках обмеженої групи учасників. Однак, з часом, ці структури можуть переходити до більш децентралізованої форми управління.

Таким чином, DAOs представляють собою інноваційні організаційні структури, що відкривають нові можливості для управління та співпраці. Однак, їх впровадження супроводжується значними юридичними викликами, які потребують уважного вивчення та можливої адаптації існуючого законодавства.

https://lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/

Боротьба з відмиванням коштів у Хорватії

Звіт «Tackling Money Laundering in Croatia: Conference Report» висвітлює ключові виклики та можливості, з якими стикається Хорватія в контексті боротьби з відмиванням коштів і фінансуванням тероризму. Звіт було створено на основі круглого столу, організованого британським аналітичним центром RUSI, та охоплює дискусії між представниками громадських організацій та журналістами. **Хорватія, яка нещодавно була включена до "сірого списку" FATF через недоліки в її системі боротьби з відмиванням грошей та фінансуванням тероризму, наразі стикається з великими викликами, зокрема у сфері корупції, незалежності судової системи та відмивання грошей через ринок нерухомості**.

Звіт також відзначає низький рівень доступу до даних, обмежену незалежність ЗМІ та відсутність ефективних механізмів тиску на уряд з боку громадянського суспільства та ЄС. Учасники заходу вказали на необхідність активізації зусиль з боку громадських організацій, особливо в контексті використання звітів ЄС про верховенство права для підвищення обізнаності

та мобілізації суспільства. Також було підкреслено важливість координації зусиль на рівні ЄС та розробки нових стратегій для підвищення прозорості та підзвітності.

Ключові висновки:

1. **Включення до "сірого списку" FATF:** Включення Хорватії до "сірого списку" FATF у 2023 році свідчить про серйозні недоліки в її системі боротьби з відмиванням коштів та фінансуванням тероризму. Основні проблеми включають нерівномірне розуміння ризиків, низьку кількість засуджень за відмивання коштів та недостатню здатність виявляти фінансування тероризму.
2. **Корупція як основний виклик:** Корупція залишається основною проблемою для Хорватії, зокрема в уряді та судовій системі. Учасники відзначили низький рівень незалежності судової системи, що підриває довіру до правосуддя. Особливу увагу було приділено питанням корупції в секторі нерухомості, де відмивання коштів через інвестиції в нерухомість стало значною проблемою.
3. **Обмежена роль громадянського суспільства та ЗМІ:** Незважаючи на важливу роль громадянських організацій і журналістів у забезпеченні підзвітності уряду, вони стикаються з численними перешкодами, включаючи обмежений доступ до даних, відсутність незалежності ЗМІ та тиск з боку різних зацікавлених сторін. Журналісти також часто стикаються з юридичними переслідуваннями, що ускладнює їхню роботу.
4. **Важливість міжнародної координації та адвокації:** Учасники підкреслили важливість використання міжнародних звітів та платформ, таких як звіт ЄС про верховенство права, для посилення адвокації на національному та міжнародному рівнях. Було запропоновано активізувати зусилля щодо підвищення обізнаності громадськості про проблеми, пов’язані з відмиванням коштів та корупцією, шляхом організації публічних заходів і конференцій.
5. **Необхідність посилення контролю та тиску з боку ЄС:** Оскільки Хорватія вже досягла значних політичних цілей, таких як вступ до Єврозони, ЄС має посилити тиск на країну через використання інших механізмів, таких як членство в ОЕСР, для забезпечення дотримання вимог FATF та боротьби з фінансовими злочинами.

Загалом, звіт підкреслює необхідність скоординованих дій громадянського суспільства, посилення ролі ЗМІ та міжнародної підтримки для ефективної боротьби з відмиванням коштів і корупцією в Хорватії.

https://static.rusi.org/croatia-tackling-money-laundering-conference-report-web-final.pdf.pdf

РЕГУЛЮВАННЯ

Уряд ОАЕ видав федеральний закон про внесення змін до положень законодавства про ПВК/ФТ.

Це оновлення спрямоване на вдосконалення правової бази, яка підтримує зусилля країни щодо боротьби з фінансовими злочинами та приведення законодавства у відповідність з міжнародними стандартами.

Ключові зміни включають створення Національного комітету з питань протидії відмиванню коштів та фінансуванню тероризму, а також Вищого комітету з нагляду за національною стратегією, який контролюватиме та оцінюватиме ефективність заходів ПВК/ФТ.

Указ також вимагає покращення координації між відповідними органами для підтримки Національного комітету та полегшення його обов'язків, включаючи підготовку до звіту про взаємну оцінку (MER) щодо міжнародної відповідності.

Крім того, для підтримки Національного комітету буде створено Генеральний секретаріат на чолі з Генеральним секретарем, який також виконуватиме функції заступника голови Національного комітету та члена Вищого комітету.

http://surl.li/sbyfsl

Аутсорсинг згідно Єдиного зводу правил протидії відмиванню коштів ЄС

Згідно з новим Регламентом щодо ПВК/ФТ (ЄС) 2024/1624 (AMLR), підзвітний суб'єкт може передати певні завдання, що випливають із цього Регламенту, постачальникам послуг. Однак перед тим, як підзвітний суб'єкт передасть завдання на аутсорс, він повинен переконатися, що постачальник послуг достатньо кваліфікований для виконання завдань, які передадуться. Умови виконання таких завдань деталізуються в письмовій угоді між підзвітним суб'єктом та виконавцем послуг.

Підзвітний суб'єкт залишатиметься повністю відповідальним за будь-які дії чи бездіяльність, пов'язані з переданими на аутсорс завданнями, які виконуються постачальниками послуг. Він повинен бути спроможним продемонструвати своїм наглядовим органам, що для кожного завдання, переданого на аутсорс, він розуміє обгрунтування діяльності, яку здійснює постачальник послуг, і підхід, який дотримується під час їх виконання, і що така діяльність пом'якшує конкретні ризики, яким наражається підзвітний суб'єкт.

Якщо підзвітний суб'єкт передає завдання на аутсорс, він повинен переконатися, що постачальник послуг і будь-який наступний суб-аутсорсинговий постачальник послуг застосовує його політику та процедури. У зв'язку з цим підзвітний суб'єкт повинен здійснювати регулярний контроль, щоб переконатися в тому, що постачальник послуг ефективно виконує політику та процедури. Крім того, підзвітний суб'єкт повинен переконатися, що аутсорсинг не погіршує здатність наглядових органів відстежувати дотримання AMLR та Регламенту про переказ коштів.

Наступні завдання не можуть бути передані на аутсорс за жодних обставин:

- пропозиція та затвердження загальногосподарської оцінки ризиків підзвітного суб'єкта
- затвердження внутрішньої політики, процедур і засобів контролю підзвітного суб'єкта;
- рішення щодо профілю ризику, який буде віднесено до клієнта;

- рішення вступити в ділові відносини або здійснити окрему операцію з клієнтом;
- звітування до ПФР про підозрілу діяльність або повідомлення на основі порогових значень, за винятком випадків, коли така діяльність передана іншому підзвітному суб'єкту, що належить до тієї ж групи та заснований в тій самій державі-члені;
- затвердження критеріїв виявлення підозрілих або незвичних операцій і діяльності.

Підзвітні суб'єкти не повинні передавати завдання постачальникам послуг, які знаходяться або зареєстровані в третіх країнах, якщо не виконуються всі наступні умови:

a) підзвітний суб’єкт доручає виконання завдань виключно постачальнику послуг, який є частиною тієї ж групи;
b) група застосовує політику та процедури з ПВК/ФТ, заходи належної перевірки клієнта та правила ведення записів, які повністю відповідають AMLR або еквівалентними правилами в третіх країнах;
c) ефективне виконання вимог, зазначених у пункті (b) цього параграфа, контролюється на рівні групи наглядовим органом держави-члена відповідно до Розділу IV Директиви ЄС 2024/1640 (AMLD6).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1624

Імплементація MiCA в країнах Європи

У світі криптовалют та цифрових активів дотримання регулятивних вимог стає ключовим фактором успіху для бізнесів, що прагнуть легально працювати на ринку. Команда Manimama завершила детальне дослідження впровадження регуляції Markets in Crypto-assets Regulation (MiCA) у різних країнах ЄС. Ці дослідження висвітлюють особливості отримання ліцензії на діяльність з криптовалютами, нові вимоги для провайдерів криптоактивів, а також процедури та ресурси, необхідні для відповідності новим правилам.

У Франції законодавчі зміни в сфері криптовалют і цифрових активів почали набирати чинності з прийняттям регуляції MiCA (Markets in Crypto-assets Regulation). Цей нормативний акт замінює існуючий режим PACTE і вимагає від криптовалютних компаній дотримання нових, більш жорстких стандартів. З 1 січня 2024 року у Франції почали діяти зміни до Генерального регламенту AMF, які адаптують національні вимоги до європейських стандартів MiCA.

Ці зміни включають вимоги до прозорості, організаційних структур, управління ризиками, внутрішнього контролю та кібербезпеки. Зокрема, провайдери цифрових активів повинні забезпечити розділення активів клієнтів і власних активів, а також дотримуватися більш суворих вимог до управління конфліктами інтересів і забезпечення безпеки інформаційних систем.

Період адаптації до нових вимог триватиме до 30 червня 2026 року, після чого всі провайдери криптоактивів повинні будуть отримати ліцензію відповідно до нових норм MiCA для продовження своєї діяльності. Це стосується як місцевих, так і іноземних компаній, які прагнуть працювати на ринку Франції.

Додатково, у рамках цих змін французький регулятор AMF запровадив можливість подачі заявок на попередній розгляд ліцензій ще до того, як MiCA повністю набуде чинності у грудні 2024 року. Це дозволяє провайдерам підготуватися до нових вимог заздалегідь, забезпечивши собі конкурентну перевагу на ринку.

Таким чином, регулятивні зміни у Франції створюють нові можливості для прозорої та безпечної роботи з криптовалютами, водночас підвищуючи стандарти ведення бізнесу в цьому динамічному секторі.

http://surl.li/hxgzow

У Нідерландах регулювання криптоактивів також зазнає значних змін у зв'язку з впровадженням регуляції MiCA (Markets in Crypto-assets Regulation). З квітня 2024 року криптовалютні компанії можуть подавати заявки на отримання ліцензій, які набудуть чинності з 30 грудня 2024 року, коли MiCA офіційно вступить у силу.

Національне законодавство вимагає від компаній, що працюють з криптоактивами, відповідати ряду вимог, таких як розділення активів клієнтів, управління конфліктами інтересів, забезпечення кібербезпеки, а також відповідність нормам AML (боротьба з відмиванням грошей) та CFT (боротьба з фінансуванням тероризму).

AFM (Autoriteit Financiële Markten) і DNB (De Nederlandsche Bank) будуть основними регуляторами, які здійснюватимуть нагляд за дотриманням цих нових норм. Компанії, що вже працюють на ринку, матимуть перехідний період до липня 2025 року, щоб адаптуватися до нових вимог. Протягом цього періоду компанії можуть скористатися процедурою попередньої перевірки (pre-scan) від AFM, що дозволяє підготуватися до подачі заявки на ліцензію і забезпечити відповідність нормам MiCA.

Ці зміни спрямовані на підвищення прозорості, безпеки та відповідності європейським стандартам, що робить ринок криптоактивів у Нідерландах більш привабливим і надійним для інвесторів.

https://www.linkedin.com/pulse/mica-implementation-netherlands-manimama-x5dqf/

В Угорщині впровадження регуляції MiCA (Markets in Crypto-assets Regulation) вимагає від криптовалютних компаній суворого дотримання нових стандартів, які регулюватиме Національний банк Угорщини (MNB). Закон про ринок криптоактивів передбачає відсутність перехідного періоду, тому провайдери криптоактивів зобов'язані відповідати вимогам MiCA з 1 січня 2025 року. Основні вимоги включають обов'язкову оплату наглядового збору, забезпечення системи обробки скарг та дотримання стандартів професійної компетенції.

Порушення вимог може призвести до значних штрафів, які можуть досягати 5% від річного обороту компанії або більше залежно від характеру порушення. Угорщина забезпечує суворий нагляд за виконанням цих вимог, що сприяє підвищенню прозорості та надійності ринку криптоактивів у країні.

https://www.linkedin.com/pulse/mica-implementation-hungary-manimama-ygroe/

САНКЦІЇ

Санкції в Європі, 2-е видання

Це 358 сторінок, які **охоплюють режими санкцій ЄС, його держав-членів та інших європейських юрисдикцій, що не входять до ЄС**, і є обов'язковим до прочитання для всіх, чий бізнес або діяльність так чи інакше має справу з санкціями, фінансовими та торговельно-економічними.

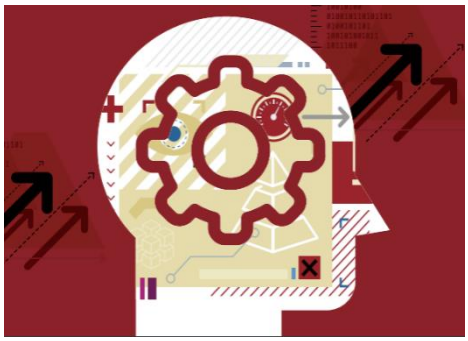
Посібник, який також доступний у вигляді електронної книги, **пояснює процес запровадження, імплементації та виконання санкцій/обмежувальних заходів (ООН, ЄС, автономні) у відповідних юрисдикціях, надаючи детальну інформацію про ключові органи (з контактною інформацією) та їхні повноваження разом із розбивкою різних покарань за порушення** та вивченням конкретних особливостей, про які слід знати.

Крім того, у ньому розглядаються зусилля відповідних органів влади та політичні чинники, які впливають на реалізацію (або інший вплив) різних заходів. У нових розділах розглядається відповідь на війну Росії проти України та розглядається вплив на Європу санкцій США.

https://www.worldecr.com/books/

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Велике прискорення: погляди CIO на генеративний ШІ



Документ "The Great Acceleration: CIO Perspectives on Generative AI" є **дослідженням, яке аналізує, як технологічні лідери інтегрують генеративний штучний інтелект (ШІ) у своїх організаціях**, використовуючи його як частину загальної стратегії штучного інтелекту. Звіт базується на інтерв'ю з високопосадовцями та експертами у різних галузях, а також на глобальному опитуванні директорів з питань інформаційних технологій (CIO). У ньому **висвітлюються ключові виклики та можливості, пов'язані з впровадженням генеративного ШІ, включаючи питання інфраструктури даних, управління ризиками, побудови та впровадження моделей, а також вплив на робочу силу**.

Ключові висновки:

1. **Трансформаційний потенціал генеративного ШІ:** Генеративний ШІ має революційний вплив на економіки та підприємства, що відображається в очікуваному збільшенні глобального ВВП на 7% завдяки автоматизації та іншим ефектам.
2. **Розширення можливостей через інфраструктуру даних:** Для ефективного використання генеративного ШІ потрібна гнучка та масштабована інфраструктура даних, що підтримує доступ до даних і аналітики на рівні підприємства. Важливим елементом є впровадження lakehouse архітектури для інтеграції структурованих та неструктурованих даних.
3. **Баланс між відкритими і закритими моделями:** Організації стикаються з вибором між використанням відкритих джерел та розробкою власних моделей ШІ, щоб захистити інтелектуальну власність та зберегти контроль над даними.
4. **Вплив на робочу силу:** Хоча існує занепокоєння щодо автоматизації робочих місць, експерти вважають, що генеративний ШІ скоріше підвищить продуктивність та дозволить співробітникам зосередитися на більш цінних завданнях, а не повністю замінить їх.
5. **Управління ризиками та відповідальність:** Використання генеративного ШІ несе в собі ризики, пов'язані з безпекою, конфіденційністю та упередженістю моделей. Це вимагає інтегрованого підходу до управління даними та суворого дотримання регуляторних вимог.
6. **Роль генеративного ШІ в різних галузях:** Звіт демонструє, як різні галузі, від охорони здоров'я до медіа та фінансів, адаптують генеративний ШІ для підвищення ефективності, покращення обслуговування клієнтів та автоматизації складних процесів.

Таким чином, звіт підкреслює необхідність стратегічного підходу до впровадження генеративного ШІ, зокрема в контексті управління даними та технологічної інфраструктури, щоб максимально використати можливості цієї революційної технології.

http://surl.li/qwkqjd

Ризик і винагорода: як тіньова економіка впливає на фінансову практику войовничих організацій

У цій статті досліджується, як бойові організації взаємодіють з тіньовими економіками для фінансування своєї діяльності. Вона аналізує симбіотичні відносини між цими групами та незаконними економіками, такими як торгівля наркотиками, контрабанда та інші форми незаконної торгівлі. Стаття надає уявлення про те, як ці організації керують фінансовими ризиками і винагородами, адаптуються до змінних обставин та забезпечують

свою фінансову стабільність, незважаючи на значний тиск з боку правоохоронних органів та заходи з протидії тероризму.

Основні моменти статті включають:

1. **Інтеграція з незаконними економіками:** Бойові групи часто діють у межах тіньових економік, займаючись такими видами діяльності, як контрабанда, здирництво та незаконна торгівля (наприклад, зброєю, наркотиками). Ця діяльність є ключовою для їхнього фінансування та виживання.
2. **Стратегії фінансового управління:** У статті розглядаються способи, якими бойові організації керують своїми фінансами, включаючи відмивання грошей, приховування активів та інвестування у легальні бізнеси для підтримки своєї діяльності.
3. **Адаптація до зовнішнього тиску:** Бойові групи постійно адаптують свої фінансові стратегії у відповідь на зовнішній тиск, такий як посилення заходів протидії тероризму, санкції та глобальні фінансові регуляції.
4. **Вплив на глобальну безпеку:** Участь бойових організацій у тіньових економіках має ширші наслідки для глобальної безпеки. Ця діяльність може підривати стабільність держав, сприяти корупції та підтримувати цикли насильства та нестабільності.

Ця стаття є надзвичайно важливою для розуміння фінансових практик бойових організацій, особливо в контексті боротьби з відмиванням коштів, фінансуванням тероризму та розповсюдженням зброї масового знищення. Вона надає цінні інсайти щодо того, як ці групи забезпечують своє фінансове виживання та які виклики стоять перед владою у спробах розірвати ці мережі.

https://www.tandfonline.com/doi/full/10.1080/09546553.2024.2381211

Шахрайство в скандинавських країнах. Один регіон, багато відмінностей

Документ "Fraud in the Nordics" є ґрунтовним звітом, що **аналізує стан шахрайства в країнах Північної Європи—Норвегії, Швеції, Данії та Фінляндії. Він досліджує різноманітні типології шахрайства, поширені в цих регіонах, зокрема атаки соціальної інженерії (фішинг, смішинг, вішинг), шахрайство з авторизованими платежами (APP fraud), а також інші види шахрайства**. У звіті підкреслюється, як **високий рівень цифровізації, широке використання електронних платежів та низька залежність від готівки роблять ці країни особливо вразливими** до таких видів шахрайства.

Кожен розділ, присвячений окремій країні, детально розглядає конкретні виклики шахрайства, регуляторні ландшафти та заходи, що вживаються для боротьби з шахрайством. Наприклад, Норвегія стикається з суттєвими проблемами, пов’язаними з вішингом та шахрайством з платіжними картками, тоді як у Швеції спостерігається зростання інвестиційного та платіжного шахрайства, зокрема через соціальну інженерію. У Данії відзначено зменшення загальних втрат від шахрайства, однак фішингові електронні листи залишаються серйозною загрозою. У Фінляндії, хоча рівень шахрайства нижчий порівняно з іншими країнами Північної Європи, різко зросла сума втрат від шахрайських схем, особливо через інвестиційне та CEO-шахрайство.

Ключові висновки:

1. **Висока цифровізація як двосічний меч:** Розвинені цифрові економіки країн Північної Європи, незважаючи на численні переваги, також піддають їх вищим ризикам шахрайства, особливо у вигляді онлайн-шахрайства та шахрайства з платежами. Висока проникність

інтернету та велика залежність від електронних платежів створюють широкі можливості для шахраїв.

2. **Переважання атак соціальної інженерії:** Шахраї все частіше використовують техніки соціальної інженерії для обману жертв. Фішинг, вішинг і смішинг стали особливо поширеними в усіх країнах Північної Європи, і їхня складність постійно зростає. Ці методи часто використовуються для отримання доступу до конфіденційних даних і викрадення особистих і банківських даних.
3. **Різниця у шахрайських тенденціях у різних країнах:** Кожна країна Північної Європи демонструє свої унікальні патерни шахрайства, що вимагає індивідуального підходу до реагування. Наприклад, у Норвегії через високу проникність інтернету більш розповсюдженим є вішинг, тоді як у Швеції зростає загроза інвестиційного шахрайства, зокрема за допомогою підроблених криптовалютних схем.
4. **Регуляторні відповіді та виклики:** Регуляторні середовища цих країн розвиваються для протидії зростаючим загрозам. Наприклад, впроваджуються заходи з блокування шахрайських дзвінків, посилюються вимоги до автентифікації клієнтів, покращується захист споживачів. Однак ефективність цих заходів варіюється, і потрібні постійні коригування для того, щоб встигати за новими методами шахрайства.
5. **Необхідність багаторівневої системи захисту від шахрайства:** Складність сучасних шахрайських атак вимагає багаторівневого підходу до їх запобігання. Це означає поєднання традиційних антисистемних рішень з новітніми технологіями, такими як поведінкова біометрія та динамічний аналіз. Особливо важливо розпізнавати різницю між законною та шахрайською діяльністю, а також застосовувати відповідний рівень захисту на всіх етапах взаємодії з клієнтами.

Ці висновки підкреслюють важливість постійного моніторингу, адаптації регуляторних механізмів і впровадження технологічних інновацій для ефективної боротьби з шахрайством у високотехнологічних економіках країн Північної Європи.

http://surl.li/vrwiye

Посібник щодо незалежного аудиту ПВК

Документ є детальним керівництвом щодо незалежного аудиту протидії відмиванню коштів. Він охоплює **всі аспекти процесу проведення незалежного AML-аудиту**, включаючи планування, виконання та подальші дії після аудиту. Описано роль незалежного аудиту у виявленні прогалин та недоліків в AML/CFT програмах організацій, а також важливість цих аудитів для підтримки відповідності законодавству та захисту бізнесу від фінансових злочинів.

Ключові висновки:

1. **Важливість незалежного AML-аудиту:** Незалежний аудит є важливим елементом контролю якості та ефективності впроваджених програм боротьби з відмиванням грошей (AML) і фінансуванням тероризму (CFT). Він забезпечує неупереджений огляд відповідності програм нормативним вимогам і виявляє можливі недоліки, що можуть загрожувати фінансовій безпеці організації.

2. **Виявлення та усунення прогалин:** Під час аудиту визначаються слабкі місця в існуючих процедурах і політиках, що можуть бути використані злочинцями для відмивання грошей. Аудитори надають конкретні рекомендації щодо усунення цих прогалин, що допомагає організаціям ефективніше боротися з фінансовими злочинами.

3. **Покращення репутації та довіри:** Регулярні незалежні аудити сприяють зміцненню репутації компанії як відповідального і законослухняного суб'єкта. Це підвищує довіру з боку клієнтів, інвесторів та регуляторів, що може сприяти залученню додаткових інвестицій і зміцненню позицій на ринку.

4. **Адаптація до змін у правовому середовищі:** Оскільки правове поле у сфері AML/CFT постійно змінюється, регулярні аудити дозволяють організаціям своєчасно адаптувати свої програми та процедури відповідно до нових вимог та загроз. Це знижує ризик виникнення правових проблем і штрафів за невідповідність.

5. **Роль у підтримці безпеки бізнесу:** Аудитори також перевіряють, наскільки ефективно організація впроваджує навчальні програми для співробітників і наскільки добре вони обізнані про свої обов'язки у сфері ПВК/ФТ. Це допомагає мінімізувати ризики, пов'язані з людським фактором, та забезпечити загальну безпеку бізнесу.

http://surl.li/tjpnda

Фінансове майбутнє Ісламської держави

Стаття Джессіки Девіс у журналі “Combating Terrorism Center” аналізує стратегії фінансування Ісламської держави (ІД) після втрати територіального контролю. ІД адаптувалася до нових умов, створивши гнучкі та стійкі фінансові мережі, які підтримують її діяльність навіть після краху халіфату. Ці мережі включають використання криптовалют, контрабанду, вимагання, а також фінансування через діаспори та інші підтримуючі групи. Ісламська держава зберігає свою здатність до виживання завдяки різноманітним джерелам доходів, що робить її значним викликом для міжнародних зусиль у боротьбі з тероризмом.

Ключові моменти статті:

1. **Адаптивність ІД:** Після втрати території група перейшла до нелегальних та напівлегальних методів фінансування, включаючи криптовалюти та контрабанду, що дозволяє їй підтримувати свою діяльність.

2. **Мережі підтримки:** ІД покладається на глобальні мережі підтримки, включаючи діаспори та прихильників, які забезпечують фінансування через різні канали.

3. **Гнучкість фінансових стратегій:** ІД постійно адаптує свої фінансові стратегії до змін у середовищі безпеки, що дозволяє їй залишатися стійкою навіть у несприятливих умовах.

4. **Загроза для глобальної безпеки:** Незважаючи на втрату територіального контролю, ІД залишається значною загрозою завдяки своїм фінансовим мережам, які підтримують її здатність до насильства та терористичної діяльності.

https://ctc.westpoint.edu/wp-content/uploads/2024/08/CTC-SENTINEL-072024.pdf

Ісламська держава в Афганістані: золота нагода для «золотої дитини»

Документ під назвою "The Islamic State in Afghanistan: A Golden Opportunity for a ‘Golden Child’" **розглядає діяльність Ісламської Держави в Афганістані, зокрема її філіалу в провінції Хорасан (ISKP), після захоплення влади Талібаном у 2021 році**. Цей розвиток подій відкрив нові можливості для ISKP, дозволяючи йому не лише закріпитися, але й збільшити свої амбіції щодо проведення міжнародних терористичних операцій. Основна увага документа приділяється фінансовим аспектам діяльності ISKP, включаючи його залежність від міжнародних мереж, які дозволяють отримувати та пересилати кошти для здійснення терористичних операцій. Описуються

різні способи фінансування, такі як криптовалюти, традиційні системи передачі грошей (наприклад, "хавала") та використання нелегальних мереж обміну грошей. Також аналізуються можливі дії, які можна вжити для боротьби з фінансовими потоками, що підтримують ISKP.

Ключові висновки:

1. **Зміцнення позицій ISKP після захоплення влади Талібаном:** Після падіння Ісламської Республіки Афганістан і захоплення влади Талібаном у серпні 2021 року, Ісламська Держава в провінції Хорасан (ISKP) отримала нові можливості для розширення своєї діяльності. Відхід іноземних військових сил з Афганістану створив вакуум влади, який дозволив ISKP переорієнтуватися і зміцнити свій вплив у країні. ISKP почав позиціонувати себе не лише як опонент Талібану, але й як важливий елемент у глобальній мережі джихадистів. Це підкріплено амбіціями ISKP проводити зовнішні терористичні операції, наприклад, проти європейських цілей, що відображає їх зростаючі можливості та загрози.

2. **Розширення фінансової мережі ISKP:** Фінансова стабільність ISKP багато в чому залежить від її включення в широку мережу фінансування Ісламської Держави. Після занепаду центрального командування Ісламської Держави в Сирії, ISKP отримує значну фінансову підтримку від міжнародної мережі, включаючи допомогу з Африки, Середнього Сходу та інших регіонів. Наприклад, офіс Al-Karrar в Сомалі виступає як ключовий координатор фінансових потоків для ISKP, забезпечуючи регулярні криптовалютні трансфери. Ці зв'язки дозволяють ISKP підтримувати активність навіть у складних умовах, зокрема під тиском з боку Талібану.

3. **Фінансова самостійність та розвиток регіональних мереж:** Незважаючи на постійну фінансову підтримку від центрального командування Ісламської Держави, ISKP все більше розвиває свою фінансову незалежність, спираючись на регіональні джерела доходів. Група активно залучає кошти через нелегальні мережі в регіоні, такі як гавала, а також через тиск на місцеве населення. Зокрема, в провінції Нангархар, що на сході Афганістану, ISKP отримує кошти від приватних донорів з країн Перської затоки, які підтримують Салафітські громади. Така фінансова самостійність дозволяє ISKP залишатися однією з найактивніших філій Ісламської Держави, зберігаючи контроль над фінансовими потоками та плануючи власні операції.

4. **Використання криптовалют для фінансування терористичної діяльності:** Зростаюча роль криптовалют у фінансовій діяльності ISKP є значним викликом для глобальної безпеки. Використання криптовалютних платежів дозволяє ISKP отримувати кошти від міжнародних донорів і переміщати їх через кордони з меншою ймовірністю бути відстеженими. Хоча існує ризик під час обміну криптовалют на готівку, ISKP використовує інфраструктуру хавадала для зберігання та переміщення таких коштів. Важливо зазначити, що це є частиною ширшої стратегії Ісламської Держави щодо адаптації до нових технологій та обмеження можливостей протидії з боку державних органів.

5. **Міжнародна співпраця для боротьби з фінансуванням тероризму:** Документ підкреслює необхідність зміцнення міжнародної співпраці в боротьбі з фінансуванням тероризму, зокрема через моніторинг фінансових потоків і впровадження санкцій. Використання блокчейн-аналітики для відстеження криптовалютних транзакцій, а також націлювання на ключових фінансових посередників, може значно обмежити фінансові можливості ISKP. Успішні операції з арешту фінансових агентів ISKP, таких як затримання Шаміля Хукуматова в Туреччині,

показують ефективність скоординованих зусиль державних органів та міжнародних організацій. Це є критично важливим для обмеження здатності ISKP фінансувати терористичні операції та зберігати свою бойову готовність.

Ці висновки висвітлюють важливі аспекти фінансових операцій ISKP, а також шляхи, якими міжнародна спільнота може протидіяти фінансуванню тероризму, підкреслюючи необхідність адаптації до нових викликів та технологій.

http://surl.li/ilfgcr

Звіт щодо глобального регулювання ШІ: перспективи щодо формування глобального та регіонального нормативного ландшафту

Документ «BRG Global AI Regulation Report 2024» відображає стан та перспективи регулювання штучного інтелекту (ШІ) на глобальному та регіональному рівнях. **У звіті представлені результати опитування понад 200 керівників компаній та юристів з різних галузей, а також інтерв'ю з експертами, що дозволило оцінити поточний стан політик регулювання ШІ, виклики, з якими стикаються організації, та погляди ключових зацікавлених сторін на подальший розвиток** ефективної політики ШІ. Документ висвітлює **складнощі, пов'язані з різноманітністю підходів до регулювання в різних юрисдикціях, та важливість знаходження балансу між інноваціями і безпекою**.

Звіт підкреслює, що **регулювання ШІ перебуває на початкових етапах розвитку**, а ефективність існуючих політик викликає неоднозначні оцінки серед керівників та юристів. **Найбільше уваги приділяється питанням захисту даних, безпеки та надійності ШІ**, а також необхідності запобігання його неетичному використанню. Окрім того, **обговорюються ризики, пов'язані з невідповідністю регуляторним вимогам, які можуть включати значні штрафи та втрату довіри з боку споживачів.**

Ключові висновки:

1. **Регулювання ШІ знаходиться на ранній стадії розвитку:** Станом на 2024 рік, регулювання штучного інтелекту (ШІ) є ще незрілим, з великими відмінностями в підходах різних юрисдикцій. Наприклад, Європейський Союз запроваджує більш ризик-орієнтований підхід через AI Act, що ставить заборони на певні види використання ШІ, тоді як у країнах Південно-Східної Азії, таких як Сінгапур, розроблено бізнес-дружні настанови щодо управління та етики ШІ. У США, підхід залишається децентралізованим, і поки не існує єдиного федерального регулювання, натомість розвивається регіональне та галузеве законодавство. Це створює не лише ризики для організацій через непослідовність нормативних вимог, але й можливості для тих, хто зможе швидко адаптуватися до змін.
2. **Неоднозначність оцінок ефективності чинних політик:** Серед опитаних керівників і юристів спостерігається суттєва різниця в оцінках ефективності поточних регуляторних підходів до ШІ. Лише третина респондентів вважає чинні політики "дуже ефективними", тоді як інші мають помірковану або низьку оцінку. Юристи, які безпосередньо стикаються з ризиками у сфері ШІ, як правило, більш скептично налаштовані щодо ефективності політик і впевненості в здатності організацій забезпечити їх виконання. Наприклад, у Північній Америці лише 28% респондентів вважають регулювання ШІ "дуже ефективним", що можна пояснити відсутністю єдиного підходу на рівні країни.
3. **Критична роль даних у регулюванні та використанні ШІ:** Основними проблемами, з якими стикаються організації та регулятори, є забезпечення захисту даних, їхньої надійності та безпеки. Оскільки ШІ може працювати лише настільки добре, наскільки якісними є дані, на яких він навчається, дані повинні бути безпечними, точними та надійними. Недостатня

увага до цих аспектів може призвести до значних правових і фінансових ризиків для компаній, включаючи штрафи та втрату довіри з боку споживачів і інвесторів. Наприклад, у Європейському Союзі порушення вимог AI Act може призвести до штрафів до 7% від глобального річного доходу компанії.

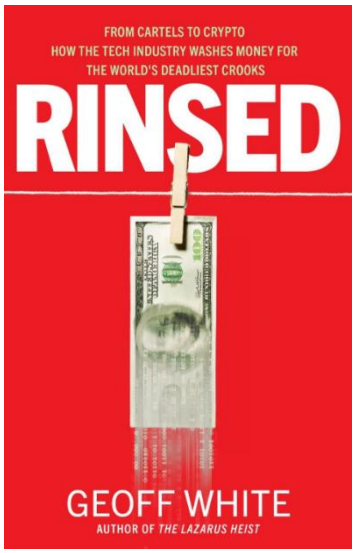
4. **Проблеми з дотриманням регуляторних вимог:** Хоча більшість опитаних організацій висловили впевненість у своїй здатності відповідати чинним регуляторним вимогам, лише 40% є "дуже впевненими" у цьому. Основні причини низької впевненості включають недостатнє внутрішнє навчання персоналу, відсутність належних протоколів управління даними та кібербезпеки, а також відсутність спеціально виділеного для цього персоналу. Це вказує на необхідність впровадження більш жорстких внутрішніх механізмів і багатопрофільних команд для управління ризиками, пов’язаними з ШІ.
5. **Необхідність комплексного підходу до регулювання:** Переважна більшість респондентів підтримує ідею широкого, універсального підходу до регулювання ШІ, який би охоплював міжнародну співпрацю та гармонізацію стандартів. Це особливо актуально в умовах швидкого розвитку технологій, коли чинні закони не завжди встигають за нововведеннями. Існують розбіжності в поглядах на те, який підхід до регулювання має бути пріоритетним: частина респондентів вважає за доцільне впровадження сектор- або країно-специфічних стандартів, тоді як інші підтримують ідею універсальних правил, які можна адаптувати в різних юрисдикціях.
6. **Перспективи майбутнього регулювання:** Хоча більшість респондентів (57%) вважають, що ефективне регулювання ШІ з’явиться в найближчі три роки, лише 36% з них впевнені, що майбутні регуляції нададуть необхідні гарантії для розвитку та використання ШІ. Це підкреслює невизначеність щодо того, як саме буде регулюватися ШІ в майбутньому, і необхідність гнучких підходів до розробки політик, що здатні адаптуватися до швидких змін у технологіях. Наприклад, існує загроза, що надмірно жорстке регулювання в ЄС може стати бар'єром для інновацій, зокрема для стартапів.

Цей документ є важливим джерелом інформації для керівників компаній та юристів, які прагнуть зрозуміти поточний стан регулювання ШІ та підготуватися до майбутніх викликів.

http://surl.li/xnxlju

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Rinsed: від картелів до крипто: як індустрія технологій відмиває rjinb для найстрашніших шахраїв у світі



"Rinsed" Джеффа Вайта — це захоплююча книга, яка досліджує, як сучасний цифровий світ змінив правила гри у сфері відмивання коштів. У книзі розкривається, як традиційні злочинні угруповання, такі як картелі та організовані злочинні синдикати, об'єдналися з висококваліфікованими кіберзлочинцями для створення глобальної машини з відмивання коштів, яка є надто складною для більшості правоохоронних органів.

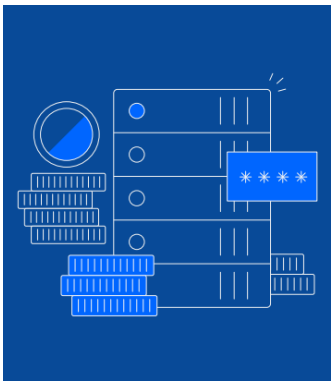
Автор досліджує історії, які ведуть читача від розкішних готелів Дубая до таємних зон Північної Кореї, розкриваючи діяльність того, що він називає "кіберсуперкартелем". Книга не тільки надає глибокі знання про технологічні основи цих злочинних мереж, але й висвітлює страшні наслідки їхньої діяльності для людей.

"Rinsed" — це проникливий погляд на те, як цифрові технології змінили ландшафт глобального фінансового злочину, і книга стане цінним ресурсом для тих, хто цікавиться взаємодією між технологіями, злочинністю та фінансами.

http://surl.li/rkdlil

ІНШІ НОВИНИ

Як IRS-CI використовувала Blockchain Intelligence, щоб знищити xDedic Marketplace



Даний документ є дослідженням, що описує розслідування Служби кримінальних розслідувань Податкового управління США (IRS-CI) у справі закриття маркетплейсу xDedic. Цей маркетплейс був платформою, де продавалися скомпрометовані облікові дані для віддаленого доступу до комп'ютерних систем по всьому світу. Через цю платформу кіберзлочинці здійснювали різні незаконні дії, такі як фінансові шахрайства, вимагання та поширення програм-вимагачів. IRS-CI, використовуючи блокчейн-аналітику та співпрацюючи з міжнародними партнерами, вдалося не лише закрити маркетплейс, але й притягнути до відповідальності 19 осіб, включаючи адміністраторів та постачальників послуг.

Ключові висновки з документа:

1. Значення міжнародної співпраці: Розслідування xDedic демонструє критичну роль міжнародної співпраці у боротьбі з кіберзлочинністю. Успіх операції був досягнутий завдяки тісній взаємодії між IRS-CI та правоохоронними органами в інших країнах, таких як Бельгія, Україна, Нідерланди та Німеччина.
2. Використання блокчейн-аналітики: Технологія блокчейн стала ключовим інструментом у відстеженні фінансових транзакцій та ідентифікації кіберзлочинців. Це підкреслює важливість новітніх технологій у сучасних розслідуваннях фінансових злочинів.
3. Розширення розслідування: Завдяки справі xDedic, IRS-CI змогла зібрати додаткові дані, які допомогли викрити інші кіберзлочинні мережі, такі як маркетплейс SSNDOB, який продавав соціальні номери понад 24 мільйонів американців.
4. Наслідки для кіберзлочинців: Закриття xDedic та притягнення до відповідальності його адміністраторів і постачальників послуг є серйозним ударом по міжнародних кіберзлочинних угрупованнях, що займаються відмиванням грошей та іншими фінансовими злочинами.

Цей документ слугує прикладом успішної боротьби з кіберзлочинністю на глобальному рівні, демонструючи важливість як технологічних рішень, так і міжнародної співпраці у сучасних умовах.

http://surl.li/fvjojb

Питання регулювання криптовалют від Elliptic

Глобальні зусилля щодо регулювання криптовалют продовжують набирати обертів, що підтверджується останніми подіями в різних країнах. Швейцарський регулятор FINMA опублікував керівництво для емітентів стейблкоїнів, підкреслюючи важливість дотримання законодавства та управління ризиками. Інші країни, такі як Франція, Індія та Катар, також працюють над створенням або удосконаленням власних нормативних баз, прагнучи забезпечити стабільність ринку та захист інвесторів. Водночас у США криптовалюта стала важливим питанням у контексті майбутніх президентських виборів.

1. **Керівництво FINMA щодо стейблкоїнів:** Швейцарський регулятор FINMA опублікував керівництво для емітентів стейблкоїнів і банків, що надають їм гарантії, для розуміння

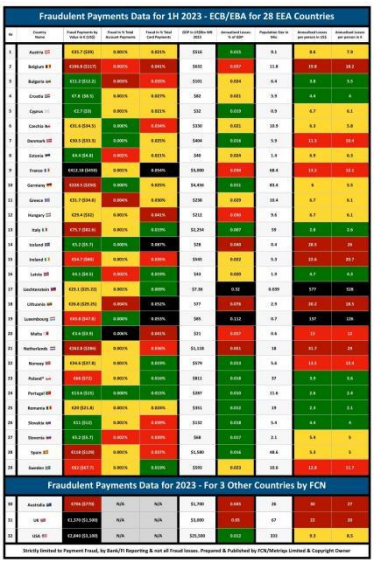
підходу до нагляду та управління ризиками в цій сфері. Стейблкоїни можуть підпадати під регулювання як банківські депозити або колективні інвестиційні схеми залежно від їх характеристик. Емітенти повинні визначити, які регуляторні вимоги застосовуються до їхніх токенів, і відповідно дотримуватися цих вимог. Багато емітентів стейблкоїнів у Швейцарії не отримують банківську ліцензію, а замість цього користуються гарантіями від інших ліцензованих банків, що дозволяє уникнути прямого нагляду FINMA. Проте такий підхід несе значні ризики для всіх сторін, і FINMA вказує на мінімальні стандарти для забезпечення гарантій. Зокрема, власники стейблкоїнів повинні мати претензії до банків, які надають гарантії у випадку банкрутства емітента. FINMA підкреслює, що емітенти повинні дотримуватися законодавства з протидії відмиванню коштів та фінансуванню тероризму навіть за відсутності банківської ліцензії. Це включає встановлення та перевірку особи власників депозитів і виявлення ризиків, пов'язаних із відмиванням коштів, ухиленням від санкцій та фінансуванням тероризму.

2. **Проект Pyxtrial та інші ініціативи:** Колектив центральних банків, включаючи BIS і Банк Англії, досліджує можливості технологічних рішень для моніторингу ризиків стейблкоїнів. У межах проекту Pyxtrial були протестовані прототипи для оцінки забезпечення активами стейблкоїнів за допомогою як ончейн, так і офчейн даних.
3. **Розвиток нормативної бази в інших країнах:** Франція почала приймати заявки на ліцензування постачальників криптоактивів відповідно до регламенту MiCA, що набирає чинності з кінця 2024 року.
4. **Криптовалюта та політика в США:** Криптовалюта стає важливим питанням у президентських виборах у США. Дональд Трамп заявив про намір зробити США "криптостолицею світу", а сенатор Сінтія Луміс запропонувала створити стратегічний резерв Bitcoin для казначейства США. Демократи також намагаються змінити свій підхід до криптоіндустрії на більш прихильний.
5. **Регуляторні плани Індії та Катару**: Індія планує опублікувати політичний документ щодо криптовалют до вересня 2024 року, а Катар планує завершити розробку регуляторної бази для токенізації активів до кінця року, що може стати основою для подальшого відкриття країни для криптоактивів.

Ці новини відображають глобальні зусилля щодо регулювання криптоактивів, підкреслюючи важливість чіткого нормативного середовища для забезпечення захисту інвесторів та стабільності ринків.

http://surl.li/ugwkgd

Шахрайство з платежами та обмін інформацією:



У двох звітах ЄС про шахрайство з платежами, нещодавно опублікованих ЕВА та ЄЦБ, знаходяться дані за 2022 рік та перше півріччя 2023 року. Збитки від шахрайства з платежами становили 4,3 мільярда євро у 2022 році та 2 мільярди євро за перше півріччя 2023 року, збитки стабілізуються після десятиліття, коли збитки швидко зростали, незважаючи на зміни в поведінці шахраїв через вжиті заходи протидії. Але все ще потрібно набагато більше, оскільки зареєстровані рівні збитків все ще близькі до рекордних, про велику кількість збитків не повідомляється, а загроза постійно розвивається.

Також відзначається, що миттєві платежі допомагають шахраям і що вони також швидко переміщують гроші через кордон, без сумніву, щоб перешкодити відстеженню. Цікаво, що ЄС цілком може бути одержувачем шахрайських платежів принаймні коли йдеться про шахрайські платежі з карток. Більшість збитків (90%)

походять від платежів за рахунками та платежів картками, причому платежі за рахунками є більшими в абсолютних значеннях, але шахрайство з платежами картками є набагато поширенішим.

Це перший випадок, коли дані ЄС поширюються, і, згідно з ЕВА/ЄЦБ, вони не зовсім надійні та мають стати кращими. Тим не менш, Франція має найвищий рівень збитків серед 29 країн ЄЕЗ, але порівняно з розміром її платіжного ринку це не викликає занепокоєння, але перегляньте таблицю для порівняльного аналізу та додаткових показників, щоб побачити концентрацію шахрайства з платежами.

ЕВА надала 5 ключових рекомендацій, які зосереджені на i) посиленні вимог безпеки, включаючи боротьбу з шахрайством у режимі реального часу ii) Постачальниках послуг (PSP), які мають запровадити систему ризиків шахрайства, iii) Ясності щодо збитків і відповідальності, iv) Наглядових органах, які мають зробити більше, щоб зосередитися на шахрайстві, v) створенні єдиної платформи для обміну інформацією про боротьбу з шахрайством для PSP із забезпеченням безпеки.

https://thefinancialcrimenews.com/eu-eea-payment-fraud-the-good-the-bad-and-the-ugly/

Перехрестя підземного світу: темні мережі та глобальна незаконна торгівля в зоні кордонів між Аргентиною, Бразилією та Парагваєм

Стаття є результатом проекту Hubs of Illicit Trade', який вивчав центри незаконної торгівлі та незаконної економіки в усьому світі та очолюваний Центром боротьби з тероризмом, транснаціональною злочинністю та корупцією (TraCCC) при Університеті Джорджа Мейсона та Міжнародною коаліцією проти Незаконних економік (ICAIE) / ICAIE під керівництвом Луїзи Шеллі, Девіда М. Луни 🌍 Конвергенція загроз ≙ Kine-Dynamics і Джудіт Дін. Доктор Рашмі Сінгх і Хорхе Ласмар були співрозслідувачами прикордонної зони між Аргентиною, Бразилією та Парагваєм.

Ця стаття є поглибленим аналізом складних і часто прихованих мереж незаконної торгівлі та темних мереж, що діють у цій зоні. Дослідження заглиблюється в тонкощі глобальної незаконної торгівлі та її глибокий вплив на регіональну та міжнародну безпеку.

http://surl.li/kitasr

Глобальна наглядова організація закликає Індію посилити контроль банків за політиками

Група розробки фінансових заходів боротьби з відмиванням коштів (FATF), глобальний наглядовий орган, який зосереджується на боротьбі з відмиванням коштів, рекомендував Індії посилити нагляд за банківськими рахунками місцевих політиків, урядовців та їхніх сімей.

Ця рекомендація є частиною поточного огляду індійської системи з ПВК/ФТ, розпочатого у 2023 році. Рекомендації FATF включають більш суворий моніторинг джерел коштів на рахунках, що належать політично значущим особам (PEP), і вимагають від вищих менеджерів банків затверджувати нові рахунки для таких осіб.

Незважаючи на те, що Індія вже запроваджує суворі перевірки щодо іноземних публічних діячів, національні публічні діячі не піддаються такому ж контролю. FATF, яка нещодавно оцінила Індію

як таку, що в значній мірі відповідає глобальним стандартам з ПВК, незабаром опублікує свій остаточний звіт. Уряд Індії має п’ять років на впровадження рекомендованих змін.

http://surl.li/xnvopu

За допомогою контрабандистів і підставних компаній Китай обходить американську заборону щодо Ш.І.

Нещодавні розслідування показали багатосторонній підхід Китаю до отримання обмежених технологій ШІ завдяки даним WireScreen. Ось як вони це роблять:

1. Сірі ринки: галасливі базари електроніки Шеньчженя відкрито продають передові мікросхеми ШІ. Подумайте, тисячі Nvidia A100 змінюють власника!
2. Shell Game: Нові компанії виникають раптово, обходячи списки підсанкційних організацій. Приклад: Nettrix, народжена з підсанкційного Sugon, швидко стала партнером Nvidia.
3. Використання лазівок: американські фірми знаходять творчі обхідні шляхи - нові партнерства, закордонні дочірні компанії.
4. Мережі контрабанди: неправильне маркування відправлень (чіпси як чай!), використання слабких правоохоронних заходів. Тактика старої школи зустрічається з високотехнологічними товарами.
5. Регіональна диверсифікація: використання сусідів, таких як Сінгапур і В’єтнам, де експорт не обмежений. «Один пояс, один шлях» в дії!

Ці методи демонструють адаптивну філософію Китаю – крок у ногу з часом. Це витончений танець легальних, квазілегальних і незаконних тактик, які служать довгостроковій меті технологічної самодостатності.

https://www.nytimes.com/2024/08/04/technology/china-ai-microchips.html

Тейлор Свіфт та економіка тероризму

У статті "Taylor Swift and the Economics of Terrorism" досліджується, як сучасна поп-культура може впливати на глобальні економічні процеси, включаючи ті, що стосуються фінансування тероризму. Автор наводить приклади того, як впливові фігури в музиці, як Тейлор Свіфт, можуть спричиняти зрушення в економічних індустріях, що, у свою чергу, може створювати нові можливості для терористичних організацій. Зокрема, обговорюється важливість розуміння цих непрямих зв'язків для розробки ефективних політик боротьби з тероризмом. Стаття підкреслює необхідність глобальної співпраці між урядами, технологічними компаніями та музичною індустрією для забезпечення безпеки та стабільності в умовах нових економічних викликів.

http://surl.li/qbumal

На Філіппінах вважають, що наркосиндикати використовують POGO для відмивання грошей

У статті йдеться про підозри щодо використання філіппінських офшорних ігрових операторів (POGOs) для відмивання грошей наркокартелями. Представники Палати представників Філіппін висловили занепокоєння, що деякі POGOs пов'язані з наркосиндикатами через спільних засновників компаній. Особливу увагу приділено зв'язкам з китайськими бізнесменами та масштабним фінансовим транзакціям, які викликають підозри. Це піднімає питання щодо необхідності посилення контролю та законодавчих змін для боротьби з цими незаконними діями.

http://surl.li/hksbjj

Економіка та безпека зближуються: чи готовий Захід?

В епоху глобальних змін економіка та безпека стають невіддільними, як ніколи раніше. У статті з RUSI йдеться про те, що Захід стикається з новими викликами, де економічна міць та технологічні інновації стають основними інструментами національної безпеки. Конкуренція з Китаєм та Росією загострює необхідність для західних держав переглянути свої стратегії, щоб зберегти конкурентоспроможність та безпеку. Зараз, як ніколи, важливо розробити комплексний підхід, який поєднує економічні та безпекові заходи для ефективної відповіді на ці виклики.

Традиційні інструменти державного впливу, такі як військова міць і дипломатія, більше не є єдиними засобами підтримання безпеки. Технологічний розвиток і економічна сила тепер також визначають вплив держави на глобальній арені. Центральні банки, технологічні гіганти та уряди мають співпрацювати тісніше, щоб забезпечити національну безпеку. Це вимагає глибоких інституційних змін і нових стратегій, які повинні враховувати нові реалії.

Щоб не відставати, Захід повинен впроваджувати політику, що об'єднує економічну міць і технологічний розвиток із традиційними підходами до безпеки. Чи готовий Захід до таких змін? Це питання, на яке потрібно шукати відповіді вже сьогодні.

http://surl.li/vcubao

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Хто такі грошові мули?

Грошовий мул — це особа, яка переказує незаконно отримані кошти від імені іншої особи. Це часто – але не завжди – відбувається без того, щоб людина навіть усвідомлювала, що бере участь у незаконній діяльності. Рахунок грошового мула діє як проміжний крок у відмиванні коштів, що ускладнює відстеження джерела.

Як це працює:

Ų Мережі відмивання коштів заманюють грошових мулів через онлайн-оголошення про роботу, соціальні мережі, сайти знайомств або навіть прямі електронні листи, які обіцяють легкі гроші за мінімальні зусилля.

Ų Зрештою, робота особи полягає в отриманні та передачі незаконно отриманих коштів за вказівками своїх «менеджерів».

Ų Багато грошових мулів часто не підозрюють, що вчиняють злочин. Вони можуть вважати, що беруть участь у законних фінансових операціях або допомагають нужденним.

У минулому багато грошових мулів були засуджені за допомогу у відмиванні грошей, що є кримінальною відповідно до більшості законів про ПВК.

Незнання закону не є захистом.

Наслідки?

- ❌ Заморожені банківські рахунки
- ❌ Судимість
- ❌ Втрата власних коштів
- ❌ Чорний список від банківської системи
- ❌ Труднощі з працевлаштуванням
- ❌ Позбавлення волі

Злочинці, наймаючи грошових мулів, часто націлюються на:

Ų Студентів: вони часто шукають легких способів заробити гроші та можуть бути менш обізнаними про ризики через свій молодий вік.

Ų Шукачів роботи: особливо ті, хто шукає швидких грошей або не мають досвіду.

Ų Людей з фінансовими труднощами: особи, які відчувають фінансові труднощі та можуть сприймати це як швидкий спосіб заробити гроші.

Червоні прапорці в облікових записах клієнтів:

- 🚩 Раптові зміни в моделях транзакцій.
- 🚩 Часті транзакції за участю іноземних держав.
- 🚩 Кошти часто переказуються третім особам або від них.
- 🚩 Клієнт ділиться адресою з іншими людьми.
- 🚩 Професія клієнта не збігається з його фінансовою діяльністю.
- 🚩 Схоже, що клієнт не є кінцевим власником коштів.

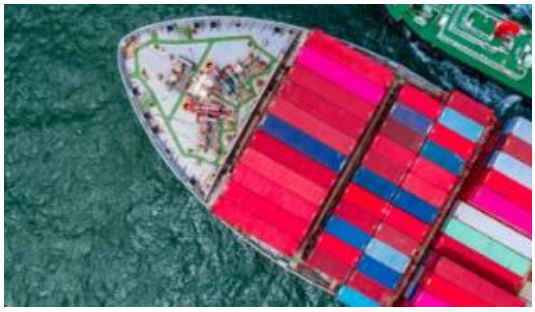
Black Market Peso Exchange

Обмін песо на чорному ринку (BMPE) виник завдяки колумбійським підприємствам, які прагнули уникнути податків. У 1970-х роках обмежувальна політика обміну валюти та високі тарифи змусили ці підприємства обійти офіційні канали, співпрацюючи з брокерами песо на чорному ринку. Пізніше ця система була використана наркоторговцями для відмивання американських наркодоларів у песо.

Для наркокартелів традиційні банківські системи були надто ризикованими через регулятивний і правоохоронний контроль. Тож зловмисники звернулися до BMPE як до альтернативи.

Ця схема передбачає продаж доларів США від продажу наркотиків брокерам, які потім використовують ці кошти для купівлі товарів у США. Ці товари експортуються до Латинської Америки, де продаються за місцеву валюту, фактично відмиваючи гроші.

З часом BMPE еволюціонував, щоб включити більш складні методи. І транснаціональні злочинні організації пристосувалися до збільшених зусиль правоохоронних органів, що стало постійним викликом у боротьбі з відмиванням грошей.



Обмін песо на чорному ринку (BMPE) включає кілька ключових гравців і етапів. Його основою є злочинні організації, які отримують незаконні доходи. Зазвичай у доларах США. Але ця схема також може використовувати валюти з усього світу, які отримані, в першу чергу, від незаконної діяльності, як-от торгівля наркотиками.

У США долари від наркотиків продаються брокерам за зниженою ціною. Потім брокери розміщують кошти на банківських рахунках і використовують долари для купівлі законних товарів від імені бізнесу, наприклад: одяг, автозапчастини, побутова техніка, комп'ютери, продукти харчування, мобільні телефони. Потім ці товари відправляються до країни чи регіону походження злочинної організації.

Ця схема часто залучає посередників, таких як місцеві підприємства, постачальники та транспортні компанії, які часто не знають про свою роль у схемі відмивання грошей. Однак підприємства, які закривають очі на BMPE, можуть потрапити до тривалого та дорогого кримінального розслідування, яке може призвести до арешту банківських рахунків та майна.

Потенційні операції з обміну песо на чорному ринку (BMPE) мають вирішальне значення для фахівців у сфері фінансів, торгівлі та правоохоронних органів, а тому важливо розуміти, які червоні прапорці можуть бути у BMPE:

- Розбіжності між торговими документами та фінансовими потоками
- Декілька внесень готівки, структурованими трохи нижче порогів звітності сумами
- Платежі третіх сторін, не пов’язані з фактичною торгівлею
- Використання компаній-оболонок або кількох посередників
- Незвичайні маршрути доставки або точки перевалки
- Транзакції з високоризиковими юрисдикціями
- Значна занижена або завищена вартість товару
- Товари не відповідають профілю ділової діяльності
- Часті зміни торгових документів
- Незвичайні або складні способи оплати

Працівники з ПВК та слідчі з фінансових злочинів також повинні стежити за швидким оборотом коштів, небажанням надавати повну інформацію та транзакціями, позбавленими економічного сенсу. Ці індикатори не обов'язково підтверджують діяльність ВМРЕ, але вони вимагають подальшого розслідування.

ВМРЕ суттєво спотворює ринки та впливає на законний бізнес різними способами. Штучно занижуючи ціни на товари, діяльність з ВМРЕ створює недобросовісну конкуренцію для законослухняного бізнесу. Така маніпуляція цінами можлива через те, що злочинні організації готові продавати долари зі знижкою, дозволяючи імпортерам знижувати ринкові ціни. Як наслідок, законним торговцям важко конкурувати, що потенційно може призвести до закриття бізнесу та втрати робочих місць.

Крім того, операції ВМРЕ можуть маніпулювати курсами валют, дестабілізуючи місцеву економіку. Вони також підривають податкові надходження, оскільки транзакції часто не реєструються або їх вартість занижується. Це ухилення від сплати податків зменшує державні ресурси на державні послуги та інфраструктуру.

Наявність ВМРЕ може стримувати іноземні інвестиції та міжнародне торгове партнерство через підвищений ризик. Законні підприємства можуть зіткнутися з посиленою перевіркою та витратами на комплаєнс, навіть якщо вони не залучені до незаконної діяльності. Тож, співробітники з ПВК та розслідувачі фінансових злочинів знаходяться на передовій захисту ширших економічних наслідків ВМРЕ, окрім виявленої злочинної діяльності.

Під час розслідувань діяльності з ВМРЕ спеціальні агенти, детективи, офіцери оперативної групи та аналітики витрачають незліченні години на:

- Діяльність під прикриттям
- Перегляд фінансової документації
- Проведення спостережень
- Опитування свідків
- Прослуховування записів розмов
- Написання звітів

І застосовують майже всі методи розслідування, включаючи перегляд сміття підозрюваного.

На завершення цих розслідувань правоохоронні органи регулярно:

- Накладають арешт на значні активи та фінансові інструменти.
- Арештовують ряд осіб у США та за кордоном.
- Знищують транснаціональні злочинні організації та організації з торгівлі наркотиками.

Наступні розслідування демонструють глобальне охоплення ВМРЕ та те, як щорічно відмиваються мільярди доларів.

Operation White Dollar

Дворічне багатонаціональне розслідування проти ВМРЕ, яке призвело до висунення звинувачень 34 особам і конфіскації 20 мільйонів доларів.

U.S. v. HSBC Bank

HSBC заплатив 1,9 мільярда доларів за збої в боротьбі з відмиванням коштів, включаючи транзакції, пов’язані з ВМРЕ.

Ismel “El Mayo” Zambada and Joaqin “Chapo” Guzman Organization

Спільною операцією ліквідовано мережу, яка відмивала мільйони через ВМРЕ.

Lebanese Canadian Bank Case

Було конфісковано 102 мільйони доларів за участь банку у схемах ВМРЕ, пов’язаних з Хезболлою.

Розуміння оцінки ризику ПВК

💡Навігація щодо ризиків в контексті ПВК вимагає комплексного підходу та розбиває процес оцінки на основі ризиків на шість основних етапів:

👉Ідентифікація ризиків🔍: розпізнавайте продукти, послуги, географічні розташування та ділові відносини, які можуть становити ризик. Примітно, що компанії в зонах високого ризику або ті, що пропонують складні фінансові продукти, часто перевіряються ретельніше.

👉Прийняття ризиків📈: оцінюйте ризики з нормативної, репутаційної, юридичної та фінансової точок зору. Визначте, які ризики можна прийняти, керувати або уникнути. Чи знаєте ви, що прийняття невизначених ризиків може призвести до серйозних штрафів і втрати довіри клієнтів?

👉Контроль ризиків🔒: запровадьте внутрішній контроль і постійний моніторинг, особливо для клієнтів із високим ризиком. Наприклад, посилена належна перевірка (EDD) має вирішальне значення для політично значущих осіб (PEPs) і клієнтів із країн зі слабким законодавством у сфері боротьби з відмиванням коштів.

👉Оцінка ризику🎯: Переконайтеся, що ризики відповідають толерантності до ризику організації та застосовуйте процеси пом'якшення для сценаріїв високого ризику. Цей крок є життєво важливим для виявлення прогалин у контролі, які можуть наражати організацію на фінансові злочини.

👉Впровадження оцінки ризиків🔗: послідовно документуйте та контролюйте процедури, приділяючи особливу увагу клієнтам із високим ризиком. Регулярне оновлення профілів ризиків є важливим для адаптації до мінливих правил і нових загроз.

👉Перевірка процесу🔬: регулярно переглядайте та тестуйте програми відповідності, особливо після значних змін у бізнесі. Постійне вдосконалення є ключовим, оскільки огляди часто виявляють ідеї, які призводять до більш надійних стратегій ПВК.

Дотримуючись цих кроків, організації можуть краще захистити себе від фінансових злочинів і підтримувати відповідність нормативним вимогам. 🛡️🔒

10 поширених методів відмивання коштів через нерухомість

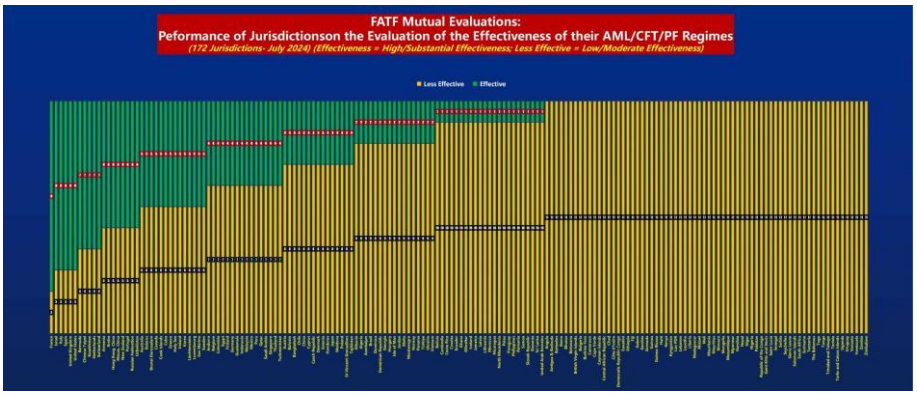
Відмивання коштів через нерухомість є поширеним методом, який використовують злочинці для приховування незаконних коштів. Ця техніка привабливa через її відносну простоту, можливість використовувати готівку, здатність приховати справжніх власників і потенціал підвищення вартості майна. Нижче наведено поширені методи відмивання коштів через нерухомість.

1. Використання третіх сторін: злочинці можуть придбати нерухомість, використовуючи як законного власника третю особу або члена сім'ї без кримінального минулого. Цей метод тримає злочинця на відстані від процесу відмивання.

2. Використання позик та іпотечних кредитів: незаконні кошти можна відмивати за допомогою позик та іпотечних кредитів, де в процесі погашення змішуються незаконні кошти з законними.
3. Маніпулювання вартістю власності:
   - Занижена оцінка: передбачає запис вартості майна нижчої за фактичну ціну придбання, а різницю сплачують незаконними коштами.
   - Завищена оцінка: включає завищення вартості майна для забезпечення більших позик, таким чином відмиваючи більше незаконних коштів.
   - Послідовні продажі: продаж майна за все більш високою ціною для створення сліду, здавалося б, законного прибутку.
4. Структурування готівкових депозитів: розміщення готівкових сум, нижчих від порогу звітності, у різних банках, щоб уникнути виявлення, а потім використання цих коштів для придбання нерухомості.
5. Орендний дохід для легалізації незаконних коштів: здача в оренду майна та використання незаконних коштів для сплати орендної плати, безпосередньо або через третю сторону, щоб приховати походження грошей.
6. Купівля нерухомості для злочинної діяльності: купівля майна для здійснення злочинної діяльності, наприклад виробництва наркотиків, і використання доходів для придбання додаткової власності.
7. Ремонт та покращення: використання незаконних коштів для реконструкції майна з метою підвищення його вартості та подальшого продажу за вищою ціною.
8. Використання підставних компаній і трастів: використання підставних компаній, компаній-оболонок, трастів і складних корпоративних структур для приховування справжньої власності та відмивання коштів через операції з нерухомістю.
9. Використання професійних фасилітаторів: залучення фахівців, таких як юристи, бухгалтери та агенти з нерухомості, для надання допомоги у процесі відмивання шляхом створення організацій та проведення транзакцій.
10. Закордонні злочинці, які інвестують у нерухомість: Злочинці з-за кордону можуть інвестувати в нерухомість, щоб приховати активи та уникнути конфіскації у своїх країнах. Ці інвестиції можуть бути здійснені через закордонні рахунки або треті сторони.

Відмивання коштів через нерухомість залишається серйозною проблемою через її потенціал для приховування незаконних коштів. Регульований сектор забезпечує певну видимість цієї діяльності, допомагаючи органам влади виявляти та боротися з такими методами.

Взаємні оцінки ризиків FATF



Зі 172 юрисдикцій, чиї взаємні оцінки були опубліковані на даний момент, лише 11% (19 юрисдикцій) мали до 50% ефективності щодо 11 безпосередніх результатів, тоді як 89% (163 юрисдикції) були визнані менш ефективними. Близько 40% (68 юрисдикцій) були визнані менш ефективними за всіма 11 безпосередніми результатами. Юрисдикції повинні працювати над належною підготовкою до наступного раунду оцінювання, усунувши недоліки, виявлені в їхніх режимах ПВК/ФТ/ФР. Злочинці працюють наполегливо та розумно, світ має працювати розумніше та наполегливіше, щоб протистояти їм.

Типи належної перевірки в AML/KYC

1. Належна перевірка клієнта (CDD)

✓ CDD є фундаментальним компонентом заходів AML/KYC. Вона передбачає ідентифікацію та перевірку особистості клієнтів, оцінку ризиків, які вони становлять, і постійний моніторинг їх діяльності.

2. Посилена належна перевірка (EDD)

✓ EDD застосовується до клієнтів із високим ризиком або транзакцій, які становлять більший потенціал для відмивання грошей або фінансування тероризму.

3. Спрощена належна перевірка (SDD)

✓ SDD використовується для клієнтів або транзакцій, які становлять менший ризик відмивання грошей або фінансування тероризму. Цей підхід передбачає менший рівень розслідування порівняно з CDD та EDD.

4. Належна перевірка транзакцій (TDD)

✓ TDD зосереджується на аналізі конкретних транзакцій для виявлення та запобігання підозрілим діям. Це передбачає:

- Моніторинг транзакцій: використовуйте автоматизовані системи для моніторингу транзакцій у режимі реального часу або періодично. Шукайте паттерни, які відрізняються від типової поведінки клієнтів.
- Повідомлення про підозрілу діяльність (SAR): розслідуйте транзакції, які викликають попередження, і надсилайте SAR у відповідні органи, якщо підозріла діяльність буде підтверджена.

5. Належна перевірка третіх сторін (TPDD)

TPDD передбачає оцінку ризику, пов’язаного зі сторонніми організаціями, такими як партнери, постачальники або посередники, щоб переконатися, що вони не становлять загрози для дотримання AML/KYC.

✓ Перевірка постачальників: оцініть історію, репутацію та відповідність AML/KYC сторонніх постачальників і партнерів.

6. Належна перевірка PEP.

Належна перевірка PEP застосовується до осіб, які обіймають або обіймали видатні державні посади, оскільки вони вважаються більш ризикованими через потенціал корупції.

7. Санкції та перевірка санкційних списків

Перевірка на санкції передбачає перевірку клієнтів і транзакцій на відповідність до різних списків санкцій і списків спостереження, щоб забезпечити дотримання міжнародних норм.

✓ Списки санкцій: порівняйте імена клієнтів зі списками, опублікованими урядами та міжнародними організаціями, які вказують на осіб або організації, що підпадають під санкції.

✓ Списки спостереження: перевіряйте списки спостереження, які відстежують осіб і організації, які причетні до злочинної діяльності, шахрайства або іншої високоризикованої поведінки.

8. Належна обачність на основі географічного ризику

Geographic Risk-Based Due Diligence оцінює ризики, пов’язані з клієнтами та транзакціями на основі їхнього географічного розташування.

✓ Оцінка ризику країни: оцінка рівня ризику, пов’язаного з країнами, де знаходяться клієнти або проводяться операції. Країни з високим ризиком можуть вимагати додаткової належної перевірки.

http://surl.li/qnddqz