Серійний номер: ДСФМУ-ДК-2024-019
Серпень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

34 звіт Групи аналітичної підтримки та моніторингу санкцій, поданий відповідно до резолюції 2734 (2024) щодо ІДІЛ (ДАІШ), Аль-Каїди та пов'язаних з ними осіб і організацій

Документ є тридцять четвертим звітом Аналітичної групи з підтримки та моніторингу санкцій, представленим відповідно до резолюції 2734 (2024) Ради Безпеки ООН щодо "Ісламської держави Іраку та Леванту" (ІДІЛ, Да'еш), "Аль-Каїди" та пов'язаних з ними осіб, груп, підприємств та організацій. **Звіт** охоплює період до 21 червня 2024 року і **надає аналіз загроз, пов'язаних з терористичною діяльністю, а також оцінку впливу санкцій, накладених на ці групи**. Документ також містить огляд регіональних подій, розвиток терористичної активності в Африці, Іраку та Леванті, на Аравійському півострові, в Європі та Азії. Крім того, **розглядається використання терористами сучасних технологій та криптовалют для фінансування своєї діяльності**.

Ключові висновки:

1. **Зростання загроз:** Загроза від ІДІЛ-К (Ісламська держава Іраку та Леванту – Хорасан) значно зросла, зокрема через масштабні терористичні атаки за межами Афганістану, що спричинило підвищення рівнів загрози в Європі та інших регіонах.
2. **Розширення діяльності в Африці:** ІДІЛ (Да'еш) зосереджує свої зусилля в Африці, зокрема у Західній Африці та Сомалі. Організація посилює координацію між групами та розширює свої фінансові можливості.
3. **Регіональні конфлікти та безпека:** В Сагелі ІДІЛ (Да'еш) та пов'язані з нею групи продовжують здобувати території, що призводить до значних людських втрат і впливає на регіональну стабільність.
4. **Використання технологій:** Терористичні групи активно використовують анонімні криптовалюти, 3D друк та безпілотні технології для здійснення атак та ухилення від санкцій.
5. **Стійкість та адаптивність:** Попри контртерористичний тиск, терористичні групи демонструють високу стійкість та здатність адаптуватися до нових умов.

6. **Фінансування:** Доходи від афілійованих з ІДІЛ груп у Сомалі є важливим джерелом фінансування для організації. Використання анонімних криптовалют стає все більш поширеним, зокрема Monero.
7. **Реорганізація та навчання:** У Афганістані спостерігається активізація діяльності ІДІЛ-К та навчання нових бойовиків, що викликає занепокоєння серед держав-членів ООН.

Ці висновки підкреслюють поточні виклики у сфері міжнародної безпеки та необхідність подальших заходів для боротьби з тероризмом і фінансуванням терористичної діяльності.

http://surl.li/zbihjv

Звіт про шахрайство з платежами 2024

Документ «Звіт про шахрайство з платежами 2024» підготовлений Європейським банківським управлінням (EBA) спільно з Європейським центральним банком (ECB) і оцінює останні дані про платіжні шахрайства, зібрані згідно з Директивою ЄС 2015/2366 (PSD2). Він охоплює дані за три референтні періоди: перша половина 2022 року, друга половина 2022 року і перша половина 2023 року, та фокусується на платіжних інструментах, таких як кредитні перекази, прямі дебети, карткові платежі, зняття готівки та транзакції з електронними грошима. У звіті аналізуються як загальні платіжні транзакції, так і шахрайські, в термінах обсягів і вартості. Звіт також надає детальний аналіз основних типів шахрайства, застосування надійної аутентифікації клієнтів (SCA), а також географічні та країнові аспекти шахрайства. Основними висновками є те, що найвищі рівні шахрайства стосуються кредитних переказів та карткових платежів, а також те, що застосування SCA значно знижує рівень шахрайства. Загалом, звіт надає всебічний огляд шахрайства у платіжних системах європейської економічної зони (ЄЕЗ) та підкреслює важливість подальшого моніторингу та вдосконалення заходів безпеки.

Ключові висновки

1. **Загальні рівні шахрайства:** Загальна вартість шахрайських транзакцій в ЄЕЗ склала 4,3 мільярда євро у 2022 році та 2,0 мільярда євро у першій половині 2023 року. Найвищі рівні шахрайства були зафіксовані для кредитних переказів та карткових платежів.
2. **Типи шахрайства:** Основні типи шахрайства включають маніпуляцію платника для ініціювання транзакцій, а також крадіжку даних карток. Більшість шахрайських кредитних переказів були ініційовані дистанційно.
3. **Сильна аутентифікація клієнтів (SCA):** Застосування SCA знижує рівень шахрайства. У 2022 та першій половині 2023 року близько 77% електронних кредитних переказів були автентифіковані за допомогою SCA.
4. **Географічні аспекти:** Шахрайські транзакції найчастіше були пов'язані з міжнародними переказами. Більшість шахрайства з картками відбувалась за межами ЄЕЗ, де вимоги SCA можуть не застосовуватися.
5. **Збитки від шахрайства:** Найбільші збитки через шахрайство зафіксовані для кредитних переказів та карткових платежів. Користувачі платіжних послуг (PSU) несли основну частину збитків від шахрайства у випадку кредитних переказів (86% у першій половині 2023 року).
6. **Проблеми якості даних:** Деякі дані можуть бути неповними або неправильно класифікованими, що ускладнює точні порівняння між країнами.
7. **Майбутні перспективи:** Загальна перспектива щодо платіжного шахрайства виглядає стабільною, але необхідно продовжувати моніторинг та вдосконалювати заходи безпеки.

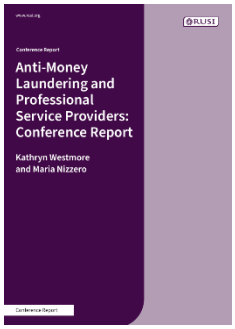
http://surl.li/pjuizg

Боротьба з відмиванням коштів та професійні постачальники послуг: звіт конференції RUSI

Звіт конференції "Anti-Money Laundering and Professional Service Providers", організованої RUSI з квітня по червень 2024 року, розглядає роль юристів і бухгалтерів у протидії відмиванню грошей.

Учасники трьох воркшопів досліджували ефективність, нагляд та заходи примусу, що необхідні для попередження, виявлення і покарання фінансових злочинів. Основна увага приділялась викликам та можливостям вдосконалення співпраці між професіоналами фінансового сектору та регуляторами в ЄС та Великобританії. Конференція також підкреслила важливість стимулювання належної практики для ефективної боротьби з відмиванням грошей.

Звіт акцентує увагу на наступних ключових аспектах:

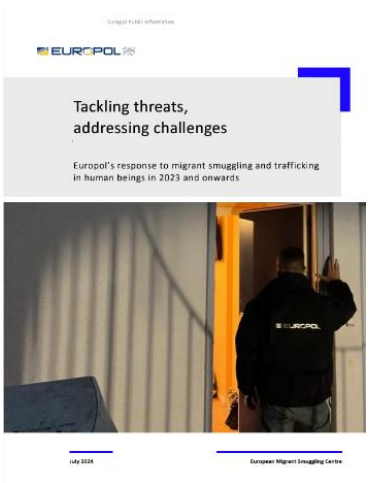


- **Ефективність:** Основні виклики у нагляді юристами і бухгалтерами включають: недостатнє розуміння звітності про підозрілу діяльність та обмежений обмін інформацією. Партнерства між зацікавленими сторонами, такі як Спільна робоча група з боротьби з відмиванням грошей у Великобританії, можуть сприяти зниженню цих викликів.
- **Застосування заходів примусу:** Різні підходи до правозастосування, від неформальної взаємодії до формальних санкцій, включаючи штрафи та публічне осудження. Обговорювались ефективність різних заходів та необхідність їх комбінації для забезпечення довгострокової відповідності.
- **Створення стимулів:** Учасники розглянули можливості стимулювання професіоналів до дотримання правил, включаючи надання зворотного зв'язку від підрозділів фінансової розвідки (ПФР), зміну наративу щодо дотримання вимог та винагороду за добре виконану роботу.

Конференція підкреслила важливість професійної обізнаності та відповідальності юристів і бухгалтерів у запобіганні фінансовим злочинам. Виявлені виклики включають нестачу узгоджених наглядових структур, необхідність покращення обміну інформацією та доступу до широкого спектру регуляторних інструментів. Очікується, що впровадження нових регуляторних структур у ЄС та Великобританії допоможе вирішити ці виклики, але важливо, щоб ці структури не створювали додаткової складності в системі.

http://surl.li/ylzuej

Протидія загрозам: відповідь Європолу на контрабанду мігрантів та торгівлю людьми у 2023 році і надалі



У звіті "Tackling Threats, Addressing Challenges - Europol's Response to Migrant Smuggling and Trafficking in Human Beings in 2023 and Onwards" розглядаються заходи, прийняті Europol для боротьби з контрабандою мігрантів і торгівлею людьми в 2023 році. Звіт підкреслює, що обидва види злочинів є серйозною загрозою для безпеки ЄС і впливають на життя нелегальних мігрантів і жертв торгівлі людьми.

У звіті зазначається, що злочинні мережі постійно адаптують свої методи для максимізації прибутків та уникнення правосуддя, використовуючи геополітичні події, економічні та соціальні кризи, а також цифрові технології для своїх операцій.

Europol's European Migrant Smuggling Centre (EMSC) грає провідну роль у боротьбі з контрабандою мігрантів, підтримуючи країни-члени ЄС у розслідуваннях та руйнуванні злочинних мереж, які займаються контрабандою та торгівлею людьми. EMSC надає оперативну підтримку

транскордонним розслідуванням, експертизу та ресурси, а також платформу для швидкого та безпечного обміну інформацією.

Важливі аспекти звіту включають аналіз взаємозв'язку між контрабандою мігрантів і торгівлею людьми з іншими видами злочинів, такими як торгівля наркотиками та зброєю. Звіт також підкреслює гнучкість і адаптивність злочинних мереж, які швидко змінюють маршрути та методи роботи у відповідь на зовнішні зміни. Особлива увага приділяється впливу геополітичних подій, таких як війна Росії проти України, яка створила нові можливості для злочинців використовувати вразливі групи людей. Крім того, звіт розглядає зростання рівня насильства з боку контрабандистів і торгівців людьми, а також використання цифрових технологій і криптовалют для полегшення їхньої діяльності.

Ключові висновки:

- **Серйозна загроза для безпеки ЄС:** Контрабанда мігрантів і торгівля людьми (THB) залишаються значними загрозами для безпеки ЄС. Ці види злочинів викликають соціальні та економічні проблеми, а також негативно впливають на права людини та безпеку постраждалих осіб.
- **Адаптивність злочинних мереж:** Злочинні мережі швидко адаптують свої методи для максимізації прибутків і уникнення правосуддя. Вони використовують сучасні технології, змінюють маршрути та способи діяльності, щоб залишатися невловимими для правоохоронних органів.
- **Вплив геополітичних подій:** Геополітичні події, такі як війна Росії проти України, створюють нові можливості для злочинців використовувати вразливі групи населення. Ці події підвищують попит на послуги контрабандистів і надають нові можливості для торгівлі людьми.
- **Використання цифрових технологій і криптовалют:** Злочинні мережі активно використовують цифрові технології та криптовалюти для полегшення своєї діяльності. Вони використовують соціальні мережі для реклами своїх послуг та залучення клієнтів, а також криптовалюти для оплати та відмивання коштів. Це ускладнює відстеження їхніх операцій правоохоронними органами.

http://surl.li/helahe

Думка на підтримку конвергентного застосування MiCA

Європейське управління з цінних паперів і ринків (ESMA) опублікувало думку щодо вирішення ризиків, пов’язаних із глобальними криптокомпаніями, які прагнуть отримати ліцензію MiCA на свої крипто-брокерські послуги, зберігаючи значну частину діяльності своєї групи поза межами регуляторної сфери ЄС. Ключові моменти думки, де ESMA:

▶ Визнає ризики, пов’язані зі складними структурами глобальних криптокомпаній, де місця виконання не входять до сфери дії MiCA.

▶ Попереджає, що такі структури можуть залучати авторизованого брокера в ЄС, який направляє ордери за межі ЄС, що може зменшити захист споживачів і створити недобросовісну конкуренцію.

▶ Закликає некомерційні організації забезпечити, щоб глобальні фірми дотримувалися MiCA під час авторизації, захищаючи споживачів і ринки.

▶ Рекомендує застосування оцінки кожного конкретного випадку, деталізуючи вимоги для найкращого виконання, конфліктів інтересів і управління криптоактивами орієнтоване на клієнта.

▶ Наголошує на тому, що місця виконання операцій з криптоактивами та комплексні правила MiCA для торгових платформ є важливими.

Глобальні криптокомпанії, які бажають отримати дозвіл MiCA на свої послуги крипто-брокера в ЄС, повинні звернути особливу увагу на наступне у своїй заявці на ліцензію MiCA:

✅ Програма операцій.

✅ Встановлення та опис засобів контролю, які демонструють захист клієнтів.

✅ Контроль управління конфліктом інтересів.

http://surl.li/gmrmpb

Децентралізовані фінанси: класифікація смарт-контрактів

Документ під назвою "Decentralised Finance: A categorisation of smart contracts" є робочою доповіддю Європейського управління з цінних паперів та ринків (ESMA), яка досліджує роль смарт-контрактів у децентралізованих фінансах (DeFi). **Документ пропонує методологію для класифікації смарт-контрактів на блокчейні Ethereum, щоб краще зрозуміти їх функціональність та особливості**. Аналіз показує, що **смарт-контракти можуть бути розділені на п'ять основних категорій: фінансові, операційні, токенізаційні, гаманцеві та інфраструктурні**. Кожна з цих категорій відображає різні аспекти DeFi, від управління фондами до підтримки інфраструктури блокчейну.

Ключові висновки:

1. **Смарт-контракти є основою DeFi:** Вони замінюють традиційних фінансових посередників, забезпечуючи автоматизоване виконання фінансових операцій на блокчейні без необхідності довіри до центральних органів.
2. **П'ять категорій смарт-контрактів:** Фінансові контракти стосуються збору і розподілу коштів; операційні контракти підтримують функціонування інших смарт-контрактів; токенізаційні контракти забезпечують створення і управління токенами; гаманцеві контракти відповідають за управління криптовалютними активами; інфраструктурні контракти підтримують основну архітектуру децентралізованих додатків (dApps).
3. **Зростаюча складність DeFi:** Складність смарт-контрактів і їх взаємозв'язок з іншими контрактами на блокчейні зростають, що призводить до нових ризиків, таких як загроза системній стабільності через взаємозалежності між протоколами.
4. **Необхідність моніторингу та регулювання:** Відсутність чітких регуляторних механізмів для смарт-контрактів створює виклики для нагляду та управління ризиками в DeFi, що вимагає від регуляторів розробки нових підходів до контролю і моніторингу цієї галузі.

http://surl.li/aeqftj

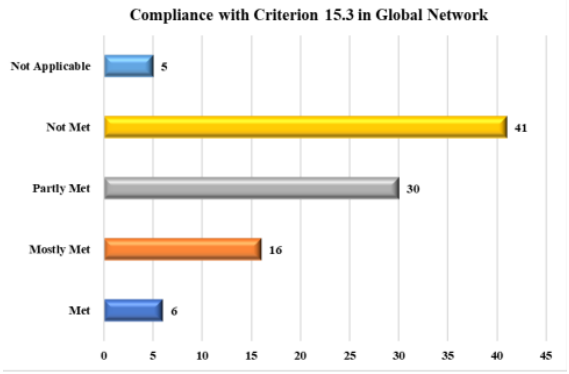
Ризик-орієнтований підхід до ВА та VASP: розуміння та пом'якшення ризиків

Документ присвячений ризик-орієнтованому підходу до віртуальних активів (ВА) і постачальників послуг, пов'язаних з віртуальними активами (VASP), **з акцентом на розуміння та пом'якшення ризиків ВК/ФТ.** У документі **визначаються поняття ВА та VASP**, підкреслюючи важливість рекомендацій FATF щодо оцінки ризиків, пов'язаних з новими технологіями, такими як віртуальні активи, та діяльність VASP. Документ **описує процес**

оцінки ризиків і необхідні заходи для їхнього пом'якшення, включаючи можливість заборони або обмеження ВА і VASP на підставі національних ризиків і нормативних вимог. Також **розглядаються глобальні виклики і недоліки в здійсненні оцінок ризиків і надаються рекомендації як для державного, так і для приватного секторів** щодо подальших дій.

Ключові висновки:

1. **Необхідність глибокого розуміння ризиків, пов'язаних із ВА та VASP:** Віртуальні активи представляють значні виклики для фінансової безпеки, оскільки вони дозволяють проводити транзакції без участі фінансових установ, зберігаючи високий рівень анонімності. Це створює сприятливі умови для відмивання коштів та фінансування тероризму. Відсутність фізичних кордонів у віртуальних активів означає, що транзакції можуть бути здійснені миттєво і практично необоротно, що ускладнює контроль та регулювання.



2. **Недостатність глобальної відповідності стандартам FATF:** Оцінка FATF показала, що 72% юрисдикцій не забезпечують належної імплементації критеріїв, що стосуються оцінки ризиків віртуальних активів та VASP. Це вказує на загальний недолік у глобальному дотриманні рекомендацій FATF, що призводить до підвищеного ризику використання ВА і VASP для незаконної діяльності. Таке широке недотримання стандартів вказує на необхідність посилення міжнародного співробітництва та підвищення обізнаності про загрози.
3. **Важливість впровадження ризик-орієнтованого підходу в національному контексті:** Країнам рекомендується проводити оцінку ризиків, пов'язаних з ВА та VASP, з урахуванням особливостей їхнього національного регуляторного середовища та існуючих загроз. Це включає оцінку таких факторів, як типи послуг, що надаються VASP, географічні ризики, а також ризики, пов'язані з клієнтами. Держави повинні вживати заходів щодо пом'якшення ризиків до запуску нових продуктів або послуг, оскільки після їх впровадження це може стати значно складніше.
4. **Ризики, пов'язані з анонімними транзакціями та P2P операціями:** Віртуальні активи, що підтримують анонімність та можливість P2P транзакцій без залучення VASP або інших підзвітних суб'єктів, становлять значний ризик з точки зору відмивання коштів і фінансування тероризму. Відсутність належного контролю та можливість обходу традиційних механізмів ПВК/ФТ вимагають додаткових зусиль з боку регуляторів для забезпечення належного нагляду та впровадження санкцій проти незаконних операцій.
5. **Роль приватного сектора у пом'якшенні ризиків:** VASP та інші учасники ринку повинні активно впроваджувати заходи з ідентифікації та пом'якшення ризиків у відповідності до Рекомендації 15 FATF. Це включає розробку та впровадження заходів з кібербезпеки, а також постійний моніторинг ризиків у контексті зростаючих загроз фінансування тероризму і розповсюдження зброї масового знищення через віртуальні активи. Приватний сектор повинен активно взаємодіяти з регуляторами для забезпечення спільного розуміння ризиків і належного реагування на них.
6. **Важливість регулярного перегляду ризиків:** Враховуючи швидку еволюцію технологій та появу нових загроз, країни повинні періодично переглядати свої оцінки ризиків, пов'язаних з VA і VASP. Це необхідно для забезпечення актуальності застосовуваних заходів та своєчасного реагування на нові виклики. Також важливо, щоб країни обмінювалися досвідом та найкращими практиками щодо збору даних, методологій оцінки ризиків та впровадження ефективних заходів з пом'якшення ризиків.

Ці висновки підкреслюють важливість гнучкого та адаптивного підходу до регулювання ринку віртуальних активів і нагляду за його учасниками для ефективного протидії відмиванню коштів, фінансуванню тероризму та розповсюдженню зброї масового знищення.

http://surl.li/noppad

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Нова система ПВК/ФТ в ЄС: повний посібник

Документ від ComplyAdvantage представляє оновлення нової системи протидії відмиванню коштів та фінансуванню тероризму Європейського Союзу. Він охоплює впровадження шостої директиви з протидії відмиванню коштів (6AMLD), створення нового наднаціонального органу по боротьбі з відмиванням коштів (AMLA), а також встановлення єдиного набору правил для приватного сектору, включаючи регулювання криптовалютних транзакцій. **Звіт надає деталі про нові законодавчі ініціативи, їх мету та вплив, а також пропонує рекомендації для компаній щодо підготовки до цих змін.**

Ключові висновки:

1. **Створення AMLA**: Новий наднаціональний орган по боротьбі з відмиванням коштів буде наділений повноваженнями наглядати за найбільш ризикованими суб'єктами у ЄС, що здійснюють транскордонну діяльність. Це включає прямий нагляд за 40 фінансовими установами, які будуть обиратися на основі ризиків.
2. **6AMLD:** Шоста директива з протидії відмиванню грошей (6AMLD) вводить нові вимоги для державних установ та покращує координацію між національними органами, включаючи обов'язкові національні та європейські оцінки ризиків.
3. **Єдиний набір правил:** Новий регламент встановлює єдині правила для суб'єктів приватного сектору, включаючи обов'язкову ідентифікацію клієнтів, ведення реєстрів власників активів та суворі вимоги до належної перевірки клієнтів.
4. **Регулювання криптовалют:** Криптовалютні провайдери тепер підлягають тим же AML/CFT правилам, що і традиційні фінансові установи, з обов'язковим наданням інформації про відправника та отримувача коштів для всіх транзакцій.
5. **Санкції та покарання:** AMLA матиме право накладати суворіші штрафи на суб'єктів, які порушують правила, зокрема штрафи до 2 мільйонів євро або 10% від річного обороту компанії.
6. **Нові вимоги до бенефіціарної власності:** Всі дані про бенефіціарів повинні бути перевірені і зберігатися в актуальному стані. Це включає інформацію про ті компанії, що підпадають під санкції ЄС.
7. **Захист викривачів:** Нові детальні вимоги щодо захисту особистих даних та судовий захист для викривачів корупції та фінансових злочинів.
8. **Підвищення прозорості:** Обов'язкове створення центральних реєстрів банківських рахунків та нерухомості для полегшення виявлення злочинних мереж та незаконних фінансових потоків.

Ці зміни спрямовані на підвищення ефективності боротьби з відмиванням грошей та фінансуванням тероризму в межах ЄС, забезпечення кращої координації між державами-членами та створення єдиного правового середовища для всіх суб'єктів.

https://get.complyadvantage.com/european-unions-new-aml-cft-framework-download

Звіт про тенденції Web 3.0 2024

«Звіт про тенденції Web 3.0 2024» від BlockStack пропонує всебічний аналіз 24 ключових тенденцій, які формуватимуть майбутнє Web 3.0 в 2024 році. Основними принципами Web 3.0 є децентралізація, інтероперабельність та самостійність користувачів. Документ досліджує такі аспекти, як токенізація, цифрові валюти центральних банків (CBDC), цифрова ідентичність, міжмережеві рішення та децентралізовані автономні організації (DAO). Розглядаються питання конфіденційності, безпеки та нові моделі управління, такі як Zero Trust. Звіт також акцентує увагу на технологічних досягненнях, включаючи інтеграцію штучного інтелекту з блокчейном, готовність до квантових обчислень та Blockchain-as-a-Service (BaaS). Документ підкреслює важливість глобальних правових норм та співпраці для підтримки інновацій та регуляторного комплаєнсу. Загалом, звіт надає дорожню карту для розуміння та адаптації до цих трансформаційних тенденцій.

Ключові висновки

1. **Токенізація** реальних активів стає все більш популярною, значно підвищуючи ліквідність і доступність ринків.
2. **Цифрові валюти центральних банків (CBDC)** мають потенціал змінити фінансові системи, підвищуючи фінансову включеність та ефективність транзакцій.
3. **Цифрова ідентичність** стає ключовим елементом цифрового суспільства, забезпечуючи безпечний доступ до послуг та транзакцій.
4. **Міжмережеві рішення** та протоколи інтероперабельності є критично важливими для забезпечення безперешкодного обміну даними між різними блокчейн-екосистемами.
5. **Децентралізовані автономні організації (DAO)** набирають популярності як нова модель управління, що дозволяє учасникам колективно приймати рішення.
6. **Технології, що зберігають конфіденційність**, такі як нульові докази знання та безпечні багаторазові обчислення, набирають обертів у відповідь на зростаючі побоювання щодо конфіденційності даних.
7. **Інтеграція штучного інтелекту з блокчейном** відкриває нові можливості для підвищення ефективності та автоматизації в різних секторах.
8. **Blockchain-as-a-Service (BaaS)** робить блокчейн-технології більш доступними для бізнесу, знижуючи витрати та складність впровадження.
9. **Глобальні нормативні рамки** та співпраця між країнами та організаціями є необхідними для підтримки інновацій та забезпечення комплаєнсу.
10. **Зростання консорціумів** між блокчейн-проєктами та традиційними індустріями сприяє інноваціям та новим можливостям для обох сторін.

https://blockstack.tech/web3-report/top-24-web3-0-trends-for-enterprises-in-2024/

Відмивання грошей через відеоігри: новий інструмент для злочинців

Дослідження "Money laundering through video games, a criminals' playground" у журналі Forensic Science International: Digital Investigation аналізує, як злочинці використовують відеоігри та вторинні ринки для відмивання грошей. Відеоігри з внутрішньоігровими економіками дозволяють здійснювати анонімні транзакції, що робить їх привабливими для злочинців.

Автори досліджували дані зі Steam Marketplace, зокрема гру Counter Strike: Global Offensive, щоб виявити підозрілі транзакції. Використовуючи існуючі методи виявлення відмивання грошей, було виявлено кілька підозрілих акаунтів і транзакцій, які можуть свідчити про відмивання грошей. Злочинці можуть використовувати торги, повторювані транзакції та складні мережі облікових записів для маскування своїх дій.

Основні висновки:

- **Сучасні методи відмивання грошей:** Відеоігри стали новим інструментом для відмивання грошей завдяки можливості анонімних транзакцій та відсутності суворого регулювання. Вторинні ринки, такі як Steam Marketplace, надають можливість здійснювати складні фінансові операції, які важко відстежити.
- **Виявлення підозрілих дій:** Аналіз частоти транзакцій допомагає виявляти підозрілі дії. Наприклад, деякі користувачі здійснюють непропорційно велику кількість транзакцій, що може свідчити про використання автоматизованих інструментів або інших маніпуляцій.
- **Методи дослідження:** У статті пропонується використовувати існуючі методи виявлення відмивання грошей, такі як аналіз частоти та обсягу транзакцій, для аналізу даних з відеоігор. Автори зазначають, що такі підходи можуть допомогти виявляти підозрілі мережі облікових записів, які використовуються для відмивання грошей.
- **Необхідність подальших досліджень:** Для ефективної боротьби з відмиванням грошей через відеоігри необхідні додаткові дослідження та розробка нових методів виявлення. Це включає аналіз великих масивів даних і застосування більш складних алгоритмів для виявлення аномалій.
- **Регуляторні виклики:** Оскільки відеоігри не підпадають під традиційні фінансові регуляції, необхідно розробити нові правила та стандарти для контролю за внутрішньоігровими економіками. Це може включати запровадження обов'язкової ідентифікації користувачів та зберігання даних про транзакції.

Автори зазначають, що незважаючи на те, що використання відеоігор для відмивання грошей ще не є широко дослідженим, потенційні ризики значні, і необхідно розробити ефективні стратегії для боротьби з цим явищем.

http://surl.li/tofonu

Поза межами ілюзій: викриття загрози синтетичних (фальшивих) медіа для правоохоронних органів

Звіт "Cyvers 2024 Web3 Security Report" аналізує стан безпеки в екосистемі Web3 за 2023 рік та пропонує прогнози на 2024 рік.

Звіт детально висвітлює основні події та інциденти безпеки, включаючи великі хакерські атаки на проекти, такі як Euler Finance ($200M), Mixin Network ($200M), BonqDAO ($120M) та Atomic Wallet ($100M). Загальна сума вкрадених коштів зменшилася з $3,6 мільярда у 2022 році до $2,1 мільярда у 2023 році, що свідчить про покращення захисних механізмів у галузі.

Звіт аналізує методи атак, зокрема використання Flash Loans, соціальної інженерії та витоків приватних ключів, підкреслюючи основні цілі — DeFi та атаки на контроль доступу.

Вплив групи Лазарус з Північної Кореї також був значним, оскільки вони використовували складні техніки для атак на криптовалютні платформи. У звіті зазначено, що взаємозв'язок між ринковою капіталізацією криптовалют та сумою викрадених коштів залишається важливим фактором. Прогнози на 2024 рік вказують на підвищення складності загроз через розвиток квантових обчислень та машинного навчання, що вимагає проактивних заходів захисту та інвестицій у новітні технології безпеки.

Ключові висновки звіту:

- **Зниження загальної суми викрадених коштів:** У 2023 році загальна сума викрадених коштів знизилася з $3,6 мільярда до $2,1 мільярда. Це свідчить про покращення захисних механізмів і підвищення ефективності заходів безпеки в екосистемі Web3. Основні події включають великі хакерські атаки на такі проекти, як Euler Finance, Mixin Network та Atomic Wallet.
- **Вплив групи Лазарус:** Кіберзлочинна група Лазарус з Північної Кореї продовжує здійснювати складні атаки на криптовалютні платформи. Вони використовують різні техніки, включаючи соціальну інженерію та витоки приватних ключів, що дозволяє їм ефективно викрадати значні суми коштів.
- **Методи атак:** Основними методами атак у 2023 році були Flash Loans, соціальна інженерія та витоки приватних ключів. Ці методи залишаються популярними серед кіберзлочинців через їхню ефективність та складність виявлення. Атаки спрямовані на DeFi-проекти та контроль доступу до криптовалютних гаманців.
- **Регуляторні ініціативи:** Важливість міжнародної співпраці та регуляторних ініціатив, таких як OSWAR від Cyvers, є критичною для стандартизації заходів безпеки у Web3. Активна співпраця з міжнародними організаціями, такими як IOSCO, допомагає формувати ефективні регуляторні рамки для цифрових активів. Це сприяє підвищенню довіри користувачів та захисту цифрових активів від зловживань.

Звіт підкреслює важливість постійного вдосконалення заходів безпеки для запобігання новим загрозам у Web3, а також навчання користувачів та розробників щодо питань безпеки в екосистемі Web3. У цілому, звіт надає всебічний аналіз безпеки Web3 за 2023 рік та пропонує конкретні рекомендації для покращення захисту цифрових активів та довіри користувачів у майбутньому.

https://cyvers.ai/2024-web3-security-report-pdf

Рекомендації щодо оцінки ризиків DeFi

Документ EEA DeFi Risk Assessment Guidelines містить **детальний огляд ризиків, пов'язаних з децентралізованими фінансами (DeFi), і пропонує найкращі практики для їх оцінки, управління та зниження**. Основна увага приділяється ризикам програмного забезпечення, управління, правового, ринкового та кредитного характеру. Підкреслюється важливість стандартизованих практик, надійних заходів безпеки та ефективних механізмів управління для зменшення вразливостей у DeFi системах.

Ключові висновки:

1. Ризики програмного забезпечення та смарт-контрактів потребують ретельної перевірки безпеки.
2. Ефективне управління та відповідність правовим нормам є критично важливими для стабільності DeFi.
3. Ринкові та ліквідні ризики вимагають розробки надійних стратегій управління ризиками.
4. Користувацький інтерфейс повинен бути зрозумілим і зручним, щоб уникнути помилок.

https://entethalliance.org/specs/defi-risks/

Керівництво з дотримання Travel Rule: Європейський Союз

Документ є посібником із дотримання правил "Travel Rule" у Європейському Союзі, що стосується передачі інформації про криптовалютні транзакції. Він пояснює, як європейські постачальники криптовалютних послуг (CASPs) повинні **забезпечувати відповідність вимогам до передачі інформації про відправників і отримувачів криптовалют**. Описуються зміни у фінальних інструкціях Європейського банківського органу (EBA) щодо "Travel Rule", які набрали чинності у 2024 році. Посібник охоплює вимоги до передачі інформації, обов'язки CASPs при обробці транзакцій, управління ризиками, пов'язаними з самостійними гаманцями, і моніторинг транзакцій, що не відповідають вимогам.

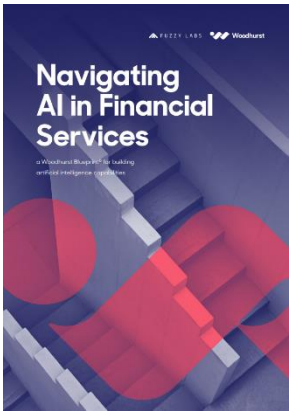
Ключові висновки:

1. **Гнучкість у виборі інформації для передачі та ідентифікації клієнтів**: Фінальні інструкції EBA 2024 року дозволяють CASPs адаптувати інформацію про відправника та одержувача для кращого забезпечення виконання санкційних перевірок та ідентифікації клієнтів. Ця гнучкість передбачає можливість використання альтернативних даних, таких як місце проживання або інший офіційний ідентифікатор, якщо це допомагає однозначно ідентифікувати клієнта та мінімізувати ризики відмивання грошей або фінансування тероризму.
2. **Спрощення процедур для транзакцій на суму до 1,000 євро:** Зміни в інструкціях дозволяють значно знизити навантаження на CASPs під час роботи з транзакціями на невеликі суми. Тепер CASPs можуть обмежитися лише збиранням інформації про клієнтів під час таких транзакцій, без необхідності верифікації їхніх даних. Це нововведення значно спрощує операційну діяльність та знижує витрати на забезпечення відповідності.
3. **Посилення управління транзакціями з неповною або відсутньою інформацією:** Відповідно до нових правил, CASPs повинні розробляти і впроваджувати чіткі процедури для виявлення та обробки транзакцій, що не відповідають вимогам Travel Rule. Якщо транзакція надходить без необхідної інформації, CASPs можуть вибирати серед декількох варіантів дій: виконання транзакції, її повернення, відхилення або тимчасове призупинення. Кінцеве рішення залежить від ступеня ризику та можливості однозначно ідентифікувати учасників транзакції.
4. **Вимоги до транзакцій із самостійними гаманцями:** Нові правила чітко окреслюють обов'язки CASPs під час роботи з самостійними гаманцями, особливо коли сума транзакції перевищує 1,000 євро. Відтепер CASPs повинні забезпечити перевірку власності або контролю над гаманцем. В інструкціях EBA передбачено використання різних технічних методів для верифікації гаманців, що забезпечує надійний контроль і мінімізацію ризиків, пов'язаних із самостійними гаманцями. Залежно від ситуації, CASPs можуть використовувати один або декілька методів для підтвердження володіння гаманцем, включаючи аналітику блокчейну та інші технічні засоби.
5. **Ризик-орієнтований підхід до транзакцій із самостійними гаманцями:** CASPs зобов'язані проводити оцінку ризиків при роботі із самостійними гаманцями, особливо якщо власник гаманця не є їхнім клієнтом. Це включає верифікацію особи одержувача або відправника та здійснення заходів, що пропорційно відповідають виявленим ризикам. Якщо виявлені ризики є високими, CASPs повинні вжити додаткових заходів для їхньої мінімізації, таких як збір додаткової інформації або посилений моніторинг транзакцій.

Ці зміни покликані підвищити ефективність контролю за криптовалютними транзакціями, забезпечити відповідність новим регуляторним вимогам та зменшити ризики, пов'язані з фінансовими злочинами.

http://surl.li/goatzh

Навігація ШІ у фінансових послугах



Документ під назвою "Navigating AI in Financial Services" є **посібником із впровадження штучного інтелекту (AI) у фінансовій галузі**. Він розглядає причини популярності AI, його потенціал для покращення клієнтського досвіду, боротьби з фінансовими злочинами, автоматизації бізнес-процесів і підвищення відповідності регуляторним вимогам. Також надається **рекомендації щодо створення умов для успішних AI-проєктів**, зокрема стосовно культури, технологій, процесів і роботи з даними. Посібник завершується описом "AI Blueprint" — рамкової методології для успішного впровадження AI в організаціях.

Ключові висновки:

1. **Штучний інтелект (AI) як стратегічний інструмент у фінансових послугах:** AI став критично важливим елементом для підвищення ефективності фінансових установ. Завдяки здатності AI аналізувати великі обсяги даних у реальному часі, він може значно покращити обслуговування клієнтів, надаючи персоналізовані поради, прискорюючи процеси обслуговування, і навіть виявляючи аномалії в фінансових транзакціях, що сприяє швидкому виявленню шахрайства. Такі функції підвищують конкурентоспроможність компаній, дозволяючи їм пропонувати кращі продукти та послуги при менших витратах.
2. **Автоматизація бізнес-процесів:** AI дозволяє автоматизувати багато рутинних завдань, що раніше вимагали значних людських ресурсів, таких як обробка паперових документів або перевірка транзакцій. Використання технологій розпізнавання тексту та аналізу даних дозволяє значно скоротити час, витрачений на виконання цих завдань, що, в свою чергу, дозволяє співробітникам зосередитися на більш стратегічних завданнях, які потребують людського інтелекту.
3. **Посилення відповідності та управління ризиками:** AI значно спрощує процес дотримання регуляторних вимог, особливо у сфері боротьби з відмиванням грошей та фінансуванням тероризму. Завдяки використанню машинного навчання та аналізу даних у реальному часі, фінансові установи можуть миттєво реагувати на підозрілі транзакції та проводити скринінг санкцій, що підвищує рівень безпеки та зменшує ризики фінансових злочинів.
4. **Необхідність підтримки культурних змін та інноваційного середовища:** Для успішної інтеграції AI організація повинна розвивати культуру, що заохочує інновації та експерименти. Це передбачає готовність до прийняття ризиків, спробу нових підходів та постійне навчання на помилках. Створення такого середовища вимагає активної участі керівництва, яке повинно надавати підтримку командам, що займаються AI-проєктами, і забезпечувати їх необхідними ресурсами.
5. **Важливість якості даних і хмарних технологій:** AI є ефективним лише настільки, наскільки якісними є дані, на яких він навчається. Створення централізованого хабу даних з чіткою архітектурою та високими стандартами якості даних є ключовим для забезпечення успішного впровадження AI. Використання хмарних технологій надає фінансовим установам можливість масштабувати AI-рішення, забезпечуючи доступ до потужних інструментів та ресурсів.
6. **Фреймворк AI Blueprint© як основа для успішної реалізації AI-проєктів:** AI Blueprint© пропонує структуру для впровадження AI-проєктів, яка включає оцінку проблем, підготовку до розробки, сам процес розробки та оперативне впровадження. Цей фреймворк

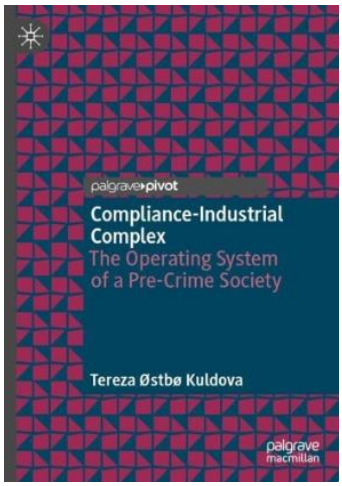
допомагає уникнути поширених помилок і забезпечує гнучкий підхід до реалізації AI-рішень, який можна адаптувати під конкретні потреби компанії.

Ці висновки підкреслюють важливість AI у сучасному фінансовому секторі та надають рекомендації щодо ефективного впровадження цієї технології для досягнення бізнес-цілей.

https://www.woodhurst.com/wp-content/uploads/2020/01/woodhurst-ai-in-financial-services-v13.pdf

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Індустріальний комплекс відповідності: Операційна система суспільства до злочину



Ця книга стверджує, що індустріальний комплекс відповідності фундаментально формує механізми управління та контролю, впливаючи на те, як люди перебувають під наглядом і як ними керують. Також стверджується, що функція відповідності відіграє важливу роль у корпоративній владі та гібридних практиках поліцейської діяльності.

Індустріальний комплекс відповідності - це сектор (так, це цілий підсектор фінансового сектору економіки!), який був створений після створення Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) та встановлення глобальних стандартів боротьби з відмиванням грошей (а пізніше - зусиль з протидії фінансуванню тероризму). Індустріальний комплекс відповідності складається з фінансових установ, їхніх офіцерів з питань відповідності (відповідальних за виявлення, запобігання та повідомлення про відмивання грошей та фінансування тероризму), компаній з регуляторних технологій, які сприяють цьому, а також політиків, консультантів, науковців та дослідників, які вивчають політики, регуляції та практики.

Цей комплекс описується як такий, що формує те, як люди керуються, як вони можуть взаємодіяти з фінансовою системою і як вони контролюються в цьому контексті.

Ця книга застосовує критичний підхід до вивчення регулювання та нагляду. Декому цей тон може здатися відштовхуючим, тому корисно пам'ятати, що цей підхід до досліджень та аналізу призначений для того, щоб кидати виклик концептуальним рамкам та перспективам. Він покликаний бути провокаційним. Тому, читаючи це, корисно подумати про те, чому автор кидає виклик і навіщо.

Кому слід прочитати цю книгу? Вона в основному орієнтована на науковців, але може бути цікавою і для політиків та фахівців з питань відповідності.

Як вона розширює наші знання?

1. Критика мови відповідності. Індустріальний комплекс відповідності має тенденцію використовувати універсалізовані терміни належного управління, такі як цілісність, прозорість, підзвітність та ризик, але при ближчому розгляді ці терміни є "вражаюче порожніми". (стор. 25) (Як часто Ви замислюєтеся над питанням, що насправді означає фраза "захистити цілісність фінансового сектору".)
2. Критика "технологічного оптимізму": Автор вважає, що існує мало доказів на підтримку ролі штучного інтелекту в покращенні результатів відповідності, а індустрія відповідності має тенденцію фетишизувати прогнози на основі даних, незважаючи на "фальшиву експертизу та брехливі обіцянки", які продаються під міфом нейтральності та об'єктивності. (стор. 123-9)
3. Складність регуляторного середовища: Автор опитала деяких людей в індустрії відповідності і виявила, що регуляторне середовище настільки складне, що воно перевищує можливості однієї людини обробити цю інформацію. Це створює відкрите питання про те, що і кому це служить. Складність додатково вимагає включення все більш складних технологічних рішень у функцію відповідності, незалежно від доказів, що підтверджують їх ефективність.

Методи: Це есе базується на антропологічному дослідженні професіоналів з питань відповідності, переважно через участь у вебінарах та конференціях, а також через інтерв'ю. Деталей методології недостатньо, щоб судити, чи прийшло б подібне дослідження до тих самих висновків. Також

неясно щодо географічного охоплення цього дослідження і чи застосовні висновки в різних юрисдикціях.

Чого не вистачає: Існує досить надійний критичний підхід до вивчення боротьби з відмиванням грошей та протидії фінансуванню тероризму. Багато хто з вас, можливо, знайомий з роботами Марієке де Гуде або Ентоні Амісель. На диво, ця книга не взаємодіє з цією літературою.

Читабельність: Ця книга орієнтована на академічну аудиторію і передбачає певні знання та знайомство з критичними дослідженнями як дисципліною.

http://surl.li/lljpcf

ІНШІ НОВИНИ

NCA викриває найпотужнішу службу оренди DDoS-атак у світі

Національне агентство по боротьбі зі злочинністю Великобританії (NCA) успішно зупинило роботу однієї з найпотужніших у світі служб оренди DDoS-атак під назвою "DigitalStress.su". Цей сервіс, який використовувався для здійснення десятків тисяч атак по всьому світу, був зупинений у рамках операції "Power Off", проведеної у співпраці з Поліцією Північної Ірландії та ФБР.

NCA взяло під контроль сайт, замінивши його на сторінку-попередження про те, що дані користувачів були зібрані правоохоронними органами. Інфільтрація була досягнута шляхом створення дзеркального сайту, на який були перенаправлені користувачі. Операція також включала арешт одного з підозрюваних контролерів сайту.

Діяльність "DigitalStress.su" включала продаж послуг для здійснення DDoS-атак, які могли завдати значної шкоди бізнесу та критичній інфраструктурі, перешкоджаючи доступу до важливих суспільних послуг. Сервіс дозволяв кіберзлочинцям створювати облікові записи та замовляти атаки в межах кількох хвилин.

Зусилля NCA показали, що навіть домени, які здаються захищеними, можуть бути вразливими до правових дій, підкреслюючи важливість міжнародної співпраці у боротьбі з кіберзлочинністю. Інформація, зібрана під час операції, буде проаналізована для подальших розслідувань, а дані щодо зарубіжних користувачів будуть передані міжнародним правоохоронним органам.

Цей успіх демонструє ефективність сучасних методів розвідки та важливість глобального підходу до вирішення проблеми кіберзлочинності. NCA продовжує працювати над виявленням та зупинкою інших подібних сервісів, щоб забезпечити безпеку кіберпростору та захистити громадськість від кіберзагроз.

Департамент NCA з питань кіберзлочинності заявив, що традиційні методи знищення сайтів та їх арештів є ключовими елементами відповіді правоохоронних органів на загрозу кіберзлочинності. Проте розробка інноваційних інструментів та методик є необхідною частиною постійних зусиль щодо дезорганізації та підриву діяльності кіберзлочинців і захисту людей.

http://surl.li/fjiobv

Частина державного боргу США в розмірі 7 трильйонів доларів пов’язана із криптозлочинністю, головним чином з біткоїнами

CYBERPOL оприлюднила приголомшливий звіт, який вказує, що приблизно $7 трлн з національного боргу США, що перевищив $35 трлн, пов'язані з криптозлочинністю, переважно з використанням Bitcoin. Президент CYBERPOL Рікардо Барецкі підкреслив, що криптозлочинність знаходиться лише на початку свого розвитку, і загроза від неї буде лише зростати. У звіті зазначається, що велика частина цього боргу пов'язана з відмиванням грошей, шахрайством та іншими незаконними операціями, здійсненими за допомогою криптовалют.

Водночас звіт наголошує на ролі високопрофільних криптозлочинів, таких як діяльність "Криптокоролеви", афера Juicy Fields та схема RS Finance, які привернули міжнародну увагу. У відповідь на ці виклики CYBERPOL пообіцяла розкрити кожен акаунт, пов'язаний з незаконними операціями, що, як очікується, допоможе підвищити прозорість і підзвітність у криптовалютному просторі.

Ситуація підкреслює необхідність зміцнення регуляторних рамок, посилення міжнародної співпраці та освітніх ініціатив для інвесторів, щоб боротися з криптозлочинністю та забезпечити стабільність світової фінансової системи.

http://surl.li/rcjewt

Навігація в регуляторному ландшафті стейблкоїнів в APAC за допомогою моніторингу екосистеми

Стаття на Elliptic досліджує регуляторне середовище стейблкоїнів у регіоні Азії та Тихого океану (APAC). У ній розглядаються різні підходи країн до регулювання стейблкоїнів, підкреслюючи важливість моніторингу екосистеми для забезпечення відповідності та довіри до цих фінансових інструментів. Стаття також акцентує на необхідності збалансованого регулювання, яке сприяє інноваціям і водночас захищає фінансову стабільність, особливо враховуючи потенціал стейблкоїнів у транскордонних операціях.

http://surl.li/vwhxhr

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Глибоке занурення: належна перевірка клієнта – елементи, виклики та тактика зменшення ризиків.

Якщо ви працюєте у сфері ПВК, ви, безсумнівно, знайомі з терміном належної перевірки клієнта (CDD). CDD є основоположним аспектом заходів з протидії відмиванню коштів, який гарантує, що фінансові установи знають своїх клієнтів і розуміють пов'язані з ними ризики. Отже, що саме передбачає CDD?

1. Ідентифікація та перевірка клієнтів
2. Виявлення та перевірка бенефіціарної власності
3. Розуміння природи бізнесу клієнта
4. Постійний моніторинг та оновлення інформації про клієнтів

Але як злочинці зловживають прогалинами та що можете зробити ви, як спеціаліст із боротьби з відмиванням коштів.

Глибоке занурення в виклики та стратегії CDD

Належна перевірка клієнта (CDD) є критично важливим процесом для фінансових установ, спрямованим на пом'якшення ризиків, пов'язаних з ВК/ФТ. Кожен із чотирьох ключових елементів містить унікальні виклики та ризики, якими можуть скористатися злочинці.

1. Ідентифікація та перевірка клієнта

Точна ідентифікація та верифікація клієнтів передбачає збір повної особистої інформації та її перевірку за допомогою надійних незалежних джерел. Для підтвердження особи фінансові установи зазвичай використовують державні документи, що посвідчують особу, наприклад паспорти та водійські права.

Як злочинці використовують слабкі місця:

Використання підроблених документів: злочинці часто використовують високоякісні підробки, щоб обійти перевірку особи. Це може включати підроблені паспорти, посвідчення особи або змінені рахунки за комунальні послуги.

Синтетичні ідентифікатори: комбінуючи справжню та підроблену інформацію, злочинці створюють синтетичні ідентифікатори, які можуть непомітно пройти через стандартні процеси перевірки.

Що ви можете зробити:

Важко, а часом і неприємно мати справу зі складними підробками та синтетичними ідентифікаторами. Шахраї та особи, які відмивають кошти, використовують найсучасніші технології, тож ми повинні запобігти зловживанню нашими системами. Передові технології перевірки, такі як біометрія та цифрова перевірка особи, можуть забезпечити надійний захист від такої тактики.

2. Виявлення та перевірка бенефіціарного власника

Ідентифікація та перевірка бенефіціарних власників організацій забезпечує прозорість і допомагає виявити потенційну незаконну діяльність.

Як злочинці зловживають прогалинами:

Складні корпоративні структури: злочинці використовують багаторівневі та непрозорі структури власності, компанії-оболонки та трасти, щоб приховати свою справжню особу. У деяких випадках ці структури розроблені таким чином, що важко, часто неможливо ідентифікувати бенефіціарного власника (власників).

Юрисдикційний арбітраж: використання юрисдикцій із слабкими законами щодо прозорості або вимогами до бенефіціарної власності для приховування справжніх власників.

Що ви можете зробити:

Виявлення бенефіціарних власників може бути складним і трудомістким завданням, і саме на це розраховують злочинці. Вони сподіваються, що установи перестануть намагатися виявити незаконну діяльність, коли використовуються складні корпоративні структури, щоб приховати власність. Однак наполегливість є важливою. Продовжуйте копати глибше та використовувати всі доступні ресурси, щоб розкрити справжніх власників компаній, навіть коли справи йдуть важко. Використання реєстрів бенефіціарних власників і безперервна перевірка є надзвичайно важливою практикою.

3. Розуміння природи бізнесу клієнта

Оцінка рівня ризику, пов'язаного з клієнтом, вимагає глибокого розуміння його ділової діяльності, джерел коштів і очікуваних типів операцій. Це передбачає збір детальної інформації про діяльність, галузь і географічне розташування клієнта.

Як злочинці зловживають прогалинами:

Неправдиве уявлення про бізнес-діяльність: злочинці можуть спотворювати характер свого бізнесу, щоб уникнути виявлення, наприклад, використовуючи законний бізнес як прикриття для своєї незаконної діяльності.

Зміна структури власності: злочинці можуть купити існуючу компанію та змінити акціонерів.

Що ви можете зробити

Розробка комплексних економічних профілів і проведення ретельної оцінки ризиків можуть допомогти вам залишатися попереду. Розуміючи всю сферу діяльності ваших клієнтів, ви можете ефективніше визначати потенційні ризики. Регулярно перевіряйте підприємства, які є вразливими до відмивання коштів, і досліджуйте будь-які зміни в їхніх структурах власності.

4. Постійний моніторинг та оновлення інформації про клієнта

CDD не є одноразовим процесом. Вона вимагає постійного моніторингу та оновлення інформації про клієнтів. Регулярна перевірка транзакцій і оновлення профілів клієнтів допомагають швидко виявляти незвичайні або підозрілі дії та реагувати на них.

Як злочинці зловживають прогалинами:

Використання періодів неуважності. Злочинці часто використовують час, коли моніторинг може бути слабким, наприклад, під час свят або в неробочий час, коли відділи комплаєнсу не мають достатньо персоналу.

Аномальні шаблони транзакцій: використання нетипових шаблонів транзакцій, щоб уникнути виявлення, наприклад, структурування транзакцій трохи нижче порогових значень звітності непов'язаними рахунками осіб, які знаходяться під їхнім контролем.

Що ви можете зробити

Важко керувати великими обсягами даних і бути напоготові весь час. Автоматизовані системи моніторингу можуть допомогти, постійно перевіряючи дані транзакцій і виявляючи підозрілі дії. Регулярний перегляд і оновлення інформації про клієнтів забезпечує точність ваших зусиль моніторингу. Використовуйте технології – вони можуть надати підтримку, необхідну для надійного нагляду.

Висновок

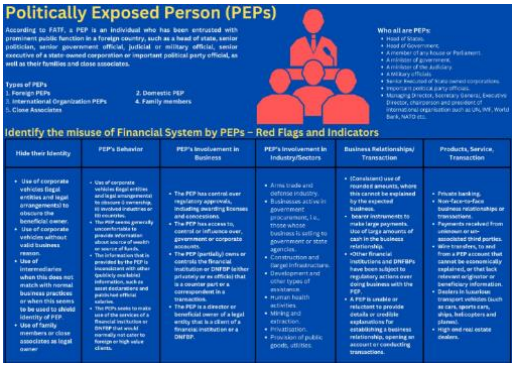
Належна перевірка клієнта (CDD) є життєво важливою для фінансових установ для боротьби з відмиванням коштів та іншою незаконною діяльністю. Запровадження ефективної практики CDD не позбавлене труднощів, від керування великими обсягами даних до роботи зі складною злочинною тактикою. Однак пильність і використання технологій можуть значно покращити ваші зусилля.

Коли ми просуваємося вперед, важливо застосовувати проактивний підхід. Постійно оновлюйте свої процеси, інвестуйте в передові системи моніторингу та співпрацюйте з іншими установами та регуляторними органами.

Зрозумійте, що, незважаючи на те, що цей шлях є складним, мета полягає у створенні безпечнішого та прозорішого фінансового середовища. Залишайтеся відданими, адаптуйтеся до нових викликів і використовуйте всі доступні ресурси для посилення своїх практик CDD. Зусилля, які ви докладете сьогодні, прокладуть шлях до більш безпечного майбутнього.

http://surl.li/vwmjvv

Розуміння політично значущих осіб (PEPs) у комплаєнсі з ПВК



Управління ризиками, пов'язаними з політично значущими особами (PEPs), має вирішальне значення для боротьби з відмиванням коштів. FATF випустила вичерпні вказівки щодо роботи з публічними діячами відповідно до Рекомендації 12, наголошуючи на посиленій належній перевірці.

🌟PEP через свою посаду можуть становити більший ризик причетності до хабарництва та корупції. Таким чином, фінансові установи повинні запроваджувати суворий контроль, коли мають справу з ними.

🔑 **Ключові моменти:**

☞Ідентифікація та перевірка🔍: потрібні надійні системи для виявлення публічних діячів та перевірки їх джерела коштів. За даними FATF, публічні діячі включають високопоставлених політиків, урядовців, судових чи військових чиновників, а також керівників державних підприємств.

☞Посилений моніторинг: регулярний моніторинг рахунків PEP для виявлення незвичних дій є важливим. Це включає спостереження за паттернами, як-от часті операції з великою кількістю готівки або операції з секторами, відомими високими ризиками, такими як торгівля зброєю чи будівництво.

☞Оцінка ризиків🔗: установи повинні постійно оцінювати рівень ризику, пов'язаного з публічними діячами, і відповідно коригувати свої стратегії ПВК. Це включає виявлення потенційних червоних прапорців, таких як використання корпоративних структур для приховування прав власності або участі в незвичайних ділових відносинах.

☞Червоні прапорці та індикатори🚩: будьте пильні щодо червоних прапорців, таких як незвичайне накопичення багатства, участь у таких галузях, як оборона чи державні закупівлі, а також використання корпоративних структур для приховування особи. Участь публічного діяча в секторах високого ризику або часті зміни в бізнес-діяльності можуть сигналізувати про потенційне зловживання фінансовою системою.

🔒 Забезпечення дотримання цих вказівок не тільки допомагає зменшити ризики відмивання коштів і корупції, але й зміцнює доброчесність і репутацію фінансових установ.

https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf

Найпоширеніші червоні прапорці щодо ПВК у фінансових установах

У сфері фінансових послуг пильність проти відмивання коштів має першочергове значення. Оскільки фінансові установи знаходяться в складному глобальному ландшафті, розуміння та виявлення сигналів протидії відмиванню коштів має вирішальне значення для захисту від незаконної фінансової діяльності.

1. Нові таємні клієнти, які уникають особистого контакту

Залучаючи нових клієнтів, фірми повинні дотримуватися надійних процедур «Знай свого клієнта» (KYC) і належної перевірки клієнта (CDD). Червоний прапорець виникає, коли клієнт відмовляється надати важливу особисту інформацію або ухиляється від запитів.

2. **Незвичайні транзакції**

Транзакції, які відрізняються від типових моделей поведінки клієнта, можуть сигналізувати про потенційне відмивання коштів. Приклади включають великі готівкові платежі, незрозумілі транзакції з третіми сторонами або використання кількох рахунків у різних юрисдикціях. Виявлення таких аномалій і повідомлення про них є критично важливими заходами ПВК.

3. **Незвичне джерело коштів**

Великі грошові депозити або невідомі джерела фінансування, включаючи криптоактиви, свідчать про потенційну діяльність з відмивання коштів.

4. **Транзакція має незвичні особливості**

Будь-яка транзакція, яка є надзвичайно великою, частою або має постійний характер із загальними характеристиками, відомими у схемах відмивання коштів, повинна викликати негайне занепокоєння.

5. **Географічні проблеми**

Транзакції, пов’язані з юрисдикціями, не пов’язаними з бізнес-операціями чи місцем проживання клієнта, часто є червоними прапорцями. Переміщення коштів між країнами або регіонами з високим ризиком і слабким наглядом вимагає посиленого контролю, щоб зменшити потенційні ризики ПВК.

6. **Політично значущі особи (PEPs)**

Особи, які обіймають високі державні посади, або пов'язані з ними особи, відомі як публічні діячі, становлять підвищений ризик через свою схильність до корупції.

7. **Невизначена кінцева бенефіціарна власність**

Складна структура власності або використання компаній-оболонок для приховування справжніх бенефіціарів транзакцій може свідчити про спроби відмивання коштів.

8. **Ризик юрисдикції**

Деякі юрисдикції відомі високим рівнем корупції та політичною нестабільністю або є гаванями для відмивання коштів. Операції, пов’язані з цими юрисдикціями, вимагають ретельного

контролю, щоб зменшити ризики, пов'язані з неналежною системою ПВК/ФТ або економічними санкціями.

9. **Санкції**

Регулярна перевірка у списках міжнародних санкцій має вирішальне значення, щоб переконатися, що клієнти не пов'язані з організаціями чи особами, які потрапили під санкції. Останні геополітичні події, такі як зміни санкційних режимів через міжнародні конфлікти, підкреслюють динамічний характер дотримання санкцій.

10. **Несприятлива інформація у ЗМІ**

Клієнти, пов'язані з негативними новинами, що стосуються фінансових зловживань чи злочинної діяльності, становлять підвищений ризик ПВК. Моніторинг несприятливої інформації у ЗМІ в усьому світі має важливе значення для швидкого виявлення та усунення потенційних загроз.

Розуміння процесу укладання ділових відносин з клієнтом відповідно до вимог KYC і ПВК

У сучасному нормативному середовищі компанії, особливо у фінансовому секторі, повинні керуватися складними вимогами відповідності, щоб забезпечити виконання зобов'язань «Знай свого клієнта» (KYC) і протидії відмиванню коштів (ПВК). Саме тут вступає в дію процес укладання ділових відносин з клієнтом, який служить критичним шлюзом для відповідності нормативним вимогам і взаємодії з клієнтами.

Що таке Укладання ділових відносин з клієнтом ❓

Це означає інтеграцію нового клієнта в систему компанії. Це передбачає збір, перевірку та підтвердження інформації, щоб переконатися, що клієнт є тим, ким він себе видає, і що його діяльність є законною.

Роль KYC і ПВК

🔘 Знай свого клієнта передбачає перевірку особистості ваших клієнтів, щоб запобігти шахрайству та забезпечити дотримання правових і нормативних стандартів. Зазвичай він включає збір персональної ідентифікаційної інформації, такої як імена, адреси та ідентифікаційні номери.

🔘 ПВК охоплює ширший набір заходів, призначених для запобігання, виявлення та повідомлення про відмивання коштів. Норми ПВК вимагають від компаній впровадження процедур моніторингу та повідомлення про підозрілу діяльність, яка може свідчити про відмивання коштів або фінансування тероризму.

Ключові кроки

1. Збір інформації:

✓ Особисті дані: зберіть основну інформацію, включаючи ім'я, дату народження, адресу та контактні дані.

✓ Документи, що посвідчують особу: візьміть офіційне посвідчення особи, як-от паспорт або водійські права, а також додаткові документи, як-от рахунки за комунальні послуги, для підтвердження адреси.

2. Підтвердження особи:

✓ Перевірка документів: використовуйте технологію для перевірки автентичності наданих документів. Це може включати розпізнавання обличчя, виявлення голограм і перевірку за державними базами даних.

✓ Біометрична перевірка: деякі організації включають біометричні перевірки, такі як відбитки пальців або розпізнавання обличчя, для підвищення безпеки.

3. Оцінка ризику:

✓ Перевірка: перевірте клієнта на наявність у глобальних списках спостереження, санкційних списках і базах даних політично значущих осіб (PEPs), щоб оцінити потенційні ризики.

✓ Профіль ризику: класифікуйте клієнта за профілем ризику на основі його досвіду, джерела коштів і запланованих транзакцій.

4. Постійний моніторинг:

✓ Моніторинг транзакцій: постійно відстежуйте транзакції клієнтів на наявність незвичайних або підозрілих дій.

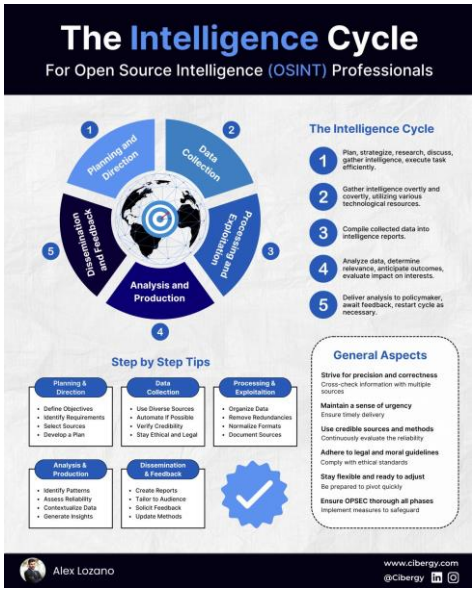
✓ Періодичні перевірки: регулярно оновлюйте інформацію про клієнтів і переоцінюйте профілі ризиків, щоб адаптуватися до будь-яких змін у їхній фінансовій поведінці чи статусі.

5. Звітування про відповідність:

✓ Звіти про підозрілу діяльність (SAR): повідомляйте відповідним органам про будь-які підозрілі дії відповідно до нормативних вимог.

✓ Ведення записів: Ведіть вичерпні записи про всі взаємодії з клієнтами, перевірки та звіти для цілей аудиту та відповідності.

Цикл розвідки для OSINT-професіоналів



Інфографічний матеріал, спрямований на професіоналів у галузі розвідки з відкритих джерел (OSINT), пропонує детальний огляд ключових етапів, необхідних для ефективного збору, обробки та аналізу даних. Цикл розвідки складається з п’яти основних кроків: планування та управління, збирання даних, обробка та експлуатація, аналіз та виробництво, а також поширення та зворотний зв'язок.

Ключові аспекти:

- Планування та управління: Визначення цілей, ідентифікація вимог та розробка плану дій.
- Збирання даних: Використання різноманітних джерел, автоматизація процесів та забезпечення легітимності даних.
- Обробка та експлуатація: Організація даних, видалення дублюючої інформації та документування джерел.
- Аналіз та виробництво: Ідентифікація закономірностей, оцінка надійності та генерація висновків.
- Поширення та зворотний зв'язок: Створення звітів, адаптація під аудиторію та оновлення методологій.

Цей підхід підкреслює важливість дотримання правових та моральних норм, використання надійних джерел та методів, а також оперативність і готовність до швидких змін. Крім того, акцентується увага на необхідності забезпечення безпеки інформації (OPSEC) на всіх етапах.

Дана інфографіка стала доступною для професійної спільноти завдяки Cibergy, компанії, що спеціалізується на кібербезпеці.

Товари подвійного використання та червоні прапорці

Стаття пояснює, що товари подвійного призначення (dual-use goods) є предметами, які можуть використовуватися як для цивільних, так і для військових цілей. Вона детально описує категорії та групи таких товарів, наводить приклади їх ідентифікації за допомогою п'ятизначних номерів класифікації експортного контролю. Особлива увага приділяється червоним прапорцям для спеціалістів з комплаєнсу, які можуть свідчити про можливі ризики чи порушення при роботі з цими товарами. Серед них — підозріла поведінка клієнтів, незвичайні маршрути доставки, сумнівні фінансові операції та інші фактори, що можуть свідчити про незаконні дії. Стаття підкреслює важливість ретельного дотримання правил контролю за експортом та здійснення належної перевірки клієнтів, щоб уникнути ризиків, пов'язаних з відмиванням грошей, фінансуванням тероризму та розповсюдженням зброї.

http://surl.li/bqetxo