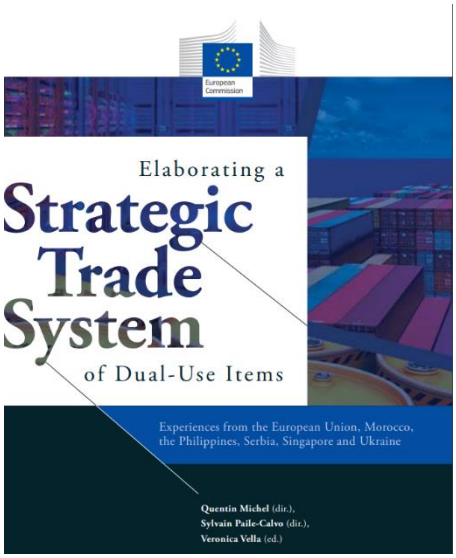
Серійний номер: ДСФМУ-ДК-2024-028
Жовтень 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Розробка стратегічної системи торгівлі товарами подвійного призначення: досвід Європейського Союзу, Марокко, Філіппін, Сербії, Сінгапуру та України



Документ містить детальну інформацію про створення стратегічної системи торгівлі товарами подвійного призначення у різних країнах, таких як Європейський Союз, Марокко, Філіппіни, Сербія, Сінгапур і Україна. **Основна мета документа полягає у створенні розуміння процесу розробки національних систем контролю торгівлі товарами подвійного призначення на прикладі досвіду зазначених країн. Він підкреслює важливість міжнародної співпраці, дотримання правових зобов'язань та безпекових стимулів для запобігання поширенню зброї масового ураження**.

Серед основних аспектів документу є 3WH-методологія, яка пояснює, чому потрібна система контролю (правові та політичні зобов'язання, безпекові інтереси, торговельні та геополітичні стимули), що вона охоплює (товари подвійного призначення та операції), хто бере участь у її розробці (включаючи державні органи, промисловість і академічні кола), та як ці правила впроваджуються на національному рівні. У документі розглядаються правові та політичні стимули для контролю торгівлі товарами, які можуть бути використані як у цивільних, так і у військових цілях.

Документ також приділяє значну увагу міжнародним зобов'язанням, таким як Договір про нерозповсюдження ядерної зброї, Конвенція про біологічну та токсичну зброю і Конвенція про хімічну зброю, а також резолюціям Ради Безпеки ООН, які створюють основні зобов'язання для країн щодо контролю експорту товарів подвійного призначення. Крім того, розглядаються недоліки та виклики міжнародної системи контролю експорту, включаючи критику щодо дискримінації країн, які не беруть участі в багатосторонніх форумах.

Ключові висновки з документу:

1. **Міжнародні безпекові зобов'язання:** Документ підкреслює, що впровадження стратегічних торгових систем (STC) є критично важливим для підтримання міжнародної безпеки та запобігання розповсюдженню зброї масового знищення (ЗМЗ). Держави повинні розробляти STC у відповідь на зобов'язання перед міжнародними угодами, такими як Договір про нерозповсюдження ядерної зброї (NPT), Конвенція про хімічну зброю (CWC)

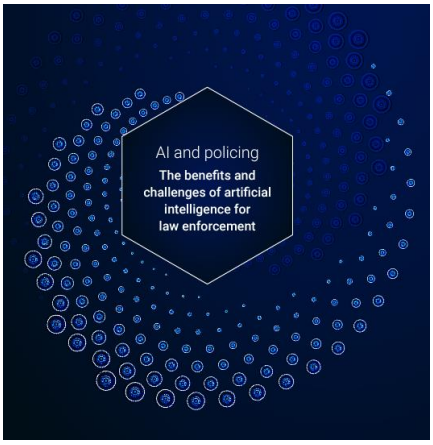
та інші. Контроль за експортом таких товарів націлений на те, щоб запобігти їх потраплянню до рук держав або недержавних суб'єктів, що можуть використовувати їх з небезпечними намірами.

2. **Глобальна співпраця та адаптація міжнародних стандартів:** Документ наголошує, що системи стратегічної торгівлі повинні базуватися на міжнародно визнаних стандартах. Багатосторонні експортні режими, такі як Вассенаарська угода, Режим контролю за ракетними технологіями (MTCR) та інші, забезпечують рекомендації щодо створення контрольних списків товарів подвійного призначення та регулюють їх міжнародну торгівлю. Важливо, щоб національні системи були узгоджені з міжнародними нормами для сприяння глобальній безпеці та уникнення непорозумінь.
3. **Роль приватного сектору та навчальних установ:** Для успішного функціонування стратегічних торгових систем необхідна тісна співпраця з приватними підприємствами, академічними та науково-дослідними установами. Це включає підвищення рівня обізнаності у компаніях про важливість дотримання норм торгівлі товарами подвійного призначення та впровадження внутрішніх програм з комплаєнсу. Приватний сектор та наукові установи повинні забезпечити відповідність своїх досліджень і виробничих процесів міжнародним стандартам, щоб уникнути використання їхніх товарів з недобрими намірами.
4. **Геополітичні та економічні стимули:** У документі наголошується, що національні системи стратегічної торгівлі повинні враховувати геополітичні та економічні фактори. Зокрема, ефективні системи контролю сприяють кращому доступу до міжнародних ринків, оскільки країни-експортери вимагають від імпортерів дотримання аналогічних стандартів безпеки. Наявність системи контролю також може підвищити конкурентоспроможність держави на глобальному ринку технологій, оскільки вона демонструє здатність забезпечувати відповідність міжнародним вимогам.
5. **Правова основа та внутрішній контроль:** Держави мають зобов’язання запровадити надійні системи контролю для регулювання внутрішнього обігу товарів подвійного призначення. Це включає в себе імпорт, реекспорт і використання таких товарів, зокрема шляхом введення законодавства та правових механізмів для запобігання їх несанкціонованого використання. Країни, що впроваджують ці системи, здатні зміцнити свою внутрішню безпеку, запобігаючи використанню товарів для виробництва ЗМЗ або терористичних актів.

Таким чином, документ надає комплексну рамку для розуміння необхідності стратегічного контролю за торгівлею товарами подвійного використання, підкреслюючи важливість міжнародного співробітництва, національної безпеки та відповідності міжнародним стандартам для досягнення глобальної безпеки.

https://op.europa.eu/en/publication-detail/-/publication/cfcac057-76f9-11ef-bbbe-01aa75ed71a1

Штучний інтелект у правоохоронній діяльності: можливості та виклики впровадження



Документ під назвою "AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement", підготовлений Європейським агентством з правоохоронної співпраці (Europol), пропонує глибокий аналіз використання штучного інтелекту (ШІ) у правоохоронній діяльності. Він висвітлює як позитивні, так і негативні аспекти інтеграції ШІ в поліцейську роботу.

Цей звіт аналізує, як технології штучного інтелекту можуть змінити правоохоронну діяльність. Він містить огляд таких ключових технологій, як аналітика даних, обробка мови (NLP), біометрія, розпізнавання облич, а також потенційні виклики, пов'язані з етичними та соціальними аспектами. Крім цього,

увага приділяється регуляторним аспектам використання ШІ, зокрема впливу регламенту ЄС про штучний інтелект (EU AI Act).

Ключові моменти:

- **Аналітика даних та прогнози:** ШІ значно покращує можливості аналізу великих даних, дозволяючи поліції ефективніше прогнозувати злочини та розуміти складні моделі поведінки злочинців.
- **Біометрія та розпізнавання облич:** Технології, такі як розпізнавання облич та аналіз відео, забезпечують швидку ідентифікацію підозрюваних. Проте викликають занепокоєння щодо приватності та можливого неправомірного використання.
- **Етичні виклики:** Використання ШІ піднімає питання про конфіденційність даних, упередженість алгоритмів і можливі загрози правам людини. Наприклад, системи ШІ можуть відтворювати «історичні упередження» у даних, що призводить до помилкових рішень.
- **Регуляція та відповідальність**: Регламент ЄС про штучний інтелект вводить правила щодо високоризикових систем ШІ, до яких належать і поліцейські застосунки. Закон передбачає обмеження на використання ШІ для певних цілей, таких як біометрична ідентифікація в реальному часі в публічних місцях.
- **Обробка мови (NLP):** Технології NLP дозволяють поліції швидше обробляти великі обсяги текстової інформації, автоматизувати аналіз розмов, текстових повідомлень та інших даних для швидшого розслідування.
- **Обмеження та виклики:** У звіті зазначено, що для ефективного впровадження ШІ необхідні значні інфраструктурні ресурси та технічна підтримка, що може бути викликом для невеликих агентств.

Висновки:

- **Баланс між інноваціями та етикою:** Впровадження ШІ в правоохоронну діяльність може суттєво підвищити ефективність, але це має бути збалансовано з етичними вимогами, захистом приватності та прав людини.
- **Роль громадської довіри:** Для успішного використання ШІ важливо забезпечити прозорість та підзвітність, що допоможе зміцнити громадську довіру до таких технологій.
- **Майбутнє використання ШІ:** Очікується, що технології ШІ продовжать розвиватися, однак для їх відповідального використання правоохоронним органам необхідно активно співпрацювати з дослідниками, технологічними компаніями та регуляторами.

http://surl.li/zesjtg

Інноваційні підходи та співпраця для ефективної боротьби з фінансовим шахрайством: роль FCA у глобальній стратегії

United Nations

General Assembly

Документ є звітом Робочої групи ООН, присвяченої дослідженню фінансування найманців та злочинців, пов'язаних із найманством. У доповіді висвітлюються сучасні тенденції та виклики, пов'язані з фінансовою підтримкою найманців, а також їхній вплив на порушення прав людини та продовження збройних конфліктів. Доповідь аналізує методи фінансування на макро- і мікрорівнях, включаючи традиційні банківські системи, криптовалюти, видобуток природних ресурсів та злочинні мережі.

Ключові моменти:

- **Фінансування найманців**: Найманці фінансуються як на державному рівні через закупівлю зброї та матеріалів, так і на індивідуальному через грошову винагороду. Серед ключових

джерел фінансування виділяються видобуток золота, алмазів, нафти та інших природніх ресурсів.

- **Інструменти фінансування:** Використовуються як традиційні банківські системи, так і альтернативні методи, включаючи криптовалюти. Банки, юридичні фірми, страхові компанії та інші комерційні організації діють як "посередники", полегшуючи рух фінансів.
- **Взаємозв'язок із організованою злочинністю:** Фінансування найманців має прямі зв'язки з іншими незаконними видами діяльності, такими як торгівля зброєю, наркотиками, людьми, а також відмиванням грошей.
- **Роль держав:** Багато держав безпосередньо чи опосередковано фінансують найманців, надаючи їм доступ до природних ресурсів або підтримуючи через військову інфраструктуру. Держави також використовують найманців для досягнення геополітичних цілей.
- **Негативні наслідки для прав людини:** Найманство сприяє порушенню прав людини, включаючи вбивства цивільних осіб, і загрожує стабільності в регіонах, багатих на ресурси. Водночас діяльність найманців перешкоджає досягненню Цілей сталого розвитку ООН.

Висновки:

- **Необхідність кращого регулювання:** Регулювання фінансування найманців є критично важливим, оскільки сучасні фінансові механізми дозволяють їм залишатися поза контролем держав.
- **Важливість прозорості:** Прозорість фінансових потоків та моніторинг діяльності осіб, залучених у фінансування найманців, є важливими кроками для боротьби з найманством.
- **Зміцнення правових норм:** Існує потреба в удосконаленні міжнародних і регіональних правових інструментів для боротьби з фінансуванням найманців і злочинних угруповань, а також у запровадженні обов'язкової правової відповідальності за участь у таких фінансових схемах.
- **Вплив на глобальну безпеку:** Фінансування найманців не тільки подовжує конфлікти, але й підриває державний суверенітет, сприяючи незаконній експлуатації природних ресурсів і поглиблюючи нерівність між країнами.

Рекомендації:

- Забезпечити регулювання діяльності приватних військових і охоронних компаній на міжнародному рівні.
- Покращити системи розслідування та моніторингу фінансових потоків, що пов'язані з найманством.
- Включити порушення прав людини та міжнародного гуманітарного права до категорії злочинів, що підлягають кримінальному переслідуванню у сфері відмивання грошей.

http://surl.li/lglhuj

Програма тематичного іспиту 2023: Зворотній зв'язок - протидія фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення

Документ надає огляд програмних перевірок, проведених у 2023 році щодо протидії фінансуванню тероризму (CFT) та фінансуванню розповсюдження зброї масового знищення (CPF) у фінансових установах Джерсі. Основна мета цих перевірок полягала в оцінці ефективності заходів, які були запроваджені підконтрольними організаціями для протидії фінансовим злочинам. У документі детально аналізуються прогалини в корпоративному управлінні, політиках і процедурах, навчанні персоналу, а також заходах щодо належної перевірки клієнтів (CDD) та постійного моніторингу.

Під час перевірок було виявлено значні прогалини в управлінні ризиками, пов'язаними з фінансуванням тероризму та розповсюдження, що могло призвести до підвищення ризику фінансових злочинів. Окремо зазначається, що багато організацій не включили відповідні аспекти протидії фінансуванню розповсюдження в свої політики та процедури, що свідчить про недостатнє розуміння ризиків.

Ключові висновки:

1. **Прогалини в корпоративному управлінні:** Багато організацій не надають достатньо уваги питанням фінансування тероризму (ФТ) та фінансування розповсюдження зброї масового знищення (ФР) на рівні правління. Регулярна оцінка ризиків ФТ/ФР часто відсутня або недостатньо актуалізована. Це створює прогалини в управлінні ризиками, оскільки рішення щодо управління ризиками фінансування тероризму та розповсюдження не завжди обговорюються на найвищих рівнях корпоративного управління.
2. **Недостатність моніторингу клієнтів та транзакцій:** У багатьох випадках виявлено, що організації не проводять достатньо ефективного моніторингу клієнтів та їхніх транзакцій для ідентифікації потенційних ризиків, пов’язаних із ФТ та ФР. Важливі елементи, такі як належна перевірка клієнтів (CDD) та регулярне оновлення профілю ризиків клієнтів, не завжди враховують аспекти ФТ/ФР. Це призводить до того, що транзакції, які можуть бути підозрілими, не виявляються або аналізуються із запізненням, що підвищує ризик невиявлення фінансових злочинів.
3. **Недоліки у навчанні персоналу:** Документ підкреслює, що багато організацій не забезпечили належне навчання співробітників, включаючи відповідальних працівників та інший персонал з комплаєнсу, щодо специфіки фінансування тероризму і розповсюдження. Відсутність регулярного і спеціалізованого навчання для співробітників означає, що персонал не завжди розуміє нові ризики, пов’язані з ФТ/ФР, або не має належних знань для впровадження заходів боротьби з цими ризиками на практиці.
4. **Проблеми з політиками та процедурами:** Багато організацій не мають чітких та відповідних політик і процедур, які б відповідали вимогам законодавства з боротьби з ФТ/ФР. Виявлено, що посилені заходи належної перевірки клієнтів (EDD), особливо щодо політично значущих осіб (PEP), часто не застосовуються або виконуються не в повній мірі. Це може значно збільшити ризики невиявлення підозрілих операцій та осіб, пов'язаних із фінансуванням тероризму чи розповсюдження зброї.

Загалом, документ вказує на необхідність покращення у сферах управління ризиками, навчання персоналу та зміцнення систем моніторингу для забезпечення відповідності вимогам щодо протидії фінансуванню тероризму і розповсюдження.

http://surl.li/uaskkl

РЕГУЛЮВАННЯ

Впровадження MiCA в Польщі (оновлений законопроект)

Проєкт закону Польщі про криптоактиви (опублікований 9 серпня 2024 року після консультацій) імплементує положення регуляції MiCA (Регламент 2023/1114). **Основні зміни стосуються скорочення перехідного періоду для отримання ліцензії CASP (до 30 червня 2025 року), а також надання KNF додаткових наглядових повноважень. KNF зможе перевіряти діяльність емітентів токенів та криптосервісів, блокувати рахунки, а також вести реєстр інтернет-доменів, що використовуються для нелегальної криптодіяльності**. Вводяться збори за нагляд і штрафи за порушення, включно з санкціями до 66 млн злотих.

Основні положення проєкту закону:

1. **Перехідний період та вимоги до ліцензування:** Віртуальні постачальники послуг з активами (VASP) повинні отримати ліцензію CASP до 30 червня 2025 року, раніше цей строк був встановлений на 31 грудня 2025 року. Якщо інші компанії подадуть заявку до 1 травня 2025 року, вони можуть продовжувати надавати послуги до моменту рішення KNF щодо їхньої ліцензії.
2. **Реєстр криптодіяльності:** Діяльність у сфері віртуальних валют, зареєстрована до набуття чинності законом, підлягає чинним вимогам боротьби з відмиванням коштів і фінансуванням тероризму. Однак з 1 липня 2025 року реєстр діяльності з віртуальними валютами буде скасовано.
3. **Розширення повноважень KNF:** Комісія з фінансового нагляду (KNF) отримає право перевіряти діяльність не тільки криптосервісів, але й емітентів токенів, а також осіб, що подають заявки на допуск криптоактивів до обігу. Це включає перевірки на відповідність положенням MiCA та іншим регуляторним вимогам.
4. **План підтримки стабільності криптоактивів:** Емітенти токенів, прив'язаних до активів або електронних грошей, мають надати KNF план щодо підтримки певного рівня вартості та обсягу операцій. Це важливо для захисту інвесторів та стабільності ринку криптоактивів.
5. **Збір за регулювання:** Введено новий щорічний збір для криптосервісів, щоб покрити витрати на нагляд. Розмір збору визначається як до 0.5% від середньорічного доходу за останні три фінансові роки, але не менше 500 польських злотих.
6. **Штрафи та покарання:** За порушення положень MiCA, криптосервіси та фізичні особи можуть бути оштрафовані на суми до 5 мільйонів злотих або ув’язнені до 5 років. У деяких випадках штрафи можуть сягати 66 мільйонів злотих (15 мільйонів євро).
7. **Захист інвесторів:** Важливим аспектом проєкту закону є заходи щодо підвищення захисту інвесторів. Наприклад, криптосервіси повинні негайно повідомляти KNF про будь-які зміни у своїй діяльності, що можуть вплинути на ринок.

Загалом, закон спрямований на забезпечення належного регулювання ринку криптоактивів у Польщі відповідно до MiCA, збільшуючи контроль за діяльністю криптоплатформ та підвищуючи рівень захисту інвесторів.

http://surl.li/jdvqqp

САНКЦІЇ

Міністерство фінансів США вживає скоординовані дії проти незаконних російських бірж віртуальних валют і тих, хто сприяє кіберзлочинам

Стаття на сайті TRM Labs детально описує дії Міністерства фінансів США щодо російських віртуальних валютних бірж PM2BTC і Cryptex, які були залучені до незаконної діяльності, пов'язаної з відмиванням коштів і підтримкою кіберзлочинності. Ці біржі використовувались для здійснення транзакцій кіберзлочинними угрупованнями, такими як Joker's Stash, і сприяли обходу міжнародних санкцій. США заморозили активи цих платформ, вилучили криптовалюти, а також наклали санкції на ключових осіб, що стоять за цими операціями.

Ключові моменти:

1. **Виявлення основних учасників:** Міністерство фінансів США разом з правоохоронними органами виявило та наклало санкції на ключових фігурантів, які керували цими платформами, таких як Сергій Іванов. Учасники таких платформ здійснювали перекази та проводили фінансові операції на суму мільйони доларів для підтримки кіберзлочинності.
2. **Використання для кіберзлочинних угруповань:** PM2BTC і Cryptex використовувалися злочинними організаціями, як-от Joker's Stash, для обміну криптовалют на фіатні гроші. Ці біржі активно використовувалися для незаконної діяльності, включаючи крадіжки, фішинг і продаж викрадених даних.
3. **Спроби обходу санкцій:** Біржі допомагали злочинцям уникати міжнародних санкцій, особливо пов'язаних з обмеженнями проти Росії, зокрема через транзакції в криптовалюті, яка на той час не регулювалася повною мірою.
4. Співпраця правоохоронних органів: Дії Міністерства фінансів США були частиною більшого міжнародного зусилля із залученням правоохоронних органів багатьох країн, включаючи європейських партнерів, для блокування серверів і вилучення активів на суму 7 мільйонів євро.
5. Замороження активів і санкції: У межах операції було заморожено активи, що належали платформам PM2BTC та Cryptex, а також запроваджено санкції проти їхніх операторів. Це стало значним ударом по мережах, які використовували ці біржі для відмивання грошей.

Таким чином, в статті акцентується на тому, як використання криптовалют може становити серйозну загрозу для міжнародної фінансової безпеки, якщо відповідні органи не вживають належних заходів для регулювання цієї сфери та протидії її використанню в злочинних цілях.

http://surl.li/fzxlxr

Як обходять санкційні обмеження: нелегальні поставки розкішних авто до Росії через Грузію

Стаття від Sky News розглядає механізм нелегального ввезення в Росію нових розкішних автомобілів з Великої Британії та Європи, попри заборони, накладені санкціями ЄС і Великої Британії. Автори досліджують, як автомобілі потрапляють на територію Росії через Грузію, незважаючи на міжнародні обмеження, спрямовані на послаблення економічних ресурсів Росії у відповідь на її вторгнення в Україну.

Ключові моменти:

- **Маршрут через Грузію:** Стаття підкреслює важливу роль Грузії як транзитної країни для поставок автомобілів у Росію. Товари, включаючи розкішні автомобілі, транспортуються через грузинські перевали до північної Росії. Незважаючи на формальну заборону на експорт таких товарів, знайдені способи обійти ці обмеження.
- **Зростання експорту в країни-сусіди Росії:** Після введення санкцій експорт багатьох товарів до Росії скоротився до нуля. Однак відбулося різке зростання поставок цих товарів до сусідніх країн, таких як Азербайджан і Киргизстан, які виступають як транзитні хаби.
- **Нелегальні механізми та обхід санкцій:** Ввезення розкішних автомобілів здійснюється через декілька схем. Одна з них передбачає оформлення авто через Вірменію, після чого автомобілі переміщують до кордону Росії з Грузією. Також зустрічається схема, коли автомобілі формально призначені для Киргизстану, але фактично залишаються в Росії.
- **Видимість та відсутність приховування:** Розслідування демонструє, що цей процес майже не приховується. Автомобілі відкрито транспортуються через грузинсько-російський кордон, і ніхто на місцях не намагається зупинити або приховати цей процес.
- **Наслідки для санкційного режиму:** Незважаючи на твердження, що західні країни докладають зусиль для дотримання санкцій, фактично ці санкції не зупиняють потоки розкішних товарів у Росію. В результаті економіка Росії залишається сильною, а доступ до західних товарів зберігається.

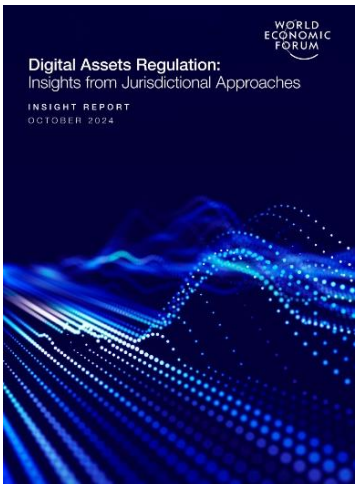
Висновки:

Стаття демонструє, як санкційні обмеження, введені проти Росії, можуть обходитися через сусідні країни, зокрема через Грузію та Вірменію. Це свідчить про те, що поточний санкційний режим має значні прогалини, які дозволяють Росії продовжувати отримувати доступ до товарів, включаючи розкішні автомобілі, незважаючи на міжнародні обмеження. Особливо важливою є відсутність приховування цих дій, що підриває ефективність санкцій та дає змогу Росії підтримувати свою економіку в умовах міжнародної ізоляції.

http://surl.li/unwxbj

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Регуляторні підходи до цифрових активів: Порівняння міжнародних практик та рекомендацій



Документ «Digital Assets Regulation: Insights from Jurisdictional Approaches» є аналітичним звітом, опублікованим Всесвітнім економічним форумом у жовтні 2024 року. Він розглядає регуляторні підходи до цифрових активів у різних юрисдикціях і аналізує, як різні країни формують політики у цій сфері. Звіт фокусується на дев'яти провідних юрисдикціях: Європейському Союзі, Гібралтарі, Гонконгу, Японії, Сінгапурі, Швейцарії, Об'єднаних Арабських Еміратах, Великобританії та США. Документ також виділяє основні виклики в регулюванні цифрових активів, включаючи протидію відмиванню коштів (ПВК) та заходи «Знай свого клієнта» (KYC), рекомендації щодо застосування регуляторних «пісочниць», специфіку децентралізованих фінансів (DeFi), а також питання конфіденційності та безпеки.

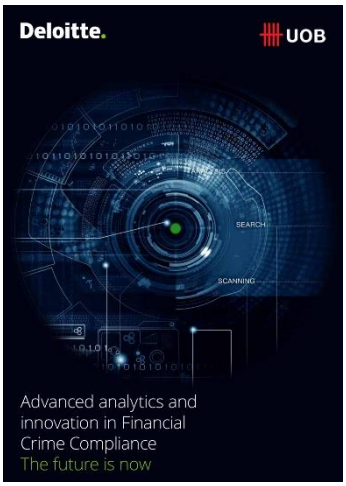
Ключові висновки:

1. **Різні підходи до регулювання цифрових активів:** Різні юрисдикції мають унікальні стратегії регулювання цифрових активів, що відповідають їхнім економічним пріоритетам, ризикам і місцевим особливостям. Це може призвести до недостатньої глобальної координації у регулюванні.
2. **Значущість ПВК та KYC:** Приділяється велика увага протидії відмиванню коштів і фінансуванню тероризму. Ключовими стратегіями є впровадження технологій для посилення перевірки клієнтів і моніторингу транзакцій, а також глобальне співробітництво між юрисдикціями для посилення боротьби з фінансовими злочинами.
3. **Регуляторні «пісочниці»:** У багатьох країнах впроваджуються регуляторні «пісочниці», які дозволяють компаніям тестувати інноваційні фінансові продукти в контрольованих умовах. Це сприяє безпечній інтеграції нових технологій у фінансові ринки та підтримує відповідність регуляторним вимогам.
4. **Децентралізовані фінанси (DeFi):** Підхід до регулювання DeFi варіюється. Деякі країни, як-от ЄС, почали досліджувати цю сферу, але пряме регулювання поки обмежене через специфіку DeFi як децентралізованої системи без посередників.
5. **Проблеми конфіденційності та безпеки:** Усі юрисдикції визнають важливість захисту даних користувачів і забезпечення безпеки транзакцій. Для цього застосовуються строгі стандарти, такі як регулювання конфіденційності GDPR у ЄС, а також заходи щодо забезпечення прозорості в обігу цифрових активів.
6. **Непередбачені наслідки:** У документі також зазначаються негативні наслідки деяких регуляторних рішень, включаючи ризики надмірної зарегульованості, що може призвести до відтоку інноваційних компаній або сприяти «регуляторному арбітражу», коли компанії обирають країни з менш жорсткими правилами.

Загалом, звіт підкреслює важливість міжнародної координації у сфері регулювання цифрових активів, оскільки відсутність глобальних стандартів може ускладнити запровадження ефективних та гармонізованих регуляторних рамок.

https://www3.weforum.org/docs/WEF_Digital_Assets_Regulation_2024.pdf

Інноваційні технології в боротьбі з фінансовими злочинами



Документ «Advanced Analytics and Innovation in Financial Crime Compliance» (Делойт та UOB) присвячений ролі передових аналітичних технологій у боротьбі з фінансовими злочинами. Він розглядає використання штучного інтелекту (ШІ), машинного навчання (МН), аналітики даних та роботизованої автоматизації процесів (RPA) для ефективної протидії відмиванню коштів та фінансуванню тероризму. Документ надає огляд технологічної трансформації, яку здійснює UOB, застосовуючи інноваційні підходи для вдосконалення своїх систем фінансової злочинності.

Описується вплив COVID-19 на фінансову індустрію, зокрема прискорення цифровізації, що привело до зростання ризиків фінансових злочинів. Акцент зроблено на тому, як інвестиції в новітні технології, зокрема у ШІ та МН, сприяли швидкому виявленню підозрілих транзакцій, підвищенню ефективності процесів моніторингу транзакцій та ідентифікації злочинних схем. Описується роль таких рішень в адаптації банків до змін у поведінці клієнтів та нових загроз.

Ключові висновки:

1. **Технологічна трансформація у сфері комплаєнсу**: UOB та Deloitte демонструють приклад успішної інтеграції ШІ, МН та RPA в процеси моніторингу транзакцій та аналізу даних. Це дозволяє значно підвищити точність виявлення підозрілих активностей і знизити кількість помилкових спрацювань (false positives).

2. **Адаптивні моделі та самонавчання**: ШІ/МН моделі можуть адаптуватися до змін у поведінці користувачів і типологіях фінансових злочинів, що дозволяє постійно підвищувати ефективність виявлення нових схем відмивання коштів.

3. **Зниження людських помилок та підвищення ефективності**: Автоматизація рутинних задач за допомогою RPA дозволила знизити кількість помилок, що виникають через людський фактор, а також оптимізувати використання робочого часу.

4. **COVID-19 як каталізатор цифровізації**: Пандемія прискорила впровадження технологій, що забезпечують безперебійну роботу в умовах віддаленої роботи та підвищення ефективності моніторингу фінансових злочинів в нових умовах.

5. **Проблеми та виклики**: Впровадження нових технологій у сфері фінансової злочинності вимагає значних фінансових вкладень і має викликати довіру з боку регуляторів. Успішна реалізація таких рішень можлива лише за умови чіткого дотримання принципів прозорості, підзвітності та етики.

6. **Співпраця між державою та приватним сектором**: У документі наголошується на важливості публічно-приватного партнерства для покращення інформаційного обміну, підвищення ефективності контролю та впровадження інноваційних рішень у сфері боротьби з фінансовими злочинами.

Таким чином, документ підкреслює важливість впровадження інноваційних технологій для підвищення ефективності боротьби з фінансовими злочинами, а також закликає до активної співпраці між фінансовими установами, технологічними компаніями та регуляторами для успішної реалізації таких рішень.

http://surl.li/ldpkkw

Роль відповідальної особи у сфері протидії відмиванню коштів (MLRO): Ключові завдання та відовідальність

Документ «Money Laundering Reporting Officer Guidebook» є керівництвом для осіб, які займаються звітністю у сфері протидії відмиванню коштів (ПВК). Він містить детальні вказівки щодо обов'язків, вимог та процедур, пов'язаних із виявленням та звітуванням підозрілих дій, що можуть свідчити про відмивання коштів або фінансування тероризму. Книга охоплює юридичні зобов'язання, рекомендації щодо звітування про підозрілі дії до Національного агентства по боротьбі з злочинністю (NCA) та інші важливі аспекти щодо дотримання законодавства у сфері ПВК.

Ключові висновки:

1. **Повноваження та обов'язки MLRO:** MLRO повинні мати достатні повноваження для прийняття незалежних рішень, а також авторитет для забезпечення належного виконання правил з ПВК. Це включає в себе право подання SAR до NCA без погодження з іншими особами, що дозволяє швидко реагувати на підозрілі операції. MLRO повинен мати час, ресурси та досвід для обробки внутрішніх SAR і своєчасного подання зовнішніх SAR.
2. **Постійний контроль за ризиками:** Ключовою функцією MLRO є моніторинг внутрішніх SAR і оцінка ризиків у рамках організації. Це включає не лише розгляд підозрілих операцій, а й систематичний перегляд внутрішніх процедур, щоб переконатися, що компанія постійно дотримується вимог з ПВК та враховує актуальні ризики. Регулярне оновлення політик та навчання співробітників є обов'язковим.
3. **Співпраця з іншими відділами та керівництвом:** Документ підкреслює важливість постійної взаємодії MLRO з іншими підрозділами, зокрема з працівником, відповідальним за комплаєнс (MLCO) та керівництвом компанії. Спільна робота сприяє обміну інформацією про ризики та забезпеченню виконання правил з ПВК на всіх рівнях компанії. Це також включає регулярне інформування керівництва про кількість поданих SAR, аналіз виявлених ризиків, зміни в регулюванні, а також заходи щодо підвищення ефективності процедур з ПВК.
4. **Навчання співробітників та підвищення обізнаності:** Документ наголошує на важливості регулярного навчання співробітників для того, щоб вони знали, які саме дії підпадають під підозрілі та як подавати звіти про підозрілі операції. MLRO повинен забезпечити, щоб кожен працівник знав, що підозрілі дії не мають мінімального порогу (deminimis), тобто будь-яка підозріла активність повинна бути зареєстрована. Регулярні оновлення щодо нових ризиків та червоних прапорців є необхідними для постійної готовності персоналу реагувати на можливі загрози відмивання коштів.
5. **Документування рішень щодо SAR:** MLRO зобов'язаний забезпечити належне зберігання поданих SAR, а також ведення обліку щодо рішень про подання або неподачу звітів до NCA. Це забезпечує прозорість процесу та захист компанії від можливих юридичних ризиків.

http://surl.li/mjhrgp

Fintech 2023: остаточні глобальні юридичні посібники з порівняльним аналізом від провідних юристів

Документ "Fintech 2023" є всебічним посібником, який пропонує глибокий аналіз правового регулювання фінансових технологій (fintech) у різних юрисдикціях світу. Посібник охоплює законодавчу базу, тенденції розвитку фінтеху та їхній вплив на фінансові ринки. Автори розглядають еволюцію технологій, зокрема, таких як блокчейн, регуляторні "пісочниці" та інновації у фінансових послугах. Документ також акцентує увагу на важливості дотримання правил ПВК та ролі автоматизованих рішень (як-от роботизовані консультанти) у модернізації фінансових інституцій.

Одним з ключових аспектів є розуміння того, як регулюються різні аспекти фінтеху у таких країнах, як Іспанія, Франція, Китай, Люксембург та багато інших. Кожен розділ присвячено окремій країні, що дозволяє читачу отримати порівняльну характеристику законодавства та практик.

Ключові висновки:

1. **Фінтех та традиційні фінансові інститути:** Документ підкреслює зростаючий вплив фінтех-компаній на ринок фінансових послуг. Нові технології, такі як блокчейн, штучний інтелект і автоматизовані платформи, стимулюють зміну бізнес-моделей традиційних банків і фінансових інститутів. Впровадження технологій дозволяє банкам оптимізувати операційні процеси, знижувати витрати та підвищувати прозорість для клієнтів. Важливо, що фінтех-компанії не лише конкурують з традиційними банками, але і часто співпрацюють з ними, надаючи їм нові рішення, такі як цифрові платформи для управління активами чи мобільні додатки для обслуговування клієнтів.
2. **Роль регуляторних "пісочниць":** У багатьох країнах фінтех-компанії можуть тестувати нові бізнес-моделі в межах так званих "регуляторних пісочниць" – спеціальних правових зон, де нові технології можуть працювати з мінімальними правовими вимогами та без наявних регуляторних ризиків. Такі ініціативи існують у Великій Британії, Сінгапурі, та інших країнах, і дозволяють стартапам отримувати доступ до фінансових ринків та тестувати нові ідеї у контрольованих умовах, водночас регулятори спостерігають за їх впливом на ринок і вивчають потенційні ризики.
3. **Регулювання криптоактивів та DeFi:** Одним із найгостріших викликів для юрисдикцій є створення ефективних регуляторних рамок для криптовалют і децентралізованих фінансів (DeFi). Деякі країни, як-от Люксембург і Швейцарія, вже ввели передові закони для контролю за блокчейн-активами, що стимулює їхній розвиток як криптохабів. Проте в багатьох юрисдикціях залишається недостатня правова база для регулювання криптовалют і NFT, що створює певну правову невизначеність і ризики для інвесторів та користувачів цих активів.
4. **Зростання важливості автоматизованих фінансових радників:** Робо-адвайзери, або автоматизовані платформи для надання фінансових порад, стають дедалі більш популярними завдяки їх здатності надавати послуги за нижчими витратами та забезпечувати індивідуалізований підхід до інвестування. Багато традиційних банків починають інтегрувати такі рішення у свої послуги для залучення нових клієнтів і надання більш технологічно просунутих послуг. Документ наголошує, що хоча такі платформи є автоматизованими, їхня діяльність усе одно підлягає регуляторному контролю, як і традиційні інвестиційні послуги.
5. **Складнощі з глобальним регулюванням:** Різні юрисдикції мають неоднакові підходи до регулювання фінтеху, що створює розбіжності у правовому полі для компаній, які працюють на глобальному ринку. Це підвищує важливість міжнародної координації регуляторів для забезпечення гармонізації правил і уникнення регулятивного арбітражу. Країни Європейського Союзу прагнуть до впровадження єдиних стандартів у сфері фінансових технологій, однак багато країн, наприклад, Китай, залишаються суворими щодо використання деяких аспектів фінтеху, таких як криптовалюти.

Таким чином, документ "Fintech 2023" надає глибоке уявлення про те, як різні країни впроваджують регуляції у фінтех-секторі, та демонструє важливість технологічних інновацій у трансформації глобальних фінансових ринків.

https://gpg-pdf.chambers.com/link/561673/i/

Довідник з платежів в Індії - 2024-2029

Документ "The Indian Payments Handbook 2024-2029" є всебічним дослідженням динаміки розвитку цифрових платежів в Індії, зокрема впровадження нових інструментів та зростання ринку платежів. Він аналізує інфраструктуру цифрових платежів, як-от UPI, кредитні картки, та FASTag, і підкреслює ключові тенденції, такі як зростання обсягу транзакцій через UPI, яке прогнозується втричі до 2029 року, та значне збільшення кількості кредитних карток. Описано також роль державних ініціатив у стимулюванні безготівкових платежів та фінансової інклюзії. **Документ акцентує на технологічних інноваціях, включаючи використання біометричних даних для верифікації транзакцій, а також зусилля з розширення інфраструктури для прийому платежів у сільських регіонах**.

Ключові висновки:

1. **Швидке зростання UPI:** Система UPI залишається ключовим драйвером зростання цифрових платежів в Індії. Її популярність і використання зростають, і очікується, що обсяг транзакцій через UPI зросте на понад 200% до 2029 року. Це пов'язано з легкістю використання системи, широким її охопленням та безперебійною інтеграцією з іншими платіжними системами. Широке впровадження цієї системи не тільки підвищує фінансову інклюзію, але й забезпечує більшу зручність для користувачів у всіх регіонах країни, включаючи сільські райони.
2. **Інтеграція кредитних карток з UPI:** Інновації, такі як інтеграція кредитних карток з UPI, дозволяють користувачам здійснювати більше різних типів платежів за допомогою вже існуючих платформ. Це підсилює позиції кредитних карток на ринку і водночас розширює можливості для користувачів, які можуть використовувати кредитні засоби через UPI. Це також забезпечує більшу гнучкість для мерчантів, що допомагає їм залучати більше клієнтів.
3. **Зміцнення інфраструктури для мерчантів:** Збільшення кількості точок продажу та впровадження нових технологічних рішень, таких як QR-коди та звукові скриньки, спрощують та розширюють можливості для прийому безготівкових платежів. Ці інновації зокрема допомагають збільшити доступ до фінансових послуг у віддалених сільських регіонах, де традиційні банківські інструменти менш поширені.
4. **Державні ініціативи та фінансова інклюзія:** Індійський уряд через ініціативи, як-от Bharat Bill Payment System (BBPS), продовжує стимулювати розвиток безготівкових платежів. Ці зусилля спрямовані на розширення доступу до фінансових послуг для населення, особливо тих, хто раніше не мав такого доступу. Це допомагає збільшити рівень фінансової інклюзії в країні та сприяє економічному розвитку.
5. **Нові технології у фінансових послугах:** Використання біометричних даних, таких як відбитки пальців та ідентифікація за обличчям, для підтвердження транзакцій підвищує безпеку платежів і зручність для користувачів. Біометрія забезпечує швидкий та безпечний доступ до фінансових послуг і зменшує ймовірність шахрайства. Інші технологічні рішення, такі як автоматизація процесів і штучний інтелект, також допомагають оптимізувати платіжні системи та поліпшують обслуговування клієнтів.

Ці висновки свідчать про те, що Індія продовжує швидко просуватися на шляху до повної цифровізації фінансового сектора. Стимулювання фінансової інклюзії, впровадження інноваційних технологій і активна підтримка уряду є основними факторами, що сприяють подальшому розвитку платіжної екосистеми країни.

https://www.pwc.in/assets/pdfs/indian-payment_handbook-2024.pdf

Незалежний аудит з питань протидії відмиванню коштів

Документ детально описує процес незалежних аудитів для забезпечення відповідності компаній вимогам законодавства щодо боротьби з відмиванням коштів (AML). Аудити спрямовані на перевірку, чи відповідають політики, контроль та процедури компанії стандартам, зокрема Положенням про відмивання грошей (MLR). **Процес складається з кількох етапів: перевірки політик і процедур, тестування знань персоналу, проведення файлових перевірок і надання звіту з рекомендаціями щодо покращення.** Документ підкреслює важливість підготовки до аудиту, залучення співробітників і вчасного впровадження змін.

Ключові висновки:

1. **Прозорість і відповідність вимогам регуляторів:** Незалежні AML-аудити допомагають компаніям не лише перевірити відповідність вимогам Положень про відмивання грошей, але й забезпечують підвищену прозорість у процесах. Важливо, що результати таких аудитів, особливо зовнішніх, можуть бути передані регуляторам, що збільшує відповідальність компаній за належне дотримання стандартів.
2. **Оцінка ефективності політик і процедур:** Ключовим завданням аудиту є перевірка відповідності політик і процедур чинним нормам MLR, а також оцінка їхньої ефективності. Аудитори не тільки вказують на недоліки, але й надають конкретні рекомендації щодо вдосконалення системи управління AML-ризиками. Особливу увагу приділяють таким аспектам, як належна перевірка клієнтів, моніторинг транзакцій, внутрішні інструкції та контрольні заходи.
3. **Важливість підготовки та залучення персоналу:** Успіх незалежного аудиту значною мірою залежить від підготовки та залучення співробітників. Відповідальні особи (MLRO, MLCO) мають підготувати всі необхідні документи та забезпечити взаємодію з аудиторською групою. Проведення тренінгів для персоналу на тему політик AML і процедур перед аудитом допомагає співробітникам краще підготуватися та продемонструвати знання та розуміння вимог.
4. **Етапи та методологія аудиту:** Процес аудиту включає кілька ключових етапів: початковий огляд політик і процедур, тестування їхньої ефективності через інтерв'ю зі співробітниками та аналіз справ, написання звіту з детальними рекомендаціями, а також фінальну перевірку на відповідність рекомендаціям. Ця багатоступенева процедура забезпечує комплексний підхід до оцінки AML-системи.
5. **Превентивний підхід та безперервне вдосконалення:** Документ наголошує на важливості превентивного підходу до незалежних аудитів, який полягає в тому, щоб не чекати на виявлення проблем під час перевірки, а вчасно виявляти та виправляти слабкі місця у системі управління AML до проведення аудиту. Окрім цього, компанії мають активно впроваджувати рекомендації аудиторів, а також регулярно переглядати та вдосконалювати свої політики та процедури для підтримки високого рівня відповідності.
6. **Тестування знань персоналу та файлові перевірки:** Важливою частиною аудиту є перевірка знань персоналу щодо процедур боротьби з відмиванням коштів, а також аналіз справ на предмет відповідності політикам AML. Аудитори перевіряють закриті кейси, щоб упевнитися, що всі ризики були правильно ідентифіковані, а також що процес моніторингу транзакцій був виконаний належним чином.
7. **Значення аудиторського звіту:** Після проведення аудиту компанії отримують звіт, який містить детальний огляд їхніх політик і процедур, а також рекомендації для покращення. Звіт також містить інформацію про конкретні положення MLR, які були перевірені, і де можливо виявлені недоліки. Компанії повинні вчасно впровадити ці рекомендації та забезпечити належний моніторинг їхньої ефективності.

Ці ключові висновки підкреслюють важливість незалежних AML-аудитів у підтримці високого рівня відповідності вимогам законодавства та забезпеченні ефективного управління ризиками в сфері боротьби з відмиванням коштів.

https://tealcompliance.com/wp-content/uploads/2023/08/AML-Independent-Audits_Digital_May-23.pdf

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Практичний погляд на ПВК/ФТ та дотримання санкцій

Посібник «Практичний погляд на ПВК/ФТ та дотримання санкцій» надає ґрунтовне висвітлення нормативно-правової бази у сфері протидії відмиванню коштів та фінансуванню тероризму. Автори акцентують увагу на важливості інтеграції комплаєнсу в загальну систему управління, надаючи практичні приклади для вирішення реальних проблем, особливо у контексті геополітичних змін. Книга також містить актуальні дані щодо регуляторних змін у Фінляндії та світі, допомагаючи професіоналам створювати надійні комплаєнс-програми в умовах сучасних викликів.

Для професіоналів, які орієнтуються у складному світі протидії відмиванню коштів (ПВК), фінансуванню тероризму (ФТ) та дотриманню санкцій, «Практичний погляд на ПВК/ФТ та дотримання санкцій» від Ацо Андерсена та Сари Салмели є обов'язковим до прочитання.

Цей ґрунтовний посібник надає:

- Всебічне висвітлення нормативно-правових актів у сфері протидії відмиванню коштів та фінансуванню тероризму з акцентом на те, як інтегрувати комплаєнс у вашу загальну систему.
- Практичні приклади, які допоможуть фахівцям застосовувати стратегії для вирішення реальних проблем, особливо в умовах розвитку геополітичних подій.
- Актуальна інформація про останні регуляторні зміни у Фінляндії та в усьому світі, а також експертний аналіз тенденцій ухилення від санкцій та комплаєнсу.
- Книга надає фінансовим установам та іншим регульованим суб'єктам інструменти, необхідні для того, щоб випереджати нові загрози та забезпечувати надійні комплаєнс-програми. Незалежно від того, чи ви тільки починаєте працювати в цій сфері, чи прагнете вдосконалити свої знання, цей посібник пропонує дієві стратегії та важливу інформацію, яка допоможе в сучасному регуляторному середовищі.

https://advisense.com/2024/08/26/practical-take-on-aml-ctf-and-sanctions-compliance/

Децентралізоване управління криптовалютою? Прозорість і концентрація в процесі прийняття рішень в Ethereum

Документ надає детальний аналіз управління блокчейном Ethereum, зокрема прозорість процесів прийняття рішень, концентрацію влади та вплив на ціни токенів. Автори досліджують механізм створення та обговорення Ethereum Improvement Proposals (EIPs), відкриту участь громади, а також роль невеликої групи впливових авторів у формуванні протоколу. Вони виявляють, що хоча процес є відкритим, значна частина пропозицій подається невеликою кількістю ключових осіб, що зосереджує владу у їхніх руках.

Ключові висновки:

1. **Прозорість управління в Ethereum:** Процес подання та обговорення EIPs є відкритим для широкого загалу, що забезпечує прозорість і доступність змін для всіх учасників мережі. Основна платформа для обговорення пропозицій — GitHub, де кожен користувач може взяти участь у дискусії та пропонувати

свої ідеї. Це створює відкриту екосистему для розвитку блокчейну, спрямовану на постійні вдосконалення протоколу.

2. **Концентрація влади:** Незважаючи на прозорість процесу, більшість ключових змін вносять кілька впливових осіб. Документ виявляє, що понад 68% усіх основних (Core) EIPs подані лише 10 авторами. Це свідчить про певну централізацію влади в системі, що потенційно суперечить базовій ідеї децентралізації, яка є основоположною для блокчейн-технологій. Така концентрація влади може обмежити справжню демократичність управління мережею.
3. **Вплив на ціни токенів:** У документі описано, як прийняття важливих пропозицій (особливо Core EIPs) впливає на ринкову вартість токенів Ethereum. Після затвердження ключових EIPs часто спостерігається підвищення ціни на токен Ether, що підкреслює вагомість процесу управління для інвесторів і трейдерів. Встановлено, що середній приріст ціни становить близько 12% у період після оголошення остаточних рішень щодо EIPs.
4. **Потенційна загроза централізації:** Документ звертає увагу на ризик централізації, пов’язаний не лише з авторами EIPs, а й із клієнтськими розробниками, постачальниками оракулів та компаніями, що випускають стейблкоїни. Ці групи відіграють ключову роль у функціонуванні мережі і, відповідно, можуть стати точками централізації влади. Якщо не контролювати їхній вплив, це може суперечити основним принципам децентралізації, закладеним у блокчейні.
5. **Регуляторні виклики:** У документі також наголошується на тому, що через стрімкий розвиток блокчейн-технологій, такі процеси як управління через EIPs, можуть привертати увагу регуляторів. Це особливо актуально у випадку змін, що можуть суттєво вплинути на фінансові аспекти або безпеку мережі. Участь різних країн у розробці глобальних стандартів може забезпечити більше прозорості та зменшити ризики, пов'язані з централізацією управління.

Таким чином, документ підкреслює важливість балансу між відкритістю процесу прийняття рішень та потребою уникнути централізації. Він також вказує на необхідність подальшого розвитку механізмів контролю, щоб забезпечити дотримання принципів децентралізації та прозорості в управлінні блокчейн-мережами, такими як Ethereum.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4691000

Боротьба з відмиванням коштів у сфері торгівлі та у сфері послуг

Егмонтська група, завдяки своїм робочим групам з обміну інформацією (IEWG) та технічної допомоги і навчання (TATWG), оголосила про запуск нового тренінгу щодо протидії відмиванню коштів у сфері торгівлі (TBML) та послуг (SBML). Це включає навчальне відео (англійською та французькою) та онлайн-курс за підтримки FINTRAC – Підрозділу фінансової розвідки Канади. Ці ресурси допоможуть підрозділам фінансової розвідки та їхнім партнерам ефективніше виявляти та боротися з цими складними формами економічних злочинів.

Тренінг щодо протидії відмиванню коштів у сфері торгівлі (TBML) та послуг (SBML), розроблений Егмонтською групою, буде корисним для підрозділів фінансової розвідки, органів фінансового моніторингу, правоохоронних органів, банківських установ, а також фахівців, які займаються протидією відмиванню коштів та фінансуванню тероризму. Участь у цьому навчанні допоможе цим суб'єктам покращити свої знання та навички у виявленні, запобіганні та розслідуванні економічних злочинів, пов'язаних з торгівлею та наданням послуг.

http://surl.li/lekwwl

ІНШІ НОВИНИ

Роль фінансових установ у боротьбі з відмиванням коштів, пов’язаних із криптовалютою

Стаття обговорює роль традиційних фінансових установ у боротьбі з відмиванням коштів та фінансовими злочинами, пов'язаними з криптовалютами. Основний посил полягає в тому, що якщо банки не почнуть активно займатися криптовалютами та їх регулюванням, вони стануть вразливими до ризиків, що виникають у цій сфері. Автори наголошують на важливості співпраці між фінансовими установами, регуляторами та технологічними компаніями для виявлення й запобігання незаконним транзакціям. Технології, як-от блокчейн-аналітика, можуть допомогти у відстеженні підозрілих операцій, а також у впровадженні регуляторних вимог.

У статті також підкреслюється, що криптовалюти та пов'язані з ними ризики розвиваються швидко, тому фінансові установи повинні швидко адаптуватися, щоб не втратити контроль над ситуацією.

http://surl.li/wctwmi

Відмивання грошей у світовій Індустрії кібер-шахрайства

Стаття під назвою "Moving Bricks: Money-Laundering Practices in the Online Scam Industry" досліджує практики відмивання грошей у кіберзлочинній індустрії, особливо в контексті Китаю та Південно-Східної Азії. Вона розглядає механізм, відомий як "переміщення цеглин" ("moving bricks"), коли брокери допомагають кібер-шахраям пересувати гроші через складні фінансові структури, зокрема використовуючи криптовалюту, банківські рахунки та послуги, які спеціалізуються на оперуванні рахунками для відмивання грошей.

Основні моменти

"Moving bricks" :

- У цьому контексті термін "переміщення цеглин" відображає діяльність, яка полягає в перерахуванні грошей через банківські рахунки та криптовалютні платформи для приховання джерела коштів.
- Цей процес використовується для "арбітражу" – виграшу на різниці в цінах активів на різних платформах, однак це також означає відмивання грошей, отриманих незаконним шляхом.

Роль Telegram та анонімних платформ:

- Telegram використовується як основний засіб комунікації між різними гравцями кібер-злочинної індустрії, що включає шахраїв, брокерів та операторів банківських рахунків. Публічні та приватні групи в Telegram полегшують проведення операцій, рекрутування партнерів та обмін інформацією.

"Гейтові" компанії та їхні функції:

- "Гейтові" компанії (gateway companies), виступають посередниками між шахраями, допомагаючи здійснювати транзакції через їхні системи. Вони забезпечують не лише комісійні послуги, а й арбітраж у випадках спорів.
- Такі компанії також виступають гарантом транзакцій, що мінімізує ризики втрати грошей для обох сторін.
- Гейтові компанії займаються керуванням ризиками, пов'язаними з заморожуванням рахунків і контролем державних установ. Розробляються спеціальні процедури для мінімізації операційних ризиків.
- Якщо під час транзакцій виникають спори, зокрема через замороження рахунків, гейтові компанії забезпечують процес арбітражу, збираючи докази від обох сторін і допомагаючи вирішити конфлікт.

Адаптація під різні регуляторні умови:

- Злочинці адаптують свої методи під вимоги законодавства країн, у яких вони працюють. Наприклад, у Китаї, через посилення заходів проти відмивання грошей, вони перейшли до використання фізичних банківських операцій, таких як зняття та переведення готівки.

Роль Камбоджі:

- Камбоджа є важливим центром для таких операцій через вільний обіг доларів США. У статті підкреслюється, що легітимність таких компаній може бути підкріплена місцевими ліцензіями, хоча їх діяльність пов'язана з міжнародними кіберзлочинними мережами.

Висновки

- Індустрія кібер-шахрайства є складною мережею, яка включає не лише шахраїв, а й численних посередників, які полегшують відмивання грошей. Ця система оперує через взаємодію з локальними та глобальними фінансовими інституціями, а також технологічними платформами, такими як Telegram.
- Гейтові компанії є ключовими посередниками, які забезпечують легалізацію доходів кіберзлочинців, використовуючи легальні банківські та фінансові інструменти, що ускладнює контроль та боротьбу з такими мережами.

http://surl.li/xfdiwc

Клімат, корупція і кока: Чому Центральна Америка стає новим центром нарковиробництва

Стаття присвячена актуальній проблемі поширення вирощування коки в Центральній Америці. Вона досліджує причини цього явища, його наслідки та потенційні загрози для регіону.

Це дослідження має важливе значення для розуміння причин поширення вирощування коки в Центральній Америці та розробки ефективних стратегій боротьби з цією проблемою. Результати дослідження можуть бути використані урядами країн регіону, міжнародними організаціями та громадянським суспільством для розробки політики, спрямованої на боротьбу з наркоторгівлею та забезпечення сталого розвитку регіону.

Ключові тези статті

- **Поширення вирощування коки:** Дослідження показало, що кліматичні та ґрунтові умови в деяких частинах Центральної Америки ідеально підходять для вирощування коки. Країни

Центральної Америки (Гондурас, Гватемала) мають сприятливі умови для вирощування коки, включаючи родючі землі.

- **Вплив боротьби з наркотиками:** Інтенсивна боротьба з наркотиками в традиційних районах вирощування коки (Колумбія, Перу) призвела до переміщення виробництва в інші регіони, зокрема в Центральну Америку.
- **Роль корупції:** Автори зазначають, що поширення вирощування коки залежить не тільки від природних умов, але й від соціальних, економічних та політичних факторів в регіоні. Корупція серед місцевих еліт сприяє поширенню кокаїнового виробництва, оскільки вона дозволяє наркоторговцям діяти безкарно.
- **Економічні фактори:** Бідність населення та відсутність альтернативних джерел доходу спонукають людей займатися вирощуванням коки.
- **Наслідки для регіону:** Поширення вирощування коки може призвести до зростання злочинності, насильства, корупції та руйнування соціальної структури в регіоні.
- **Необхідність нових стратегій:** Автори дослідження підкреслюють, що традиційні методи боротьби з наркотиками не є ефективними і вимагають розробки нових стратегій, які б враховували соціальні, економічні та політичні фактори.

Висновки

- **Проблема має комплексний характер:** Поширення вирощування коки в Центральній Америці є результатом взаємодії природних, соціальних, економічних та політичних факторів.
- **Необхідність комплексного підходу:** Для ефективної боротьби з наркоторгівлею необхідно розробляти комплексні стратегії, які б включали не тільки боротьбу з вирощуванням коки, але й вирішення соціальних проблем, розвиток економіки та боротьбу з корупцією. Альтернативні стратегії розвитку, спрямовані на боротьбу з бідністю, створення нових робочих місць і зміцнення державних інститутів, є ключем до успіху в цій боротьбі.
- **Міжнародне співробітництво:** Для вирішення цієї проблеми необхідна тісна співпраця між країнами регіону, міжнародними організаціями та громадянським суспільством.

http://surl.li/bunxen

Кібербезпека та фінансова розвідка

Президент FATF б’є на сполох щодо кібершахрайства: найприбутковіший фінансовий злочин у світі

Президент FATF Еліза де Анда Мадразо у статті для Business Resilience попереджає про зростаючу загрозу, яку становить кібершахрайство, яке зараз стало найпоширенішою формою економічної злочинності в усьому світі. Вона підкреслила:

> «*Однієї кібербезпеки недостатньо. Щоб перемогти кіберзлочинність, ми повинні використовувати дані фінансової розвідки для виявлення та ліквідації злочинних мереж і повернення вкрадених коштів*».

Глобальна оцінка фінансового шахрайства Інтерполу, травень 2024 року, показує тривожне зростання технологічного шахрайства, спрямованого проти жертв у всьому світі:

- Африка: розвиток мобільного банкінгу призвів до зростання BEC, фішингу та шахрайства з криптовалютою. Зокрема, шахрайство з гібридними криптоінвестиціями поширене в Західній і Південній Африці
- Америка: пандемія спричинила зростання фінансового шахрайства в Інтернеті, використовуючи попит на медичні товари. Операція Інтерполу Turquesa V також виявила торгівлю людьми синдикатами Південно-Східної Азії

- Азія: швидке зростання цифрових ринків підвищило ризик фінансового шахрайства, особливо шахрайства, пов'язаного з криптовалютою, і телекомунікаційного шахрайства шляхом видавання себе за орган влади. Користувачі віком від 30 до 49 років в основному вразливі через соціальні мережі та платформи обміну повідомленнями
- Європа: понад 80% зареєстрованих випадків шахрайства пов'язані з кіберпросторами, націленими на мобільні додатки з такими схемами, як інвестиційне шахрайство та BEC. Оскільки такі технології, як deepfakes, стають все більш поширеними, прогнозується зростання шахрайства

У відповідь FATF запровадила реформи для підвищення глобальних стандартів повернення викрадених активів, зосередившись на використанні технологій для боротьби з фінансовими злочинами. Ці зусилля включають поширення правил боротьби з відмиванням коштів на криптоактиви, оновлення прозорості платежів і підвищення безпеки транскордонних транзакцій.

Країнам наполегливо пропонується віддати пріоритет відстеженню незаконних фінансових потоків у рамках своїх стратегій боротьби з кіберзлочинністю.

http://surl.li/xqkwyi

Розробники Tornado Cash готуються до суду за роль платформи у відмиванні коштів на суму понад 1 мільярд доларів

Стаття розповідає про майбутній судовий процес над розробниками платформи Tornado Cash, Романом Штормом та Романом Семеновим, яких звинувачують у сприянні відмиванню понад 1 мільярда доларів США через їхню криптовалютну платформу для змішування транзакцій. Справу порушили після того, як уряд США виявив, що Tornado Cash використовувалася для проведення нелегальних операцій, зокрема для угрупування Лазаря, яке має зв'язки з Північною Кореєю. Роман Шторм намагався оскаржити звинувачення, але суддя відхилив його клопотання, і тепер він чекає судового процесу, запланованого на грудень 2024 року. Роман Семенов залишається в розшуку, уникаючи арешту.

У статті підкреслюється, що платформа Tornado Cash дозволяє користувачам змішувати криптовалютні транзакції, приховуючи сліди походження коштів, що часто використовується злочинцями для відмивання грошей. Це викликає серйозне занепокоєння у світових регуляторів, оскільки така анонімність ускладнює боротьбу з фінансуванням тероризму та незаконною діяльністю. Уряд США наполягає на тому, що Tornado Cash порушила норми про реєстрацію платіжних сервісів і стала одним із найбільших каналів відмивання грошей через криптовалюти.

Цей процес є частиною ширших зусиль урядів щодо контролю за криптосервісами, які сприяють нелегальній фінансовій діяльності. Використання Tornado Cash для маскування слідів незаконних коштів підкреслює важливість регуляторного нагляду у криптоіндустрії, а також загрозу, яку такі платформи можуть становити для глобальної безпеки.

http://surl.li/ngeuzw

Інші новини в сфері ПВК/ФТ

- Банки Великобританії матимуть право призупиняти платежі на термін до 4 днів, щоб дати їм більше часу для розслідування шахрайства. Зараз перекази мають бути оброблені або відхилені до кінця наступного робочого дня, але новий закон дозволить продовжити ще на 3 дні.

- Управління фінансової поведінки Великобританії оштрафувало Starling Bank на 29 мільйонів фунтів стерлінгів після виявлення недоліків у системах контролю за відмиванням грошей і санкцій.
- Суд Сінгапуру засудив колишнього міністра до 12 місяців ув'язнення за перешкоджання правосуддю та отримання подарунків на суму понад 300 тисяч доларів.
- Власник 11 незареєстрованих криптографічних банкоматів у Великобританії визнав себе винним у кількох звинуваченнях, пов’язаних із його бізнесом, включаючи шахрайство та відмивання коштів.
- Золоті злитки на суму 1,4 мільйона євро та 500 тисяч євро готівкою вилучили у 2 жінок з Дубліна, звинувачених у відмиванні коштів.
- Влада Аргентини заарештувала 4 осіб за переказ 1,8 мільйонів доларів у криптовалюті на віртуальний рахунок, пов’язаний з Хезболлою. Віртуальний гаманець отримав 34 перекази з березня по червень цього року, був позначений OFAC як підозрілий в контексті фінансування тероризму.
- Група російських компаній отримала дозвіл на використання криптовалют для китайського імпорту відповідно до пілотної правової бази. Ця ініціатива, яка контролюється центральним банком Росії та Міністерством фінансів, націлена на фірми, які працюють із продукцією подвійного призначення та стикаються з проблемами міжнародних платежів, зокрема з Китаєм.
- Загальний суд ЄС підтвердив заборону на надання юридичних послуг російським юридичним і фізичним особам. Рішення було прийнято після того, як нідерландська асоціація адвокатів Брюсселя, паризька адвокатура та інші попросили скасувати цей захід.

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

Останні тренди в KYC

✅ Інтеграція ШІ та машинного навчання

Останнім часом у процесі KYC відбулися більш значні зміни завдяки інтеграції штучного інтелекту (ШІ) і машинного навчання. У процесі перевірки особи, а також в оцінці ризиків ці технології роблять процес більш точним і ефективним.

✅ Цифрове підтвердження особи

Нова технологія перевірки особи в цифровому світі є однією з найбезпечніших і найефективніших тенденцій KYC. Ця тенденція включає в себе використання біометричних ідентифікаторів, таких як відбитки пальців або розпізнавання обличчя, щоб гарантувати точну перевірку ідентифікації своїх клієнтів.

✅ Технологія блокчейн

Роль блокчейну значно впливає на тенденції впровадження KYC. Він забезпечує розширене ведення записів, створюючи безпечний, незмінний запис про клієнта та відгуки про його транзакції. Використовуючи цю технологію, фінансові установи можуть отримати прямий, швидкий і безпечний доступ до свіжих чистих даних клієнтів.

✅ Моніторинг KYC і транзакцій у реальному часі

Країни визнали необхідність відстежувати тенденції впровадження KYC у режимі реального часу, а також транзакції з метою протидії фінансовим злочинам. Аналіз транзакцій у режимі реального часу може виявити випадки шахрайства або порушення системи боротьби з відмиванням коштів, щоб підвищити ефективність їх виявлення.

✅ Інтеграція регуляторних технологій (RegTech).

Підприємства використовують рішення RegTech, щоб краще та ефективніше керувати відповідністю KYC. Такі автоматизовані платформи відповідності та інструменти оцінки ризиків мінімізують можливість невідповідності.

✅ Постійний KYC і моніторинг

Постійний KYC (pKYC) — це новіша форма належної перевірки клієнта, за якої інформація про клієнта відстежується та оновлюється в режимі реального часу. Можливість запровадити pKYC є важливою порівняно з традиційними методами визначення тенденцій дотримання вимог KYC, оскільки вона дає змогу фінансовим установам, пов’язаним із FinTech, визначати будь-які зміни в профілі ризику в реальному часі.

✅ Рішення KYC на основі API

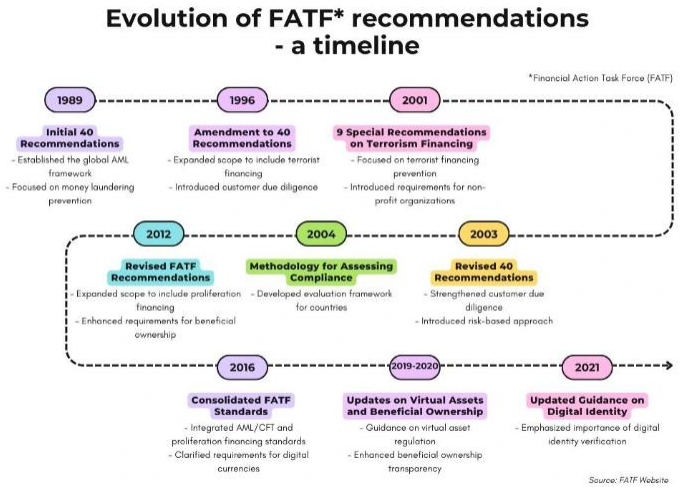
Інтеграція API зростає, оскільки вона може легко підключатися до існуючих і зовнішніх баз даних, покращуючи рішення KYC. Ці API допомагають швидко та зручно перевіряти особу клієнта та відповідність вимогам AML.

✅Децентралізовані рішення ідентифікації

З прогресом технологій у сфері блокчейну буде розроблено більше рішень для забезпечення децентралізованої ідентифікації для керування тенденціями KYC. Такі системи дозволяють особам гарантувати, що вони отримують регулярний контроль над своїми даними, водночас маючи можливість надати фінансовій установі облікові дані, які можна перевірити.

Еволюція рекомендацій FATF: хронологія

Група розробки фінансових заходів з протидії відмиванню коштів (FATF) формує глобальний ландшафт ПВК/ФТ з 1989 року.



1989: Початкові 40 рекомендацій

- Створено глобальну систему боротьби з відмиванням коштів
- Зосередження на запобіганні відмиванню коштів

1996: Поправка до 40 Рекомендацій

- Розширено сферу, щоб включити фінансування тероризму
- Запроваджено належну перевірку клієнта

2001: 9 спеціальних рекомендацій щодо фінансування тероризму

- Зосередження на запобіганні фінансуванню тероризму
- Запроваджено вимоги до неприбуткових організацій

2003: Переглянуто 40 рекомендацій

- Посилена належна перевірка клієнтів
- Запроваджено ризик-орієнтований підхід

2004: Методологія оцінки відповідності

- Розроблена система оцінювання для країн

2012: Переглянуті рекомендації FATF

- Розширено сферу дії, включаючи фінансування розповсюдження
- Посилені вимоги до бенефіціарної власності

2016: Консолідовані стандарти FATF

- Інтегровані стандарти ПВК/ФТ і фінансування розповсюдження
- Уточнені вимоги до цифрових валют

2019-2020: Оновлення щодо віртуальних активів і бенефіціарної власності

- Інструкції щодо регулювання віртуальних активів
- Покращена прозорість бенефіціарної власності

2021: Оновлені рекомендації щодо цифрових ідентифікаційних даних

- Наголошено на важливості цифрової перевірки особи