Серійний номер: ДСФМУ-ДК-2024-034
Листопад 2024

ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

Організоване шахрайство: глобальні виклики та стратегії протидії

Документ "Organized Fraud Issue Paper" підготовлений Відділом підтримки конференцій Управління Організованої Злочинності та Незаконного Обігу наркотиків ООН (UNODC). Цей документ аналізує природу організованого шахрайства, його зв'язок з організованою злочинністю та описує типи шахрайств, їхні характеристики, мотивацію правопорушників, а також способи протидії. Основна увага приділена впливу шахрайства на громадян, бізнес та держави, а також його глобальному поширенню завдяки технологіям.

Ключові моменти

- **Визначення шахрайства:**

Шахрайство — це використання обману для отримання фінансової чи матеріальної вигоди із завданням шкоди іншим. У багатьох юрисдикціях немає єдиного визначення шахрайства, що ускладнює його кримінальне переслідування, а використання технологій (кіберзлочини) значно розширило масштаби шахрайства.

- **Роль організованих злочинних груп:**

Злочинні групи можуть варіюватися від локальних мереж до міжнародних кіберзлочинних альянсів. Структура таких груп часто адаптується до конкретного типу шахрайства.

- **Типи шахрайств:**
  - Шахрайство з товарами та послугами (онлайн-магазини підробок).
  - Інвестиційні шахрайства (фінансові піраміди, фальшиві інвестиції).
  - Шахрайства з ідентифікацією (викрадення персональних даних).
  - Шахрайства, пов'язані з довірою (романтичні шахрайства, підроблені робочі пропозиції).
  - Шахрайства в бізнесі (маніпуляції контрактами, корпоративні змови).

- **Фактори, які сприяють шахрайству:**
  - Технології полегшують масштабування злочинів.
  - Використання мас-маркетингу та соціальних медіа для маніпуляцій.
  - Відмивання коштів для легалізації здобутих активів.

- **Міжнародна відповідь:**

Увага приділяється превентивним заходам, переслідуванню злочинців та захисту постраждалих. Рекомендації включають покращення співпраці між державами, посилення законодавства та розвиток технологій для ідентифікації шахрайств.

Висновки

- **Глобальна загроза:** Організоване шахрайство є серйозною проблемою, що негативно впливає на економіку, довіру до законодавства та суспільний порядок.
- **Необхідність комплексної стратегії:** Ефективна протидія потребує інтегрованого підходу, що включає превенцію, міжнародну співпрацю, розробку типологій шахрайства та застосування сучасних технологій.
- **Роль жертв:** Багато випадків шахрайства залишаються нерозкритими через недостатнє звітування жертв, що потребує покращення комунікації та довіри до правоохоронних органів.

http://surl.li/olfemo

Оцінка Стратегічної Розвідки

Документ від Companies House є комплексним аналізом ключових загроз та викликів, пов'язаних із використанням корпоративних структур у Великій Британії для незаконної діяльності. Він **акцентує увагу на впровадженні нових повноважень після прийняття Закону про економічну злочинність і прозорість корпорацій (Economic Crime and Corporate Transparency Act) 2023**, який трансформує роль Companies House із пасивного реєстратора у проактивного захисника економічної системи. **Основний акцент зроблено на відмиванні коштів, ухиленні від сплати податків, використанні корпоративних структур для шахрайства, організованій злочинності та сучасному рабстві**. Нові механізми, такі як Реєстр іноземних юридичних осіб (ROE), покликані забезпечити прозорість бенефіціарної власності нерухомості та протидіяти використанню корпоративних структур для обходу санкцій. Аналіз загроз охоплює зловживання адресами, особистими даними, масові реєстрації компаній і створення фіктивних директорів. У документі наводяться приклади зловживань, такі як шахрайство з Bounce Back Loans, а також виявлення кіберзагроз і ризиків від використання сучасних технологій злочинними угрупованнями. Зазначено необхідність міжвідомчої співпраці та використання сучасних цифрових інструментів для забезпечення ефективного контролю. Компанія стикається з викликами, пов'язаними із загрозами кіберзлочинності, «фінансового туризму» та зловживанням професійними послугами для обходу регуляторних норм.

Ключові висновки:

1. **Посилення ролі Companies House завдяки новим повноваженням.**

Прийняття ECCT Act 2023 надало Companies House можливість не лише реєструвати компанії, а й перевіряти достовірність даних, видаляти чи виправляти оманливу інформацію. Це забезпечує вищий рівень прозорості та запобігає використанню корпоративних структур для незаконної діяльності, таких як відмивання коштів або ухилення від сплати податків.

2. **Відмивання коштів через корпоративні структури залишається серйозною загрозою.**

Особливу увагу приділено схемам із залученням іноземних компаній, що купують нерухомість у Великій Британії для приховування бенефіціарної власності. Очікується, що нові команди з аналізу, фінансовані через збори за економічну злочинність, допоможуть глибше зрозуміти механізми зловживань.

3. **Реєстр іноземних юридичних осіб (ROE) – важливий інструмент прозорості.**

Впровадження ROE дозволило зробити прозорішим питання володіння нерухомістю у Великій Британії іноземними суб'єктами, обмеживши їхню можливість приховувати бенефіціарних власників. Це значно підвищує ефективність санкцій та допомагає боротися з відмиванням коштів через іноземні структури.

4. **Масові реєстрації компаній і «фінансовий туризм».**

Документ ілюструє тенденцію до масових реєстрацій компаній у Великій Британії, зокрема для уникнення податків, шахрайства або підвищення легітимності іноземних бізнесів. З'являється новий тренд «туризму для створення компаній», коли злочинні групи залучають іноземців для використання їхніх персональних даних у фіктивних реєстраціях.

5. **Шахрайство з державними програмами, такими як Bounce Back Loans.**

Пандемія COVID-19 стала каталізатором для зловживань державними програмами підтримки. Документ наводить приклади, коли компанії використовували фіктивні дані для отримання кредитів, які ніколи не були повернуті.

6. **Кіберзагрози та використання сучасних технологій.**

Кіберзагрози та атаки на критичну інфраструктуру залишаються однією з ключових проблем. У документі зазначено, що відсутність належної уваги до кібербезпеки в минулому може зробити Companies House ціллю для атак, що загрожує репутації організації та економіці Великої Британії загалом.

7. **Ризики від використання професійних послуг і формування агентів.**

Деякі фахівці, такі як бухгалтери або агенти з реєстрації, можуть сприяти зловживанням, навмисно чи через недбалість. Впровадження нового статусу авторизованих корпоративних сервіс-провайдерів (ACSPs) дозволить покращити регулювання та прозорість у цій сфері.

8. **Необхідність міжвідомчої співпраці.**

Боротися з масштабними зловживаннями можливо лише за умови тісної координації з іншими органами влади та міжнародними партнерами. Companies House планує посилити свою взаємодію з національними й глобальними гравцями у сфері протидії економічній злочинності.

Цей документ підкреслює, що нові повноваження та стратегічні ініціативи Companies House є лише початком роботи над усуненням значних ризиків і загроз у корпоративному секторі Великої Британії.

http://surl.li/gnkqvp

Рекомендації для організацій щодо злочину, пов'язаного з нездатністю запобігти шахрайству

Документ пояснює положення щодо нового злочину у Великобританії - «нездійснення запобігання шахрайству», передбаченого Законом про економічну злочинність та корпоративну прозорість 2023 року (Economic Crime and Corporate Transparency Act 2023). **Мета документа — допомогти великим організаціям розробити ефективні процедури для запобігання шахрайству, а також забезпечити дотримання законодавчих вимог.**

У документі викладено ключові аспекти нового закону, зокрема:

- Організації несуть відповідальність за шахрайство, скоєне їхніми працівниками, агентами чи дочірніми структурами, якщо це було зроблено для отримання вигоди організації чи її клієнтів, а організація не мала «розумних процедур запобігання шахрайству».
- Наведено визначення «великих організацій», які підпадають під дію закону, та типи шахрайства, які охоплюються цим злочином (наприклад, шахрайство шляхом подання неправдивої інформації, зловживання посадою тощо).

- Визначено принципи, які організації мають враховувати при розробці процедур запобігання шахрайству: високий рівень зобов'язань керівництва, оцінка ризиків, пропорційні заходи, належна перевірка, комунікація та навчання, моніторинг і перегляд.

Документ надає практичні рекомендації щодо впровадження антикорупційних процедур, зокрема: як аналізувати ризики, адаптувати механізми до особливостей бізнесу, навчати персонал, використовувати технології для моніторингу та впроваджувати санкції за порушення. Також підкреслюється важливість підтримки культури нетерпимості до шахрайства на всіх рівнях організації.

Розглядаються потенційні сценарії шахрайства, методи ідентифікації ризиків, інструменти належної перевірки та процедури реагування у випадку виявлення порушень. Зазначено, що організації повинні проводити регулярні оцінки своїх процедур і мати чіткі механізми документування.

Ключові висновки:

1. **Підвищення відповідальності організацій за відсутність запобігання шахрайству.**

Закон про економічну злочинність та корпоративну прозорість 2023 року вводить новий злочин — «нездійснення запобігання шахрайству», який зобов'язує організації впроваджувати ефективні заходи для запобігання шахрайським діям їхніх працівників, агентів або дочірніх компаній. У разі невиконання цих вимог компанія може бути притягнута до відповідальності незалежно від фактичної участі керівництва у шахрайських діях. Це створює новий стандарт корпоративної відповідальності, спрямований на підвищення прозорості та чесності у діловій практиці.

2. **Широкий спектр форм шахрайства, охоплений законодавством.**

Закон охоплює численні види шахрайства, включаючи:

- Подання неправдивої інформації для отримання фінансових вигод.
- Зловживання посадою, наприклад, використання службового становища для отримання неправомірної вигоди.
- Фальсифікацію облікових даних і документів.

Це підкреслює необхідність системного підходу до оцінки ризиків у всіх аспектах діяльності організації, від бухгалтерського обліку до маркетингу та взаємодії з підрядниками.

3. **Пропорційний і ризик-орієнтований підхід до запобігання шахрайству.**

Законодавство передбачає, що організації повинні адаптувати процедури запобігання шахрайству до специфіки своєї діяльності. Це означає, що великі транснаціональні корпорації та невеликі місцеві компанії повинні використовувати різні підходи. Організації мають проводити оцінку ризиків на основі таких факторів, як масштаб діяльності, характер бізнесу, рівень взаємодії з посередниками та історія попередніх інцидентів. Пропорційність заходів забезпечує їхню ефективність без надмірного адміністративного навантаження.

4. **Зміцнення корпоративної культури нетерпимості до шахрайства.**

Документ підкреслює, що ключовим елементом запобігання шахрайству є створення культури етики та прозорості на всіх рівнях організації. Керівництво має активно демонструвати нетерпимість до будь-яких форм шахрайства, інтегруючи антикорупційні політики у всі аспекти управління. Це включає створення механізмів для безпечного повідомлення про порушення, регулярне навчання співробітників та заохочення відкритої комунікації з питань етики.

5. **Регулярний моніторинг і перегляд процедур.**

Процедури запобігання шахрайству повинні бути динамічними та постійно переглядатися. Організації мають враховувати зміни у своєму бізнес-середовищі, такі як нові законодавчі вимоги, технологічні зміни чи нові ризики, які можуть виникнути через глобальні економічні чи політичні тенденції. Регулярний моніторинг дозволяє виявляти слабкі місця у процедурах і вчасно впроваджувати вдосконалення.

6. **Впровадження навчання та комунікації для персоналу.**

Документ наголошує на важливості навчання всіх працівників щодо політик і процедур запобігання шахрайству. Це включає регулярні тренінги, які підвищують обізнаність щодо ризиків шахрайства, та комунікаційні кампанії, що підкреслюють важливість етики у роботі. Особливу увагу слід приділити працівникам, які працюють у зонах підвищеного ризику, таких як відділи закупівель, продажів чи фінансів.

7. **Міжнародний контекст і координація з іншими юрисдикціями.**

Багато організацій діють у глобальному масштабі, тому їхні процедури запобігання шахрайству повинні враховувати не лише національні, але й міжнародні вимоги. Це передбачає врахування законів інших країн, гармонізацію політик між юрисдикціями та використання глобальних антикорупційних стандартів. Координація з міжнародними партнерами та регуляторами допомагає виявляти транскордонні шахрайські схеми.

8. **Використання технологій для підвищення ефективності.**

Інноваційні технології, такі як системи моніторингу транзакцій, штучний інтелект для аналізу ризиків чи автоматизація звітності, дозволяють значно підвищити ефективність процедур запобігання шахрайству. Організації, що впроваджують такі рішення, можуть більш ефективно ідентифікувати потенційні загрози та вчасно реагувати на них.

9. **Чіткий механізм документування та звітності.**

Документ підкреслює важливість належного документування всіх процедур запобігання шахрайству. Це включає ведення записів про оцінку ризиків, проведення навчань, впровадження політик і реагування на інциденти. Така прозорість дозволяє організації захиститися від звинувачень у недотриманні закону та демонструє її зобов'язання щодо запобігання шахрайству.

Ці висновки відображають багатовимірний підхід до запобігання шахрайству, який включає нормативні, організаційні та технологічні аспекти, забезпечуючи ефективну відповідність закону та захист бізнесу від фінансових і репутаційних ризиків.

http://surl.li/zbumas

Гайденс Комісії з фінансових послуг Гібралтару: сфера застосування DLT Framework

Документ є офіційним посібником, виданим Комісією з фінансових послуг Гібралтару (GFSC), який пояснює межі застосування регуляторної структури для постачальників технологій розподіленого реєстру (DLT Providers). **Основна мета документу — визначити, які види діяльності підпадають**

під регулювання згідно з Законом про фінансові послуги 2019 року (FSA) та регламентом DLT Providers 2020 року.

GFSC наголошує, що регуляторний підхід є принципово-орієнтованим і сфокусованим на результатах, що дозволяє забезпечити ефективність у сфері швидко змінюваних технологій. **Документ підкреслює важливість дотримання таких цілей, як зменшення системних ризиків, захист споживачів, підвищення довіри до ринку та боротьба з фінансовими злочинами**.

У документі визначаються ключові поняття, включаючи "зберігання" та "передачу" цифрової цінності, а також обговорюються критерії, які визначають, чи підпадає конкретна діяльність під регуляцію. GFSC також розглядає специфіку використання DLT для децентралізованих застосунків (DApps), смарт-контрактів, стейблкоїнів та інших форм віртуальних активів. Документ включає приклади видів діяльності, які підпадають або не підпадають під регуляцію, та пояснює важливість прозорості, дотримання регуляторних стандартів і уникнення подвійної регуляції.

Окремо аналізується вплив рекомендацій FATF на розробку DLT Framework, а також забезпечення відповідності стандартам боротьби з відмиванням коштів та фінансуванням тероризму. Документ спрямований на забезпечення балансу між інноваціями та регуляторними вимогами, що дозволяє розвивати безпечне середовище для DLT-операторів і їх клієнтів.

Ключові висновки:

1. **Принципово-орієнтований та гнучкий підхід до регулювання DLT**

GFSC застосовує регуляторну модель, яка базується на принципах, а не на жорстких правилах. Цей підхід дозволяє адаптувати регулювання до швидкозмінних технологій у сфері розподілених реєстрів. Гнучкість такої моделі забезпечує баланс між інноваціями та безпекою, дозволяючи індустрії розвиватися без зайвих обмежень, але в межах відповідних стандартів. Завдяки цьому Гібралтар зберігає свою конкурентоспроможність як юрисдикція, сприятлива для технологічних інновацій.

2. **Фокус на захисті споживачів і підтримці довіри до ринку**

Одним із ключових завдань DLT Framework є створення прозорого та безпечного середовища для взаємодії споживачів і провайдерів. GFSC забезпечує, щоб компанії, які працюють у сфері DLT, мали чіткі політики щодо управління ризиками, дотримувалися вимог до захисту даних клієнтів та надавали точну інформацію про послуги. Це сприяє підвищенню довіри до ринку та мінімізує ризики для кінцевих користувачів.

3. **Чітке визначення меж регуляції для різних видів діяльності**

GFSC регулює діяльність, пов’язану зі зберіганням та передачею цінності іншої особи з використанням DLT. Наприклад, біржі криптовалют, послуги стейблкоїнів або цифрові гаманці зазвичай підпадають під регулювання. У той же час діяльність, яка не передбачає прямого зберігання чи управління цінністю (наприклад, розробка відкритого коду для DLT), не регулюється. Це забезпечує чіткість для бізнесу щодо їхньої відповідності регуляторним вимогам.

4. **Регулювання децентралізованих застосунків (DApps) і смарт-контрактів**

DApps і смарт-контракти можуть підпадати під регуляцію, якщо вони мають централізований контроль або приносять прибуток розробникам. Наприклад, якщо DApp виконує роль посередника для транзакцій або контролює доступ до сервісів, це може вважатися діяльністю, що регулюється. GFSC також аналізує вплив розробників на функціональність DApps і їхню роль у транзакціях для визначення відповідності регуляторним стандартам.

5. **Імплементація стандартів FATF у регуляторну практику GFSC**

GFSC активно враховує рекомендації FATF щодо боротьби з відмиванням коштів та фінансуванням тероризму у своїй регуляторній моделі для DLT. Провайдери зобов'язані дотримуватися вимог до ідентифікації клієнтів (KYC), моніторингу транзакцій та звітування про підозрілі операції. Це забезпечує відповідність Гібралтару міжнародним стандартам і підсилює його позиції як відповідальної юрисдикції.

6. **Уникнення подвійного регулювання для різних видів діяльності**

GFSC визначає, що деякі види діяльності можуть регулюватися іншими законодавчими актами, такими як Proceeds of Crime Act 2015. Це дозволяє уникнути дублювання регуляторних вимог і спрощує діяльність для компаній, що працюють у сфері DLT. Такий підхід забезпечує ефективне використання регуляторних ресурсів і зменшує адміністративне навантаження на бізнес.

7. **Підтримка інновацій при дотриманні регуляторних стандартів**

Документ акцентує увагу на важливості підтримки інноваційного середовища для компаній, які працюють з DLT. Провайдери отримують можливість експериментувати та впроваджувати нові рішення, дотримуючись базових стандартів безпеки, прозорості та управління ризиками. Це сприяє розвитку технологій і підтримує репутацію Гібралтару як інноваційного хабу для DLT.

8. **Забезпечення прозорості та звітності**

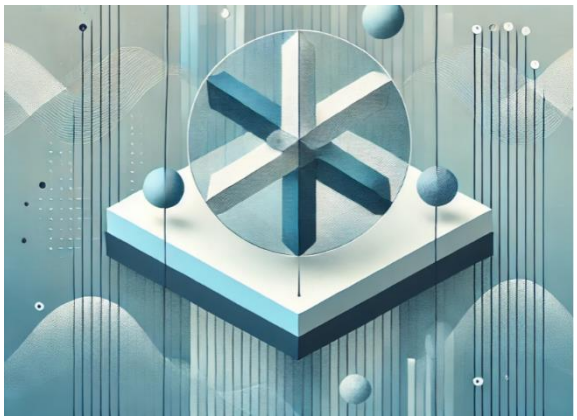
GFSC вимагає від DLT-провайдерів забезпечувати прозорість операцій та звітність перед регуляторними органами. Це включає ведення відповідної документації, регулярне інформування про виконання вимог і готовність до аудиту. Такий підхід дозволяє регулятору оперативно реагувати на ризики та зміцнює довіру до DLT-сектору.

Ці висновки демонструють, що регуляторний підхід GFSC створює умови для безпечного розвитку DLT-сектора, забезпечуючи баланс між інноваціями, захистом споживачів та міжнародними стандартами.

http://surl.li/aefskq

РЕГУЛЮВАННЯ

Розподіл Відповідальності між Banca D'italia та Consob Відповідно до MICAR



Документ представляє собою аналітичний огляд розподілу відповідальностей між Банком Італії та Комісією з цінних паперів та бірж (Consob) у рамках впровадження регулювання ринків криптоактивів (MiCAR) та оновлених положень щодо переказів коштів (TFR recast). Введення MiCAR встановлює єдину нормативну базу для ЄС щодо випуску, пропозиції та обслуговування криптоактивів, не охоплених існуючим фінансовим законодавством, зокрема активів, що базуються на токенах, електронних грошових токенів (EMTs), та діяльності постачальників послуг з криптоактивами (CASPs).

Банк Італії виступає компетентним органом з питань AML/CFT, пруденційного нагляду, управління кризами та контролю стабільності фінансової системи. Він відповідає за авторизацію та моніторинг EMT і ART (asset-referenced token) емітентів, а також за належне управління активами та внутрішніми процесами організацій.

Consob займається наглядом за прозорістю, чесною поведінкою на ринку, захистом інвесторів, а також запобігає зловживанню ринком. Вона також відповідає за контроль щодо випуску та обігу інших криптоактивів, які не класифікуються як EMT чи ART.

Окремо зазначається про систему розподілу відповідальностей для нагляду за CASPs, де пруденційний контроль здійснюється Банком Італії, а захист інвесторів і прозорість регулюються Consob.

Ключові висновки:

1. **Розподіл відповідальності між Банком Італії та Consob** базується на чіткому розмежуванні завдань відповідно до спеціалізації цих органів. Банк Італії зосереджується на забезпеченні стабільності фінансової системи через пруденційний нагляд, управління кризами та здійснення AML/CFT контролю. Його мандат охоплює нагляд за банківськими установами, фінансовими посередниками та іншими суб'єктами, залученими до випуску токенів ARTs і EMTs, а також постачальниками послуг з криптоактивами. Consob, у свою чергу, відповідає за захист інвесторів, забезпечення прозорості ринку, моніторинг поведінки учасників ринку та попередження ринкових зловживань. Такий підхід дозволяє ефективно розподілити функції для досягнення комплексного нагляду за криптоактивами та ринковими послугами.
2. **Регламент MiCAR запроваджує єдину нормативну основу для Європейського Союзу**, що дозволяє гармонізувати регулювання ринків криптоактивів. Це охоплює стандарти для випуску, обігу та обслуговування криптоактивів, які не підпадають під існуюче фінансове законодавство. MiCAR поєднано з оновленим Регламентом про переказ коштів (TFR recast), який розширює зобов'язання щодо супроводження переказів інформацією про відправника та отримувача на криптоактиви. Це дозволяє забезпечити їхню простежуваність і ефективно виявляти підозрілі транзакції. Завдяки цьому посилюється боротьба з відмиванням коштів і фінансуванням тероризму.
3. **Впровадження нових правил нагляду за постачальниками послуг з криптоактивами (CASPs)** є важливим елементом MiCAR. CASPs підлягають як пруденційному нагляду, так і контролю за прозорістю та справедливою поведінкою. Банк Італії здійснює моніторинг організаційних структур, капітальної достатності та управління ризиками CASPs, тоді як Consob забезпечує відповідність стандартам чесної поведінки та захисту інвесторів. Для CASPs передбачено як дозвільні процедури, так і спрощені механізми залежно від

ризиковості послуг, що дозволяє інтегрувати їх у регуляторну систему без шкоди для ефективності контролю.

4. **Акцент на AML/CFT аспектах регулювання криптоактивів свідчить про ризик-орієнтований підхід регуляторів**. AML/CFT контроль поширюється на банківські та фінансові установи, але виключає спеціалізованих емітентів ARTs, оскільки їхні операції не вважаються високоризиковими для відмивання коштів. Проте бізнес-моделі цих емітентів оцінюються регуляторами з точки зору потенційного впливу на ризики відмивання коштів та фінансування тероризму. Це дозволяє підтримувати баланс між розвитком ринку криптоактивів та забезпеченням безпеки фінансової системи.
5. **Регуляторна структура MiCAR передбачає гнучкі механізми моніторингу та реагування на ризики**. Завдяки спільному використанню повноважень між Банком Італії та Consob, регулятори можуть ефективно здійснювати інтервенції у разі виникнення ризиків для фінансової стабільності чи ринкової прозорості. Інструменти управління кризами, пруденційний нагляд і механізми попередження ринкових зловживань є частиною інтегрованого підходу, що забезпечує стабільність ринку криптоактивів, захист інвесторів та дотримання норм прозорості.

http://surl.li/rscrix

САНКЦІЇ

Як Росія обходить санкції: механізми адаптації економіки в умовах глобального тиску

Стаття CBS аналізує способи, якими Росія обходить міжнародні санкції, накладені після її вторгнення в Україну. У статті розглядаються основні стратегії обходу економічних обмежень, як-от використання "темного флоту" для транспортування нафти, зміна маршрутів торгівлі через треті країни, а також адаптація внутрішнього ринку для підтримки економіки під час конфлікту. Водночас аналізується ефективність санкцій та їхній вплив на економіку Росії.

Ключові моменти

- **Економічне зростання Росії:**

Незважаючи на санкції, МВФ прогнозує зростання економіки Росії на 3%, що перевищує показники США та Європи. Зростання підкріплене збільшенням державних витрат на військові потреби, хоча це спричинило інфляцію на рівні 9% та ставки кредитування до 19%.

- **Нафтовий сектор:**

Росія залишається третім найбільшим виробником нафти у світі, попри заборону G7 на імпорт її нафти. Запроваджено механізм "темного флоту", що включає приблизно 200 танкерів, які щодня перевозять мільйон барелів нафти, використовуючи маніпуляції сигналами та передачі нафти в морі.

- **Обхід санкцій:**

Операції з "темним флотом" дозволяють Росії продавати нафту вище встановленої ціни в $60 за барель. Індія та Китай стали ключовими покупцями російської нафти, при цьому її продукти (наприклад, бензин) з Індії експортуються в США.

- **Заміщення імпорту:**

Відхід західних компаній сприяв розвитку внутрішнього виробництва. Наприклад, локальні аналоги створено для багатьох відомих брендів. Зростання кількості малих і середніх підприємств у Росії досягло рекордного рівня.

- **Енергетична залежність США:**

США продовжують імпортувати російський збагачений уран для живлення атомних електростанцій. Незалежність у цьому питанні очікується лише через 6-7 років після масштабного розширення внутрішніх виробничих потужностей.

Висновки

- **Ефективність санкцій:** Санкції не змогли значно послабити економіку Росії у короткостроковій перспективі. Економіка залишається стійкою завдяки адаптації торгових маршрутів і внутрішньої економічної політики.
- **Вразливості російської економіки:** Попри видиме зростання, економічна стабільність підривається високою інфляцією, процентними ставками та залежністю від державних витрат.

- **Складність міжнародного контролю**: Виявлення та припинення діяльності "темного флоту" вимагає міжнародної координації, яка гальмується дипломатичними і економічними інтересами.
- **Адаптивність російської економіки**: Російський ринок демонструє гнучкість, заміщуючи імпорт і розвиваючи нові ланцюжки постачання. Це створює довгострокові виклики для західної санкційної політики.

http://surl.li/gvynfo

Міністерство торгівлі США націлене на мережі незаконних закупівель, через які здійснюються постачання російській армії

Документ є офіційним пресрелізом Бюро промисловості та безпеки США (BIS) від 30 жовтня 2024 року, в якому **викладаються заходи, спрямовані на протидію підтримці російської військової агресії проти України через заборонені мережі постачання. BIS додало 40 іноземних суб'єктів та 4 адреси до списку осіб, яким обмежено експорт (Entity List), та посилило обмеження для 49 інших суб'єктів, які вже перебували у цьому списку**. Нові суб'єкти розташовані у Китаї, Індії, Малайзії, Росії, Сингапурі, Туреччині, Естонії, Фінляндії, ОАЕ та Великій Британії. **Ці заходи спрямовані на запобігання доступу Росії до продукції американського походження, зокрема мікроелектроніки, хімічних прекурсорів та інших товарів, які можуть бути використані у військових цілях.**

Також були введені нові обмеження на експорт 9 хімічних прекурсорів, які Росія може використовувати для створення хімічної зброї та агентів для контролю масових заворушень. Ці дії викликані порушенням Росією положень Конвенції про хімічну зброю (CWC) через використання хімічних агентів як зброї проти українських військових. Рішення про доповнення Entity List ґрунтуються на підставах, пов'язаних із національною безпекою та зовнішньополітичними інтересами США, і приймаються міжвідомчим комітетом, до якого входять представники декількох ключових американських відомств.

Документ акцентує увагу на важливості стратегічного використання експортного контролю для уповільнення російської військової машини та демонструє готовність США працювати з міжнародними партнерами задля захисту національної безпеки та підтримки України.

Ключові висновки:

1. **Посилення експортного контролю для обмеження російських військових можливостей.**

США розширили та посилили експортні обмеження для суб'єктів, які сприяють зміцненню російської військової інфраструктури. Додатково 40 суб'єктів і 4 адреси внесено до списку Entity List через підозри в участі у незаконному постачанні товарів американського походження до Росії через треті країни, такі як Китай, Індія, Малайзія, ОАЕ, Туреччина, Естонія, Фінляндія, Сингапур і Велика Британія. Також для 49 суб'єктів, які вже перебували у списку, введено розширені обмеження, щоб унеможливити використання російськими закупівельними мережами товарів, зокрема мікроелектроніки, що мають критичне значення для російських військових потреб.

2. **Фокус на хімічних прекурсорах для протидії використанню хімічної зброї Росією.**

США запровадили нові обмеження на експорт 9 хімічних прекурсорів, які можуть бути використані у виробництві хімічної зброї або агентів для контролю масових заворушень. Такі дії зумовлені доведеним використанням Росією хімічної зброї, зокрема хлорпікрину, під час бойових дій проти України, що є порушенням Конвенції про хімічну зброю (CWC). Ці обмеження мають на меті

перешкоджати Росії у використанні хімічних речовин як засобу війни, навіть якщо їх первинне застосування може мати комерційний характер.

3. **Впровадження структурованого міжвідомчого підходу до прийняття рішень.**

Додавання суб'єктів до Entity List здійснюється міжвідомчим комітетом (ERC), до складу якого входять Міністерства торгівлі, оборони, енергетики, фінансів і державний департамент США. Цей процес передбачає узгоджений підхід до аналізу ризиків, пов'язаних із діяльністю суб'єктів, та прийняття колективних рішень щодо запровадження обмежень. Усі рішення про внесення нових суб'єктів приймаються більшістю голосів, тоді як виключення із списку можливе лише за одностайного рішення.

4. **Акцент на технологічних і геополітичних аспектах протидії Росії.**

Пресреліз підкреслює, що Росія є одним із основних викликів для національної безпеки США. Запровадження експортного контролю використовується як стратегічний інструмент для стримування технологічного прогресу Росії в галузях, критичних для її військової інфраструктури. Особлива увага приділяється протидії російським закупівельним мережам, що діють через треті країни, зокрема Китай, і намагаються обійти санкції.

5. **Демонстрація міжнародної рішучості у підтримці України.**

Цей пресреліз є частиною більш широких заходів США та їх союзників, спрямованих на стримування агресії Росії. Він підтверджує політичну рішучість США забезпечувати Україну не лише фінансовою та військовою допомогою, але й дипломатичними та регуляторними заходами, що перешкоджають доступу Росії до ключових ресурсів для ведення війни.

6. **Забезпечення глобального виконання санкцій та попередження обходу обмежень.**

США продовжують працювати з міжнародними партнерами для моніторингу та усунення шляхів обходу санкцій. Додавання нових адрес та компаній до Entity List спрямоване на подолання ризиків транспортування заборонених товарів через треті країни або використання російськими компаніями посередників для доступу до високотехнологічних товарів. Це демонструє глобальний підхід США до захисту санкційного режиму від маніпуляцій.

http://surl.li/tmhwdr

ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

Оновлення Basel AML Index 2024: Інтеграція ризиків шахрайства у глобальну методологію боротьби з відмиванням коштів

Документ описує оновлення методології Basel AML Index, що є інструментом оцінки ризиків відмивання коштів (AML) по всьому світу. Головним нововведенням 2024 року є включення показників шахрайства в методологію індексу. Це рішення зумовлене зростанням значущості шахрайства як злочину, що передує відмиванню коштів, а також його суттєвими соціальними та економічними наслідками. Оновлення будуть впроваджені в 13-му публічному виданні індексу, яке планують опублікувати 2 грудня 2024 року. Ці зміни також зачіпатимуть спеціалізовані версії індексу: Expert Edition і Expert Edition Plus.

Основні положення та ключові моменти

- **Шахрайство як зростаючий ризик:**

Згідно з даними з США, Великобританії, Швейцарії та Сингапуру, шахрайство є одним із провідних злочинів, пов'язаних з підозрілими транзакціями. У звіті США з оцінки ризиків відмивання коштів на 2024 рік зазначено, що шахрайство залишається найбільшим злочином, який генерує доходи, що підлягають відмиванню. Шахрайські схеми (інвестиційні, романтичні, авансові платежі) викликають серйозні наслідки для фінансових систем і звичайних громадян.

- **Технології як фактор ризику:**

Використання штучного інтелекту та криптовалют робить шахрайство більш складним для розслідування. У ініціативі FATF, INTERPOL та Egmont Group зазначено зв’язок між шахрайством та іншими формами злочинності, такими як торгівля людьми та фінансування розповсюдження зброї.

- **Практичний підхід:**

Basel AML Index інтегрує показники шахрайства із зазначенням їхніх обмежень. Дані будуть черпатися з Global Organized Crime Index у двох категоріях: Фінансові злочини (шахрайство, ухилення від сплати податків, розтрата). Кіберзлочини (шкідливе програмне забезпечення, хакінг, криптовалютне шахрайство).

- **Вагові коефіцієнти та зміни в структурі індексу:**

Показники шахрайства отримають вагу: 5% для фінансових злочинів і 2,5% для кіберзлочинів. Було видалено три застарілі індикатори:

  - Прозорість компаній (World Bank).
  - Стандарти аудиту (World Economic Forum).
  - Дані Tax Justice Network будуть перенесені до іншого домену.

Висновки та рекомендації

- **Значущість змін:** Інтеграція показників шахрайства в методологію Basel AML Index підкреслює зростаючу роль цього ризику в AML-аналізі. Це сприятиме більш повній оцінці ризиків для юрисдикцій і регульованих суб’єктів.

- **Технологічна складність:** Використання новітніх технологій для шахрайства створює виклики для правоохоронних органів, підкреслюючи важливість інноваційних підходів у протидії.
- **Покращення аналітики:** Включення нових категорій допоможе ідентифікувати юрисдикції, які є вразливими до фінансових та кіберзлочинів, із точнішими індикаторами.
- **Обмеження:** Недостатність якісних даних і відсутність глобальних стандартів залишаються основними перешкодами для ефективного аналізу шахрайства як ризику.

Документ підкреслює важливість адаптації до змін у глобальному середовищі AML/CFT, особливо в контексті технологічного розвитку і складності транскордонних злочинів.

http://surl.li/gujwzh

Злочинна геополітика Ірану: Як Тегеран використовує нелегальні ринки для досягнення стратегічних цілей

Документ під назвою "Iran's Criminal Statecraft: How Tehran Weaponizes Illicit Markets", підготовлений J.R. Mailey для Global Initiative Against Transnational Organized Crime (GI-TOC), є комплексним аналізом того, як Іран використовує злочинні ринки для досягнення стратегічних цілей. У звіті розглядається взаємозв'язок між державними структурами Ірану та транснаціональними злочинними мережами, а також висвітлюються механізми, які Тегеран використовує для зміцнення впливу в регіоні та на міжнародній арені.

Ключові Моменти

- **Роль злочинних проксі**

Іран активно співпрацює з ідеологічно близькими угрупованнями (наприклад, Хезболла), місцевими злочинними організаціями, кібератаками та транснаціональними злочинними угрупованнями. Ці мережі виконують важливі завдання, включаючи:

  - Політичні вбивства та викрадення.
  - Фінансування терористичних операцій через відмивання грошей.
  - Торгівлю нафтою та зброєю.

- **Контроль над стратегічними галузями**

Іранські структури, такі як Корпус вартових ісламської революції (КВІР), контролюють:

  - Нафтогазову промисловість, яка залишається головним джерелом валютних надходжень.
  - Транспорт, зокрема судноплавство та порти, які забезпечують контрабандні поставки.
  - Банківську систему для забезпечення нелегального обігу коштів.

- **Використання транснаціональних мереж**

Іран співпрацює з організованими злочинними угрупованнями, такими як «Дубайський суперкартель», для обміну ресурсами та послугами. Через ці мережі держава проводить операції з

відмивання грошей та використовує злочинців для виконання завдань, таких як кібератаки чи організація вбивств.

- **Зловживання наркотиками та зброєю**

Іранські проксі відіграють ключову роль у виробництві та поширенні наркотиків, таких як метамфетамін та каптагон. Наприклад, метамфетамін використовується для отримання доларової готівки в умовах санкцій, каптагон постачається через Сирію на ринки Близького Сходу.

- **Геополітична стратегія**

Іран інструменталізує злочинні ринки для підтримки своїх інтересів у таких регіонах, як:

  - **Ірак:** захоплення економічної інфраструктури, контроль за кордонами.
  - **Сирія:** підтримка режиму Башара Асада через проксі-угруповання.
  - **Ємен:** постачання зброї повстанцям-хуситам.

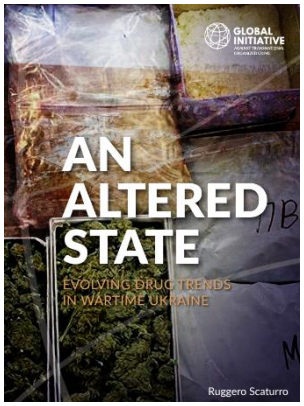
Висновки

- **Інституціоналізація злочинності:** Іран ефективно перетворив злочинну діяльність на державний інструмент зовнішньої політики. Взаємодія з організованою злочинністю стала невід'ємною частиною іранської стратегії.
- **Глобальні наслідки:** Злочинні мережі Ірану впливають на стабільність не лише в регіоні, але й у глобальному масштабі. Це створює виклики для міжнародного співтовариства в контексті протидії тероризму, відмиванню коштів і кібератакам.
- **Рекомендації щодо протидії:**
  - Ідентифікація ключових учасників іранських злочинних мереж.
  - Виявлення вразливих юрисдикцій та посилення санкцій.
  - Співпраця між державними структурами, приватним сектором та аналітичними центрами для розробки ефективних стратегій протидії.

Документ демонструє, як злочинна діяльність стає інструментом геополітичної стратегії для держав, що перебувають під санкціями. Це потребує нових підходів до глобальної безпеки та моніторингу злочинних ринків.

http://surl.li/mdglse

Наркотичний ландшафт воєнної України: нові виклики і загрози в умовах війни



Документ «An Altered State: Evolving Drug Trends in Wartime Ukraine» досліджує зміни в тенденціях попиту та пропозиції наркотиків в Україні під час війни. Війна значно вплинула на ринок наркотиків, спричинивши перебої в традиційних маршрутах постачання, зростання попиту на синтетичні наркотики, зміни у виробництві та появу нових каналів розповсюдження. Центральне місце в дослідженні займає організація «Хімпром», яка, ймовірно, монополізувала ринок синтетичних наркотиків в Україні.

Ключові моменти:

- **Тенденції попиту**

Війна та попит на наркотики: Зростання стресу та травматизації серед військових і цивільного населення спричинили підвищення попиту на наркотики, особливо синтетичні стимулятори (альфа-PVP, мефедрон) та канабіс.

Медичний канабіс: Ухвалення законопроєкту про легалізацію медичного канабісу в Україні у 2023 році, спрямоване на лікування посттравматичного стресового розладу (ПТСР), викликає питання щодо регулювання ринку та запобігання нелегальному використанню.

Синтетичні опіоїди: Відсутність героїну через перебої в постачанні спричинила поширення метадону та інших дешевих замінників.

- **Тенденції пропозиції**

Порушення логістичних маршрутів: Закриття порту Одеси та інші військові дії змінили маршрути транспортування наркотиків. Зокрема, кокаїн тепер потрапляє до України через західні кордони.

Локальне виробництво: Зростає виробництво синтетичних наркотиків в Україні. Лабораторії для виробництва амфетамінів і солей виявляють у різних регіонах країни.

«Хімпром»: Транснаціональна організація, яка має розгалужену мережу виробництва та розповсюдження синтетичних наркотиків, активно експлуатує нові умови ринку.

- **Ризики та виклики**

Психосоціальні наслідки: Зростання вживання наркотиків створює серйозні загрози для здоров'я та соціальної стабільності.

Легалізація канабісу: Хоча цей крок може допомогти у лікуванні ПТСР, існують ризики нелегального використання канабісу через недостатнє регулювання.

Зміцнення організованої злочинності: Домінування «Хімпрому» в наркотичному ринку посилює корупційні зв'язки з владою та ускладнює боротьбу з незаконним обігом.

Висновки:

- **Потреба у міжнародному співробітництві:** Ефективне вирішення проблем із наркотиками потребує координації між Україною та міжнародними партнерами, зокрема в сфері моніторингу прекурсорів і обміну даними.
- **Посилення роботи з попередження:** Необхідно вдосконалити програми зменшення шкоди, зокрема шляхом впровадження спеціалізованих тренінгів для медиків, правоохоронців і соціальних працівників.
- **Реформування регуляторної бази:** Легалізація медичного канабісу має супроводжуватися жорсткими заходами контролю для запобігання нелегальному використанню.
- **Боротьба з організованою злочинністю:** «Хімпром» становить серйозну загрозу для безпеки. Важливо зосередитись на боротьбі з їхньою мережею виробництва та логістики.

Цей документ є важливим джерелом даних для аналізу ситуації на ринку наркотиків в Україні під час війни та формування політик, спрямованих на мінімізацію пов'язаних ризиків.

http://surl.li/dmmtuv

Використання Росією організованої злочинності як інструменту державного управління

Документ під назвою "Gangsters at War: Russia's Use of Organized Crime as an Instrument of Statecraft" авторства Марка Галеотті досліджує взаємозв'язок між організованою злочинністю в Росії та її використанням як інструменту державної політики. Автор аналізує, як Росія використовує кримінальні структури для досягнення геополітичних цілей, включаючи обхід санкцій, фінансування спецоперацій, поширення пропаганди, саботаж та інші види «активних заходів». **Особливу увагу приділено періоду після 2022 року, коли вторгнення в Україну суттєво змінило підходи Кремля до мобілізації всіх ресурсів, включаючи нелегальні**.

Документ детально описує еволюцію зв'язків російської держави з кримінальним світом — від радянської доби, через хаос 1990-х, до сучасної гібридної моделі, де організована злочинність стала важливим активом для Кремля. Російські кримінальні групи мають глобальне охоплення та виконують ролі контрабандистів, кіберзлочинців, фінансових операторів і навіть агентів розвідки. Вони співпрацюють з державними структурами в обмін на захист, доступ до ресурсів чи можливість уникнення покарання.

Розділи документа охоплюють ключові аспекти, такі як роль кримінальних мереж у фінансуванні обходу санкцій, участь у підривних діях за кордоном, використання міграції як зброї, а також зростання кіберзлочинності під прикриттям держави. Аналізуються конкретні кейси, наприклад, незаконні фінансові операції через Кіпр чи використання кримінальних угруповань для передачі розвідувальних даних. Водночас розглядаються нові тенденції, включаючи «донбасизацію» конфліктів, коли кримінальні елементи інтегруються у військові структури.

Документ завершується рекомендаціями для міжнародної спільноти, які включають посилення розвідувальної співпраці, створення механізмів для обмеження фінансових потоків і запровадження більш жорстких санкцій проти організацій та осіб, пов'язаних із Кремлем.

Ключові висновки:

1. **Організована злочинність як інструмент державної політики Росії**

Росія систематично використовує організовану злочинність як частину своєї державної стратегії для досягнення зовнішньополітичних цілей. Це не просто співіснування держави та криміналу, а інтеграція злочинних угруповань у механізм державного управління. Кримінальні мережі виконують роль "інструментів державного впливу," діючи там, де офіційні структури не можуть бути залучені відкрито. Злочинні угруповання беруть участь у підривних операціях, саботажі, розвідці та фінансуванні військових і політичних операцій Кремля.

2. **Міжнародне охоплення російських кримінальних мереж**

Російські організовані злочинні угруповання мають потужну глобальну присутність, працюючи у Європі, Азії, Африці та Латинській Америці. Вони спеціалізуються на контрабанді товарів (зокрема зброї та технологій), відмиванні коштів через офшорні юрисдикції, фінансових махінаціях і навіть торгівлі людьми. Зокрема, в документі висвітлюється використання таких схем для обходу міжнародних санкцій, що дозволяє Росії зберігати доступ до важливих ресурсів і технологій.

3. **Фінансування через нелегальні економічні механізми**

Російські кримінальні мережі активно використовуються для фінансування державних ініціатив через нелегальні джерела. Сюди входять відмивання коштів, обхід санкцій, торгівля енергоресурсами через посередників, а також контрабанда стратегічних товарів. Ці дії спрямовані на пом'якшення впливу санкцій, запроваджених після початку війни в Україні, та забезпечення стабільного фінансування військових операцій.

4. **Залучення кримінальних елементів у військові операції та підривну діяльність**

Після 2022 року спостерігається посилення інтеграції організованої злочинності у військові операції. Документ описує "донбасизацію" конфліктів, коли кримінальні елементи інтегруються у військові підрозділи для виконання підривних дій, саботажу чи участі у боях. Крім того, кримінальні угруповання використовуються для організації міграційних криз на кордонах, маніпулюючи потоками мігрантів для створення політичного тиску на європейські країни.

5. **Кіберзлочинність як частина гібридної війни**

Кремль активно залучає російські хакерські групи та кіберзлочинців до реалізації державних завдань. Кіберзлочинці проводять атаки на інфраструктуру країн НАТО, викрадають фінансові дані, поширюють пропаганду та дезінформацію. У документі зазначено, що такі дії є невід'ємною частиною стратегії гібридної війни, яку використовує Росія.

6. **Нова ера кримінального впливу після початку війни в Україні**

Повномасштабне вторгнення в Україну стало каталізатором для більш активного використання організованої злочинності в інтересах держави. Кримінальні угруповання дедалі частіше виконують завдання, пов'язані із обходом санкцій, забезпеченням постачання військової техніки, нелегальними фінансовими операціями та саботажем на території інших держав. Ці зміни свідчать про глибшу інтеграцію кримінального сектору у стратегію національної безпеки Росії.

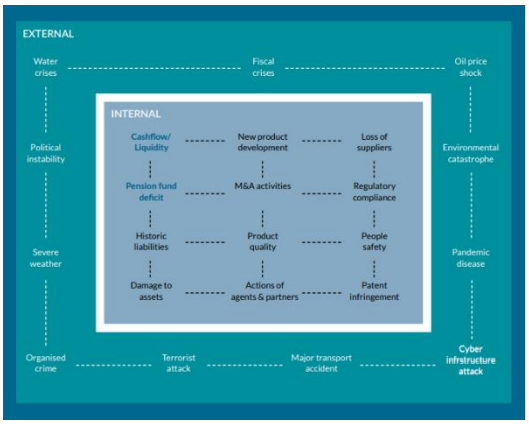
7. **Необхідність міжнародної співпраці для протидії**

Документ наголошує на важливості скоординованих дій міжнародної спільноти для протидії використанню Росією організованої злочинності. Рекомендується посилити обмін розвідувальною інформацією між країнами, запровадити жорсткіші санкції проти фізичних осіб та організацій, пов'язаних із кримінальними мережами, і вдосконалити механізми боротьби з відмиванням коштів. Лише спільними зусиллями можна ефективно протистояти цій загрозі.

Ці висновки відображають масштаб і складність російської стратегії використання організованої злочинності як інструменту державної політики, а також підкреслюють нагальну потребу у міжнародній співпраці для її нейтралізації.

http://surl.li/uatymi

Ризик і управління ризиком



Документ є комплексним посібником з управління ризиками, створеним для допомоги організаціям у впровадженні ефективних програм управління ризиками. Основний акцент зроблено на визнанні управління ризиками як критично важливого елемента для досягнення стратегічних цілей, захисту цінностей і адаптації до складного середовища, яке швидко змінюється.

Головна мета посібника — забезпечити організації методологічними інструментами для ідентифікації, оцінки та управління ризиками. Він базується на міжнародних стандартах, зокрема ISO 31000:2018 та COSO ERM, і охоплює ключові аспекти, такі як визначення ризику, принципи управління ризиками, створення корпоративної культури, відповідальність керівництва, управління нематеріальними та виникаючими ризиками, а також безперервне вдосконалення.

Документ підкреслює важливість інтеграції управління ризиками в загальну стратегію організації, ефективного управління невизначеністю і розробки структурованого підходу до вирішення ризиків. Особливу увагу приділено важливості комунікації, моніторингу ризиків і залучення всіх рівнів організації в процес управління ризиками.

Ключові висновки:

1. **Інтеграція управління ризиками як основи стратегії організації**

Управління ризиками є невід'ємною частиною успішного стратегічного планування організації. Документ підкреслює, що управління ризиками повинно бути інтегроване у всі аспекти діяльності

компанії, починаючи від управління фінансами і закінчуючи корпоративною культурою. Організації, які впроваджують цілісний підхід до ризик-менеджменту, здатні ефективніше адаптуватися до змін у зовнішньому середовищі, мінімізувати ризики і використовувати можливості, які виникають у процесі роботи. Це вимагає чіткої координації між всіма рівнями управління і підрозділами.

2. **Принципи управління ризиками як основа для прийняття рішень**

Восьми принципам ISO 31000:2018, зокрема динамічності, адаптивності, прозорості, використанню найкращої інформації та відповідності цілям організації, приділено центральну увагу. Вони забезпечують основу для побудови структурованого, але гнучкого процесу управління ризиками. Зокрема, інклюзивність передбачає залучення всіх зацікавлених сторін до ідентифікації та управління ризиками, а пропорційність дозволяє організаціям адаптувати свої дії до масштабу і складності ризиків.

3. **Роль керівництва у створенні ефективної культури управління ризиками**

Ефективне управління ризиками неможливе без активного лідерства керівництва. Керівники повинні бути ініціаторами впровадження культури ризик-менеджменту, визначаючи апетит до ризику (тобто рівень ризику, який організація готова прийняти), встановлюючи чіткі цілі і забезпечуючи ресурси для реалізації програм управління ризиками. Документ підкреслює, що лідерство повинно також забезпечувати регулярне інформування персоналу та стимулювати відкриту комунікацію.

4. **Фокус на виникаючих ризиках та управління невизначеністю**

Зі зростанням складності світового середовища виникаючі ризики, такі як кіберзагрози, кліматичні зміни чи соціальні потрясіння, становлять значну небезпеку для організацій. Їх важко передбачити, але вони можуть мати значний вплив на операційну стабільність. Документ акцентує увагу на необхідності побудови систем моніторингу та сценарного моделювання для визначення цих ризиків на ранніх етапах.

5. **Значення управління нематеріальними активами та репутаційними ризиками**

У сучасному світі нематеріальні активи, такі як бренд, репутація, інтелектуальна власність та людський капітал, стають центральними для стійкості організації. Документ наголошує, що управління цими активами вимагає спеціалізованих підходів, включаючи регулярні оцінки ризиків і розробку стратегій захисту. Репутаційний ризик є одним із найважчих для управління, оскільки він може бути спровокований зовнішніми чинниками, такими як криза у соціальних мережах чи негативна реакція громадськості.

6. **Постійний розвиток і вдосконалення процесів управління ризиками**

Ефективність програм управління ризиками залежить від їхнього безперервного вдосконалення. Організації повинні регулярно проводити ревізії своїх ризик-менеджмент процедур, оновлюючи їх відповідно до змін у бізнес-середовищі, нових нормативних вимог чи технологічних інновацій. Документ пропонує систематичний підхід до моніторингу і оцінки процедур із використанням ключових показників ефективності (KPI).

7. **Використання сучасних інструментів та методів для підвищення ефективності**

Документ рекомендує впровадження технологічних рішень для підвищення ефективності управління ризиками, таких як системи автоматизованого моніторингу ризиків, прогнозувальні аналітичні моделі, штучний інтелект для аналізу великих даних, а також використання програм для побудови ризикових сценаріїв. Це дозволяє організаціям швидше реагувати на зміни і знижувати вплив потенційних загроз.

8. **Забезпечення комунікації та залучення всіх рівнів персоналу**

Документ підкреслює важливість відкритої комунікації в процесі управління ризиками. Залучення всіх рівнів персоналу забезпечує кращу ідентифікацію ризиків і сприяє підвищенню обізнаності

щодо їхнього значення. Навчання працівників і регулярна комунікація щодо стратегій управління ризиками формують середовище, де кожен співробітник відчуває відповідальність за стабільність і безпеку організації.

Ці висновки демонструють, що управління ризиками є багатовимірним процесом, який потребує інтеграції стратегічного мислення, технологічних рішень і людського фактору для досягнення максимальної ефективності в умовах постійної невизначеності та змін.

https://www.airmic.com/system/files/technical-documents/airmic-explained-risk-and-managing-risk.pdf

Цифрове золото: оцінка стратегічного біткоїн-резерву для Сполучених Штатів

Документ досліджує потенціал створення стратегічного резерву біткоїнів (SBR) як національного активу для США. У ньому висвітлено роль біткоїна в сучасному фінансовому ландшафті та його можливості як засобу для забезпечення економічної стабільності, технологічного лідерства, геополітичного впливу та захисту демократичних цінностей.

Автори зазначають, що біткоїн з моменту свого створення пройшов шлях від експериментальної технології до глобально визнаного активу, здатного впливати на економічну і стратегічну політику країн. Використання біткоїна як державного резерву може зміцнити позицію США у фінансовій сфері, сприяти розвитку нових технологій, підтримати енергетичну незалежність та забезпечити нові можливості для захисту прав людини.

Документ висвітлює ключові аспекти потенційного впровадження SBR: від стратегічних цілей, таких як підтримка монетарного домінування США та протидія геополітичним супротивникам, до конкретних питань, пов'язаних із закупівлею, зберіганням і регулюванням. **Крім того, у звіті аналізуються ризики, пов'язані із волатильністю біткоїна, екологічним впливом майнінгу та регуляторними викликами, пропонуючи рішення для їхньої мінімізації**.

Окремий розділ присвячений аргументам «за» і «проти» створення резерву, серед яких значення біткоїна як активу, що забезпечує фінансову гнучкість, і можливості використання його в якості інструменту економічного впливу. Висновок документа закликає до розробки правової бази, створення прозорої стратегії закупівель та інтеграції біткоїна з існуючою фінансовою системою.

Ключові висновки:

1. **Біткоїн як стратегічний актив для збереження монетарного домінування США**

Створення стратегічного резерву біткоїнів (SBR) може допомогти США залишатися лідером у глобальній фінансовій системі, адаптуючись до цифрової економіки. Збереження долара як основної резервної валюти у світі залежить від здатності інтегрувати нові фінансові інструменти. Біткоїн, завдяки своїй обмеженій емісії та визнанню на глобальному рівні, може стати резервним активом, що зміцнить довіру до фінансової системи США. Впровадження біткоїна також відкриває можливість для підтримки стейблкоїнів, прив'язаних до долара, які вже активно використовуються у міжнародних транзакціях.

2. **Геополітична роль біткоїна у протистоянні супротивникам США**

У документі зазначено, що цифрові валюти, розроблені геополітичними конкурентами, такими як Китай (цифровий юань), можуть загрожувати економічному впливу США. Створення стратегічного резерву біткоїнів дозволить США просувати фінансову систему, яка підтримує відкритість і демократичні цінності. Прозора природа біткоїна також робить його потужним інструментом для

відстеження транзакцій і реалізації санкцій, що сприяє посиленню позицій США у глобальній політиці.

3. **Підтримка інновацій у сфері енергетики через майнінг біткоїна**

Майнінг біткоїна, часто критикований через високе енергоспоживання, може стати каталізатором для інновацій у відновлюваній енергетиці. Гнучкість у використанні електроенергії для майнінгу дозволяє стабілізувати енергетичні мережі, знижувати навантаження на піках споживання та сприяти інтеграції зелених джерел енергії. Документ наголошує, що розвиток майнінгу на основі чистих джерел енергії допоможе досягти кліматичних цілей США, водночас забезпечуючи фінансові вигоди.

4. **Біткоїн як інструмент фінансової інклюзії та захисту прав людини**

Децентралізована природа біткоїна дозволяє надавати фінансові послуги людям у країнах із репресивними режимами чи обмеженим доступом до банківських систем. США можуть використати це для підтримки демократичних цінностей, сприяючи фінансовій свободі для маргіналізованих груп населення по всьому світу. Це також підсилює роль США як глобального захисника прав людини.

5. **Ризики, пов'язані з волатильністю та екологічним впливом біткоїна**

Незважаючи на його стратегічну цінність, біткоїн залишається волатильним активом, що може створити фінансові ризики для національного резерву. Документ рекомендує застосовувати стратегії хеджування та інтегрувати біткоїн у портфелі з іншими активами для зниження ризиків. Щодо екологічного впливу майнінгу, пропонуються заходи для впровадження екологічно чистих технологій та стимулювання переходу майнерів на відновлювану енергію.

6. **Необхідність прозорості та регулювання для впровадження стратегічного резерву**

Впровадження стратегічного резерву біткоїнів потребує створення чіткої правової бази, яка забезпечить прозорість і підзвітність процесу закупівлі та зберігання. Документ наголошує, що США мають розробити довгострокову стратегію інтеграції біткоїна у свою фінансову систему, включаючи процедури управління ризиками, зберігання активів і регуляторний нагляд. Це дозволить забезпечити довіру громадськості до такого нововведення.

7. **Важливість своєчасного впровадження для зміцнення конкурентоспроможності США**

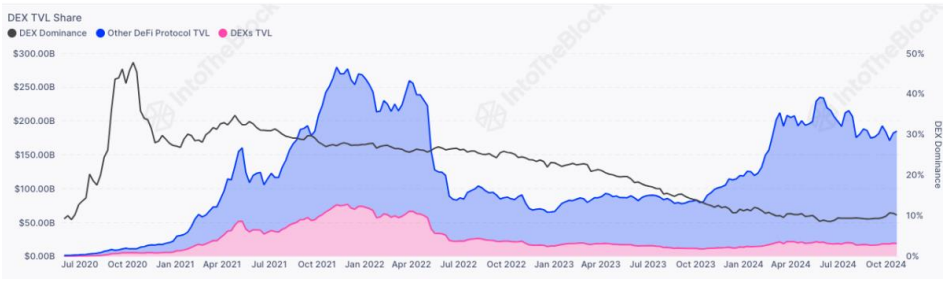
Документ підкреслює, що затримка з впровадженням стратегічного резерву біткоїнів може послабити позиції США у фінансовій і технологічній сферах. Інші країни, такі як Китай і Росія, вже активно досліджують можливості цифрових активів для зміцнення свого впливу. Прийняття біткоїна у національну фінансову стратегію дозволить США зберегти лідерство у глобальній економіці.

Ці висновки свідчать про значний потенціал біткоїна як стратегічного активу, що може зміцнити економічне та геополітичне лідерство США, сприяти інноваціям у сфері енергетики, захисту прав людини та адаптації до нових викликів цифрової економіки.

https://www.btcpolicy.org/articles/digital-gold-evaluating-a-strategic-bitcoin-reserve-for-the-united-states

Наступний рубіж DeFi: інституційні можливості, виклики та шлях уперед

Документ досліджує стан, виклики та перспективи розвитку децентралізованих фінансів (DeFi), зокрема їхню взаємодію з традиційними фінансовими системами. У ньому аналізуються історичні передумови появи DeFi, поточні інновації та перспективи інтеграції цих технологій у фінансовий сектор. Основна увага приділяється вивченню можливостей для інституційних інвесторів, викликів, пов'язаних із регуляцією та ліквідністю, і шляхам подолання бар'єрів для ширшого впровадження DeFi.



DeFi визначено як рушійну силу для створення більш прозорих, ефективних та інноваційних фінансових послуг. **Технології блокчейн і смарт-контрактів дозволяють виконувати фінансові операції без посередників, що знижує витрати та підвищує швидкість транзакцій. Однак цей сектор стикається з викликами, такими як технічні ризики, регуляторні обмеження та фрагментація ліквідності.**

У документі також розглянуто основні категорії DeFi-протоколів: децентралізовані біржі (DEX), кредитування, ліквідний стейкінг та інноваційні рішення, такі як токенізація реальних активів і протоколи для управління ризиками. Приділяється увага новим фінансовим інструментам, включаючи автоматизовані ринки, децентралізовані деривативи та алгоритмічні стейблкоїни. Висвітлюються успішні приклади використання DeFi-протоколів, а також уроки, отримані після значних криз і зломів, які підкреслюють необхідність покращення безпеки.

Документ акцентує увагу на потенціалі інтеграції DeFi з традиційними фінансами через створення гібридних моделей, які поєднують переваги обох систем. Такі моделі можуть стати ключовими для залучення інституційного капіталу, створення стабільної ліквідності та вдосконалення управління ризиками.

Ключові висновки:

1. **Еволюція DeFi: від нішевого продукту до глобального феномену**

DeFi пройшов шлях від експериментальної ідеї до важливого сегмента криптовалютної екосистеми. Починаючи з простих фінансових операцій, таких як кредитування і торгівля, DeFi розширився до складних фінансових рішень, включаючи децентралізовані деривативи та токенізацію реальних активів.

2. **Рушійні сили інституційного інтересу**

Інституційні інвестори дедалі більше цікавляться DeFi через його здатність знижувати витрати, підвищувати ліквідність та забезпечувати інноваційні можливості для диверсифікації портфелів. Особливо привабливими є токенізовані реальні активи та алгоритмічні протоколи управління ліквідністю.

3. **Основні виклики для впровадження DeFi серед інституційних учасників**

Головні бар'єри для залучення інституцій включають відсутність регуляторної ясності, недостатню ліквідність на ринку, високі технічні ризики та недостатність інституційного рівня інфраструктури, зокрема інтегрованих гаманців і механізмів управління ризиками.

4. **Роль регуляції та безпеки**

Регуляторна невизначеність є однією з головних причин повільного впровадження DeFi серед інституцій. Документ підкреслює важливість створення чітких регуляторних рамок, які підтримують інновації та забезпечують захист інвесторів. Значна увага приділяється питанням безпеки, адже багатомільйонні зломи протоколів DeFi залишаються серйозною проблемою.

5. **Нові інновації в DeFi**

Інноваційні рішення, такі як автоматизовані ринки ліквідності, децентралізовані кредитні системи та алгоритмічні стейблкоїни, демонструють потенціал для створення більш ефективних фінансових

ринків. Зокрема, токенізація реальних активів відкриває нові можливості для ліквідності та фінансової інтеграції.

6. **Перспективи гібридних фінансових моделей**

Інтеграція DeFi з традиційними фінансовими системами може створити гібридні моделі, які поєднують переваги обох підходів. Це включає автоматизацію смарт-контрактів, зменшення витрат і забезпечення прозорості, водночас дотримуючись регуляторних вимог.

7. **Потреба в покращенні інфраструктури**

Для забезпечення більш широкого впровадження DeFi необхідно створити інфраструктуру, яка відповідає стандартам інституційних учасників. Це включає покращення інтеграції між блокчейнами, забезпечення глибокої ліквідності та впровадження гаманців інституційного рівня.

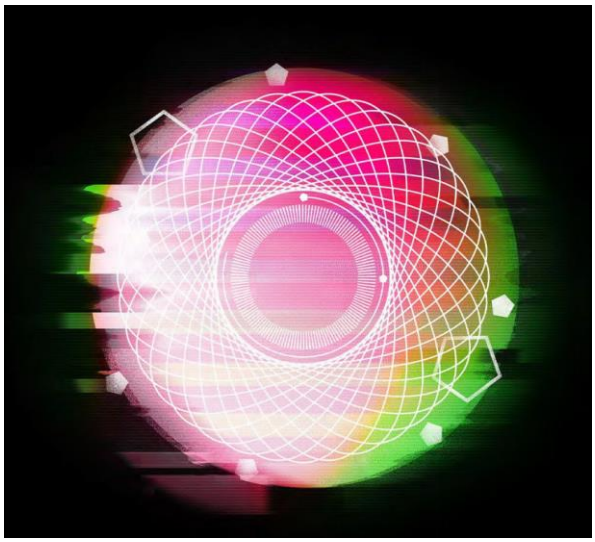
8. **Майбутнє DeFi як рушійної сили фінансових інновацій**

У довгостроковій перспективі DeFi має потенціал стати основою майбутньої фінансової системи, яка буде більш відкритою, прозорою та інклюзивною. Для цього необхідно подолати виклики, пов'язані із впровадженням, і зосередитися на розвитку рішень, які відповідають потребам як роздрібних, так і інституційних учасників.

Ці висновки підкреслюють як потенціал DeFi для трансформації фінансової екосистеми, так і необхідність вирішення критичних питань, які стримують його розвиток.

https://www.intotheblock.com/defi-next-frontier

Стаття 75: Нова можливість більш ефективно боротися зі злочинністю



Документ аналізує значення нової статті 75 Регламенту ЄС 2024/1624, яка спрямована на покращення боротьби з фінансовими злочинами через створення механізмів для обміну інформацією між зацікавленими сторонами. Стаття визначає нові рамки для співпраці між державним і приватним секторами, включаючи фінансові установи, наглядові органи та підрозділи фінансової розвідки (ПФР). Її мета — створити ефективний інструмент для ідентифікації та перешкоджання ВК/ФТ.

Стаття підкреслює, що більшість існуючих механізмів обміну інформацією є фрагментованими, часто не передбачають прямої співпраці між банками і значно залежать від централізованих структур, таких як ПФР. Це створює вузькі місця, які сповільнюють обмін інформацією та обмежують ефективність боротьби зі злочинами. У цьому контексті стаття є кроком вперед, дозволяючи прямий обмін даними між зобов'язаними суб'єктами, забезпечуючи юридичну базу для такої співпраці.

Документ висвітлює принципи обміну інформацією, включаючи захист конфіденційності, чітко визначені ролі учасників, управління ризиками, а також прозорість і підзвітність. У ньому зазначено, що обмін даними можливий тільки за наявності вагомих причин, таких як високий рівень ризику клієнта чи підозра у відмиванні коштів. Впровадження партнерств передбачає значні інфраструктурні зусилля, включаючи аудит, оцінку впливу на конфіденційність (DPIA) та погодження з регуляторами.

Документ також аналізує переваги нової статті, серед яких: підвищення оперативності у виявленні злочинних мереж, розвиток довіри між зацікавленими сторонами, зниження втрат для фінансових установ і більш ефективне використання існуючих ресурсів. Водночас, у звіті зазначено, що стаття має обмеження, пов'язані з її процедурною складністю та необхідністю забезпечення відповідності широкому спектру регуляторних вимог.

Ключові висновки:

1. **Ефективність обміну інформацією як ключовий елемент боротьби з фінансовими злочинами**

Стаття 75 Регламенту ЄС 2024/1624 представляє собою важливий прорив у створенні умов для обміну інформацією між банками, фінансовими установами та іншими підзвітними суб'єктами. Раніше обмін інформацією був значно обмежений, що створювало перешкоди для ефективного виявлення підозрілих транзакцій і злочинних мереж. Впровадження механізмів прямого обміну даними між учасниками дозволяє значно скоротити час реагування на ризики, знижуючи ймовірність успішного завершення злочинних операцій.

2. **Розширення кола учасників у рамках нових партнерств**

Новий підхід передбачає інтеграцію не лише банків і фінансових установ, а й інших категорій підзвітних суб'єктів, таких як юристи, аудитори, агенти з нерухомості тощо. Ця міжгалузева співпраця забезпечує ширший погляд на схеми злочинної діяльності, зокрема через можливість виявлення зв'язків між секторами, які раніше залишалися поза увагою. Це також сприяє формуванню більш цілісної стратегії боротьби з відмиванням коштів і фінансуванням тероризму.

3. **Захист конфіденційності як невід'ємна умова обміну інформацією**

Для того щоб уникнути зловживання даними та забезпечити довіру до нових механізмів, обмін інформацією можливий тільки за дотримання суворих стандартів конфіденційності. Це включає проведення оцінки впливу на захист даних (DPIA), застосування методів псевдонімізації та шифрування. Такі заходи допомагають збалансувати потребу у співпраці з обов'язком захищати права клієнтів.

4. **Зміцнення довіри між учасниками процесу**

Юридичне закріплення механізмів обміну інформацією сприяє зміцненню довіри між учасниками ринку. Учасники отримують чіткі гарантії того, що їхні дії узгоджені із законодавством, а обмін інформацією відбувається у правовому полі. Це підвищує рівень координації та сприяє формуванню довгострокових партнерств.

5. **Розширення можливостей ризик-орієнтованого підходу**

Завдяки новим механізмам обміну даними фінансові установи можуть точніше ідентифікувати клієнтів із високим рівнем ризику. Це дозволяє зосередити ресурси на виявленні серйозних загроз, таких як фінансування тероризму або міжнародні схеми відмивання коштів, водночас знижуючи адміністративне навантаження для менш ризикових клієнтів.

6. **Виклики процедурної складності та інтеграції**

Впровадження нових механізмів обміну інформацією вимагає значних ресурсів, включаючи адаптацію внутрішніх політик і процедур, узгодження з наглядовими органами та проведення аудиту. Ці виклики потребують створення чітких інструкцій і кращих практик, щоб допомогти учасникам адаптуватися до нових вимог. Документ підкреслює, що процедурна складність може стати перешкодою, якщо вона не буде належним чином вирішена.

7. **Стимулювання інновацій та автоматизації**

Запровадження статті 75 відкриває можливості для розвитку нових технологій і рішень у сфері обміну інформацією. Це включає автоматизацію передачі даних, стандартизацію форматів звітності

та впровадження аналітичних платформ для моніторингу транзакцій. Використання таких технологій допомагає значно підвищити ефективність боротьби з фінансовими злочинами.

8. **Можливість для зниження втрат фінансових установ**

Розширення обміну інформацією дозволяє швидше ідентифікувати шахрайські схеми, що зменшує втрати фінансових установ. Крім того, більш ефективна координація між учасниками ринку знижує ймовірність виникнення репутаційних ризиків і штрафів за недотримання законодавства.

9. **Стратегічна перевага у міжнародній співпраці**

Механізми, передбачені статтею 75, сприяють кращій координації з міжнародними партнерами та інтеграції в глобальну систему боротьби з фінансовими злочинами. Це особливо важливо у випадках транскордонних схем відмивання коштів або фінансування тероризму, де координація між різними юрисдикціями є критичною.

Ці висновки підкреслюють значення статті 75 як інструменту для модернізації підходів до боротьби з фінансовими злочинами, забезпечуючи не лише ефективність, а й прозорість та захист прав клієнтів. Успіх її впровадження залежить від активної участі зацікавлених сторін, створення довіри та розробки технологічних рішень.

http://surl.li/ukoycl

РЕКОМЕНДОВАНІ МАТЕРІАЛИ

Документи Лабораторії інновацій Європолу щодо штучного інтелекту

На веб-сторінці «Документи Лабораторії інновацій Європолу щодо штучного інтелекту» представлено низку публікацій, які досліджують вплив штучного інтелекту (ШІ) на правоохоронну діяльність. Ці документи аналізують як потенційні переваги, так і виклики, пов'язані з інтеграцією ШІ в роботу правоохоронних органів.

Серед основних тем, висвітлених у цих публікаціях:

- **Використання ШІ в поліцейській діяльності**: дослідження того, як ШІ може підвищити ефективність правоохоронних органів, зокрема через аналіз великих даних, прогнозування злочинів та цифрову криміналістику.
- **Етичні та соціальні аспекти**: обговорення питань, пов'язаних із упередженістю даних, конфіденційністю, підзвітністю та прозорістю при застосуванні ШІ в правоохоронній сфері.
- **Законодавчі рамки**: аналіз впливу Європейського акту про штучний інтелект на діяльність правоохоронних органів, включаючи вимоги до високоризикових систем ШІ та винятки для правоохоронних цілей.
- **Майбутні перспективи**: розгляд потенційних технологічних досягнень, таких як квантові обчислення та мережі 6G, і їхній можливий вплив на правоохоронну діяльність.

Ці публікації спрямовані на інформування правоохоронної спільноти про сучасні тенденції та виклики, пов'язані з впровадженням ШІ, а також надання рекомендацій щодо відповідального та ефективного використання цих технологій.

http://surl.li/tvnboy

ІНШІ НОВИНИ

ЄОКЗР розкриває китайську підпільну банківську мережу, підозрювану в шахрайстві з ПДВ на 113 мільйонів євро

25 жовтня 2024 року Європейська прокуратура (ЕРРО) повідомила про розкриття масштабної мережі незаконного банкінгу в Італії, що використовувалася для відмивання коштів та ухилення від сплати податків. Операція, проведена в Болоньї та Мілані, виявила схему ухилення від сплати ПДВ на суму 113 мільйонів євро, а також складний механізм міжнародного податкового шахрайства через «фантомні компанії». Було заарештовано сім осіб, включаючи двох керівників угруповання.

Злочинна схема мала оборот близько 500 мільйонів євро, використовуючи імпорт товарів з Китаю через «трикутники» з Болгарією та Грецією, щоб приховати походження вантажів. Прибутки від шахрайства відмивалися через китайську підпільну банківську мережу, а кошти проходили через кілька європейських країн, включаючи Німеччину, Францію та Великобританію, перш ніж повернутися до Італії для інвестування в легальні бізнеси.

Під час обшуків було вилучено значну кількість документації, заарештовано активи на суму 116 мільйонів євро, включаючи п'ять ресторанів, один торговий центр, житлові приміщення, елітні автомобілі та банківські рахунки. Операція проводилася за участю італійської фінансової поліції Guardia di Finanza, а також правоохоронних органів Болгарії, Німеччини та Греції.

Ця справа демонструє рішучість Європейського Союзу боротися зі злочинами, які загрожують його фінансовим інтересам, використовуючи міжнародну співпрацю та суворі розслідування. Усі підозрювані вважаються невинуватими, доки їхня провина не буде доведена у суді.

http://surl.li/dwkdih

ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

12 найкращих практик для створення відділу комплаєнсу у сфері ПВК

Стаття акцентує увагу на ключових кроках, які необхідно зробити, щоб забезпечити ефективність роботи відділу, спрямованого на дотримання вимог щодо протидії відмиванню коштів (ПВК). Вона розглядає основні аспекти створення, структурування та функціонування такого департаменту з урахуванням як законодавчих вимог, так і найкращих міжнародних стандартів.

1.Забезпечення відповідного лідерства та підтримки з боку керівництва. Успіх будь-якого AML-департаменту залежить від підтримки на рівні керівництва компанії. Потрібно призначити компетентного керівника (офіцера з ПВК), який забезпечуватиме ефективну реалізацію політики.

2.Розробка чіткої політики та процедур. Необхідно мати документально оформлені політики, які базуються на чинному законодавстві, включаючи правила щодо ідентифікації клієнтів (KYC), моніторингу транзакцій та звітності про підозрілі операції.

3. **Впровадження ризик-орієнтованого підходу (РОП).** Департамент повинен розробити систему оцінки ризиків клієнтів, продуктів, географій та інших факторів, щоб зосереджувати ресурси на найризиковіших напрямах.
4. **Вибір та використання сучасних технологій.** Використання програмного забезпечення для моніторингу транзакцій, управління даними та автоматизації звітності є важливим аспектом ефективного виконання ПВК-завдань.
5. **Підготовка та навчання персоналу.** Регулярне навчання співробітників допомагає підтримувати високий рівень обізнаності щодо останніх нормативних змін і практик виявлення ризиків.
6. **Створення механізмів внутрішнього контролю.** Відділ повинен мати незалежні механізми внутрішнього аудиту, які оцінюватимуть ефективність політик і процедур ПВК.
7. **Моніторинг та звітність.** Департамент має забезпечувати постійний моніторинг операцій та транзакцій, включаючи регулярне подання звітів про підозрілі операції відповідним органам.
8. **Забезпечення конфіденційності та захисту даних.** AML-департамент повинен відповідати за належний захист персональних даних клієнтів та конфіденційної інформації.
9. **Адаптація до змін у законодавстві.** Постійний моніторинг нормативних змін і адаптація політик є критично важливими для відповідності чинному законодавству.
10. **Взаємодія з регуляторами та звітність.** AML-департамент повинен підтримувати відкритий діалог із регуляторними органами, демонструючи прозорість у своїй роботі.
11. **Побудова культури комплаєнсу в організації.** Культура відповідності має бути закладена на всіх рівнях організації, щоб забезпечити дотримання норм кожним працівником.
12. **Ефективна взаємодія між департаментами.** Відділ комплаєнсу повинен співпрацювати з іншими функціями, такими як юридичний, фінансовий та IT-департаменти, для забезпечення комплексного підходу до управління ризиками.

Ці практики спрямовані на створення департаменту з комплаєнсу, який не тільки виконує нормативні вимоги, але й активно сприяє загальній фінансовій стійкості та репутації компанії.

https://amluae.com/12-best-practices-for-setting-up-an-aml-compliance-department/