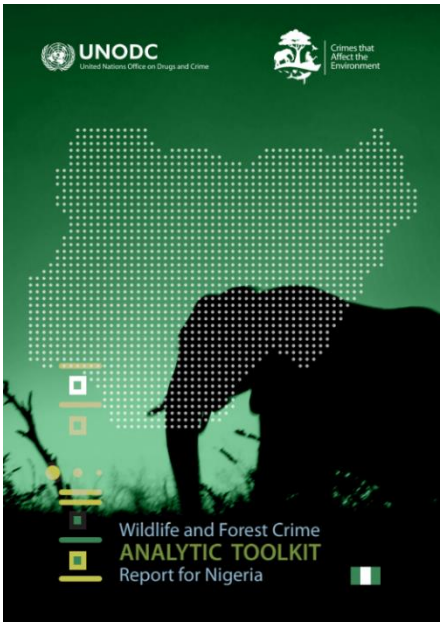
Серійний номер: ДСФМУ-ДК-2024-026
Вересень 2024

# ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

## Злочини проти дикої природи та лісів. Звіт щодо Нігерії




**Метою звіту є оцінка зусиль Нігерії у боротьбі зі злочинами проти дикої природи та лісів, використовуючи аналітичний інструментарій ICCWC** (Міжнародного консорціуму по боротьбі зі злочинами проти дикої природи), **який аналізує законодавчу базу, можливості правоохоронних органів, механізми судочинства та антикорупційні заходи**.

У звіті наводиться огляд біорізноманіття Нігерії, де проживає понад 1340 видів тварин, включно з такими відомими видами, як західноафриканський лев, панголін і африканський слон. Однак браконьєрство, втрата середовища існування та діяльність організованих злочинних мереж серйозно загрожують цим видам. **Нігерія є важливим центром для нелегальної торгівлі дикою природою, особливо слоновою кісткою та лусками панголінів, і має зв'язки з транскордонними мережами, які використовують місто Лагос як вузловий пункт для транспортування контрабанди до Китаю та В'єтнаму.**

**Окремо розглядається стратегія Нігерії щодо боротьби зі злочинами проти дикої природи та лісових ресурсів на період 2022–2026 років, розроблена спільно з UNODC. Ця стратегія передбачає ключові кроки для підвищення ефективності боротьби зі злочинами, включаючи покращення координації правоохоронних органів, реформу законодавства та підвищення потенціалу у проведенні розслідувань і судових процесів**.

Документ також аналізує правову базу Нігерії щодо злочинів проти дикої природи. **Хоча Нігерія є стороною багатьох міжнародних угод, таких як CITES та Конвенція ООН проти транснаціональної організованої злочинності, національне законодавство має значні прогалини. Зокрема, покарання за правопорушення в сфері дикої природи часто є недостатньо суворими, щоб слугувати ефективним стримуючим фактором**. Однією з головних рекомендацій є прийняття законопроєкту про захист видів, що знаходяться під загрозою, який підвищить відповідальність за злочини у цій сфері.

Ще однією важливою проблемою є **недостатня координація між державними органами. Хоча були позитивні приклади співпраці, наприклад, створення Міжвідомчої групи з охорони дикої природи, все ще існують труднощі з ефективною координацією на місцевому та**

**національному рівнях**. Рекомендується створити спільну транскордонну слідчу групу для боротьби з високопрофільними випадками нелегальної торгівлі дикою природою.

Що стосується судочинства, звіт наголошує на тому, що **нігерійські прокурори та судді не мають достатньої спеціалізації для розгляду таких справ**. Крім того, корупція є серйозним бар'єром на шляху до ефективної боротьби з цими злочинами, що створює додаткові виклики.

**Ключові висновки звіту:**

1. **Нігерія є ключовим центром незаконної торгівлі дикою природою, особливо слоновою кісткою та панголінами.**

Транснаціональні організовані злочинні мережі активно використовують Нігерію як транзитний центр для нелегальної торгівлі продукцією дикої природи, зокрема слоновою кісткою та лусками панголінів. Велика частина цього товару транспортується до Китаю та В'єтнаму через порт Лагоса. Звіт підкреслює, що, незважаючи на значні міжнародні конфіскації (у 2019 році 8 з 13 найбільших конфіскацій слонової кістки та лусок панголінів мали зв'язок з Нігерією), кількість арештів і судових процесів залишається незначною. Це свідчить про недостатню ефективність правоохоронних органів у боротьбі з цими мережами, особливо в питаннях розслідування та переслідування винних. Для вирішення цієї проблеми потрібні кращі методи розслідування та міжнародна співпраця.

2. **Законопроєкт про захист видів, що знаходяться під загрозою, є критично важливим для зміцнення правової бази.**

Прийняття законопроєкту про охорону видів, що знаходяться під загрозою, має на меті привести національне законодавство Нігерії у відповідність з міжнародними зобов'язаннями, такими як Конвенція про міжнародну торгівлю видами, що знаходяться під загрозою зникнення (CITES). Існуючі закони не передбачають достатньо суворих покарань, що дозволяє злочинним організаціям діяти з відносною безкарністю. Законопроєкт, який було розроблено Федеральним міністерством навколишнього середовища Нігерії у 2022 році, має посилити правові наслідки за злочини, пов'язані з незаконним обігом тварин і лісових ресурсів, включаючи суттєві штрафи та збільшення строків ув'язнення. Прискорення його прийняття стало б сигналом для міжнародної спільноти про серйозність намірів Нігерії.

3. **Покращення координації між державними установами та створення спеціалізованих слідчих груп.**

Однією з ключових проблем, виявлених звітом, є відсутність ефективної координації між різними національними правоохоронними та судовими органами, зокрема митною службою, Національним агентством з охорони навколишнього середовища (NESREA) та Службою національних парків. Хоча були створені координаційні платформи, такі як Міжвідомча група з охорони дикої природи, їхня операційна ефективність залишається низькою через обмежену координацію та відсутність спільних розслідувань. У звіті рекомендується створити спільну міжвідомчу транскордонну слідчу групу, яка б включала досвідчених слідчих і фахівців з організованої злочинності та забезпечила централізоване керування розслідуваннями складних кримінальних справ.

4. **Низький рівень спеціалізації серед прокурорів та суддів у справах про злочини проти дикої природи.**

У Нігерії обмежена кількість суддів і прокурорів мають досвід у розгляді справ, пов'язаних з незаконною торгівлею дикою природою. Це призводить до того, що судові справи ведуться повільно, вироки є м'якими, а покарання не відповідають рівню серйозності злочинів. Звіт закликає до проведення тренінгів для суддів та прокурорів, підвищення їхньої обізнаності про екологічні злочини та введення посібників зі стандартів для забезпечення справедливого і послідовного судочинства, включно з конфіскацією доходів, отриманих від злочинної діяльності.

5. **Корупція є серйозним бар'єром для боротьби з екологічними злочинами.**

Корупція в правоохоронних та судових органах Нігерії підриває зусилля з боротьби з організованими злочинними мережами. Незаконна діяльність часто залишається безкарною через

корумпованість чиновників, які можуть сприяти ухиленню від відповідальності або приймати хабарі для покриття злочинів. У звіті наголошується на необхідності посилення антикорупційних заходів, зокрема через підвищення прозорості в розслідуваннях і судових процесах, а також шляхом суворішого контролю за співробітниками правоохоронних органів. Крім того, слід активізувати співпрацю з міжнародними організаціями для виявлення та притягнення до відповідальності корумпованих посадовців.

http://surl.li/hrbskx

## Нагляд з ПВК з боку наглядових органів за правовими та бухгалтерськими фахівцями


Документ розглядає результати роботи Офісу з нагляду за органами професійного контролю (OPBAS) у сфері протидії відмиванню коштів в юридичному та бухгалтерському секторах у Великій Британії. OPBAS контролює діяльність 22 органів професійного контролю (PBS) з метою підвищення ефективності їхнього нагляду та сприяння обміну інформацією між PBS та правоохоронними органами.

Звіт підкреслює роль юридичних і бухгалтерських фірм як ключових посередників у економіці Великої Британії, що робить їх вразливими до ризиків відмивання коштів. OPBAS прагне до забезпечення високого стандарту нагляду в цих секторах для підтримання репутації країни як глобального фінансового центру.

**Документ описує результати оцінки ефективності нагляду 9 органів PBS у 2023/2024 роках. Оцінка охоплює такі аспекти, як ризик-орієнтований підхід, обмін інформацією, застосування правозастосовних заходів та управління ресурсами**. Звіти підкреслюють, що хоча PBS загалом виконують свої обов'язки, значна кількість із них демонструє часткову ефективність у ключових аспектах. Наприклад, **органи часто стикаються з труднощами в адаптації ризик-орієнтованого підходу, а деякі з них не використовують наявні правозастосовні заходи для забезпечення належного дотримання вимог AML**.

**Однією з ключових проблем, виявлених у звіті, є відсутність ефективного обміну інформацією та недостатня кількість спільних розслідувань між PBS та іншими регуляторами і правоохоронними органами**. **Крім того, деякі PBS передають на аутсорсинг значну частину своєї роботи з AML, що викликає занепокоєння щодо якості контролю за виконанням наглядових функцій.**

**Ключові висновки:**

1. **Часткова ефективність органів професійного контролю (PBS):** Хоча PBS виконують свої обов'язки з ПВК, значна кількість органів продовжує демонструвати часткову ефективність у ключових сферах, таких як нагляд, управління ризиками та правозастосування. Лише 3 з 9 оцінених PBS продемонстрували покращення, тоді як більшість залишаються на попередньому рівні або зазнали незначного зниження ефективності. Основними проблемами є недотримання вимог в таких областях, як підхід до управління ризиками та недостатня розробка стратегії нагляду.
2. **Проблеми з ризик-орієнтованим підходом:** Багато PBS не змогли належним чином визначити профілі ризиків своїх піднаглядних суб'єктів. Це включає недостатнє використання широкого спектру індикаторів ризику, таких як тип клієнта, продукти, послуги та географічні ризики. Деякі органи також спираються на самодекларацію учасників без додаткової перевірки. Такий обмежений підхід до оцінки ризиків знижує якість нагляду та управління потенційними загрозами.

3. **Недоліки в обміні інформацією:** Попри деякі покращення, значна частина PBS продовжує демонструвати обмежену участь в обміні інформацією з іншими органами та правоохоронними структурами. Обмежене використання платформ обміну інформацією, таких як FIN-NET або SIS, впливає на здатність ефективно виявляти та реагувати на порушення. Відсутність активного обміну інформацією, особливо щодо поточних розслідувань, знижує загальний рівень ефективності протидії відмиванню коштів.
4. **Проблеми з примусовими заходами:** Багато PBS не використовують свої повноваження для забезпечення дотримання норм AML належним чином. Водночас кількість штрафів і примусових заходів знизилася у 2022/2023 роках порівняно з попередніми роками, попри збільшення кількості порушень. Це свідчить про недостатньо стримувальний характер правозастосовних дій PBS.
5. **Аутсорсинг наглядових функцій:** Деякі PBS передають значну частину своїх інспекційних функцій зовнішнім підрядникам, що викликає занепокоєння щодо належного контролю за їх діяльністю. Відсутність ефективного нагляду за субпідрядниками може призвести до зниження якості інспекцій і підвищити ризики виявлення порушень на пізніших етапах.
6. **Обмежені ресурси:** Деякі PBS не мають достатньо ресурсів для ефективного виконання своїх функцій. Низький рівень фінансування та брак кадрових ресурсів впливають на здатність органів забезпечувати якісний AML нагляд. Наприклад, PBS можуть покладатися на одного ключового співробітника, що створює ризики, пов'язані з залежністю від цього працівника.
7. **Недостатній рівень навчання персоналу:** Деякі PBS не забезпечують належного рівня підготовки для своїх працівників. Брак спеціалізованих навчальних програм з AML, включаючи навчання з обробки повідомлень про підозрілу діяльність (SAR), впливає на здатність персоналу приймати обґрунтовані рішення щодо належного управління ризиками.

Загалом, звіт підкреслює необхідність покращення ефективності роботи PBS шляхом посилення підходу до управління ризиками, примусових заходів, обміну інформацією та належного навчання персоналу для зниження ризиків відмивання коштів у Великій Британії.

https://www.fca.org.uk/publication/opbas/opbas-report-progress-themes-supervisory-work-2023-24.pdf

## Рекомендації щодо виконання зобов'язань ПВК/ФТ стосовно платіжних рахунків із базовими функціями

Документ «Guidance Note on AML/CFT obligations in relation to payment accounts with basic features» є інструкцією для кредитних установ щодо виконання вимог з у сфері протидії відмиванню коштів (ПВК) та фінансуванню тероризму (ПФТ) стосовно платіжних рахунків із базовими функціями. Він виданий Управлінням з фінансової розвідки (FIAU) для того, щоб допомогти фінансовим установам виконувати зобов'язання щодо запобігання злочинним фінансовим операціям під час надання послуг базових платіжних рахунків відповідно до нормативних актів Мальти. У документі детально розглядаються вимоги щодо ідентифікації клієнтів, верифікації їхньої особи, а також заходи моніторингу з метою виявлення підозрілих транзакцій.

**Ключові висновки:**

1. **Верифікація особи клієнта на основі ризик-орієнтованого підходу**: Кредитні установи мають збирати та перевіряти інформацію про клієнтів відповідно до рівня ризику. Для клієнтів з низьким ризиком можливе спрощення процесу ідентифікації, однак для підвищеного ризику потрібні більш суворі процедури.

2. **Особливі категорії клієнтів**: Документ визначає, що клієнти, які не мають постійної адреси (наприклад, безпритульні або ті, хто проживає на яхтах), або ті, хто отримав статус

міжнародного захисту, також мають право на відкриття платіжних рахунків із базовими функціями. Для таких клієнтів можуть застосовуватися альтернативні методи верифікації.

3. **Застосування червоних прапорців для виявлення підозрілих операцій**: У документі описані ознаки підозрілих транзакцій, такі як надмірний обіг коштів, структуровані готівкові депозити, часті перекази на онлайн-платіжні системи, використання рахунків у ролі «грошових мулів». Це дозволяє установам визначати потенційні ризики відмивання коштів.

4. **Неприпустимість відкриття рахунків без належної верифікації**: Якщо кредитна установа не може належним чином ідентифікувати особу клієнта, це має призвести до відмови у відкритті рахунку. У таких випадках також може бути подано звіт про підозрілі транзакції до FIAU.

5. **Підвищений моніторинг для високоризикових клієнтів**: Кредитні установи зобов'язані проводити постійний моніторинг клієнтських рахунків на основі ризику. Для клієнтів з високим рівнем ризику застосовуються частіші перевірки та оновлення профілю клієнта.

6. **Документи для верифікації особи**: У документі надані приклади різних видів документів, які можуть бути використані для ідентифікації клієнтів, зокрема для осіб, які отримали статус міжнародного захисту, біженців, осіб без постійного місця проживання тощо.

Документ націлений на забезпечення фінансової інклюзії при дотриманні суворих вимог щодо запобігання злочинним діям, таким як відмивання коштів і фінансування тероризму.

http://surl.li/oaugji

## Вплив нелегальних криптообмінних платформ на розширення кримінальної економіки


Документ «Crypto exchange providers - Professional Money Launderers» підготовлений підрозділом фінансової розвідки Швеції (ПФР Швеції) і описує загрози, пов'язані з незаконними операціями обміну криптовалют. У документі йдеться про те, що нелегальні провайдери криптообміну, які здійснюють незареєстровані та незаконні послуги з обміну криптовалют, відіграють ключову роль у відмиванні коштів для організованої злочинності. Злочинці використовують криптовалюти для конвертації нелегальних доходів у готівку або інші активи. Провайдери обміну криптовалют є професійними відмивачами коштів (PML), і їхня діяльність підтримує розширення кримінальної економіки. ПФР Швеції виділяє чотири основні профілі таких провайдерів і наголошує на важливості міжнародної співпраці правоохоронних органів у боротьбі з ними.

**Ключові висновки:**

1. **Роль криптовалют у відмиванні коштів**: Криптовалюти широко використовуються для відмивання коштів, зокрема в кіберзлочинності, торгівлі наркотиками, шахрайстві та ухиленні від санкцій. Незважаючи на те, що криптовалюти можна відстежувати, існують інструменти для приховування транзакцій, такі як криптоміксери та свопери, що ускладнює роботу правоохоронних органів.

2. **Профілі нелегальних провайдерів обміну криптовалют**: ПФР Швеції виділила чотири основні групи нелегальних криптопровайдерів:

    - **Node Exchange Providers** – інтегровані у кримінальні мережі та мають доступ до кур'єрів, готівки та криптовалют.

- **Hawala Exchange Providers** – пов'язані з системою «гавала» і мають міжнародні зв'язки, зокрема з країнами Близького Сходу.
- **Asset Exchange Providers** – систематично використовують криптоактиви для своїх потреб і мають високу здатність до обміну великих обсягів криптовалют.
- **Platform Exchange Providers** – працюють на відкритих P2P платформах і обслуговують дрібних злочинців, таких як покупці наркотиків.

3. **Співпраця з організованою злочинністю**: Провайдери обміну криптовалют зазвичай надають послуги одразу кільком кримінальним мережам. Вони є важливим елементом злочинної інфраструктури, що підтримує діяльність організованої злочинності на міжнародному рівні.
4. **Рекомендації для правоохоронних органів**: Документ наголошує на необхідності підвищення моніторингу та контролю криптовалютних платформ, а також міжнародної співпраці для виявлення та ліквідації таких провайдерів. Зокрема, правоохоронним органам потрібно співпрацювати з платформами, банками та іншими фінансовими установами для виявлення підозрілих транзакцій і закриття доступу до їхніх послуг злочинцям.
5. **Вплив на кримінальну економіку**: Відмивання коштів через криптовалюти є критично важливим для підтримки кримінальної економіки. Придушення діяльності нелегальних криптовалютних провайдерів може серйозно порушити роботу організованих злочинних мереж.

Цей документ акцентує увагу на важливості боротьби з нелегальними провайдерами обміну криптовалют як ключовими особами у процесах відмивання коштів та підтримки організованої злочинності.

https://polisen.se/siteassets/dokument/finanspolisen/rapporter/crypto-exchange-providers-open.pdf

## Роль ПФР у процесі національної оцінки ризиків


Документ "The Role of FIUs in the National Risk Assessment Process" досліджує роль підрозділів фінансової розвідки (ПФР) у проведенні національних оцінок ризиків (НОР) щодо відмивання коштів та фінансування тероризму. Він розглядає їх участь у координації НОР, залучення різних зацікавлених сторін та обмін інформацією. **ПФР відіграють ключову роль у зборі та аналізі даних, забезпечуючи всебічний огляд ризиків у країні. Вони також співпрацюють з іншими органами для розробки та реалізації стратегій щодо протидії ВК і ФТ. Документ охоплює методології оцінки ризиків, участь приватного сектору, використання сучасних технологій та міжнародних стандартів.**

**Ключові висновки:**

1. **Координаційна функція ПФР:** Підрозділи фінансової розвідки є центральними органами в процесі НОР, виконуючи функцію координатора між різними державними структурами, приватним сектором та міжнародними партнерами. Вони збирають і аналізують величезні обсяги даних, щоб оцінити ризики відмивання коштів і фінансування тероризму. Ця координаційна роль також передбачає надання рекомендацій та звітів урядам для ухвалення стратегічних рішень.

2. **Збір та аналіз даних:** ПФР відіграють ключову роль у зборі інформації з різних джерел, включаючи фінансові установи, правоохоронні органи та міжнародних партнерів. Вони аналізують ці дані для виявлення схем ВК/ФТ та оцінки загроз на національному рівні. Цей аналіз включає як кількісні, так і якісні методи, що дозволяє створювати комплексну картину ризиків.

3. **Міжнародна співпраця:** ПФР відіграють активну роль у міжнародному обміні інформацією щодо підозрілих фінансових потоків та типологій злочинів. Співпраця з іншими країнами та міжнародними організаціями, такими як FATF, сприяє виявленню транснаціональних злочинних схем та тенденцій. Міжнародний обмін даними дозволяє краще розуміти глобальні ризики, пов'язані з ВК та ФТ, що особливо важливо у випадку транскордонних злочинів.

4. **Постійне оновлення НОР:** ПФР регулярно оновлюють свої НОР, адаптуючись до нових загроз і змін у законодавстві. Такі регулярні оновлення дозволяють зберігати актуальність стратегій протидії ВК та ФТ і впроваджувати нові заходи у відповідь на нові виклики. Вони також допомагають вчасно виявляти нові ризики та змінювати підходи до боротьби з ними.

5. **Інноваційні технології:** ПФР активно використовують сучасні технології для підвищення ефективності своїх процесів. Наприклад, вони застосовують аналіз великих даних (Big Data), штучний інтелект та інші цифрові інструменти для ідентифікації підозрілих транзакцій і прогнозування можливих ризиків. Це дозволяє покращити швидкість та точність виявлення злочинних схем і реагування на загрози.

6. **Участь приватного сектору:** Приватний сектор відіграє важливу роль у процесі НОР, оскільки саме фінансові установи і компанії першими виявляють підозрілі фінансові потоки. ПФР залучають приватні компанії до процесу оцінки ризиків, що дозволяє краще розуміти специфічні ризики у різних секторах економіки. Взаємодія між державою та приватними підприємствами сприяє створенню більш повної картини загроз та підвищенню ефективності заходів протидії.

7. **Виклики для ПФР:** Основними викликами, з якими стикаються ПФР у процесі НОР, є складність збору та обробки великих обсягів даних, недостатність ресурсів для аналізу та потреба у тісній координації між державними установами та приватним сектором. Також важливим аспектом є постійна взаємодія з міжнародними партнерами для обміну інформацією та гармонізації методологій оцінки ризиків.

8. **Розробка національних стратегій:** ПФР активно беруть участь у формуванні національних стратегій боротьби з ВК та ФТ, спираючись на результати оцінки ризиків. Їх аналіз та рекомендації є важливими для розробки політик та заходів, які спрямовані на зниження ризиків у національній фінансовій системі. Вони також відіграють важливу роль у моніторингу впроваджених заходів та їх ефективності.

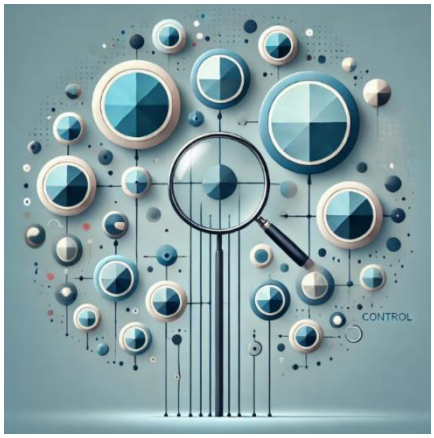
9. **Технічна допомога та навчання:** Багато країн отримують технічну підтримку від міжнародних організацій для вдосконалення процесу НОР. Це може включати тренінги для підвищення кваліфікації співробітників ПФР, розробку нових інструментів для аналізу ризиків та впровадження найкращих практик. Підвищення кваліфікації є важливим для адаптації до швидких змін у злочинних схемах та технологіях.

Ці ключові висновки демонструють критичну роль ПФР у забезпеченні надійного функціонування системи НОР, що спрямована на боротьбу з відмиванням коштів і фінансуванням тероризму.

http://surl.li/plaodu

# РЕГУЛЮВАННЯ

## Ідентифікація та перевірка особи КБВ у Люксембурзі




Документ "Circular CSSF 24/861" зосереджується на важливості ідентифікації кінцевих бенефіціарних власників (КБВ) для протидії відмиванню коштів і фінансуванню тероризму. **Ця директива є оновленням до попереднього циркуляру 19/732 і додає нові уточнення щодо вимог до ідентифікації та верифікації бенефіціарних власників для фахівців, які підлягають нагляду CSSF у Люксембурзі. Документ регулює, як компанії та організації повинні застосовувати ризик-орієнтований підхід під час встановлення і перевірки КБВ, зокрема для складних правових структур та міжнародних операцій**.

Основна мета циркуляру полягає в тому, щоб гарантувати, що фінансові установи і професійні учасники ринку повністю розуміють структуру власності своїх клієнтів і можуть виявляти реальних фізичних осіб, які контролюють компанії або виграють від їхньої діяльності. Він також підкреслює, що складні корпоративні структури, які не мають явної комерційної мети, можуть становити підвищений ризик для відмивання коштів, і тому вимагають особливої уваги.

**Циркуляр також встановлює триступеневий процес для ідентифікації КБВ: визначення прямих або непрямих власників із часткою понад 25%, визначення осіб, що здійснюють контроль іншим шляхом, і, в разі неможливості ідентифікації, визначення старшого керівного персоналу як КБВ.**

**Ключові законодавчі норми:**

1. **Ідентифікація кінцевих бенефіціарних власників (КБВ):** Фахівці повинні ідентифікувати осіб, які прямо або опосередковано володіють або контролюють щонайменше 25% акцій або прав голосу компанії. У випадках, коли КБВ неможливо ідентифікувати через частку володіння, необхідно встановити осіб, які контролюють компанію іншими способами, такими як право призначати або відкликати членів ради директорів.
2. **Контроль іншими засобами:** Якщо неможливо ідентифікувати КБВ через пряме володіння, фахівці повинні визначити осіб, що здійснюють контроль іншим чином, наприклад через договірні або інші неформальні механізми впливу на компанію. Це може стосуватися тих, хто контролює рішення компанії без формального права власності на акції.
3. **Триступеневий підхід:** У випадку неможливості встановити бенефіціарів через пряме володіння або контроль іншими засобами, фахівці повинні визнати старший керівний персонал компанії (керівників) як кінцевих бенефіціарних власників. Це вимагає детальної перевірки та документування спроб встановити справжніх власників або контролерів.
4. **Ризик-орієнтований підхід:** Процедури з ідентифікації та верифікації КБВ повинні відповідати рівню ризику, що його може становити клієнт або транзакція. Високоризикові клієнти, особливо ті, хто працює в складних корпоративних структурах або в міжнародному контексті, потребують більш ретельного моніторингу та перевірки. Це означає, що до кожного клієнта застосовується індивідуальний підхід, залежно від наявних ризиків.
5. **Документування та зберігання даних:** Фахівці зобов'язані зберігати всі записи, що стосуються ідентифікації та верифікації КБВ, для забезпечення прозорості та можливості перевірки з боку регуляторів. Важливо також забезпечити регулярне оновлення цієї інформації, щоб враховувати зміни в структурі власності або контролю клієнтів.

https://www.cssf.lu/wp-content/uploads/cssf24_861eng.pdf

# Новий наглядовий орган OTSI: Забезпечення дотримання торговельних санкцій у Великій Британії

12 вересня 2024 року уряд Великої Британії офіційно оголосив про створення Office of Trade Sanctions Implementation (OTSI) – нового органу, який контролюватиме виконання торговельних санкцій. Орган запрацює з 10 жовтня 2024 року, а його завдання полягають у розслідуванні порушень санкцій та накладенні адміністративних стягнень, включаючи штрафи до £1 мільйона або 50% від вартості порушення.

**Основні функції OTSI:**

1. **Розслідування порушень торговельних санкцій** – OTSI має право досліджувати випадки порушень і, за результатами розслідувань, накладати штрафи на фізичних та юридичних осіб, що порушили вимоги санкційного законодавства Великої Британії. Штрафи можуть досягати значних сум і стосуються порушень, таких як надання заборонених товарів, їх постачання чи трансфер.

2. **Сувора відповідальність за порушення** – однією з новацій стало введення принципу «суворої відповідальності», що означає, що особа чи компанія можуть бути оштрафовані навіть за відсутності наміру порушити закон. Це нововведення викликало занепокоєння серед бізнесів, оскільки навіть найкращі комплаєнс-програми тепер можуть виявитися недостатніми для уникнення штрафів. Навіть якщо компанія виконала всі заходи для дотримання санкцій, вона все одно може бути оштрафована у випадку, якщо порушення буде виявлено.

3. **Повноваження та співпраця з іншими органами** – OTSI може видавати попередження про порушення, публікувати інформацію про санкційні порушення, а також передавати справи до HMRC для кримінального розслідування. Крім цього, OTSI працюватиме спільно з іншими британськими органами, такими як OFSI (Office of Financial Sanctions Implementation), що відповідає за дотримання фінансових санкцій.

4. **Запит документів та інформації** – OTSI матиме право вимагати документи та інформацію від компаній для перевірки дотримання вимог санкційного законодавства або у процесі надання ліцензій на торгівлю. Водночас орган буде займатися управлінням санкційних виключень, видачею ліцензій, а також відповідати на запити з боку бізнесу щодо дотримання санкцій.

**Виклики для бізнесу:**

Нові правила, що включають «сувору відповідальність», створюють значні ризики для компаній, особливо у торговельній сфері. Бізнеси повинні переглянути свої політики комплаєнсу та переконатися, що вони відповідають новим вимогам. Тим не менше, навіть з найсучаснішими інструментами дотримання правил, компанії не можуть контролювати дії контрагентів після експорту товарів, що створює додаткові ризики для потенційних порушень.

OTSI буде важливим гравцем у зміцненні санкційної політики Великої Британії, що спрямована на забезпечення глобальної стабільності та недопущення нелегальних торгових операцій із забороненими країнами або суб'єктами.

**Висновки:**

Створення OTSI відображає серйозний підхід Великої Британії до дотримання торговельних санкцій. Запровадження «суворої відповідальності» в рамках цього органу покликане підвищити ефективність санкційної політики, але водночас створює нові виклики для бізнесу, який тепер змушений адаптувати свої комплаєнс-процедури до нових реалій.

## The Partnership for Information Sharing

Це новий механізм, запроваджений у законодавстві ЄС (Regulation (EU) 2024/1624), який створює **умови для обміну інформацією між підзвітними суб'єктами та відповідними органами для запобігання та боротьби з відмиванням коштів**, фінансуванням тероризму та пов'язаними злочинами. Відмінність PFIS у тому, що це не є окрема структура, а **гнучкий механізм, який дозволяє створювати кілька партнерств для обміну інформацією як на національному, так і на міжнародному рівнях.**

**Учасниками PFIS можуть бути тільки підзвітні суб'єкти** (банки, фінансові установи тощо) та, за певних умов, **компетентні органи**, зокрема підрозділи фінансової розвідки (ПФР), **наглядові органи та правоохоронні органи.** Головна мета PFIS полягає в тому, щоб полегшити обмін інформацією в межах існуючих зобов'язань щодо ПВК/ФТ, але тільки тоді, коли це є абсолютно необхідним.

**PFIS базується на принципі суворої необхідності, що означає, що інформація може обмінюватися лише тоді, коли її передача виправдана певною метою, як-от виконання зобов'язань щодо процедури належної перевірки (CDD) або подання STR/SAR**. Закон також передбачає створення єдиних звітів для зобов'язаних суб'єктів, які працюють у кількох країнах-членах, щоб уникнути дублювання звітів до ПФР у різних державах.

**Ключові висновки:**

1. **Гнучкість та інноваційність:** PFIS – це новий механізм обміну інформацією, що дозволяє створювати кілька партнерств як на національному, так і на міжнародному рівнях. На відміну від попередніх структур ЄС, цей підхід не обмежується лише групами з єдиним управлінням чи наглядом. PFIS дає змогу обмінюватися інформацією між підзвітними суб'єктами (RE) та компетентними органами, включаючи ПФР та наглядові органи. Це робить можливим обмін даними на рівні ЄС для більш скоординованої боротьби з ВК та ФТ.

2. **Сувора мета обміну інформацією:** PFIS створено виключно для боротьби з відмиванням коштів, фінансуванням тероризму та їх предикатними злочинами. Учасники можуть обмінюватися інформацією лише тоді, коли це є абсолютно необхідним для виконання зобов'язань щодо запобігання фінансовим злочинам. Зокрема, інформація повинна бути спрямована на виконання завдань з належної обачності клієнтів (CDD) або подання підозрілих повідомлень (SAR/STR). Інформація може бути обмінювана між кількома учасниками PFIS за умови відповідності регламентованим цілям.

3. **Координація з національними ПФР:** RE можуть співпрацювати з ПФР та компетентними органами для координації подання звітів про підозрілі транзакції (STR). Якщо кілька RE мають однакові підозри щодо діяльності клієнта, вони можуть призначити одного учасника для подання єдиного звіту. Це особливо важливо в транснаціональних PFIS, коли підзвітні суб'єкти з різних держав-членів ЄС мають координувати подання до національних ПФР.

4. **Захист даних:** У рамках PFIS особливу увагу приділено захисту даних. RE повинні забезпечити відповідність процесів обміну інформацією вимогам Загального регламенту захисту даних (GDPR). Перед тим, як почати обмін інформацією, PFIS повинно провести оцінку впливу на захист даних (DPIA). Це забезпечує баланс між вимогами обміну інформацією для боротьби з фінансовими злочинами та захистом особистої інформації клієнтів.

5. **Обмежений доступ до інформації:** Доступ до інформації, що обмінюється у PFIS, є суворо обмеженим. Інформація може бути передана лише тим учасникам партнерства, яким це необхідно для виконання завдань. Важливо, що інформація може стосуватися лише клієнтів

з високим ризиком ВК або ФТ, і передача даних повинна бути обмежена до тієї міри, яка необхідна для виконання завдань PFIS.

6. **Інтернаціональний підхід:** PFIS дозволяє створювати партнерства не лише на національному рівні, але й у межах кількох країн-членів ЄС. Це є важливим інструментом у розбудові єдиного європейського підходу до боротьби з фінансовими злочинами, що дозволяє координувати дії між різними країнами. Це також включає можливість обміну інформацією з органами країн, які не входять до ЄС, за умови дотримання регламентів ЄС щодо захисту даних та прав людини.

7. **Підвищені вимоги до внутрішніх політик та процедур:** Кожен RE, що бере участь у PFIS, зобов'язаний впровадити відповідні внутрішні політики та процедури, які забезпечують контроль за обсягом і характером інформації, що передається. Ці політики повинні чітко визначати оцінку ризиків, ситуації, коли можливо передавати інформацію, та визначати ролі і відповідальність кожного учасника партнерства.

8. **Незалежний аудит:** Для забезпечення належного функціонування PFIS, учасники зобов'язані замовляти незалежний аудит діяльності партнерства, якщо наглядові органи вважатимуть це необхідним. Результати таких аудитів повинні надаватися наглядовим органам для перевірки відповідності діяльності PFIS вимогам законодавства ЄС.

PFIS є важливим інструментом у посиленні боротьби з відмиванням коштів і фінансуванням тероризму на рівні ЄС, забезпечуючи одночасно належний захист персональних даних та суворе дотримання регламентів.

# САНКЦІЇ

## Потужний удар санкцій: США б'є по таємним угодам Росії та Північної Кореї


Стаття описує нові санкції США, спрямовані на припинення таємних фінансових операцій між Росією та Північною Кореєю, які допомагають обходити міжнародні санкції. Міністерство фінансів США наклало санкції на п’ять компаній і одну фізичну особу, пов’язаних із фінансовими мережами, які фінансують розробку ядерної та балістичної зброї Північної Кореї. Ці мережі також підтримують Росію в її війні проти України. У списку підсанкційних суб’єктів фігурує регіон Південної Осетії, який також був залучений до таких операцій.

Санкції спрямовані на посилення міжнародної безпеки, обмеження доступу Росії до фінансових ресурсів і зупинку розвитку програм зброї масового знищення в Північній Кореї. США прагнуть досягти ширшого впливу на глобальні фінансові ринки шляхом залучення до відповідальності учасників цих операцій, що порушують міжнародне право.

https://regtechtimes.com/powerful-sanctions-strike-u-s-targets-russia-and/

## Керівництво з цивільного виконання санкцій щодо торгівлі, авіації та судноплавства у Великобританії


Керівництво роз’яснює обов’язки, накладені на фізичних та юридичних осіб відповідно до регламентів 2024 року. Відповідно до цих положень, впроваджуються суворі штрафи за порушення санкцій, зокрема через невиконання вимог про надання інформації та звітність. Офіс з впровадження санкцій (OTSI) отримує повноваження накладати грошові штрафи до £1 мільйона або 50% вартості порушення, а також оприлюднювати інформацію про порушення та передавати справи для кримінальних розслідувань.

**Ключові висновки**

1. **Сувора відповідальність:** OTSI може накладати санкції незалежно від умислу. Це означає, що компанії чи фізичні особи можуть бути оштрафовані навіть за відсутності обізнаності про порушення.
2. **Фінансові санкції:** OTSI має право накладати штрафи до £1 мільйона або 50% від вартості порушення (залежно від того, яка сума більша). Ця значна міра покликана стимулювати дотримання санкційного режиму.
3. **Публікація порушень:** OTSI може оприлюднювати інформацію про порушення санкцій. Це служить як попередження для інших гравців ринку та є частиною механізму забезпечення прозорості.
4. **Співпраця з іншими органами:** OTSI тісно співпрацюватиме з іншими британськими органами, такими як HMRC, для проведення кримінальних розслідувань у разі порушення торгівельних санкцій, що має на меті посилення координації у виконанні санкційного режиму.
5. **Добровільне розкриття порушень:** OTSI стимулює компанії та фізичних осіб до добровільного розкриття інформації про можливі порушення. Це може бути суттєвим пом'якшувальним фактором, який може зменшити штрафи до 50%.

6. **Нові звітні вимоги:** Керівництво встановлює чіткі вимоги до звітування, що покладаються на "відповідних осіб", таких як фінансові інституції та оператори авіаційної та морської галузей. Ці особи повинні повідомляти про порушення санкцій, якщо вони дізналися про це під час виконання своїх професійних обов'язків.

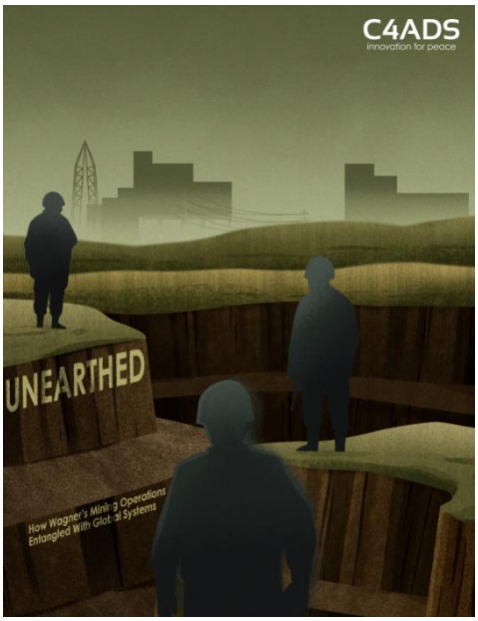
7. **Підвищені вимоги до комплаєнсу:** Компанії повинні оновити свої процедури комплаєнсу, щоб вони відповідали новим стандартам, оскільки навіть найсучасніші програми дотримання можуть не гарантувати захисту від відповідальності за порушення.

8. **Важливість надання інформації:** OTSI має право вимагати надання документів і інформації, що стосуються санкційних порушень або виконання ліцензій на торгівлю. Це підвищує вимоги до прозорості операцій і забезпечення дотримання нормативно-правових актів.

http://surl.li/uvtndv

# ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

## Як видобувна діяльність Вагнера переплiталася з глобальними системами




Документ під назвою "Unearthed" від організації C4ADS досліджує діяльність приватної військової компанії (ПВК) "Вагнер" в Африці, зокрема у таких країнах як Судан і Центральноафриканська Республіка (ЦАР). **Основна увага приділяється тому, як ПВК "Вагнер" використовувала легальні міжнародні фінансові, транспортні та логістичні мережі для ведення своєї видобувної діяльності, що дозволило приховати зв'язки між законними та нелегальними діями. У звіті детально описуються основні механізми, які компанія використовувала для переміщення ресурсів і коштів, залучення західних банків і міжнародних транспортних компаній, які, часто не знаючи цього, обслуговували діяльність ПВК "Вагнер"**. Завдяки взаємодії з місцевими політиками та використанню фіктивних компаній, ПВК змогла інтегруватися у видобувні сектори цих країн.

**Документ підкреслює, що незважаючи на міжнародні санкції, компанії, пов'язані з ПВК "Вагнер", продовжували свою діяльність у видобувній сфері, використовуючи складні фінансові та транспортні шляхи**. Проаналізовані дані з leaked contracts показують, що угоди, підписані з компаніями в Китаї, Росії та Африці, включали переміщення коштів через банки-посередники, такі як JPMorgan і HSBC. ПВК "Вагнер" також використовувала західні судноплавні компанії для транспортування обладнання та матеріалів.

**Ключові висновки:**

1. **Використання міжнародних фінансових і транспортних мереж:** ПВК "Вагнер" спромоглася вбудуватися в глобальну фінансову та логістичну інфраструктуру, використовуючи західні банки та транспортні компанії для пересування коштів і ресурсів. Ці операції часто залишалися непоміченими, що дозволило організації вести незаконну діяльність в Африці через легальні канали.
2. **Взаємодія між легальними та нелегальними системами:** ПВК використовувала фіктивні компанії та місцевих посередників для маскування своєї діяльності, що ускладнювало виявлення її зв'язків з незаконною експлуатацією природних ресурсів. Такі компанії часто виглядали незалежними, але насправді діяли в інтересах Пригожина та його мережі.
3. **Роль західних банків і транспортних компаній:** Західні банки, зокрема JPMorgan та HSBC, були залучені як посередники для фінансових операцій ПВК "Вагнер". Ці банки, хоч і не знали про зв'язок з ПВК, зіграли ключову роль у забезпеченні фінансової підтримки операцій в Судані та Центральноафриканській Республіці (ЦАР). Транспортні компанії, такі як Maersk та Mediterranean Shipping Company, також були залучені до перевезення матеріалів для видобувної діяльності.
4. **Спроби обходу санкцій через фіктивні компанії:** Після введення санкцій проти компаній, пов'язаних з ПВК "Вагнер", організація вдалася до створення фіктивних компаній, щоб продовжити свою діяльність під іншими назвами. Наприклад, компанія Al-Solag Mining була використана замість Meroe Gold для продовження експлуатації золотих копалень у Судані.
5. **Розширення операцій після санкцій:** Незважаючи на міжнародні санкції, діяльність компаній, пов'язаних з ПВК "Вагнер", продовжувалася і навіть розширювалася. Наприклад, супутникові зображення показали, що видобувні операції в ЦАР, зокрема на золотому руднику Ndassima, збільшилися після введення санкцій у 2023 році.
6. **Необхідність підвищення контролю та співпраці:** Для ефективної протидії подібним організаціям необхідне посилення міжнародного контролю за фінансовими та логістичними мережами, які використовуються для переміщення ресурсів. Співпраця між банками,

транспортними компаніями та урядовими органами є критично важливою для відстеження та блокування незаконних операцій.

7. **Роль після смерті Пригожина:** Після загибелі Євгена Пригожина у 2023 році деякі елементи ПВК "Вагнер" були інтегровані в структури Міністерства оборони Росії. Це створює нові виклики для міжнародного співтовариства щодо контролю та впровадження санкцій, оскільки операції можуть продовжуватися під егідою російських державних органів.

https://c4ads.org/wp-content/uploads/2024/09/Unearthed-C4ADS.pdf

## Використання криптовалют для фінансування дезінформаційних кампаній та підривної діяльності: виклики та можливості для протидії


Документ «Malign Interference and Crypto» досліджує, як криптовалюти можна використовувати для виявлення та зупинення операцій з дестабілізації, зокрема в контексті кампаній дезінформації. У звіті надані приклади, які демонструють, як державні та недержавні суб'єкти використовують криптовалюти для фінансування дезінформаційних кампаній, впливових операцій та інших незаконних дій. Водночас наголошується на тому, що блокчейн-технології, хоч і використовуються для таких операцій, також забезпечують прозорість, що дозволяє відслідковувати рух коштів і виявляти мережі, які стоять за цими операціями. Документ розглядає конкретні випадки російського втручання, фінансування парамілітарних угруповань та дезінформаційних медіа, таких як SouthFront та російські військові блогери, які використовують криптовалюти для фінансування своїх операцій.

**Ключові висновки:**

1. **Криптовалюти як інструмент фінансування дезінформаційних кампаній**:

   - Криптовалюти часто використовуються для фінансування дезінформаційних операцій завдяки їхній сприйнятій анонімності та глобальному доступу. Однак технологія блокчейн дозволяє відслідковувати ці транзакції, що надає урядовим органам можливість ідентифікувати й відстежувати суб'єктів, причетних до таких кампаній.

   - У випадку російського втручання, дезінформаційні платформи, такі як SouthFront, використовують криптовалютні пожертви для фінансування своєї діяльності. Подібні групи отримують кошти через Bitcoin та інші криптовалюти, що дозволяє зберігати анонімність і уникати санкцій.

2. **Використання криптовалют парамілітарними угрупованнями**:

   - Російські парамілітарні угруповання, такі як Task Force Rusich та інші, активно залучають криптовалютні пожертви для фінансування військових дій, зокрема у війні проти України. Використання криптовалют дозволяє їм обходити міжнародні санкції та забезпечувати свою діяльність за допомогою глобальних донорів.

   - Ці групи, включно з Wagner Group, використовують Telegram та інші соціальні платформи для поширення дезінформації та збору пожертвувань. У звіті підкреслюється, що такі донори часто підтримують кілька різних екстремістських угруповань одночасно, що ускладнює боротьбу з їхньою діяльністю.

3. **Санкції OFAC та блокування криптовалютних адрес**:

   - Міністерство фінансів США (OFAC) активно застосовує санкції до осіб та організацій, причетних до підривної діяльності. Часто в цих санкціях зазначаються криптовалютні адреси, що дозволяє відстежувати рух коштів та блокувати транзакції.

- Наприклад, у березні 2024 року OFAC наклало санкції на російських громадян Іллю Гамбашидзе та Миколу Тупікіна за їхню участь у кампаніях дезінформації. У санкційні списки було додано їхні криптовалютні гаманці, що містили понад 200 тис. доларів у Tether, які були заморожені.

4. **Глобальна загроза дезінформації**:

   - Дезінформаційні кампанії є глобальною проблемою, і їхні наслідки відчуваються далеко за межами США та Європи. Наприклад, російська дезінформація активно поширюється в Латинській Америці, а китайські операції впливу – в Азіатсько-Тихоокеанському регіоні.

   - Іран також використовує криптовалюти для фінансування своїх дезінформаційних кампаній. Наприклад, Іранське інформаційне агентство Islamic World News (ISWN) має зв'язки з російськими пропагандистськими організаціями і також отримує криптопожертви для фінансування пропаганди та військових операцій.

5. **Технології для відстежування криптовалютних транзакцій**:

   - У звіті наголошується на важливості використання інструментів для аналізу блокчейну, таких як Chainalysis, які дозволяють відстежувати транзакції криптовалют та ідентифікувати підозрілих осіб і групи.

   - Завдяки прозорості блокчейнів, уряди можуть ефективніше виявляти зв'язки між дезінформаційними кампаніями, військовими угрупованнями та їхніми джерелами фінансування. Наприклад, було виявлено взаємопов'язані криптотранзакції між такими групами, як SouthFront, ISWN та парамілітарними організаціями, які обмінювалися коштами через криптовалютні біржі.

6. **Зв'язки з нелегальними онлайн-сервісами**:

   - Дезінформаційні суб’єкти часто користуються послугами нелегальних онлайн-сервісів для покупки вкрадених акаунтів соціальних мереж або для оренди інфраструктури для своїх операцій. У звіті згадується Ubar Store – російський нелегальний сервіс, який продає вкрадені акаунти для масштабування дезінформаційних кампаній, отримуючи оплату в криптовалюті.

   - Такі послуги дозволяють зловмисникам уникати перевірок і використовувати легітимні платформи для поширення фальшивої інформації.

7. **Інфраструктура для підтримки дезінформаційних кампаній**:

   - Окрім вкрадених акаунтів, суб’єкти дезінформації використовують хостингові та інші технологічні сервіси, щоб поширювати фальшиві новини. Наприклад, хостингова компанія Shinjiru (Малайзія) була використана для розміщення сайту DCLeaks, який відіграв ключову роль у втручанні Росії у вибори 2016 року в США.

   - Хоча такі сервіси можуть бути законними, вони також надають інфраструктуру для незаконної діяльності. Криптовалюти часто використовуються для оплати таких послуг, що створює додаткові можливості для розслідувань на основі блокчейну.

8. **Роль міжнародної співпраці**:

   - Оскільки дезінформаційні кампанії є глобальною загрозою, міжнародна співпраця стає критично важливою для ефективного протистояння цьому явищу. Різні уряди та міжнародні організації повинні співпрацювати для відстеження транзакцій, ідентифікації зловмисників та блокування джерел їхнього фінансування.

   - Використання криптотехнологій як інструменту підривних операцій є тенденцією, що тільки зростає, особливо з розвитком технологій штучного інтелекту та кібероперацій.

Звіт закликає до міжнародної співпраці у боротьбі з використанням криптовалют у дестабілізаційних операціях, наголошуючи на тому, що ці дії становлять зростаючу глобальну загрозу для демократії та стабільності.

https://www.chainalysis.com/wp-content/uploads/2024/07/malign-interference-and-crypto-release.pdf

## Взаємодія платіжних систем: ключ до ефективних транскордонних фінансових операцій


Документ "The road ahead: Towards seamless payment interoperability" досліджує важливість та проблеми взаємодії різних платіжних систем у сучасній цифровій економіці, особливо в контексті транскордонних платежів. У звіті детально розглядаються технічні стандарти, закони і регулювання, які формують екосистему глобальних платежів, а також проблеми, які виникають через відсутність взаємодії між платіжними системами. Документ також пояснює, як технологічні рішення, такі як API, блокчейн і реальні платіжні мережі, можуть сприяти інтеграції платіжних систем. Особливу увагу приділено ролі регуляторних ініціатив та стандартів, таких як ISO 20022, у розвитку транскордонних платежів.

**Ключові висновки:**

1. **Взаємодія платіжних систем критично важлива для економічного зростання:** Можливість різних платіжних систем безперешкодно обмінюватися інформацією та транзакціями допомагає стимулювати глобальну торгівлю, знижувати витрати на транзакції та покращувати інноваційні рішення. Відсутність цієї взаємодії призводить до додаткових витрат, обмежує доступ бізнесу до ринків та стримує зростання.

2. **Складнощі взаємодії платіжних систем через застарілі технології:** Багато платіжних систем були розроблені без урахування потреб у майбутній інтеграції, що створює технічні бар'єри. Також виникають проблеми з регуляторними обмеженнями, коли певні платіжні методи не відповідають стандартам інших країн.

3. **Транскордонні платежі стають дедалі важливішими:** За прогнозами, ринок міжнародних платежів у 2023 році оцінюється в 190,1 трлн доларів США. Зростання цього ринку пов'язане зі збільшенням міграції, попиту на грошові перекази, розширенням ланцюгів постачання та зростанням електронної комерції.

4. **Регуляторні стандарти відіграють ключову роль:** Стандарти ISO 20022 та ініціативи G20 сприяють покращенню взаємодії між платіжними системами. Наприклад, впровадження ISO 20022 збільшує прозорість і доступність даних у банківських операціях.

5. **Інноваційні технології, такі як блокчейн та API, сприяють вирішенню проблем з інтеграцією:** API дозволяють різним платіжним системам обмінюватися інформацією та забезпечують зручніший процес обробки транзакцій. Блокчейн зменшує залежність від посередників і забезпечує швидшу та безпечнішу взаємодію між різними системами.

6. **Перспективи взаємодії цифрових валют:** Цифрові валюти Центрального банку (CBDC) та криптовалюти можуть значно вплинути на платіжну взаємодію, але їх інтеграція в існуючі системи вимагатиме значних змін у технологіях і стандартах.

7. **Транскордонні ініціативи для покращення платежів:** Програми, такі як SEPA у Європі та платіжні мережі в Азії, демонструють успіх у створенні інтегрованих рішень для транскордонних платежів, що сприяє спрощенню міжнародної фінансової взаємодії.

Загалом, документ підкреслює важливість спільної роботи урядів, банків та технологічних компаній для створення ефективної глобальної платіжної системи, яка зможе адаптуватися до сучасних вимог ринку і сприяти фінансовій інклюзії.

https://www.thunes.com/the-road-ahead-seamless-payment-interoperability/

## Огляд можливостей FinTech у Саудівській Аравії


Документ "Unlocking the Future: An Overview of the FinTech Opportunity in Saudi Arabia" надає **комплексний огляд розвитку фінансових технологій у Саудівській Аравії в контексті амбітної стратегії Vision 2030**. Після ухвалення плану розвитку фінансового сектора країна продемонструвала значний прогрес у цифровізації фінансових послуг, залученні інвестицій, розвитку малого і середнього бізнесу та стартапів. **Документ аналізує ключові напрями, такі як регуляторні зміни, впровадження інновацій, розвиток відкритого банкінгу, цифрових гаманців, кредитування та інші фінансові рішення. Також значна увага приділяється залученню глобальних інвесторів, розвитку фінансових технологій та створенню інфраструктури для подальшого зростання фінтеху.**

**Ключові висновки:**

1. **Роль фінтеху у Vision 2030:** Фінансові технології є важливим елементом у диверсифікації економіки Саудівської Аравії. З моменту впровадження Vision 2030, країна демонструє прогрес у цифровізації фінансових послуг, зокрема, завдяки підвищенню інвестицій і розвитку стартапів. Це сприяє зростанню економіки, зменшенню залежності від нафтогазового сектора, а також стимулює інновації.

2. **Зростання фінтех-компаній та стартапів:** У 2024 році Саудівська Аравія перевершила очікування за кількістю фінтех-компаній, що виросла до 226, із середньорічним темпом зростання 61%. Більшість з них працюють у галузі цифрових платежів, що складає 30% від усіх фінтехів, з великою часткою також у таких секторах, як краудфандинг, InsurTech, та RegTech. Очікується подальше зростання у міру розвитку відкритого банкінгу та цифрових банків.

3. **Підтримка з боку уряду та регуляторів:** Саудівський центральний банк (SAMA) і Управління з питань ринку капіталу (CMA) відіграють ключову роль у створенні сприятливого середовища для розвитку фінтеху. Вони запровадили регуляторні пісочниці, відкритий банкінг, а також ініціативи для підтримки малих і середніх підприємств. Нові правила для компаній BNPL (Buy Now Pay Later) і запуск лабораторії відкритого банкінгу стимулюють інновації та посилюють регуляторний нагляд.

4. **Інвестиційний бум:** Незважаючи на глобальні труднощі з венчурним фінансуванням, Саудівська Аравія продовжує залучати значні інвестиції в фінтех. У 2023 році було інвестовано 791 мільйон доларів США, що є збільшенням на 231% порівняно з попереднім роком. Ключовими секторами інвестицій залишаються цифрові платежі та BNPL, зокрема, компанії Tabby та Tamara залучили суттєві суми для розширення.

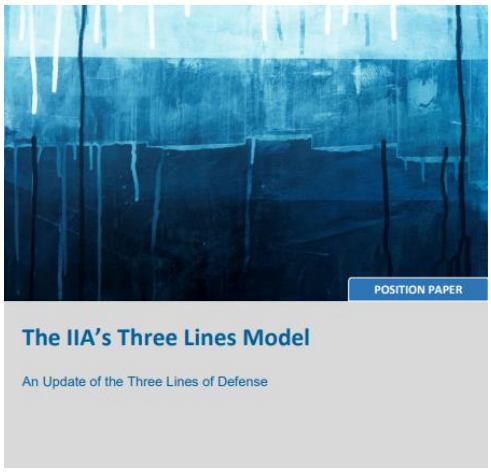
5. **Майбутні тренди:** Очікується, що технологічні інновації, такі як Web3, цифрові двійники та просторові обчислення (AR, VR), продовжать впливати на фінансовий сектор Саудівської Аравії. Запровадження відкритих банків, цифрових банків, а також інвестиції в сталий розвиток та кліматичні технології зміцнять позицію країни як глобального фінтех-хабу.

6. **Виклики для довгострокового зростання:** Для підтримання зростання та утвердження на світовому ринку фінтеху Саудівська Аравія повинна посилити регуляторні рамки для адаптації до швидких технологічних змін і дотримуватися міжнародних стандартів.

Інфраструктурні інвестиції, розвиток фінансової грамотності та забезпечення інклюзивності також є ключовими факторами для стійкого розвитку.

https://assets.kpmg.com/content/dam/kpmg/sa/pdf/2024/09/unlocking-future-fintech-sa.pdf

## Три лінії захисту




Документ "The Three Lines Model" є оновленою версією попередньої концепції "Три лінії захисту", яка застосовується для управління ризиками та покращення корпоративного управління. Модель була створена для організацій, що працюють в умовах постійної невизначеності та складності, з метою допомогти їм досягати своїх цілей через розподіл ролей та відповідальності. У моделі три основні складові: управління (перша лінія), підтримка та моніторинг ризиків (друга лінія) та внутрішній аудит (третя лінія). Управлінська відповідальність розподілена між керівним органом і управлінням компанії, що відповідає за управління ризиками, тоді як внутрішній аудит забезпечує незалежний нагляд і оцінку. Основна мета моделі полягає в тому, щоб створювати та захищати вартість організації, забезпечуючи при цьому прозорість та ефективне управління ризиками. Модель також підкреслює важливість координації та комунікації між усіма учасниками для досягнення синхронізованої роботи організації.

**Ключові висновки:**

1. **Принцип управління та відповідальності:** Відповідальність за управління організацією покладена на керівний орган, який делегує ресурси та повноваження управлінню для досягнення стратегічних цілей. Ключовим є прозоре управління через процеси ризик-менеджменту та відповідальність перед стейкхолдерами. Це вимагає від керівного органу формувати чіткі структури та процедури для забезпечення прозорості, етики та управління ризиками на всіх рівнях організації.

2. **Розподіл ролей між першою, другою та третьою лініями:** Перша лінія (управління) відповідає за щоденне управління бізнесом та реалізацію завдань, безпосередньо пов'язаних з клієнтами. Друга лінія забезпечує підтримку та моніторинг процесів управління ризиками, включаючи контроль за дотриманням законодавства, етичних норм, безпекою даних та якістю операцій. Третя лінія (внутрішній аудит) має незалежну позицію і забезпечує об'єктивну оцінку ефективності управління та контролю.

3. **Незалежність внутрішнього аудиту:** Основою третьої лінії є її незалежність від управлінських функцій, що дозволяє внутрішньому аудиту забезпечувати об’єктивність у наданні рекомендацій та проведенні оцінок ризиків. Важливо, щоб внутрішній аудит був підзвітний безпосередньо керівному органу, що захищає його від втручання з боку управління і дозволяє зберігати авторитет та довіру до його діяльності.

4. **Створення та захист вартості:** Всі лінії повинні працювати спільно для досягнення організаційних цілей та захисту вартості. Це досягається через інтегровану співпрацю між управлінням, керівними органами та внутрішнім аудитом, що забезпечує прозорість процесів прийняття рішень та належне управління ризиками. Кожна з трьох ліній виконує унікальні функції, які мають бути синхронізовані для підтримки ефективної роботи організації.

5. **Співпраця та координація:** Успішне впровадження моделі вимагає чіткої координації між усіма учасниками. Комунікація між першою, другою та третьою лініями повинна бути регулярною і ефективною, щоб уникнути дублювання функцій та прогалин у процесах

управління ризиками. Важливо, щоб внутрішній аудит тісно співпрацював з управлінськими структурами для забезпечення актуальності своїх оцінок і висновків, що сприяє кращому прийняттю рішень та досягненню цілей організації.

6. **Адаптація моделі до потреб організації:** Модель "Трьох ліній" є універсальною і може бути адаптована до будь-якої організації. Вона дозволяє враховувати специфічні потреби кожної компанії, зокрема розмір, структуру та сферу діяльності. Організації можуть впроваджувати різні рівні нагляду, створювати додаткові комітети для аудиту, ризиків чи фінансового планування, щоб забезпечити належну відповідність внутрішніх структур та процесів до їхніх цілей і стратегії.

http://surl.li/qnzoon

# РЕКОМЕНДОВАНІ МАТЕРІАЛИ

## Виклик обходу санкцій

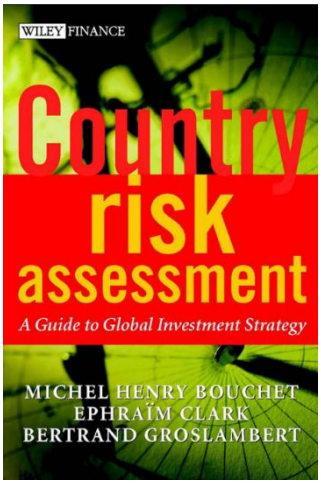
🔍Обхід санкцій є центральною темою в політичних дискусіях щодо обмежувальних заходів — проблеми, яка досліджується в серії подкастів RUSI «Звіт про підозрілі транзакції» на початку цього року.

⚠Нещодавні викриття, опубліковані в Financial Times, щодо використання Вагнером Євгена Пригожина таких великих банків, як JPMorgan і HSBC, щоб обійти санкції, підкреслюють, наскільки критичною є ця проблема.

🎯Такі звіти підкреслюють важливість роботи в сфері протидії обходу санкцій, оскільки досліджується, що насправді означає обхід санкцій, як це підриває глобальні зусилля щодо забезпечення відповідальності та що можна зробити, щоб закрити ці лазівки.

https://www.rusi.org/podcasts/suspicious-transaction-report/episode-7-challenge-sanctions-circumvention

## Оцінка ризиків країн: Посібник з глобальної інвестиційної стратегії




Автори: Мішель Генрі Буше, Ефраїм Кларк та Бертран Гросламбер

📘 Короткий зміст книги

1. Вступ

   - 📜 *Історичний контекст ризиків країн*: Вивчення історичних прикладів економічних криз та їх впливу на сучасні підходи до оцінки ризиків.

   - 🌍 *Вплив глобалізації на економічні кризи*: Аналіз того, як глобалізація впливає на поширення економічних криз.

2. Огляд ризиків країн

   - 🛡 *Визначення та класифікація ризиків*: Розгляд різних типів ризиків, включаючи природні катастрофи, соціально-політичні та економічні ризики.

   - 🔍 *Джерела ризиків*: Вивчення основних джерел ризиків, таких як природні катастрофи, політична нестабільність та економічні фактори.

3. Економічні та фінансові основи оцінки ризиків країн

   - 📉 *Вплив девальвації на економіку*: Аналіз наслідків девальвації для економіки країни.

   - 💰 *Монетарний підхід до аналізу платіжного балансу*: Вивчення монетарних факторів, що впливають на платіжний баланс.

4. Методології оцінки ризиків країн: якісний підхід

   - 📊 *Аналіз соціальних та економічних показників*: Використання соціальних та економічних показників для оцінки ризиків.

   - 💼 *Оцінка зовнішньої заборгованості та ліквідності*: Аналіз зовнішньої заборгованості та ліквідності країни.

5. Методології оцінки ризиків: рейтинги

- 🌐 *Глобальні рейтинги ризиків країн*: Огляд основних рейтингів ризиків країн.

- 📈 *Кредитні рейтинги країн*: Аналіз кредитних рейтингів та їх вплив на інвестиційні рішення.

6. Економетричні та математичні методи

- 📉 *Дискримінантний аналіз*: Використання дискримінантного аналізу для оцінки ризиків.

- 📊 *Логіт та пробіт моделі*: Застосування логіт та пробіт моделей для прогнозування ризиків.

- 📈 *Регресійний аналіз та моделювання*: Використання регресійного аналізу для моделювання ризиків.

7. Моделі ризиків

- 💳 *Оцінка кредитного ризику*: Методи оцінки кредитного ризику.

- 📉 *Інвестиційний ризик та його вплив на рішення*: Аналіз інвестиційного ризику та його вплив на прийняття рішень.

Висновок

- 🏘️ *Комплексний підхід до оцінки ризиків країн*: Важливість інтеграції кількісних та якісних методів для точнішої оцінки ризиків.

- 🔄 *Важливість постійного моніторингу*: Необхідність постійного оновлення даних для актуальності оцінок.

Рекомендації

- 🛠️ *Використання різних методологій*: Рекомендації щодо використання різних методологій для точнішої оцінки ризиків.

- 📊 *Моніторинг та оновлення даних*: Поради щодо постійного моніторингу та оновлення даних для забезпечення актуальності оцінок.

---

📘 *Оцінка ризиків країн: Посібник з глобальної інвестиційної стратегії* - це незамінний ресурс для інвесторів, аналітиків та економістів, які прагнуть зрозуміти та управляти ризиками, пов'язаними з інвестиціями в різні країни. Автори пропонують глибокий аналіз методологій та інструментів, що допомагають оцінити ризики та приймати обґрунтовані інвестиційні рішення.

🔍 *Основні теми:*

- Історичний контекст та вплив глобалізації на економічні кризи

- Класифікація та джерела ризиків країн

- Економічні та фінансові основи оцінки ризиків

- Якісний та кількісний підходи до оцінки ризиків

- Використання економетричних та математичних методів

📊 *Методології:*

- Дискримінантний аналіз

- Логіт та пробіт моделі

- Регресійний аналіз та моделювання

- Оцінка кредитного ризику та інвестиційного ризику

🌍 *Практичне застосування:*

- Оцінка ризиків для інвестиційних рішень

- Моніторинг та управління ризиками в умовах глобальної економіки

---

🔗 *Детальніше про книгу та її авторів:*

- Мішель Генрі Буше, Ефраїм Кларк та Бертран Гросламбер - провідні експерти в галузі фінансів та економіки, які мають багаторічний досвід у дослідженні ризиків країн.

📚 *Рекомендовано для:*

- Інвесторів

- Фінансових аналітиків

- Економістів

- Студентів та викладачів економічних факультетів

http://surl.li/jnatpm

# ІНШІ НОВИНИ

## Євген Пригожин таємно використовував JPMorgan і HSBC для платежів Wagner

Стаття розповідає, як JPMorgan Chase і HSBC опрацьовували платежі для африканських компаній, пов'язаних із Євгенієм Пригожиним і його приватною армією "Вагнер". Документи, отримані Центром досліджень передової оборони (C4ADS), показують, що у 2017 році через ці банки здійснювалися транзакції на користь китайських компаній для придбання обладнання. Ці операції дозволили Пригожину побудувати кримінальну імперію в Африці, експлуатуючи природні ресурси через фінансові системи Заходу.

C4ADS зазначає, що операції "Вагнера" в Африці були можливі завдяки використанню легальних фінансових структур для незаконної діяльності. Через такі схеми "Вагнер" зміг закріпитися в країнах, як-от Судан та Центральноафриканська Республіка, де використовував мережі фінансових та транспортних послуг для пересування ресурсів та отримання прибутків.

Після загибелі Пригожина у 2023 році операції "Вагнера" в Африці були інтегровані в структури, що контролюються безпосередньо Міністерством оборони Росії.

https://www.ft.com/content/4e6062da-61b6-4f2e-8995-52793225f77e

## Серйозні порушення банком Mirabaud & Cie SA законодавства про фінансові ринки: заходи FINMA та наслідки

Документ — пресреліз швейцарського органу з нагляду за фінансовими ринками (FINMA), що повідомляє про серйозні порушення закону про фінансові ринки банком **Mirabaud & Cie SA**. У результаті розслідування FINMA було встановлено, що банк порушив зобов'язання щодо протидії відмиванню коштів. Mirabaud неадекватно перевірив та задокументував економічну суть клієнтських відносин і транзакцій, що створило підвищені ризики для відмивання коштів. Банк також не забезпечив достатньо ефективне управління ризиками для запобігання цим порушенням. Як результат, FINMA заборонила банку приймати нових клієнтів із підвищеним ризиком відмивання коштів до відновлення дотримання вимог законодавства, конфіскувала незаконно отримані прибутки у розмірі 12,7 мільйона швейцарських франків і розпочала три окремі провадження проти фізичних осіб.

finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

**Ключові висновки:**

1. **Серйозні порушення вимог фінансового ринку**: Банк Mirabaud & Cie SA виявився винним у недостатньому контролі за клієнтськими відносинами та транзакціями, що створювало підвищений ризик відмивання коштів, зокрема у зв'язку з кваліфікованим ухиленням від сплати податків.

2. **Недостатня організація та управління ризиками**: Банк не мав адекватної структури управління та механізмів для належного моніторингу та запобігання ризикам відмивання коштів, незважаючи на явні попередження з 2018 року.

3. **Фінансові санкції**: FINMA конфіскувала 12,7 мільйона франків незаконно отриманих прибутків, а також запровадила обмеження на прийняття нових клієнтів з підвищеним ризиком до повного відновлення відповідності законодавству.

4. **Запроваджені заходи**: Банк співпрацював з FINMA під час розслідування та вжив певних заходів для поліпшення системи управління ризиками та протидії відмиванню коштів.

Однак регулятор зобов’язав банк продовжити перегляд усіх клієнтських відносин з підвищеними ризиками та вдосконалити політику оплати праці для відповідального управління ризиками.

5. **Розслідування щодо посадових осіб**: Окрім заходів проти банку, FINMA розпочала три провадження проти фізичних осіб, пов’язаних із цими порушеннями, але не розкрила їхніх імен.

Цей випадок підкреслює важливість дотримання суворих стандартів у сфері протидії відмиванню коштів та управління ризиками у фінансових установах, а також демонструє роль регуляторів у забезпеченні фінансової безпеки.

http://surl.li/cpmgzt

## Шахрайство та криптовалюта в Німеччині: уряд Німеччини закрив 47 бірж за порушення KYC та відмивання коштів

Стаття описує нещодавні дії уряду Німеччини, спрямовані на закриття 47 криптовалютних бірж, які порушили вимоги щодо процедур "Знай свого клієнта" (KYC) та законів про боротьбу з відмиванням коштів (AML). Цей захід підкреслює зростаючу стурбованість німецького уряду щодо використання криптовалют для нелегальної діяльності, зокрема шахрайства, відмивання грошей та інших фінансових злочинів. Біржі, які не дотримуються цих вимог, надають можливості для прихованих операцій, що ускладнює їх виявлення та контроль з боку правоохоронних органів.

Згідно з регуляторними вимогами, криптовалютні платформи повинні забезпечувати належний нагляд за своїми користувачами через процеси KYC та AML. Це передбачає перевірку ідентифікаційних даних клієнтів, моніторинг підозрілих транзакцій та звітування про будь-яку активність, що може бути пов’язана з фінансовими злочинами. Проте багато бірж не виконують ці вимоги, що призвело до таких жорстких дій з боку уряду.

Закриття бірж також вказує на зростаючу тенденцію у світі щодо більш жорсткого регулювання криптовалютного сектора, особливо в Європі. Криптовалюти мають високий потенціал для використання у схемах ухилення від податків та фінансування тероризму, що робить цей сектор важливою метою для урядів, які прагнуть посилити глобальну фінансову безпеку.

Німецькі регулятори прагнуть продемонструвати, що навіть у сфері децентралізованих активів необхідно забезпечити прозорість і відповідність до міжнародних стандартів. Цей випадок підкреслює потребу криптоплатформ у дотриманні суворих вимог для забезпечення легальної та безпечної діяльності в межах країни та за її межами.

Такі кроки Німеччини є частиною загальноєвропейських зусиль із посилення контролю за криптовалютним ринком, що швидко розвивається. Це також сигнал для інших країн та криптовалютних бірж у світі, що порушення вимог KYC та AML не залишаться безкарними.

http://surl.li/uwrsps

# ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

## ПВК у страхуванні: як виявити та боротися з відмиванням коштів

Стаття на ComplyAdvantage глибоко аналізує важливість впровадження механізмів протидії відмиванню коштів (AML) у страховій галузі. У ній пояснюється, що страхові компанії, особливо ті, що займаються страхуванням життя, піддаються високим ризикам через великі грошові транзакції та тривалість дії контрактів. Шахраї можуть використовувати страхові продукти для відмивня грошей, укладаючи поліси з великими преміями, а потім достроково їх викуповуючи. Регулятори вимагають від страхових компаній впровадження більш жорстких заходів контролю, включаючи перевірку клієнтів (CDD) та моніторинг транзакцій.

AML у страховій галузі включає кілька ключових аспектів, серед яких:

1. **Оцінка ризиків:** Страхові компанії повинні здійснювати оцінку ризиків кожного клієнта і транзакції, щоб виявляти підозрілі дії. Це може включати перевірку джерел доходів клієнтів, вивчення їхньої фінансової історії та оцінку їхньої репутації на ринку.
2. **Належна перевірка клієнтів (CDD):** Страховики повинні здійснювати глибоку перевірку клієнтів як на етапі початкової угоди, так і під час всієї тривалості контракту. Це допомагає виявляти потенційних ризиків відмивання коштів, особливо коли йдеться про високі страхові виплати або страхові продукти з можливістю дострокового викупу.
3. **Моніторинг транзакцій:** Страхові компанії повинні впроваджувати сучасні системи моніторингу, що дозволяють виявляти підозрілі транзакції в режимі реального часу. Це допомагає запобігти зловживанням через укладання фіктивних полісів або надмірно складні схеми виплат.
4. **Міжнародні регуляторні вимоги:** Страховики зобов'язані дотримуватися вимог регуляторів різних країн, включно з FATF (Financial Action Task Force) та іншими міжнародними організаціями, які встановлюють стандарти боротьби з відмиванням коштів. Компанії повинні регулярно оновлювати свої політики та процедури відповідно до нових вимог.
5. **Підвищення обізнаності персоналу:** Окрім технічних систем, страхові компанії повинні навчати своїх співробітників, щоб вони могли розпізнавати потенційні схеми відмивання коштів. Підвищення обізнаності та впровадження стандартних операційних процедур є важливими для виявлення та запобігання порушенням.

Висновки підкреслюють необхідність тісної співпраці між страховиками, регуляторами та іншими фінансовими установами для посилення контролю за відмиванням грошей у секторі.

http://surl.li/ntpvvv

## Фінансування транснаціональних репресій – це форма фінансування тероризму


Сучасний світ стикається з новими викликами у сфері глобальної безпеки, одним із яких є феномен транснаціональних репресій. Це явище охоплює переслідування, залякування, викрадення або інші форми тиску на опонентів уряду чи режиму, навіть за межами країни походження. Фінансування таких репресивних заходів має багато спільного з фінансуванням тероризму.

По-перше, обидві форми фінансування спрямовані на придушення свободи вираження поглядів і порушення основоположних прав людини. Фінансування тероризму підтримує насильницькі дії з

метою залякування суспільства та досягнення політичних цілей. Аналогічно, транснаціональні репресії використовують ресурси для насильницького пригноблення політичних противників та інакодумців, зокрема через викрадення, вбивства чи залякування. Такий підхід підриває демократію і верховенство права.

По-друге, джерела фінансування для обох явищ часто мають подібне походження. Недержавні актори, злочинні угруповання або корумповані уряди використовують нелегальні або напівлегальні схеми для підтримки своїх операцій за кордоном. Це можуть бути кошти, отримані від незаконних операцій, корупції або торгівлі зброєю. Результатом є глобальне поширення нестабільності та порушення міжнародних норм.

Фінансування транснаціональних репресій слід розглядати як серйозну загрозу, подібну до фінансування тероризму. Воно підриває міжнародну безпеку, знецінює людські права і підживлює глобальну напруженість. Необхідно посилити міжнародні механізми протидії таким діям та інтегрувати їх до загальної стратегії боротьби з фінансуванням тероризму.

https://www.fbi.gov/investigate/counterintelligence/transnational-repression