Серійний номер: ДСФМУ-ДК-2024-024
Вересень 2024

# ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

## Відмивання грошей і шкода від організованої злочинності

Документ Австралійського інституту кримінології, досліджує вплив відмивання грошей на шкоду, пов'язану з організованою злочинністю. **Основою дослідження є пов'язування даних про підозрілі фінансові транзакції з інформацією про групи організованої злочинності, відомі правоохоронним органам Австралії.** Важливим висновком є те, що **чим більше грошей відмивають злочинні групи, тим більше шкоди вони завдають суспільству**, використовуючи незаконні кошти для фінансування нових злочинних операцій. Зокрема, **групи, що займаються відмиванням грошей, завдають у 2,5 рази більше шкоди, ніж ті, що не займаються цією діяльністю**.

**Ключові висновки:**

1. **Вплив відмивання грошей на злочинність:** Організовані злочинні групи, що займаються відмиванням грошей, на 1,7 рази частіше вчиняють злочини, а також завдають суспільству значно більше шкоди, реінвестуючи незаконно отримані кошти в подальші кримінальні операції. Шкода від таких груп у 2,5 рази перевищує шкоду від тих, що не займаються відмиванням.
2. **Зв'язок між відмиванням грошей та зростанням злочинної активності:** Збільшення суми відмитих коштів передує зростанню кримінальної активності. Кожен 1% зростання відмитих коштів збільшує шкоду на 0,05%. Це вказує на те, що отримані незаконні кошти використовуються для підтримки і розширення подальшої злочинної діяльності, зокрема у сферах наркотрафіку та шахрайства.
3. **Роль секторів економіки у відмиванні грошей:** Найбільше грошей відмивається через нерухомість і азартні ігри. Групи, що використовують ці сектори, є більш організованими та часто займаються торгівлею наркотиками.
4. **Недоліки звітності про підозрілі транзакції:** Незважаючи на збільшення кількості звітів про підозрілі транзакції, значна частина підозрілої активності залишається поза увагою правоохоронців, що свідчить про недосконалість механізмів виявлення і фіксації цих операцій.

5. **Необхідність посилення боротьби з відмиванням грошей:** Обмеження можливостей для відмивання грошей може істотно знизити рівень злочинної активності та зменшити шкоду для суспільства.

https://www.aic.gov.au/publications/special/special-18

## Боротьба зі зростанням шахрайства з подарунковими картками: Вплив на економіку та національну безпеку

Документ на сайті Міністерства внутрішньої безпеки США описує проблему зростання шахрайства з подарунковими картками та заходи, які вживаються для боротьби з цим злочином. Зокрема, йдеться про проект "Red Hook", в якому беруть участь правоохоронні органи та приватний сектор. Шахрайство з подарунковими картками призводить до втрат у сотні мільйонів доларів щороку, а отримані кошти часто використовуються для фінансування серйозних злочинів, таких як виробництво фентанілу, торгівля людьми та незаконна міграція.

**Серед основних методів шахрайства виділяють:**

- фізичне втручання в подарункові картки (шляхом крадіжки даних з магнітної смужки або прихованих кодів),
- шахрайство з використанням цифрових технологій (фішинг, викрадення даних через онлайн-платформи)
- обман жертв, які купують підроблені або вкрадені картки.

Також документ детально розглядає ознаки шахрайства (червоні прапорці), на які можуть звернути увагу споживачі та бізнес, щоб попередити незаконні дії.

Проект "Red Hook" підкреслює важливість співпраці між бізнесом і правоохоронними органами. Важливу роль у боротьбі з шахрайством грають технологічні інновації, зокрема, інструменти для виявлення підроблених карток та запобігання їх використанню. Також особливо підкреслюється необхідність інформування громадськості про небезпеки та схеми шахрайства.

**Основні висновки документа**:

- Шахрайство з подарунковими картками є великою проблемою, яка призводить до значних економічних втрат.
- Отримані кошти використовуються для фінансування важких злочинів.
- Успішна боротьба з цим явищем вимагає спільних зусиль правоохоронців і приватного сектору.
- Сучасні технології можуть допомогти знизити рівень шахрайства, але необхідна постійна увага до ознак підробок та інформування суспільства.

Цей документ висвітлює критичні моменти проблеми шахрайства з подарунковими картками, зокрема його вплив на національну безпеку та необхідність об'єднання зусиль для вирішення проблеми.

http://surl.li/qixiyw

## Річний звіт DWP 2023-2024: Боротьба з шахрайством, помилками та фінансовими злочинами у системі соціального забезпечення

Документ «Annual Report and Accounts 2023-24» є річним звітом Департаменту праці та пенсій Великобританії (DWP) за фінансовий рік, що закінчився 31 березня 2024 року. Він охоплює основні операційні аспекти діяльності відомства, зокрема, соціальне забезпечення, виплати пенсій, програми для працевлаштування, а також впровадження програм боротьби з шахрайством та забезпечення точності виплат. Документ також містить фінансову звітність DWP, аналіз ефективності діяльності та детальні плани щодо подальших реформ.

**Ключові моменти, що стосуються фінансових злочинів:**


- **Боротьба з шахрайством та помилками:** У звіті підкреслюється робота DWP щодо боротьби з шахрайством і помилками у виплатах соціальної допомоги. У 2023-2024 роках департамент зекономив 1,3 мільярда фунтів стерлінгів через зусилля у сфері боротьби з шахрайством і помилками. Це досягнуто завдяки впровадженню нових інструментів для виявлення підозрілих транзакцій та посиленню контролю за соціальними виплатами.
- **Звіт щодо шахрайства, помилок та заборгованостей:** Документ містить спеціальний розділ «Fraud Error and Debt Report», який аналізує заходи з виявлення та запобігання фінансовим злочинам. У цьому розділі описуються нові методи аналізу даних та впровадження технологій, таких як машинне навчання, для виявлення підозрілих транзакцій.
- **Ризики та заходи з управління ними:** DWP визнає, що однією з основних загроз для його операційної діяльності є зростання рівня шахрайства у системі соціального забезпечення. Для цього було розроблено плани щодо зниження ризиків, пов'язаних із збільшенням навантаження на систему та кіберзагрозами, включаючи загрози фінансових махінацій.
- **Використання технологій для протидії шахрайству:** У звіті детально розглядаються зусилля з розширення можливостей контролю за шахрайством через використання машинного навчання для аналізу поведінки отримувачів допомоги. Це дозволило покращити точність виплат і знизити кількість невиправданих або шахрайських заявок.

**Висновки:**

- **Ефективність контролю за виплатами:** DWP демонструє значний прогрес у боротьбі з фінансовими злочинами, шахрайством та помилками у сфері соціального забезпечення, завдяки новим технологіям і програмам моніторингу.
- **Підвищення рівня захисту системи:** Важливим досягненням стало впровадження систем, які використовують дані для прогнозування шахрайських дій, що дозволяє знизити витрати держави на неправомірні виплати.
- **Залишаються ризики:** Попри досягнуті результати, документ визнає, що департамент стикається з постійними викликами щодо управління ризиками шахрайства, що вимагає подальших інвестицій у безпеку та інновації.

Цей звіт чітко підкреслює, що протидія фінансовим злочинам є однією з основних пріоритетів DWP у їхній діяльності.

http://surl.li/lanhfb

## Регуляторні підходи до штучного інтелекту у сфері фінансів

Документ, опублікований OECD у вересні 2024 року, **аналізує використання та регулювання штучного інтелекту (ШІ) в фінансовому секторі. Він охоплює дослідження серед 49 юрисдикцій, як членів OECD, так і не членів, щодо впровадження ШІ в такі сфери, як обслуговування клієнтів, виявлення шахрайства та управління ризиками**. У документі підкреслюються як **переваги ШІ, такі як підвищення ефективності та продуктивності**, так і **ризики, серед яких кіберзагрози, маніпуляції на ринку та дискримінація через упереджені алгоритми**. Рекомендації OECD спрямовані на використання технологічно нейтрального підходу в регулюванні, коли чинні фінансові закони також поширюються на штучний інтелект, однак передбачаються додаткові настанови для боротьби з новими загрозами.

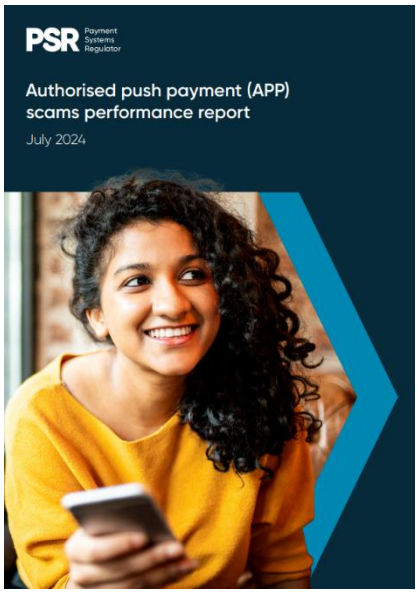

**Ключові висновки:**

1. **Баланс між перевагами та ризиками ШІ:** Документ підкреслює, що ШІ здатний значно підвищити ефективність фінансових установ, особливо в обслуговуванні клієнтів, прогнозуванні ринкових трендів та управлінні ризиками. Проте існують серйозні ризики, які потребують уваги. Наприклад, використання поганих даних або упереджених алгоритмів може призвести до дискримінації окремих груп клієнтів. Інші ризики включають підвищення кіберзагроз та потенціал для ринкових маніпуляцій через автоматизовані операції.
2. **Технологічно нейтральний підхід до регулювання:** Більшість юрисдикцій підтримують підхід, коли існуючі фінансові закони застосовуються до ШІ без необхідності прийняття специфічних для технології правил. Це означає, що вже чинні закони щодо захисту споживачів, фінансової стабільності та боротьби з шахрайством повинні діяти на рівні з правилами для ШІ. Такий підхід дозволяє уникнути дублювання законів і спрощує регулювання.
3. **Необхідність додаткових настанов та адаптації законодавства:** Попри те, що існуючі регуляторні рамки застосовуються до ШІ, регулятори визнають необхідність адаптації або уточнення настанов. Швидкий розвиток ШІ створює нові виклики, зокрема стосовно прозорості алгоритмів, відповідальності за автоматизовані рішення та управління ризиками, пов'язаними з автоматизацією. Багато юрисдикцій переглядають свої підходи до цих питань, щоб впоратися з новими загрозами.
4. **Регуляторні прогалини та майбутні перспективи:** Хоча деякі юрисдикції вважають, що чинні закони є достатніми, інші, особливо ті, що активно інвестують у розвиток фінансових технологій, переглядають свої підходи. В документі зазначено, що відсутність чітких стандартів для ШІ може створити прогалини в регуляції, особливо в сфері захисту споживачів. Деякі країни вже запроваджують нові законодавчі ініціативи або створюють спеціальні наглядові органи для моніторингу використання ШІ.

Таким чином, документ OECD підкреслює важливість гнучкого регулювання, яке дозволяє отримувати вигоди від використання ШІ у фінансах, одночасно мінімізуючи ризики, пов’язані з технологічними змінами та новими викликами.

http://surl.li/izymvi

## Звіт про результати шахрайства авторизованих push-платежів (APP).




**Документ** "APP Scams Performance Report" за липень 2024 року **висвітлює масштаби шахрайських операцій через авторизовані платіжні транзакції у Великій Британії**. **У 2023 році загальна втрата коштів через такі шахрайські операції склала £341 мільйон, що на 12% менше порівняно з 2022 роком. Однак кількість таких випадків зросла на 12%**. Згідно зі звітом, рівень відшкодування жертвам шахрайства збільшився з 61% у 2022 році до 67% у 2023 році. Основну увагу приділено діяльності 14 найбільших банківських груп, з яких вимагалося надання даних про кількість шахрайських транзакцій та рівень відшкодувань.

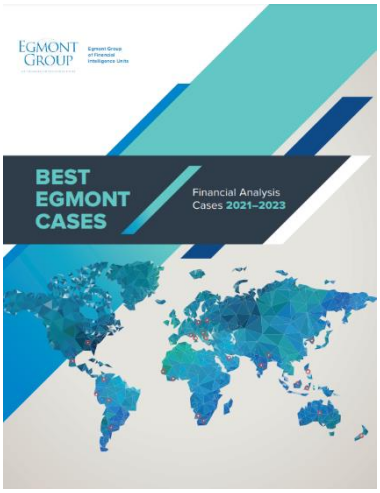
**Ключові висновки:**

1. **Зниження втрат через шахрайство:** Загальна сума втрат через шахрайство у 2023 році зменшилась на 12%, що свідчить про певний прогрес у боротьбі зі схемами шахрайства. Цьому сприяло покращення механізмів відстеження підозрілих транзакцій та підвищення обізнаності клієнтів щодо шахрайства.
2. **Зростання кількості шахрайських випадків:** Хоча загальна вартість шахрайства знизилась, кількість випадків APP шахрайств зросла на 12%. Більшість цих випадків стосуються невеликих сум (до £1,000), при цьому такі випадки склали понад 80% загальної кількості шахрайських транзакцій у 2023 році.
3. **Відшкодування збитків жертвам:** Підвищення рівня відшкодування шахрайських втрат — з 61% у 2022 році до 67% у 2023 році. Однак рівень відшкодування залишається неоднорідним серед різних банків. Найвищий рівень відшкодувань забезпечував банк TSB — 88%, тоді як деякі банки не змогли досягти навіть 20%.
4. **Проблеми менших платіжних систем:** Невеликі фінансові установи демонструють значно вищий рівень шахрайських транзакцій, ніж найбільші банки. У 2023 році вони склали 38% від загальної кількості шахрайських операцій, хоча їхня частка в загальному обсязі платежів становила лише 17%.
5. **Майбутні покращення у регулюванні:** Звіт підкреслює важливість нового обов'язкового механізму відшкодування збитків, який набуде чинності в жовтні 2024 року. Нові правила зобов'язують обидві сторони (і банк, що відправляє транзакцію, і банк, що її приймає) нести відповідальність за компенсацію втрат від шахрайства.

https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/

## НАЙКРАЩІ КЕЙСИ EGMONT 2021-2023

**Документ "Best Egmont Cases 2021–2023" представляє збірник найкращих кейсів з аналізу фінансових злочинів, підготовлений підрозділами фінансової розвідки (ПФР) країн-учасниць Egmont Group**. Основна мета – поділитися ефективними методами розслідування злочинів, пов'язаних з відмиванням коштів та фінансуванням тероризму, а також використанням фінансової аналітики для викриття складних схем. **Документ охоплює різноманітні категорії правопорушень, зокрема хабарництво, корупцію, кіберзлочинність, контрабанду наркотиків та шахрайство**.




**Ключові висновки:**

1. **Міжнародна співпраця між ПФР:** Документ підкреслює ключову роль співпраці між підрозділами фінансової розвідки (ПФР) різних країн. Багато з успішних справ було розкрито завдяки обміну фінансовою інформацією між юрисдикціями. Це дозволило швидко відстежувати транскордонні фінансові потоки та виявляти злочинні мережі, які використовують міжнародні операції для відмивання коштів та фінансування тероризму. Співпраця включала як формальні канали, так і неформальні зв'язки між ПФР, що сприяло оперативному реагуванню.
2. **Застосування передової фінансової аналітики:** Документ демонструє важливість використання сучасних аналітичних інструментів для аналізу фінансових транзакцій. ПФР активно використовували аналітичні системи для моніторингу фінансових потоків, ідентифікації підозрілих транзакцій та виявлення аномалій. Ці інструменти були критичними у розслідуванні складних схем із залученням підставних компаній, кіберзлочинності, відмивання грошей через криптовалюти та незаконних операцій у сферах нерухомості й товарообігу. Використання цих технологій дозволило швидше виявляти аномалії та запобігати подальшій злочинній діяльності.
3. **Ефективність моніторингу підозрілих транзакцій:** У багатьох випадках моніторинг підозрілих фінансових операцій став ключовим фактором у виявленні організованих злочинних груп. Документ вказує, що відстеження та аналіз підозрілих транзакцій дозволив ПФР розкрити складні міжнародні схеми відмивання грошей. У деяких випадках ці схеми включали кілька рівнів участі, зокрема використання офшорних компаній, що ускладнювало процес розслідування. Проте завдяки активному моніторингу й аналітичній роботі ці операції були вчасно виявлені, що допомогло запобігти подальшим фінансовим втратам.
4. **Різноманітність фінансових злочинів:** У документі представлені випадки, які охоплюють широкий спектр типологій злочинів. Це включає фінансові махінації, корупцію, шахрайство, хабарництво, контрабанду наркотиків та фінансування тероризму. Важливо, що ці типи злочинів часто були тісно пов'язані з міжнародними фінансовими потоками, що ускладнювало їхнє виявлення і розслідування. Наприклад, корупційні схеми часто були пов'язані з незаконними переказами через офшорні рахунки, а відмивання грошей включало використання криптовалют для маскування слідів. Ці різні форми злочинної діяльності вимагали застосування спеціалізованих підходів до розслідування та аналізу фінансових даних.
5. **Покращення міжнародних стандартів:** Документ підкреслює важливість розробки та впровадження єдиних міжнародних стандартів для боротьби з фінансовими злочинами. Це дозволяє ПФР ефективніше взаємодіяти між собою та швидше реагувати на нові загрози. Стандартизація процесів моніторингу та обміну інформацією дозволяє швидше відстежувати злочинні фінансові потоки та підвищувати прозорість міжнародних транзакцій.

Цей звіт демонструє важливість аналітичного підходу та співпраці між країнами для успішної боротьби з фінансовими злочинами.

https://egmontgroup.org/wp-content/uploads/2024/09/EGMONT_2021-2023-BECA-III_FINAL.pdf

# РЕГУЛЮВАННЯ

## Пропозиція внести зміни до Директиви (ЄС) 2019/1153: Єдина точка доступу до реєстрів банківських рахунків

Нова директива ЄС посилює транскордонний доступ до банківських рахунків: наступна хвиля придушення фінансових злочинів!

9 липня 2024 року ЄС запустив революційне оновлення, спрямоване на підвищення фінансової прозорості та посилення боротьби з фінансовими злочинами. **Ця директива вносить зміни до Директиви (ЄС) 2019/1153 і запроваджує централізовану систему доступу до реєстрів банківських рахунків у державах-членах ЄС**. Завдяки цій зміні правоохоронні органи матимуть спрощений доступ до фінансової інформації, яка допоможе у конфіскації злочинних доходів.

**Основні моменти для фінансових установ:**

1. **Підвищені вимоги до звітності:** установи повинні підготуватися до більш суворих вимог щодо своєчасного та точного звітування фінансових даних.
2. **Розширене керування даними:** компаніям потрібно буде оновити системи, щоб забезпечити безпечний обмін даними з централізованою точкою доступу ЄС.
3. **Суворіші протоколи відповідності:** Внутрішні процедури відповідності потребуватимуть коригування, зосереджуючись на швидкому реагуванні на запити правоохоронних органів.
4. **Навчання та ресурси:** можуть знадобитися додаткові інвестиції для підтримки персоналу в адаптації до цих значних нормативних змін.

Основні положення включають статті 5 і 6, які гарантують, що доступ до даних надається лише в кожному окремому випадку. Крім того, Директива наголошує на захисті даних і узгоджується з GDPR (General Data Protection Regulation) для захисту особистої інформації.

Важливо, що Директива також поширює свою дію на криптоактиви, дозволяючи правоохоронним органам отримувати доступ до записів постачальників послуг з криптоактивами.

**Оновлення, опубліковане 2 вересня 2024 року, надає державам-членам ЄС час до 10 липня 2027 року для прийняття необхідних правових положень**. Фінансові установи повинні почати адаптувати свої процеси зараз, щоб відповідати вимогам цієї директиви.

Хоча нові заходи розширюють транскордонну співпрацю, фінансові установи зіткнуться з підвищеними операційними вимогами щодо дотримання цих правил.

https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)729425

## Зміни до вимог ідентифікації кінцевих бенефіціарних власників: Циркуляр CSSF 24/861

Документ представляє собою циркуляр **CSSF 24/861**, що вносить зміни до циркуляра CSSF 19/732 від 20 грудня 2019 року. Він надає додаткові **роз'яснення щодо вимог ідентифікації та верифікації кінцевого бенефіціарного власника (КБВ)** у контексті боротьби з відмиванням коштів та фінансуванням тероризму. Основна мета полягає у **підвищенні прозорості фінансових операцій та забезпеченні належної ідентифікації осіб, які стоять за юридичними особами або іншими структурами, зокрема через запровадження підходу, що базується на оцінці ризиків**.

Документ роз'яснює **процедури виявлення кінцевих бенефіціарних власників для юридичних осіб, трастів, благодійних організацій та інших суб'єктів**. Він також уточнює **вимоги до верифікації отриманих даних**, враховуючи складність структури власності, а також необхідність **вживання додаткових заходів для підвищення прозорості**.

**Ключові висновки:**

1. **Оцінка ризиків і підхід на основі ризиків**: Ідентифікація та верифікація кінцевого бенефіціарного власника повинні здійснюватися з урахуванням ризиків. Комплексні структури власності або ті, що включають іноземні суб'єкти, можуть вимагати додаткових заходів для підтвердження особи бенефіціара.

2. **Каскадний підхід до визначення КБВ**: Процедура визначення КБВ ґрунтується на трьох етапах — визначення осіб з часткою понад 25% акцій, виявлення осіб, які здійснюють контроль іншим способом, і, як останній крок, визначення вищих керівників, якщо попередні заходи не дали результату.

3. **Прозорість та належна документація**: Документ підкреслює важливість забезпечення прозорості та надання доказів ідентифікації КБВ через офіційні джерела, включаючи державні реєстри або інші надійні джерела інформації.

4. **Особливі вимоги до правових утворень та трастів**: Для трастів та правових утворень, таких як асоціації, документ вимагає ідентифікації всіх осіб, які мають реальний контроль над активами або приймають важливі рішення.

5. **Чутливі суб'єкти та потенційні ризики**: До особливої уваги варто віднести структури з іноземними бенефіціарами, а також політично значущих осіб (PEP), оскільки вони можуть представляти підвищений ризик відмивання коштів або фінансування тероризму.

Циркуляр покликаний зміцнити фінансову прозорість та запобігти зловживанню корпоративними структурами у злочинних цілях, таких як ухилення від сплати податків або фінансування терористичної діяльності.

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

## Оновлення регулювання ЄС щодо експорту товарів подвійного призначення: зміни у списку товарів та відповідність міжнародним зобов'язанням

**Документи, що містять регуляторні акти та додатки до них, пов'язані зі змінами у законодавстві Європейського Союзу щодо контролю за експортом товарів подвійного призначення. Перший документ є пояснювальною запискою** до Делегованого регламенту Європейської комісії, який змінює Регламент (ЄС) 2021/821 з метою оновлення списку товарів подвійного призначення. Товари подвійного призначення – це товари, які можуть бути використані як для цивільних, так і для військових цілей, або сприяти поширенню зброї масового знищення. Оновлення є необхідним для забезпечення відповідності міжнародним зобов'язанням, а також для забезпечення конкурентоспроможності економічних операторів у ЄС. **Другий документ є додатком, який містить сам оновлений список товарів подвійного призначення, розбитий на різні категорії**, що охоплюють матеріали, технології, обладнання та програмне забезпечення, які підлягають експортному контролю.

**Ключові висновки**

1. **Актуалізація списку товарів подвійного призначення**: Список регулярно оновлюється відповідно до змін у міжнародних режимах контролю за експортом і нерозповсюдженням, включаючи такі організації, як Група ядерних постачальників, Wassenaar Arrangement, Австралійська група та Режим контролю за ракетними технологіями.

2. **Вплив міжнародних зобов'язань**: ЄС зобов'язаний оновлювати свій список товарів відповідно до рішень міжнародних організацій, щоб відповідати глобальним стандартам безпеки та уникати сприяння поширенню зброї масового знищення.

3. **Роль економічних операторів**: Оновлений список сприяє прозорості для європейських компаній, що експортують товари подвійного призначення, дозволяючи їм бути в курсі актуальних вимог та регулювати свої операції відповідно до змін у законодавстві.

4. **Реакція на поточні події**: Складність у оновленні міжнародних режимів контролю через глобальні політичні події, такі як війна Росії проти України, є важливим контекстом для оновлення списку товарів подвійного призначення.

5. **Сфери контролю**: Документ містить деталізовані категорії товарів, включаючи ядерні матеріали, електроніку, авіоніку, навігаційні системи, телекомунікаційне обладнання, програмне забезпечення та інші технології, що підлягають контролю при експорті та транзиті.

https://is.gd/2FjEpX

# САНКЦІЇ

## Міністерство фінансів США вживає заходів у рамках відповіді уряду на операції зловмисного зовнішнього впливу Росії


У рамках нещодавніх дій Сполучених Штатів, спрямованих на протидію агресивній політиці Росії, Міністерство фінансів США через Управління контролю за іноземними активами (OFAC) запровадило черговий раунд санкцій. Санкції, зокрема, націлені на нові зарубіжні філії та дочірні підприємства російських фінансових установ, створених з метою обходу економічних обмежень. США особливо підкреслюють ризики для міжнародних фінансових установ, що можуть сприяти фінансуванню військово-промислової бази Росії через такі новостворені структури. OFAC попереджає про важливість ретельного нагляду за подібними фінансовими організаціями, особливо тими, що займаються транзакціями або операціями з коштами на користь військових цілей РФ.

Також варто зазначити, що санкції підкреслюють важливість суворого контролю за ланцюгами постачань у критично важливих секторах, таких як технології, будівництво, авіація та оборонні матеріали. Під нові обмеження потрапляють компанії та особи, які підтримують ці галузі, що робить глобальні фінансові операції значно ризикованішими.

Важливим є й те, що США зберігають можливості для міжнародної співпраці в сферах, таких як телекомунікації, продовольчі поставки та медичні послуги, дозволяючи підсанкційним організаціям продовжувати роботу за певних обставин, але при цьому попереджають про використання таких "вузьких місць" для обходу санкційних обмежень.

Нещодавні зміни, включені в General License 25E, дозволяють певні операції, пов'язані з обміном інформацією через інтернет, що зменшує вплив на громадськість, але залишає жорсткий контроль за фінансовими операціями, зокрема тими, що стосуються державних компаній та осіб із санкційного списку.

Ці заходи є ще одним кроком у глобальній стратегії Сполучених Штатів із запобігання фінансовій підтримці російської військової агресії, і вони вимагають пильної уваги з боку міжнародних фінансових установ для мінімізації ризиків порушення санкційних режимів.

https://home.treasury.gov/news/press-releases/jy2559

## Поширені питання щодо замороження активів та заборони надання коштів та економічних ресурсів


**Документ надає вичерпні відповіді на поширені питання щодо санкцій Європейського Союзу, накладених на Росію та Білорусь через їхню агресію проти України**. Він охоплює ключові аспекти замороження активів, заборони на надання фінансів або економічних ресурсів особам, зазначеним у списку санкцій, а також питання, пов'язані з власністю та контролем активів. Документ пояснює, як активи, що перебувають під контролем осіб із санкційного списку, повинні бути заморожені, навіть якщо їх контролюють через третіх осіб.

**Ключові висновки:**

1. **Замороження активів осіб із санкційних списків:** Документ детально пояснює, що всі активи осіб, які перебувають під санкціями ЄС, повинні бути заморожені, незалежно від того, чи належать вони безпосередньо зазначеній особі, чи контролюються через третіх осіб. Це включає як фізичні активи, так і грошові кошти, нерухомість та фінансові ресурси.
2. **Поняття контролю над активами:** Якщо особа, що перебуває під санкціями, продовжує контролювати активи через третіх осіб, такі активи повинні залишатися замороженими. ЄС застосовує концепцію "опосередкованого контролю", що передбачає замороження активів навіть тоді, коли підсанкційна особа не володіє активами прямо, але може здійснювати над ними контроль через пов'язаних юридичних або фізичних осіб. Якщо є сумніви щодо того, хто контролює активи, національні органи можуть проводити розслідування та ухвалювати відповідні рішення.
3. **Винятки з правил та можливі дерогації:** Документ надає можливості для певних винятків або дерогацій у випадках, коли замороження активів може вплинути на критичні фінансові операції. Наприклад, це може стосуватися виплати заробітної плати працівникам, виплат за контрактами, укладеними до введення санкцій, або для забезпечення основних потреб осіб, що перебувають під санкціями. В кожному випадку ці винятки повинні бути схвалені національними компетентними органами та відповідати законодавству ЄС.
4. **Захист прав власності:** Хоча санкції обмежують доступ осіб до їхніх активів, ЄС гарантує, що санкції не призводять до експропріації власності. Це означає, що особи, чиї активи заморожені, продовжують володіти ними, але не можуть користуватися або реалізовувати їх до моменту скасування санкцій. Право власності залишається за ними, проте на активи накладаються жорсткі обмеження щодо їх використання або переміщення.

http://surl.li/whytwk

# ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

## Криптовалютна стратегія Росії: Легалізація як інструмент для обходу санкцій

Стаття на Chainalysis присвячена тому, як Росія почала використовувати криптовалюти для обходу західних санкцій, що були введені після початку війни з Україною.

Відчуваючи значний економічний тиск, російська влада ухвалила рішення легалізувати майнінг криптовалют та створити правову базу для використання цифрових активів у міжнародних розрахунках. Однією з ключових мотивацій цього кроку є зниження залежності від долара США та традиційних фінансових систем, де Росія під санкціями має обмежений доступ.

Одним із центральних елементів цього процесу є роль Центрального банку Росії, який, хоча й раніше був обережним у питанні криптовалют, тепер відіграє ключову роль у регулюванні криптоактивів у країні. Під егідою уряду, країна почала створювати інфраструктуру для національних криптовалютних бірж та міжнародних платежів у криптовалютах. Зокрема, співпраця із такими країнами, як Китай та Іран, допомагає Росії розробляти альтернативні фінансові канали, обминаючи західні санкції.

Проте, стаття зазначає, що широкомасштабне обходження санкцій за допомогою криптовалют стикається із низкою перешкод. Однією з основних є проблема ліквідності: великі суми криптовалют, необхідні для проведення значних фінансових операцій, важко перетворити в гроші без помітного впливу на ринок. Окрім того, великі міжнародні біржі залишаються під жорстким наглядом регуляторів, що значно ускладнює використання криптовалют для великих транснаціональних операцій.

Також стаття підкреслює ризики для глобальної фінансової системи, якщо Росія досягне успіху в створенні повноцінної криптовалютної інфраструктури. Це може спонукати інші країни, які перебувають під санкціями, скористатися подібними механізмами для ухилення від міжнародних фінансових обмежень. Однак, поки що, криптовалюта є лише частковим рішенням для Росії, а не повноцінною заміною традиційним фінансовим каналам.

**Зі статті можна винести кілька ключових висновків:**

- **Стратегія Росії щодо санкцій:** Росія активізує використання криптовалют для обходу західних санкцій, легалізуючи майнінг і впроваджуючи криптовалютні розрахунки для міжнародної торгівлі.
- **Роль Центрального банку:** Центральний банк Росії відіграє ключову роль у регулюванні цього процесу, сприяючи розвитку криптобірж та міжнародних платежів у криптовалютах.
- **Обмеження та ризики:** Незважаючи на спроби обійти санкції, проблема ліквідності на крипторинках та міжнародний контроль ускладнюють масштабні операції.

http://surl.li/wycszw

## Регулювання платежів в Азії

Документ «Payments Regulation in Asia» є аналітичним звітом, який досліджує тенденції регулювання платіжних систем у чотирьох країнах Азійсько-Тихоокеанського регіону: Японії, Індії, Сінгапурі та Австралії. Основна увага приділяється ключовим аспектам ринку карткових платежів, зокрема витратам на їхнє приймання, регулюванню міжбанківських комісій (інтерчейндж), політиці

ко-бейджингу та рутінгу транзакцій, а також впровадженню нових платіжних систем. Документ також розглядає політики регулювання у цих країнах з акцентом на заходи, які спрямовані на зниження витрат на приймання карткових платежів для торговців, зокрема через встановлення лімітів на комісії, а також розвиток альтернативних платіжних методів, таких як мобільні гаманці та системи миттєвих платежів.


**Ключові висновки:**

1. **Зростання витрат на приймання карткових платежів**: У всіх чотирьох країнах витрати на приймання карткових платежів для торговців зросли, що зумовило необхідність втручання регуляторів.
2. **Міжбанківські комісії**: Лише Австралія з-поміж розглянутих країн має діючі обмеження на міжбанківські комісії, тоді як у Сінгапурі та Індії вони відсутні, а в Японії ці обмеження було скасовано.
3. **Альтернативи картковим платежам**: В деяких країнах, таких як Індія та Сінгапур, зростає популярність альтернативних платіжних методів, таких як UPI та PayNow, що дозволяє зменшити залежність від карткових платежів та їхніх витрат.
4. **Регулювання ко-бейджингу та рутінгу**: В Австралії діє регулювання ко-бейджингових карт, що дозволяє торговцям самостійно вибирати, через яку мережу проводити транзакцію, знижуючи таким чином витрати на приймання платежів.
5. **Прозорість у ціноутворенні**: Регулювання прозорості тарифів на міжбанківські комісії є актуальним лише в Австралії та Японії. Це сприяє більшій конкурентоспроможності та ефективності ринку.
6. **Ефект регуляторних втручань**: У країнах, де були впроваджені регуляторні заходи, спостерігається зниження витрат на обробку карткових платежів, що покращує умови для торговців і потенційно знижує ціни для споживачів.

Звіт є важливим інструментом для розуміння впливу регулювання на платіжні ринки та надає цінні рекомендації щодо політик, які можуть допомогти знизити витрати на приймання платежів у майбутньому.

https://marketing.cmspi.com/view/285851179/27/

## Майбутнє фінансів: Розвиток токенізації реальних активів (RWAs) та їх вплив на глобальні ринки


**Документ «RWAs and the Future of Finance» присвячений аналізу розвитку токенізації реальних активів (Real-World Assets, RWAs) через блокчейн-технології. Він містить огляд ключових подій, тенденцій, технологічних інновацій та регуляторних ініціатив у цій галузі, які охоплюють ринки нерухомості, фінансові інструменти, спорт**. Основну увагу приділено впровадженню токенізації великими фінансовими установами, такими як Goldman Sachs, Ripple, Coinbase, BlackRock, що робить значний внесок у глобальні ринки.

**Крім аналізу регуляторного середовища в США, ЄС, Південній Кореї та Японії, у документі розглядаються проблеми, з якими стикаються учасники ринку в різних юрисдикціях**. Увага також приділяється проєкціям майбутнього зростання ринку токенізації, включно з впровадженням інновацій, таких як

автоматизовані маркетмейкери (AMM) і децентралізовані ідентифікатори (DID), що сприяють залученню інституційних інвесторів.

**Ключові висновки:**

1. Токенізація реальних активів є перспективним напрямком, який забезпечує ліквідність, прозорість та доступ до традиційно неліквідних активів, таких як нерухомість, державні облігації, та навіть мистецькі і спортивні об'єкти.
2. Основні учасники ринку, такі як Goldman Sachs, Ripple і Coinbase, активно розширюють свої пропозиції щодо токенізації, при цьому використовуючи як публічні, так і дозволені блокчейни для відповідності регуляторним вимогам.
3. Регуляторне середовище залишається складним: різні юрисдикції, включно з США, ЄС та Азією, впроваджують власні норми для забезпечення безпеки та прозорості токенізованих ринків.
4. Окрім фінансових інструментів, токенізація проникає в нові сфери, такі як спорт, мистецтво і сталий розвиток, створюючи нові можливості для інвесторів та учасників ринку.
5. Очікується суттєве зростання ринку токенізованих активів, де до 2034 року він може досягти мільярдних обсягів, що робить цю галузь ключовою для майбутнього фінансів.

Таким чином, документ пропонує всебічний огляд стану і майбутнього розвитку токенізації реальних активів, акцентуючи на її ролі в трансформації глобальних фінансових ринків.

https://is.gd/FdFwe1

## Золото як стратегічний ресурс Росії у війні: економічний інструмент виживання під санкціями


Документ *«Gold Rush: How Russia is using gold in wartime»* розглядає питання використання золота Росією в контексті війни з Україною. **Золото стало стратегічним ресурсом для Росії, впливаючи на її здатність генерувати доходи, проводити грошово-кредитну політику та зміцнювати позиції на міжнародній арені через ініціативу дедоларизації**. Документ також висвітлює роль золота у торгівельних відносинах Росії з такими країнами, як Китай, Туреччина, Іран та ОАЕ, де його використовують для отримання валюти, закупівлі зброї та товарів. Російська влада активно поповнює державний фонд дорогоцінних металів та каменів, що дозволяє гнучко реагувати на економічні виклики. Однак, через санкції Західних країн, російська золотовидобувна промисловість стикається з труднощами, що включають втрату іноземних інвесторів та складності з доступом до західного обладнання.

**Ключові висновки:**

1. Золото стало важливим стратегічним ресурсом для Росії у відповідь на санкції Заходу, його використовують для підтримки бюджету та як інструмент дедоларизації.
2. Росія збільшила свої золотовалютні резерви та активно поповнює таємний державний фонд дорогоцінних металів і каменів, що забезпечує можливості для гнучкого реагування на фінансові кризи.
3. Санкції Західних країн значно вплинули на російську золотовидобувну промисловість, яка значною мірою залежала від західного обладнання та інвесторів.

4. Незважаючи на амбіції стати найбільшим світовим виробником золота, російська внутрішня продукція не демонструє значного зростання, що змушує країну шукати впливу в золотовидобувних галузях Африки та Центральної Азії.

5. Золото стало важливим інструментом у торгівельних відносинах з такими країнами, як Китай, Туреччина, Іран та ОАЕ, де його використовують для отримання валюти, закупівлі зброї та інших товарів.

6. Росія продовжує розробляти нові золоті родовища і намагатися знизити залежність від імпортного обладнання, хоча зростання продуктивності галузі під питанням.

Таким чином, золото для Росії стало важливим інструментом виживання в умовах санкцій і економічної ізоляції.

https://is.gd/1sLyqW

## Боротьба з незаконною діяльністю в морському просторі за допомогою даних Planet

Документ аналізує використання даних для боротьби з незаконною діяльністю в морському секторі. Він **досліджує, як супутникові дані та сучасні технології допомагають відслідковувати рух суден, виявляти підозрілу поведінку та запобігати нелегальним операціям, таким як контрабанда, нелегальна риболовля та перевезення підсанкційних товарів**. Документ підкреслює важливість інтеграції аналітики та обробки великих даних для ефективної боротьби з цими загрозами.

**Ключові висновки:**

1. **Використання супутникових даних для моніторингу:** У документі підкреслюється, що супутникові зображення забезпечують безпрецедентні можливості для моніторингу суден у реальному часі. Це дозволяє виявляти судна, які вимикають свої системи автоматичної ідентифікації (AIS) для уникнення відстеження, або тих, що змінюють маршрут для уникнення контролю.
2. **Поєднання різних джерел даних:** Інтеграція супутникових даних з іншими джерелами, такими як AIS, логістичні та митні дані, надає глибше розуміння комерційної діяльності суден і дозволяє виявляти невідповідності, що можуть свідчити про незаконну діяльність.
3. **Виявлення підозрілої поведінки:** Документ акцентує увагу на використанні аналітики великих даних для виявлення аномальних патернів поведінки суден. Це може включати незвичні маршрути, тривалі простої або заходження в порти, де не було запланованих зупинок. Такий аналіз є ключовим для запобігання незаконним операціям, включаючи контрабанду, нелегальну риболовлю або перевезення санкційних товарів.
4. **Запобігання незаконній діяльності:** Документ деталізує, як дані допомагають виявляти та запобігати різним формам незаконної діяльності в морському секторі, зокрема торгівлі людьми, наркотиками, зброєю та нелегальній риболовлі. Оперативний аналіз і доступ до даних дозволяють швидко реагувати на потенційні загрози та обмежувати їхній вплив.
5. **Міжнародна співпраця та обмін даними:** Важливість глобальної співпраці у боротьбі з незаконною діяльністю на морі підкреслюється як одна з ключових рекомендацій документа. Спільне використання супутникових і аналітичних даних між урядами, міжнародними організаціями та приватним сектором є необхідним для ефективної боротьби з загрозами, які часто є транскордонними за своєю природою. Це дозволяє створити глобальну мережу моніторингу для виявлення і припинення незаконної діяльності.

6. **Роль технологій у забезпеченні морської безпеки:** Використання передових технологій, таких як штучний інтелект і машинне навчання, дозволяє створювати більш точні та ефективні системи для аналізу даних і виявлення загроз. Документ відзначає, що такі технології можуть суттєво підвищити швидкість і точність аналізу великих обсягів даних, що стає важливим чинником у виявленні незаконної діяльності на морі.

https://learn.planet.com/Planet-MDA-ebook-gated.html

## Порушення та трансформація інфраструктури фінансового ринку


Документ "Securities Services Evolution 2024", підготовлений Citi, розглядає **сучасні виклики та трансформації у сфері фінансових ринкових інфраструктур (FMI). Він зосереджений на трьох основних аспектах: прискоренні розрахунків до T+1, використанні розподілених реєстрів (DLT) та цифрових активів, а також зростанні ролі роздрібних інвесторів**. У звіті підкреслюється, що перехід до T+1 був успішним, але складнішим, ніж очікувалося. Важлива увага приділяється ролі FMI як лідерів у впровадженні нових технологій, таких як токенізація та цифрова ліквідність.

**Ключові висновки:**

1. **Перехід до T+1:** Одним із найважливіших досягнень 2024 року є перехід на цикл розрахунків T+1 (замість традиційного T+2), що дозволяє завершувати операції з цінними паперами на один день швидше. Це скорочує фінансові ризики для інвесторів і підвищує ліквідність. Однак для впровадження цього нововведення компанії зіткнулися з необхідністю перегляду своїх операційних процесів, що вимагає значних інвестицій у технології та автоматизацію. Ринки, які впровадили цю модель, зокрема США, Канада та Індія, вже показують покращену ефективність у системах розрахунків. Проте цей процес виявив і певні проблеми, зокрема збільшення тиску на внутрішні системи управління ліквідністю та контроль фінансових ризиків, що потребує більшої координації між учасниками ринку та регуляторами.
2. **Впровадження розподілених реєстрів (DLT) та цифрових активів:** Звіти вказують на те, що технології розподілених реєстрів (DLT) стають ключовим елементом для фінансових ринків, особливо у контексті токенізації активів. DLT забезпечує нові можливості для зниження вартості пост-трейдових операцій та підвищення прозорості ринкових процесів. У країнах Європи та Азії зростає використання токенізації, що дозволяє створювати більш ефективні та швидкі інструменти для обігу цифрових активів. Токенізація традиційних активів також сприяє зниженню витрат та часу для операцій із цінними паперами, а також надає інвесторам більше можливостей для участі у ринках капіталу.
3. **Зростання ролі роздрібних інвесторів:** Одним із важливих трендів у сфері цінних паперів є значне зростання кількості роздрібних інвесторів. Це зростання особливо відчутне в таких країнах, як Індія, де кількість нових роздрібних рахунків збільшилася на 36 мільйонів протягом року. Така активність вимагає від інфраструктур фінансових ринків (FMI) адаптації своїх систем до обробки великих обсягів дрібних транзакцій. Роздрібні інвестори грають дедалі більшу роль у ринках капіталу, створюючи нові виклики щодо обробки та розподілу великих обсягів транзакцій у режимі реального часу.
4. **Стандартизація та оптимізація процесів:** Однією з головних тенденцій є впровадження стандартів і оптимізація ринкових процесів для створення більш стійких інфраструктур. Це стосується як традиційних фінансових інструментів, так і нових цифрових активів, де

стандартизація стає критично важливою для забезпечення злагодженого функціонування ринків. Крім того, стандартизація допомагає мінімізувати ризики та створювати єдині регуляторні підходи, що полегшують впровадження інновацій, таких як DLT та токенізація.

https://www.citibank.com/icg/docs/Citi_Securities_Services_Evolution_2024.pdf

# РЕКОМЕНДОВАНІ МАТЕРІАЛИ

## Схильність до нечесності та її вплив на повсякденну економічну злочинність у Великобританії


Стаття під назвою "The Dishonest Disposition and Everyday Economic Criminality of the British Public", написана Девідом Шепардом, Марком Баттоном та Хлоєю Хокінс, розглядає поширення повсякденної економічної злочинності серед британського населення та зв'язок між схильністю до нечесної поведінки і економічними злочинами. Основний акцент зроблено на дослідженні зв'язку між ставленням до нечесності та економічною злочинністю, вивчаючи, якою мірою нечесна поведінка впливає на повсякденні злочини економічного характеру.

**Основні моменти**

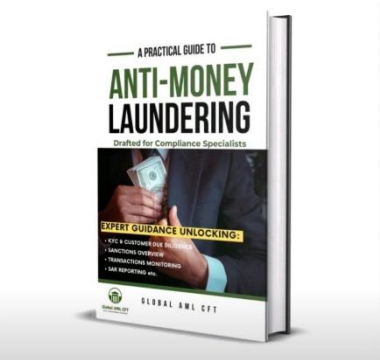
- **Ціль дослідження:** Основною метою дослідження є встановлення зв'язку між схильністю до нечесної поведінки та економічними злочинами. Для цього автори провели онлайн-опитування серед британців у 2023 році, яке включало оцінку схильності до нечесної поведінки та аналіз фактичної економічної злочинності.
- **Поширеність економічних злочинів:** В результаті дослідження було встановлено, що близько 26% дорослих у Великобританії здійснили принаймні один економічний злочин протягом року. До найпоширеніших злочинів належать ухилення від сплати податків, збереження помилково виданих коштів, купівля контрафактних товарів тощо.
- **Статева та вікова відмінності**: Статистичний аналіз показав, що чоловіки більш схильні до економічних злочинів (34% проти 18% у жінок). Молоді люди також демонструють більшу схильність до здійснення злочинів. Це підтверджується тим, що у віковій групі 18-25 років частка злочинців становить 45%, тоді як у групі 66 років і старших лише 7%.
- **Полі-девіантність:** Більшість злочинців (65%) здійснювали більше ніж один вид злочинів. Серед чоловіків середня кількість злочинів на одного злочинця – 4,4, а серед жінок – 3,6.
- **Чесність і злочинність:** Автори виявили сильний зв'язок між чесністю та рівнем злочинної діяльності. Люди з низьким рівнем чесності частіше скоюють злочини і проявляють більшу полі-девіантність. Ті, хто завжди виправдовують брехню, в п'ять разів частіше скоюють економічні злочини.
- **Розвиток моральної схильності**: Виявлено, що моральна схильність до нечесної поведінки змінюється з віком. Молодші групи більш схильні до нечесності, але з віком їх чесність зростає. Проте автори наголошують на відставанні чоловіків у цьому процесі – їх моральний розвиток відбувається із запізненням приблизно на 10 років у порівнянні з жінками.

**Висновки**

- **Зростання ролі нечесності:** Автори приходять до висновку, що схильність до нечесної поведінки є важливим фактором, що визначає рівень економічної злочинності. Чоловіки та молоді люди частіше скоюють злочини через свою більш нечесну схильність.
- **Необхідність втручання:** Для зменшення рівня економічної злочинності, автори рекомендують вжити заходів, спрямованих на зміну ставлення молоді та чоловіків до нечесної поведінки, адже саме ці групи є найбільш вразливими до злочинних дій.
- **Зміни у соціальних нормах:** Згідно з дослідженням, рівень моральних стандартів серед молодих людей знизився порівняно з попередніми поколіннями, що означає, що для збереження високих рівнів соціальної чесності нові покоління мають долати значні моральні перешкоди.

http://surl.li/juczxr

## Практичний посібник з протидії відмиванню коштів




Книга «Практичний посібник з протидії відмиванню коштів» охоплює основні принципи та практичні аспекти боротьби з відмиванням коштів та фінансуванням тероризму. Вона глибоко розглядає ключові процедури, такі як перевірка клієнтів (CDD), аналіз підозрілої активності (SAR) та управління ризиками, пов'язаними з санкціями. Автор акцентує увагу на відповідності міжнародним стандартам, зокрема рекомендаціям FATF, і надає реальні приклади застосування цих стандартів у фінансових установах.

**Основні розділи книги:**

1. **Основи AML/CFT**: Огляд ключових концепцій, термінології та міжнародних стандартів, таких як рекомендації FATF. Описується важливість відповідності регуляторним вимогам та найкращим практикам для зниження ризиків відмивання грошей.
2. **Процеси ідентифікації клієнтів (CDD)**: Пояснення, як фінансові установи повинні здійснювати перевірку клієнтів. Розглядаються методи збору інформації та оцінки ризиків, а також застосування процесу KYC (Знай свого клієнта).
3. **Підозрілі операції (SAR)**: Розділ присвячений тому, як правильно виявляти, оцінювати та звітувати про підозрілу активність. Автор дає практичні поради щодо звітності та роботи з відповідними регулюючими органами.
4. **Санкції та ризики**: Вивчаються методи управління ризиками, пов’язаними з міжнародними санкціями. Описано, як санкції впливають на роботу фінансових установ і як потрібно налаштовувати системи моніторингу для виявлення санкційних ризиків.
5. **Управління ризиками AML/CFT**: Висвітлюються процеси створення і підтримання ефективних систем управління ризиками у фінансових установах. Окрему увагу приділено оцінці та моніторингу ризиків, а також інструментам їх зниження.
6. **Практичні приклади**: Книга містить реальні кейси та сценарії, що допомагають зрозуміти, як застосовувати концепції на практиці. Це надає читачам змогу отримати більш глибоке розуміння реальних викликів, з якими стикаються фінансові установи.
7. **Сучасні тренди AML/CFT**: Огляд новітніх методів та технологій, які використовуються для боротьби з відмиванням коштів та фінансуванням тероризму, таких як машинне навчання, штучний інтелект, та аналітика великих даних.

Посібник орієнтований на те, щоб допомогти фахівцям фінансової галузі та комплаєнсу розвивати практичні навички у виявленні та попередженні фінансових злочинів.

https://globalamlcft.gumroad.com/l/atjmg

# ІНШІ НОВИНИ

## Колишнього міністра транспорту Кіпру звинуватили у відмиванні грошей і корупції через програму «Золотий паспорт»


Колишній міністр транспорту Кіпру, Мариос Дімітріадіс, був звинувачений у відмиванні грошей та корупції через участь у програмі "Золотих паспортів", що надавала громадянство Кіпру іноземцям в обмін на інвестиції. Однак вона стала платформою для фінансових злочинів, таких як відмивання грошей і корупція. Програма надавала можливість особам з сумнівними доходами легалізувати свої фінанси, інвестуючи в нерухомість та бізнес на Кіпрі, отримуючи при цьому громадянство ЄС. Це викликало міжнародний скандал, і після численних розслідувань програму було закрито через масштабні зловживання. Дімітріадіс є однією з ключових фігур, залучених до цієї схеми, що стала об'єктом розслідування правоохоронних органів.

http://surl.li/fgxtwc

## Іран виплатив мільйони у вигляді викупу, щоб покласти край масовій кібератаці на банки, кажуть чиновники


Іран став жертвою масової кібератаки, під час якої хакери націлилися на державні банки та вимагали викуп у мільйони доларів. Зловмисники отримали доступ до критичної банківської інфраструктури, що призвело до серйозних перебоїв у фінансовій системі та викликало обурення серед клієнтів. Атака виявила вразливість іранської кібербезпеки, яка раніше вже ставала ціллю подібних атак. Згідно з повідомленнями, напад є частиною ширшої тенденції зростання кібератак в регіоні, що підкреслює слабкі місця фінансових та державних систем країн, таких як Іран.

У ході атаки хакери вимагали викуп у криптовалюті, що є популярною практикою серед кіберзлочинців, які використовують цифрову анонімність для уникнення відповідальності. Атака, ймовірно, була спрямована на дестабілізацію банківського сектору країни, що вже перебуває під значним міжнародним тиском через санкції. Влада Ірану намагалася мінімізувати наслідки атаки, проте кібератака продемонструвала недоліки в їхніх зусиллях щодо забезпечення кібербезпеки.

Цей інцидент став частиною ширшої глобальної проблеми, оскільки кібератаки на фінансові установи стають дедалі частішими і вимагають більшої уваги до кіберзахисту.

https://www.politico.eu/article/iran-millions-ransom-massive-cyberattack-banks/

## Швейцарський суд визнав винними двох топ-менеджерів PetroSaudi у зв’язку зі скандалом із малайзійським фондом 1MDB

Швейцарія завершила масштабне розслідування фінансових злочинів, пов'язаних із малайзійським державним інвестиційним фондом 1MDB, через який було виведено понад 4 мільярди доларів. Фонд, створений для розвитку економіки Малайзії, став об'єктом шахрайства і відмивання грошей, а його кошти використовувалися для фінансування розкішних покупок, таких як нерухомість, яхти і твори мистецтва. Багато відомих міжнародних фінансових установ були залучені до цього


скандалу. Швейцарські прокурори оштрафували кілька банків і заморозили активи, пов'язані з цими операціями.

Цей скандал привернув глобальну увагу через залучення вищих посадових осіб з Малайзії, Саудівської Аравії та інших країн, які використовували фонд для власного збагачення. Основна схема передбачала складне переплетення транзакцій через офшорні компанії і підставні фірми для приховування справжніх власників і джерел коштів. У межах розслідування Швейцарія відіграла ключову роль завдяки своїй банківській системі, де проходила частина цих фінансових операцій. Це розслідування завершилось значними штрафами та заходами щодо запобігання подібним махінаціям у майбутньому.

http://surl.li/chzsfy

## Міжнародна боротьба з фінансовими злочинами: Операція проти глобальної мережі «Black Axe»


Стаття BBC висвітлює широкомасштабну боротьбу міжнародних правоохоронних органів з діяльністю кримінальної організації «Black Axe», яка займається відмиванням коштів, кіберзлочинами та іншими видами фінансових правопорушень.

Операція Jackal III, скоординована Інтерполом, включала арешти понад 300 осіб і замороження активів на суму понад $35 млн, поширюючись на 21 країну. Під час операції використовувалися нові технології для протидії кіберзлочинам, в тому числі аналітика великих даних, співпраця з національними поліціями та контроль за банківськими рахунками.

Ключові моменти, що стосуються фінансових злочинів:

- **Масштабне відмивання коштів:** Одним із основних джерел доходів «Black Axe» є відмивання грошей через криптовалюти та інші фінансові технології (фінтех). У 2017 році канадські органи правопорядку виявили схему відмивання коштів на суму $5 млрд, пов’язану з «Black Axe».
- **Кіберзлочинність:** Організація активно займається кіберзлочинами, використовуючи сучасні фінансові інструменти, включаючи криптовалюту, онлайн-шахрайства та кіберкрадіжки. Це дозволяє їм працювати глобально та переміщувати незаконні кошти через кордони.
- **Фінансовий вплив і збитки:** Операція призвела до арештів сотень членів банди та замороження банківських рахунків у різних країнах. Наприклад, в Ірландії через мережу «Black Axe» було відмито мільйони євро через схеми з використанням банків і криптовалют. Ірландська поліція виявила 1000 осіб, які мали зв'язки з організацією, і здійснила сотні арештів за шахрайства та кіберзлочини.
- **Технологічна боротьба з злочинністю:** Інтерпол почав використовувати нові технології, такі як механізм Глобальної взаємодії платежів (I-GRIP), що дозволяє державам-членам блокувати банківські рахунки по всьому світу. Ця технологія була застосована для замороження рахунків на $40 млн, що належали сингапурській бізнес-мережі. Також проводяться спільні навчання з місцевими правоохоронними органами для поліпшення боротьби з кіберзлочинністю.

- **Вплив на бідні регіони:** Основні рекрутингові бази для «Black Axe» розташовані в Нігерії, де багато людей живе за межею бідності. Умови життя та корупція в регіоні сприяють притоку нових членів до організації, що робить боротьбу з нею ще складнішою.
- **Фінансові технології та злочини:** «Black Axe» активно використовує нові технології для проведення злочинних операцій. Фінансові технології, такі як мобільні додатки та криптовалюти, дозволяють організації легко переміщувати великі суми грошей через кордони, уникаючи традиційних фінансових систем і правоохоронних органів.

Ця стаття демонструє, що фінансові злочини глобальних кримінальних організацій стають все більш складними через нові технології, що вимагає гнучкого підходу до боротьби з ними з боку міжнародних правоохоронних структур.

http://surl.li/yxfzqb

## Виявлення та вилучення незаконних криптоактивів за допомогою рішення Chainalysis для розслідувань

Стаття від Chainalysis детально пояснює, як правоохоронні органи та фінансові установи можуть ефективно ідентифікувати та вилучати незаконні криптоактиви, використовуючи передові аналітичні інструменти. Першим етапом є ідентифікація криптовалютних гаманців, пов'язаних із злочинною діяльністю, такими як відмивання грошей, кіберзлочини та торгівля забороненими товарами. Аналітичні інструменти, як Chainalysis Reactor, дозволяють відслідковувати рух коштів через блокчейн, визначати ключові фінансові вузли та осіб, що беруть участь у злочинних схемах.

Стаття також описує, як аналіз блокчейнів допомагає фіксувати незаконні транзакції в реальному часі, що дає можливість швидко реагувати на нові загрози. Окрім технічної частини, Chainalysis зазначає, що юридична складова також є важливою. Уряди та правоохоронні органи працюють над розробкою законодавчої бази, яка б спрощувала вилучення криптоактивів, пов'язаних із злочинами, та полегшувала процес повернення незаконно отриманих коштів.

Платформи для моніторингу блокчейн-транзакцій відіграють вирішальну роль у процесі протидії фінансовим злочинам у криптовалютному просторі. Наприклад, завдяки таким інструментам вдалося заарештувати активи вартістю сотні мільйонів доларів, пов'язані з кіберзлочинністю. Chainalysis підкреслює, що ефективність цього процесу залежить не лише від технології, але й від активної співпраці між урядами, правоохоронними органами та криптовалютними біржами.

На практиці ідентифікація та вилучення криптоактивів часто пов'язані з певними труднощами, зокрема через децентралізований характер блокчейнів і псевдонімність користувачів. Але завдяки технологіям аналітичного моніторингу та співпраці між державними та приватними структурами значну частину незаконних активів можна відслідкувати та повернути.

https://www.chainalysis.com/blog/identifying-and-seizing-illicit-crypto-assets/

# ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

## Як зменшити кількість помилкових спрацьовувань у сфері ПВК


Стаття на сайті ComplyAdvantage детально аналізує проблему помилкових спрацювань у системах ПВК і пропонує стратегії для їх зменшення. Однією з головних проблем є надмірна кількість "помилкових спрацювань", коли підозрілі транзакції виявляються безпідставними, що вимагає додаткових ресурсів на їх перевірку і уповільнює процес фінансового моніторингу. У статті підкреслюється необхідність удосконалення технологій аналізу, зокрема використання штучного інтелекту та машинного навчання для зменшення кількості таких помилкових сигналів.

Одним із методів, які пропонуються, є оптимізація даних, що використовуються для аналізу. Використання більш точних і актуальних даних дозволить фінансовим установам точніше визначати підозрілі операції, зменшуючи кількість фальшивих сигналів. Інший підхід — це вдосконалення алгоритмів шляхом інтеграції аналізу ризиків і контекстної інформації про клієнтів, що дозволяє більш глибоко розуміти їхню поведінку і унікальні фінансові шаблони. Стаття також наголошує на важливості регулярного оновлення правил та профілів ризику для мінімізації ризику помилкових сигналів.

Крім того, акцент робиться на впровадження інструментів автоматизації процесу перевірки транзакцій і даних про клієнтів, що допоможе зменшити навантаження на аналітиків фінансового моніторингу. Штучний інтелект здатен виявляти складні шаблони, які могли бути пропущені традиційними системами моніторингу, підвищуючи тим самим точність роботи систем протидії відмиванню коштів.

Таким чином, ефективне зниження кількості помилкових спрацювань у системах ПВК дозволить фінансовим установам оптимізувати свої процеси, зменшити витрати та підвищити загальну ефективність боротьби з відмиванням грошей.

http://surl.li/htlidt

## Огляд ZK та Optimistic Rollups


У статті на Chainalysis детально розглядаються два рішення для масштабування блокчейн-технологій: Zero-Knowledge Rollups (ZK-Rollups) та Optimistic Rollups. Обидва підходи спрямовані на покращення швидкості та ефективності блокчейн-систем шляхом обробки великої кількості транзакцій за межами основного ланцюга.

ZK-Rollups використовують криптографічні докази для миттєвого підтвердження транзакцій, що робить їх більш безпечними та швидкими. У свою чергу, Optimistic Rollups припускають, що всі транзакції є дійсними, якщо протягом певного часу немає оскарження, що робить їх менш енергозатратними, але з більшим ризиком.

Основні відмінності між цими двома рішеннями полягають у підходах до верифікації та швидкості роботи. ZK-Rollups є ідеальними для додатків, де потрібна висока швидкість і безпека, тоді як Optimistic Rollups краще підходять для проєктів, де важлива масштабованість і економія ресурсів.

Загалом, обидва рішення допомагають суттєво підвищити продуктивність блокчейн-проєктів, знижуючи витрати на обробку транзакцій і покращуючи користувацький досвід.

https://www.chainalysis.com/blog/zero-knowledge-rollups-optimistic-rollups-overview/