



Серійний номер: ДСФМУ-ДК-2024-029  
Жовтень 2024

## ЗВІТИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ та ОКРЕМИХ ЮРИСДИКЦІЙ

### Використання мобільних платіжних систем та платіжних систем в мережі інтернет для відмивання коштів та фінансування тероризму



Документ від CFATF розглядає зростаючу загрозу використання інтернет- та мобільних платіжних систем для фінансування злочинної діяльності. Автори наголошують, що ці системи можуть піддаватися ризикам, пов'язаним із високою анонімністю транзакцій та швидкістю переказів, що ускладнює виявлення незаконної діяльності. Особлива увага приділяється віртуальним активам і криптовалютам, які використовуються для анонімних транзакцій, та схемам, які дозволяють шахраям створювати безліч облікових записів з підробленими документами.

#### Ключові ризики, згадані у документі, включають:

**Анонімність:** Оскільки багато транзакцій здійснюється без особистих зустрічей, це збільшує ризик приховування справжньої ідентичності зловмисників. Використання псевдоанонімних криптовалют також додає складнощів у відстеженні учасників операцій.

**Віртуальні активи:** Використання криптовалют і цифрових активів на платформах для здійснення міжнародних транзакцій дозволяє злочинцям швидко переміщати кошти між різними юрисдикціями, уникаючи контролю.

**Складність транзакцій:** Переплетення коштів через кілька рахунків, часто з використанням підроблених документів або від імені третіх осіб, ускладнює виявлення джерела коштів. Ці складні схеми використовуються для легалізації незаконних доходів.

**Роздріблення платежів:** Використовуючи стратегії дроблення платежів (smurfing), зловмисники можуть уникати встановлених порогів для обов'язкової звітності про підозрілі операції. Платежі можуть здійснюватися з кількох рахунків через мобільні або онлайн-банківські додатки.

**Відмивання коштів у сфері торгівлі:** В документі описано, як злочинці можуть маніпулювати рахунками-фактурами або завищувати вартість товарів та послуг у міжнародній торгівлі, використовуючи онлайн-платіжні системи для переміщення незаконних коштів через кордони.

Для зменшення ризиків рекомендується впровадження жорсткіших заходів щодо перевірки особи клієнтів, моніторингу транзакцій та зберігання інформації. Необхідно приділяти увагу тому, як

фінансові установи взаємодіють із віртуальними активами, що можуть сприяти відмиванню коштів. Суворий нагляд і контроль з боку регуляторів, включаючи позапланові перевірки, є ключовими для зниження загроз, пов'язаних із використанням анонімних технологій.

<https://lnkd.in/eyjQY6GG>

## Рекомендації Міжвідомчого Комітету Сінгапуру щодо посилення системи протидії відмиванню коштів

Документ, який був підготовлений міжвідомчим комітетом Сінгапуру з питань протидії відмиванню коштів, містить детальний аналіз антилегалізаційних механізмів держави. Сінгапур є важливим міжнародним фінансовим центром, і його репутація значною мірою залежить від зусиль із забезпечення прозорості та безпеки фінансових транзакцій. У серпні 2023 року влада розкрила великий кейс з відмивання коштів, що підкреслило складність сучасних злочинних схем і важливість оновлення існуючих механізмів протидії.

Значна частина документу присвячена тому, як у відповідь на цей кейс була створена міжвідомча комісія для перегляду та посилення наявної нормативної бази. **Серед нововведень – покращення стандартів боротьби з відмиванням коштів для фінансових установ та ВНУП. Документ підкреслює важливість чіткого виконання законодавства, підвищення кваліфікації відповідальних осіб та тісної співпраці між урядовими органами та приватним сектором.**



Однією з ключових складових стратегії є підхід "запобігання, виявлення, реагування", що спрямований на запобігання відмиванню коштів на ранніх етапах. Запровадження нових технологій та платформ для обміну інформацією, таких як COSMIC, покликане підвищити ефективність виявлення підозрілих фінансових операцій. Крім того, важливим є посилення контролю над рахунками номінальних директорів компаній, що часто використовуються для приховування незаконної діяльності.

Документ також містить рекомендації для покращення процедур контролю за корпоративними структурами, які можуть бути використані злочинцями для відмивання коштів. Окремо наголошено на важливості навчання для осіб, залучених до фінансових операцій, і підвищення якості їх обізнаності щодо ризиків. Уряд зобов'язується продовжувати співпрацювати з міжнародними організаціями для забезпечення відповідності міжнародним стандартам, таким як ті, що встановлюються Групою розробки фінансових заходів боротьби з відмиванням коштів (FATF).

### Ключові висновки:

- Посилення стандартів протидії відмиванню коштів:** Для запобігання злочинним діям важливо встановити жорсткіші вимоги для фінансових установ та ВНУП. Ці вимоги включають проведення належної перевірки клієнтів (CDD) та фіксацію підозрілих транзакцій. Окрім цього, документ підкреслює, що важливо підтримувати баланс між жорсткістю заходів і економічною свободою, щоб не обмежувати законну діяльність бізнесів.
- Розширення механізмів виявлення:** Сінгапур активно вдосконалює методи виявлення злочинних схем через інформаційно-аналітичні системи. Введення платформи COSMIC дозволяє фінансовим установам обмінюватися даними про підозрілих клієнтів і транзакції, покращуючи координацію між установами. Це значно збільшує швидкість і ефективність виявлення потенційних загроз.

3. **Запобігання використанню компаній для відмивання коштів:** Крім фінансових установ, компанії та корпоративні структури також можуть бути використані для приховування нелегальних активів. Зокрема, документ розглядає зловживання "оболонковими" компаніями та фіктивними підприємствами для приховування джерел коштів. Для протидії цьому Сінгапур ввів нові вимоги для номінальних директорів і посилив регуляторний контроль за корпоративними службами.
4. **Міжвідомча співпраця та обмін інформацією:** Документ акцентує на необхідності тісної співпраці між державними органами, щоб оперативного реагувати на нові схеми відмивання коштів. Було створено спеціальні групи, як наприклад **AML Case Coordination Network**, які дозволяють державним органам швидко координувати дії, виявляти та розслідувати злочинні угруповання.
5. **Міжнародне співробітництво:** Враховуючи транснаціональний характер відмивання коштів, Сінгапур продовжує активно співпрацювати з іноземними правоохоронними органами для збору доказів і запобігання незаконним фінансовим операціям. Багато з коштів, що відмиваються через Сінгапур, надходять з-за кордону, тому міжнародна координація є критично важливою для успішної протидії.
6. **Сильніші правові важелі:** Сінгапур постійно оновлює свої правові механізми відповідно до нових схем відмивання коштів. Важливими змінами є посилення можливостей щодо переслідування злочинців, пов'язаних із іноземною злочинною діяльністю, і введення жорсткіших покарань для фінансових установ, що не дотримуються AML вимог. Це підвищує ефективність правоохоронних дій та забезпечує більший вплив на злочинців.

Таким чином, цей документ представляє всебічну стратегію Сінгапуру для протидії відмиванню коштів через підходи до запобігання, виявлення та переслідування.

<http://surl.li/gjmuhl>

## ГАЙДЕНС ЩОДО ВНУТРІШНЬОЇ ОЦІНКИ РИЗИКІВ ВІДМИВАННЯ КОШТІВ / ФІНАНСУВАННЯ ТЕРОРИЗМУ



Документ представляє всебічний посібник для підзвітних установ (RE), таких як банки та небанківські фінансові компанії (NBFCs), що працюють під наглядом Резервного банку Індії (RBI). Він визначає загальні принципи проведення внутрішньої оцінки ризиків (IRA), пов'язаних із відмиванням коштів, фінансуванням тероризму та фінансуванням розповсюдження зброї масового знищення. **Основна мета документа — допомогти RE зрозуміти рівень ризику, до якого вони схильні, та ефективно використовувати свої ресурси для управління цими ризиками. Посібник детально описує підходи до оцінки ризиків, які виникають через взаємодію з клієнтами, продуктами, географічними регіонами та каналами доставки послуг, а також рекомендує методи контролю та заходи для їх зниження.**

**У першому розділі документа наведено загальні положення та принципи проведення оцінки ризиків.** Важливим аспектом є дотримання ризик-орієнтованого підходу (РОП), згідно з рекомендацією FATF. Оцінка ризиків повинна бути детальною та охоплювати як рівень бізнесу, так і індивідуальні ризики, пов'язані з клієнтами.

**У другому розділі описано методологію оцінки ризиків, яка включає етапи ідентифікації внутрішніх факторів ризику, оцінку ефективності внутрішніх контролів та розрахунок залишкового ризику.** Документ пропонує інструменти для класифікації ризиків на високий, середній та низький рівні, а також рекомендації щодо визначення ваги різних факторів ризику.

**Третій розділ наголошує на важливості комунікації результатів оцінки ризиків до керівництва РЕ, а також на необхідності розробки планів дій для зниження залишкових ризиків.** Особлива увага приділяється впровадженню ризиків фінансування розповсюдження зброї масового знищення в загальну оцінку ризиків.

#### **Ключові висновки:**

### **1. Необхідність використання РОП для ефективного управління ризиками ВК/ФТ/ФР.**

Основним принципом цього документа є застосування РОП, що передбачає налаштування систем контролю та розподіл ресурсів відповідно до ідентифікованих ризиків. РОП дозволяє фінансовим установам спрямовувати свої зусилля на ті сфери, де ризик найбільш значний, тим самим оптимізуючи використання своїх ресурсів для боротьби з ВК/ФТ/ФР. Застосування цього підходу передбачає регулярне оновлення оцінок ризиків, що враховують специфіку клієнтів, продуктів, географічних регіонів та каналів постачання.

### **2. Внутрішня оцінка ризиків має бути двоетапною: бізнес-рівень та індивідуальний рівень.**

Оцінка ризиків повинна проводитися на двох рівнях. Перший рівень – це бізнес-рівень, де оцінюються загальні ризики, пов'язані з характером бізнесу, масштабом операцій, складністю продуктів і послуг, а також рівнем взаємодії з різними юрисдикціями. Другий рівень – індивідуальний рівень, який стосується ризиків конкретних клієнтів або транзакцій. Наприклад, певні категорії клієнтів можуть вважатися більш ризикованими через свою діяльність або географічне розташування, тому їм повинна бути приділена більша увага під час проведення процедур належної перевірки (CDD). Важливо враховувати як кількісні, так і якісні аспекти при визначенні ваги ризиків.

### **3. Методологія оцінки ризиків включає ідентифікацію, оцінку та впровадження заходів контролю для зниження ризиків.**

Процес оцінки ризиків передбачає кілька етапів, зокрема ідентифікацію ризиків (наприклад, клієнтських, продуктово-сервісних, географічних), визначення їхнього рівня ризику та впровадження внутрішніх заходів контролю. Після оцінки контролюючих заходів установи повинні оцінити залишковий ризик, який залишається після впровадження цих заходів. Залишковий ризик допомагає визначити, чи достатні існуючі заходи для ефективного управління ризиками ВК/ФТ/ФР, чи необхідно впроваджувати додаткові заходи.

### **4. Ідентифікація ключових факторів ризику є критично важливою для точного оцінювання ризиків.**

Оцінка повинна включати визначення таких ризикових факторів, як тип клієнтів (індивідуальні чи юридичні особи, політично значущі особи (PEP)), географічні ризики (наприклад, країни з високим рівнем корупції або слабким контролем з ПВК/ФТ), ризики, пов'язані з продуктами або послугами (особливо у випадках, коли прозорість транзакцій низька), а також ризики, пов'язані з використанням нових технологій або цифрових продуктів. Ці фактори повинні регулярно переглядатися та оновлюватися з урахуванням нових загроз.

### **5. Ключова роль документування та комунікації результатів оцінки ризиків.**

Результати оцінки ризиків повинні бути документовані та передані відповідним керівникам та бізнес-підрозділам підзвітної установи. Це включає як стислий виклад профілю ризиків установи, так і детальні заходи щодо їх пом'якшення. Крім того, важливо регулярно інформувати керівництво про результати оцінки та вчасно реагувати на нові ризики. Чітке документування дозволяє залучати до процесу управління ризиками всі необхідні сторони та допомагає регуляторним органам оцінити ефективність політик управління ризиками.

### **6. Інтеграція ризиків фінансування розповсюдження зброї масового знищення у загальну оцінку ризиків.**

Документ підкреслює необхідність включення ризиків ФР у загальну внутрішню оцінку ризиків. Це включає ризики, пов'язані з недотриманням санкцій, що можуть бути накладені Радою Безпеки ООН, або спроби обійти ці санкції. Оцінка ризиків ФР є важливим кроком у забезпеченні відповідності міжнародним стандартам та вимогам FATF щодо протидії фінансуванню розповсюдження зброї.

## 7. Постійний моніторинг ризиків та їх адаптація до нових загроз.

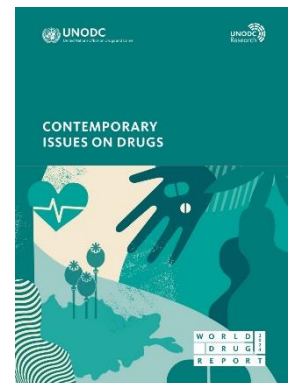
Важливим висновком документа є те, що оцінка ризиків повинна бути не статичною, а динамічною, з регулярними переглядами у відповідь на зміни у бізнесі або появу нових загроз. Наприклад, зміни в продуктах або розширення діяльності на нові юрисдикції можуть вимагати проведення повторної оцінки ризиків раніше встановлених термінів. Це також стосується змін у міжнародних санкційних режимах або появи нових технологій, що можуть підвищити ризик зловживань.

Таким чином, документ створює структуру для всебічної оцінки та управління ризиками відмивання коштів, фінансування тероризму та розповсюдження зброї масового знищення, з акцентом на адаптивність процесів і регулярний перегляд у відповідь на динамічні зміни в глобальному середовищі загроз.

<http://surl.li/izrvce>

## Наслідки заборони наркотиків, зростання синтетичних ринків та соціально-економічні виклики

Звіт «World Drug Report 2024», підготовлений Управлінням ООН з наркотиків та злочинності (UNODC), розглядає ключові тенденції у виробництві, торгівлі та використанні наркотиків у світі, приділяючи особливу увагу новим викликам. Огляд містить спеціальні розділи, присвячені впливу заборони вирощування опіумного маку в Афганістані, зростанню ринку синтетичних наркотиків та їхньому впливу на жінок і молодь, а також законодавчим змінам у сфері канабісу та психоделіків. Звіт наголошує на зв'язку між наркотрафіком та організованою злочинністю в ключових регіонах, таких як Золотий Трикутник, і підкреслює необхідність забезпечення права на здоров'я для всіх осіб, які вживають наркотики.



### Ключові висновки:

#### 1. Афганістан: Заборона вирощування опіумного маку та її наслідки

- **95% скорочення** вирощування опіумного маку після введення заборони Талібаном у 2022 році призвело до різкого падіння виробництва опіуму та зниження доходів фермерів.
- **Економічні втрати:** Загальні доходи фермерів від продажу опіуму **впали на 92%**, що викликало значне економічне напруження. Хоча частина сільськогосподарських земель була переорієнтована на вирощування пшениці, це не компенсувало втрати.
- **Потенційна нестабільність:** Продаж активів та зростання напруженості у сільських районах можуть призвести до насильницьких заворушень у разі погіршення гуманітарної ситуації.
- **Ціни на опіум різко зросли** після заборони, досягнувши \$800 за кг у грудні 2023 року, що стимулювало спекуляції та подальшу контрабанду залишків зберіганих запасів.

#### 2. Метамфетамін: Зростання виробництва попри заборону наркотиків

- **Збільшення виробництва метамфетаміну:** Попри заборону на всі наркотики, виробництво метамфетаміну в Афганістані зростає, використовуючи дику ефедру як сировину.
- **Регіональний наркотрафік:** Ключовими транзитними точками є **Іран та Пакистан**, які звітують про значні вилучення афганського метамфетаміну, що експортується до Південної Азії, Близького Сходу та Африки.
- **Посилення заходів контролю:** Закриття ринку ефедри у провінції Фарах та знищення лабораторій демонструють зусилля Талібану з протидії виробництву синтетичних наркотиків, але їхній вплив поки обмежений.

### 3. Гендерні виклики та право на здоров'я

- **Стигматизація жінок:** Жінки, які вживають наркотики, стикаються з дискримінацією та обмеженим доступом до лікування, що підвищує їхню вразливість.
- **Рекомендації звіту включають забезпечення рівного доступу** до медичних та реабілітаційних послуг, що відповідають принципам прав людини та зберігають гідність осіб, які вживають наркотики.
- **Розширення використання синтетичних наркотиків** серед молоді, зокрема метамфетаміну та таблеток «К», вимагає створення програм профілактики та лікування.

### 4. Наркотрафік та організована злочинність у Золотому Трикутнику

- **Конфлюєнція наркаторгівлі з іншими видами злочинів**, включаючи торгівлю людьми, ускладнює боротьбу з організованою злочинністю.
- Необхідні **більш комплексні та міждержавні підходи** до протидії наркаторгівлі, які включають розвиток соціально-економічних можливостей та підвищення рівня безпеки у регіоні.

### 5. Законодавчі зміни щодо канабісу та психоделіків

- **Лібералізація законодавства** щодо канабісу та психоделіків у ряді країн створює нові можливості для їхнього регульованого використання. Це може сприяти розвитку ринків, але водночас вимагає відповідних заходів контролю для запобігання зловживанню.

### 6. Соціально-економічні наслідки боротьби з наркотиками

- **Відсутність альтернативних джерел доходу** для фермерів, які втратили прибутки від вирощування опіуму, збільшує ризики бідності та соціальної нестабільності.
- **Зростання безробіття та економічні втрати** підвищують ризик радикалізації молоді та залучення її до нелегальної діяльності, зокрема наркаторгівлі.
- Для **ефективного скорочення наркаторгівлі необхідні довгострокові програми розвитку**, які включають не лише заміщення нелегальних культур, а й створення умов для соціального та економічного зростання.

### 7. Глобальні наслідки для ринків наркотиків

- **Скорочення пропозиції опіуму з Афганістану** може призвести до дефіциту опіатів на світових ринках, особливо в Європі, Африці та Азії. Це може стимулювати зростання попиту на інші наркотики, зокрема синтетичні опіоїди.
- **Перекриття афганських каналів наркотрафіку** може призвести до переорієнтації потоків наркотиків на інші маршрути, що потребує адаптації міжнародних програм боротьби з наркотрафіком.

Цей звіт наголошує на **необхідності комплексних підходів до протидії наркотикам**, які включають не лише посилення правоохоронних заходів, а й розробку програм економічної підтримки та розвитку. Міжнародна співпраця залишається ключовою для забезпечення довгострокових рішень у сфері боротьби з наркотрафіком та зменшення шкоди від вживання наркотиків.

[https://www.unodc.org/documents/data-and-analysis/WDR\\_2024/WDR24\\_Contemporary\\_issues.pdf](https://www.unodc.org/documents/data-and-analysis/WDR_2024/WDR24_Contemporary_issues.pdf)

# Рекомендації CRI для організацій під час інцидентів шахрайства з програмами-вимагачами

Цей документ, виданий в рамках міжнародної ініціативи Counter Ransomware Initiative (CRI), надає вказівки для організацій щодо реагування на інциденти, пов'язані з програмами-вимагачами. У 2023 році CRI визнала проблему таких програм глобальною, закликавши країни та організації до співпраці, щоб знизити вплив таких атак.



Guidance  
**CRI guidance for organisations during ransomware incidents**  
Published 2 October 2024

## Ключові моменти дослідження:

### Наслідки виплат викупу:

- Оплата викупу стимулює злочинців продовжувати діяльність.
- Виплата викупу не гарантує відновлення даних або припинення атаки.

- Викуп може використовуватись для подальшої злочинної діяльності.

## Рекомендації CRI щодо оплати викупу:

- **Оплату викупу не рекомендують через низку ризиків**, у тому числі незахищеність систем навіть після отримання ключа шифрування.
- Організаціям радять ретельно оцінювати всі можливі наслідки та варіанти перед прийняттям рішення.

## Співпраця з кіберстраховими компаніями:

- Кіберстрахування відіграє важливу роль у підвищенні стійкості до кібератак.
- CRI та страхові організації заохочують постраждалі компанії звертатися за підтримкою до страхових компаній та експертів для покращення прийняття рішень.

## Підготовка до інцидентів:

- **Організаціям рекомендується завчасно** готувати плани безперервності бізнесу, **створювати резервні копії даних, а також мати чіткі політики реагування** на атаки.
- Важливо відслідковувати правові аспекти платежів, оскільки в деяких юрисдикціях оплата викупу може бути незаконною, особливо якщо платіж спрямовується на санкціоновані організації.

## Співпраця з правоохоронними органами:

- Повідомлення про інцидент органам влади на ранніх етапах може допомогти в розслідуванні, захисті організації та запобіганні подальшим атакам.

## Оцінка альтернатив:

- Перш ніж сплатити викуп, організації мають розглянути можливість використання резервних копій, сторонніх інструментів декодування та інші шляхи відновлення даних.

## Записування процесу ухвалення рішень:

- Для подальших звітів і аналізу інциденту важливо вести детальний запис прийнятих рішень та дій, що допоможе не лише у правовому контексті, а й у подальшому зміцненні кіберзахисту.

## Основні висновки:

- **Мінімізація шкоди:** Документ наголошує на важливості ретельного оцінювання всіх можливих наслідків інциденту, включаючи ризики для клієнтів та можливість крадіжки даних, перш ніж розглядати виплату викупу.
- **Співпраця із зовнішніми експертами:** Організаціям рекомендується залучати зовнішніх експертів (страховиків, технічних консультантів, правоохоронні органи) для допомоги у прийнятті рішень.
- **Постінцидентний аналіз:** Документ підкреслює важливість аналізу причин інциденту та вжиття заходів для запобігання повторенню атак, таких як управління обліковими даними та сегментація мережі.
- **Попередження про ненадійність злочинців:** Навіть у разі виплати викупу немає гарантій, що злочинці дотримуються своїх обіцянок і не оприлюднять викрадені дані.

Документ надає чітке керівництво для організацій щодо прийняття обґрунтованих рішень у разі інциденту з програмою-вимагачем, зосереджуючись на тому, як мінімізувати втрати та знизити ризик виплати викупу, що сприяє довготривалій кіберстійкості.

<http://surl.li/eyoudw>



# РЕГУЛЮВАННЯ

## FinTech 2024



Документ є всебічним довідником з аналізу правових питань, що стосуються фінансових технологій (Fintech) у глобальному масштабі. У ньому представлено порівняльний огляд правових систем різних юрисдикцій у контексті фінансових інновацій, таких як блокчейн, цифрові активи та платіжні системи. Посібник також охоплює регуляторні питання, зокрема боротьбу з відмиванням коштів та вимоги щодо фінансової прозорості. Особлива увага приділяється змінам у регуляторному середовищі для забезпечення відповідності стандартам та вимогам у сфері Fintech.

### Ключові висновки:

- 1. Взаємодія технологій та фінансів:** Документ підкреслює, що всі фінансові установи зараз є технологічними компаніями, оскільки їхні операції повністю залежать від технологій. Це змушує регуляторів розробляти нові стандарти для відповідальності та ліцензування фінансових технологій.
- 2. Регуляція нових цифрових активів:** Створення активів за допомогою коду (наприклад, токенизація) викликає потребу у правовому визнанні та класифікації таких активів. Blockchain вирішує складні проблеми, пов'язані з унікальністю цифрових предметів та власністю на них.
- 3. Регуляторні пісочниці:** Багато юрисдикцій впроваджують концепцію «пісочниць», яка дозволяє тестувати інноваційні бізнес-моделі та нові технологічні рішення в умовах регуляторного контролю. Це допомагає уникати законодавчих перешкод і одночасно перевіряти безпеку нових продуктів і послуг.
- 4. Кібербезпека та захист даних:** З розвитком цифрових рішень зростає необхідність посилення захисту споживачів та особистих даних, а також забезпечення кібербезпеки. Це викликає балансуювання між потребами у захисті конфіденційної інформації та вимогами правоохоронних органів.
- 5. Еволюція глобальних ринків:** Інтернет усуває фізичні кордони, дозволяючи активам торгуватися по всьому світу. Це викликає виклики для збереження цілісності ринків, зокрема через появу глобальних децентралізованих ринків та платформ. Документ акцентує на необхідності нових підходів до регулювання глобальних торгів.
- 6. Конфлікт між фінтехом та регуляторами:** Напруга між фінтех-компаніями та регуляторами є конструктивною, оскільки вона спонукає обидві сторони краще розуміти принципи захисту споживачів, забезпечення цілісності ринків та розробки інноваційних продуктів.

<https://practiceguides.chambers.com/practice-guides/fintech-2024>

# САНКЦІЇ

## Стратегічні виклики та можливості експортного контролю: вплив на напівпровідникову галузь США та зростання інновацій у Китаї



Звіт «The Double-Edged Sword of Semiconductor Export Controls» (жовтень 2024) від Центру стратегічних та міжнародних досліджень (CSIS) досліджує двозначний вплив експортного контролю напівпровідникових технологій з боку США. Основна увага зосереджена на тому, як ці обмеження впливають на сповільнення технологічного прогресу Китаю та водночас створюють нові стимули для китайських компаній обходити ці обмеження або розробляти власні технології. Особлива увага приділяється новітнім методам пакування чипів, таким як чиплети та гібридне з'єднання, які дозволяють досягати високих показників без використання передових напівпровідникових технологій США. Документ досліджує ризики для довгострокового технологічного лідерства США в умовах таких китайських контрстратегій, пропонуючи рекомендації для ефективної політики.

### Ключові висновки:

#### 1. Експортний контроль як стратегічний інструмент США

Експортні обмеження на напівпровідникові технології стали основним елементом економічної стратегії США для стримування зростання технологічного потенціалу Китаю. США прагнуть зберегти своє лідерство в галузі критичних технологій, включаючи штучний інтелект та високопродуктивні обчислення, запобігаючи доступу Китаю до передових напівпровідників.

#### 2. Контрстратегії Китаю: «design-out» та «design-around»

- **Design-out:** Китай активно замінює американські технології власними або залучає рішення з третіх країн. Це дозволяє уникнути ризиків, пов'язаних із залежністю від США.
- **Design-around:** Розробляються альтернативні технології, які забезпечують аналогічні функціональні можливості, що й заборонені американські технології, але без їхнього використання. Це пришвидшує розвиток внутрішньої інноваційної бази в Китаї.

#### 3. Інноваційні досягнення в галузі пакування чипів

Китай фокусується на розвитку передових методів пакування, таких як чиплети та гібридне з'єднання. Ці інновації дозволяють досягати високої продуктивності без використання найсучасніших виробничих технологій США, що відкриває шлях до нових додатків у штучному інтелекті та високопродуктивних обчисленнях.

#### 4. Загроза довгостроковому лідерству США

Втрата позицій на ринку напівпровідників може підірвати технологічне лідерство США. Якщо китайські компанії продовжать успішно обходити американські обмеження, це зменшить частку США на світових ринках, що критично вплине на їхні доходи та інвестиції в дослідження і розробки.

#### 5. Парадоксальна шкода від експортних обмежень

Експортні обмеження, спрямовані на стримування Китаю, стимулюють розвиток власних технологій у Китаї. Китайські компанії відмовляються від американських компонентів і прискорюють інновації, що може вивести їх на рівень технологічного лідерства.

#### 6. Проблеми багатосторонньої координації

Різні підходи до експортних обмежень серед союзників США ускладнюють контроль за експортом напівпровідників. Країни, такі як Нідерланди, Південна Корея та Німеччина, не завжди підтримують жорсткі заходи, що відкриває лазівки для китайських компаній.

## 7. Стратегічні рекомендації для США

Замість запровадження нових обмежень, США мають зосередитися на інвестиціях у власні технології пакування та розвиток партнерств з союзниками. Програма NAPMP (National Advanced Packaging Manufacturing Program) під CHIPS Act є прикладом таких інвестицій, спрямованих на підтримку інновацій у пакуванні.

## 8. Інноваційний зсув у Китаї

Поточна політика США провокує культурний зсув у Китаї від копіювання західних технологій до створення власних інноваційних рішень. Це становить довгострокову загрозу для конкурентоспроможності США.

## 9. Можливі наслідки для національної безпеки

Якщо Китай досягне незалежності від американських технологій, це обмежить можливості США відстежувати військові можливості Китаю та контролювати розвиток критичних технологій.

## 10. Перевага Китаю в галузі пакування

Китай займає лідерські позиції у сфері традиційного пакування напівпровідників, що дозволяє йому швидше розвивати нові методи. Водночас США не мають значних переваг у цій сфері, що створює вікно можливостей для китайських компаній досягти лідерства.

## 11. Необхідність перегляду підходу до експортного контролю

Повернення до стратегії «ковзної шкали» може стати ефективнішим підходом, ніж поточний «жорсткий бар'єр». Це дозволить зберігати технологічний відрив без стимулювання інтенсивних інновацій у країнах-конкурентах, як це відбувається зараз.

## 12. Загальний висновок

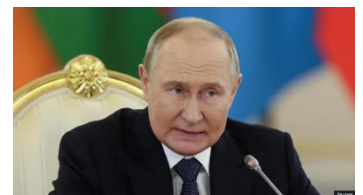
Стимування доступу Китаю до американських технологій прискорює його інноваційний розвиток і створює нові виклики для глобального лідерства США в напівпровідниковій галузі. Відповідь США має полягати в інвестиціях, міжнародній координації та розвитку власних технологій, а не лише в обмеженнях.

Ці висновки вказують на те, що поточна політика США може мати протилежний до очікуваного ефект, зміцнюючи позиції Китаю на глобальних ринках.

<https://www.csis.org/analysis/double-edged-sword-semiconductor-export-controls>

## Фірми, пов'язані з Великобританією, підозрюються в порушенні санкцій проти Росії

Стаття на BBC описує розслідування британського уряду щодо 37 компаній, які підозрюються в порушенні санкцій щодо російської нафти. Основний акцент робиться на санкції, що обмежують ціну на нафту з Росії до \$60 за барель, щоб стримати прибутки Кремля. Ці компанії, ймовірно, включають морські страхові фірми, які можуть брати участь у транспортуванні російської нафти за цінами, що перевищують встановлену межу. Незважаючи на відкриті розслідування, жодні штрафи наразі не накладені.



Британське казначейство підкреслює складність цих справ, що пояснює затягування процесу. Проте критики, зокрема сер Вільям Браудер, відомий критик Путіна, вважають, що відсутність штрафів є ознакою слабкості уряду в боротьбі з економічними злочинами. За його словами, Великобританія є "однією з найменш жорстких" держав у світі щодо впровадження таких санкцій. Браудер зазначає, що у країні спостерігається як проблема ресурсів, так і культурна проблема, коли справа стосується переслідування економічних злочинців або ухилення від санкцій.

Дані, отримані через закони про свободу інформації, показують, що 52 компанії, пов'язані з Великою Британією, підозрюються в порушенні обмежень, встановлених для російської нафти, з яких 37 розслідувань тривають, а 15 вже завершено. Критики, включаючи Луїса Вілсона з організації Global Witness, називають це «вражаючим» фактом, що жодна компанія досі не отримала штрафу. Вілсон також наголошує на тому, що ці санкції виглядають як «паперовий тигр», неефективний у боротьбі з порушеннями.

Офіс з реалізації фінансових санкцій (OFSI), який проводить ці розслідування, отримав додаткове фінансування у розмірі £50 млн для посилення режиму санкцій у Великій Британії. Проте Луїс Вілсон висловлює занепокоєння щодо того, що компанії можуть отримати документи, які фактично звільняють їх від відповідальності за порушення, навіть якщо вони брали участь у транспортуванні нафти за цінами, вищими за встановлені межі. Вілсон стверджує, що ці документи є "добровільними паперами", які легко отримати.

Також у статті зазначається, що уряди Заходу, включаючи США, можуть бути неохочими до посилення режиму санкцій через побоювання, що це може призвести до зростання світових цін на нафту.

Консервативний міністр закордонних справ Дама Гаррієт Болдвін заявила, що санкції спрямовані на те, щоб "закрити джерела фінансування російської військової машини" і завершити незаконне вторгнення в Україну. Вона наголосила на тому, що в разі виявлення навмисних порушень з боку британських компаній, вони мають бути оштрафовані. Болдвін також зазначила, що є докази того, що російська нафта постачається до Великої Британії через треті країни після її переробки, що дозволяє обійти санкції.

Останнім часом було розпочато парламентське розслідування щодо ефективності санкцій проти Росії, але результати не були опубліковані через розпуск комітетів після оголошення виборів. Також стаття згадує, що OFSI недавно наклав перший штраф у розмірі £15,000 на лондонську компанію за роботу з клієнтом, чії активи були заморожені згідно з російськими санкціями.

Таким чином, у статті висвітлюється складність та суперечливість впровадження санкційного режиму проти Росії, а також виклики, з якими стикається уряд Великої Британії у цій боротьбі.

<https://www.bbc.com/news/articles/c5y97k4w7llo>

# ЗВІТИ ОКРЕМИХ КОМПАНІЙ та ЕКСПЕРТІВ

## Атаки на DAO



Документ під назвою "SoK: Attacks on DAOs" є детальним дослідженням атак на децентралізовані автономні організації (DAO), які використовуються для децентралізованого управління проектами на блокчейні. DAO відіграють ключову роль у багатьох популярних DeFi-протоколах і управляють значними фінансовими активами. У документі описуються чотири основні категорії атак: підкуп, контроль над токенами, атаки на взаємодію людини з комп'ютером та вразливості коду й протоколів. Автори аналізують 28 реальних атак на DAO, а також потенційні атаки, які були виявлені під час аудиту. Основні вектори атак стосуються не тільки технічних вразливостей, а й людських факторів, що значно ускладнює їх виявлення та попередження. Документ також виділяє сім ризиків, яким піддаються DAO, та пропонує стратегії їхнього пом'якшення.

### Ключові висновки:

- Категорії атак на DAO:** Атаки на DAO можна розділити на чотири основні категорії: підкуп учасників голосування, контроль над токенами, вразливості у взаємодії людини з комп'ютером та технічні вразливості в кодї та протоколах. Кожна з цих категорій має свої специфічні механізми впливу, що ускладнює захист DAO від потенційних атак.
- Історичні атаки та потенційні загрози:** Документ детально аналізує 28 реальних інцидентів, що відбулися на чотирьох блокчейнах, і показує, що ці атаки охоплюють всі чотири категорії векторів атак. Крім цього, обговорюються атаки, описані в наукових роботах, та ті, що були виявлені під час аудиту. Більшість виявлених у ході аудиту атак стосуються технічних вразливостей у кодї та протоколах, що свідчить про недостатню увагу до людського фактора.
- Вплив людського фактора:** Окрім технічних вразливостей, багато атак DAO спрямовані на використання слабкостей у процесі управління та голосування, де часто задіяні люди. Такі вразливості важко передбачити та попередити через їхню нетехнічну природу, і це підкреслює необхідність ретельного аудиту не тільки технічних аспектів, а й процедур управління.
- Визначення основних ризиків DAO:** Серед основних ризиків виділяються низька активність учасників голосування, висока ліквідність токенів управління, недостатньо налаштовані контракти для голосування, централізація токенів, а також технічні та комунікаційні проблеми. Менші DAO, через обмежені ресурси, є більш вразливими до цих загроз.
- Стратегії захисту та пом'якшення ризиків:** Документ пропонує низку стратегій для зменшення ризиків атак на DAO, серед яких консервативніші підходи до впровадження функцій DAO, обмеження управлінських прав, наявність можливості екстреного зупинення діяльності DAO, а також застосування механізму форків для уникнення атак.

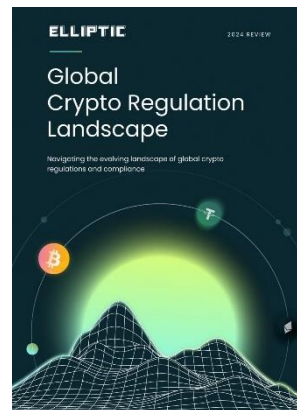
Загалом, цей документ є ключовим дослідженням безпекових викликів DAO і містить практичні рекомендації щодо зміцнення безпеки децентралізованого управління.

[https://liobaheimba.ch/assets/pdf/Papers/SoK\\_Attacks\\_on\\_DAOs.pdf](https://liobaheimba.ch/assets/pdf/Papers/SoK_Attacks_on_DAOs.pdf)

## Еволюція регулювання криптовалют: глобальний огляд та основні виклики

Документ «Global Crypto Regulation Landscape, 2024» пропонує детальний огляд глобальних тенденцій у регулюванні криптовалют та цифрових активів станом на 2024 рік. Він описує нові регуляторні ініціативи в різних регіонах світу, зокрема в ЄС, США, Великобританії, та Азії, що

спрямовані на зміцнення фінансової стабільності, захист споживачів та боротьбу з фінансовими злочинами. Основна увага приділяється **трьома ключовим напрямкам**: введенню в дію регуляції MiCA в ЄС, розширенню дії Travel Rule на криптовалютні транзакції та регулюванню стейблкоїнів. Документ також розглядає **виклики для учасників ринку, пов'язані з дотриманням нових вимог у різних юрисдикціях**, та надає **прогнози щодо розвитку нормативних рамок**.



### **Ключові висновки:**

#### **1. Європейська регуляція MiCA: структура та вплив**

- **MiCA** (Markets in Cryptoassets Regulation) стає однією з найважливіших регуляторних ініціатив у світі.
- **Впровадження з червня 2024 року для стейблкоїнів та повне охоплення криптосервісів до кінця 2024 року** сприятиме уніфікації регулювання в країнах ЄС.
- **«Паспортизація» ліцензій** дозволить криптосервісам надавати послуги по всьому ЄС, що значно спрощує діяльність для операторів.
- **Вплив на глобальний ринок**: принципи MiCA вже стають прикладом для інших регіонів, таких як ОАЕ, Сінгапур і Великобританія.

#### **2. Travel Rule та його глобальний вплив на ПВК/ФТ**

- **Travel Rule** розширює зобов'язання для постачальників віртуальних активів (VASPs) щодо обміну даними про транзакції та контрагентів.
- **ЄС та інші регіони** зобов'язують VASP надавати інформацію про відправників та отримувачів коштів без порогу мінімальної суми, що підвищує прозорість та зменшує можливості для фінансування тероризму та відмивання коштів.
- **Імплементація Travel Rule залишається нерівномірною**: багато юрисдикцій все ще мають прогалини у впровадженні цього стандарту FATF, що створює ризики для глобальної фінансової системи.

#### **3. Регулювання стейблкоїнів як пріоритет**

- **ЄС, Гонконг, Сінгапур та ОАЕ** встановлюють вимоги для забезпечення стейблкоїнів резервами, щоб захистити споживачів та уникнути системних ризиків.
- **Резерви та права викупу**: стейблкоїн-емітенти повинні мати прозорі механізми підтримки своїх токенів, щоб уникнути ризиків ліквідності.
- **Відсутність регулювання у США** створює невизначеність для емітентів стейблкоїнів і може обмежити розвиток ринку.

#### **4. Політична та регуляторна невизначеність у США**

- **Посилення контролю з боку SEC та CFTC**: регулятори активно застосовують санкції, особливо до DeFi-проектів.
- **Відсутність єдиного федерального регуляторного підходу** спричиняє правову невизначеність для криптовалютних компаній.
- **Політичні події** (як-от президентські вибори) впливають на формування законодавчих актів, зокрема через лобювання інтересів індустрії криптовалют.

#### **5. Недостатнє впровадження стандартів ПВК/ФТ за версією FATF**

- **75% юрисдикцій** не повністю виконують вимоги FATF щодо віртуальних активів. Основні прогалини пов'язані з **оцінкою ризиків, інспекціями VASP та реалізацією Travel Rule**.
- **Важливість міжнародної координації**: FATF підкреслює необхідність посилення нагляду та контролю за сектором криптовалют.

#### **6. Розвиток нових регуляторних центрів та криптохабів**

- **ОАЕ, Великобританія та Франція** прагнуть стати провідними хабами для криптовалют, пропонуючи сприятливі умови для бізнесу при дотриманні високих стандартів ПБК/ФТ.
- **Успішне впровадження МіСА у Франції** та видача першої ліцензії для стейблкоїн-емітента USDC підтверджують амбіції країни у цій сфері.
- **ОАЕ продовжує розвиток своєї CBDC-стратегії**, що дозволяє інтегрувати цифрові валюти в міжнародну фінансову систему.

## 7. Тенденції розвитку крипторегулювання в інших регіонах

- **Бразилія та Болівія** активізують законодавчі ініціативи у сфері криптовалют, що підкреслює зростаючий інтерес до нових фінансових технологій у Латинській Америці.
- **Гонконг** формує нову нормативну базу для ліцензування платформ обміну та стейблкоїнів, позиціонуючись як регіональний криптохаб в Азії.

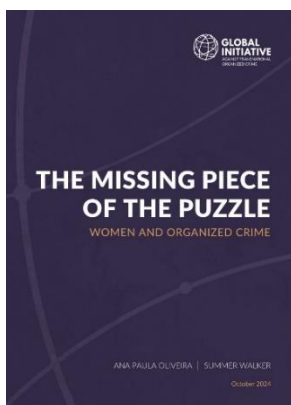
## 8. Взаємозв'язок політичних та економічних факторів з регулюванням криптовалют

- **Вибори та зміна урядів** можуть впливати на затримки або перегляд регуляторних ініціатив (як у випадку з Великобританією).
- **Посилення боротьби з кіберзлочинністю та санкційними ризиками:** санкції на криптогаманці, пов'язані з тероризмом та ухиленням від санкцій, свідчать про зростання значущості криптовалют у сфері міжнародної безпеки.

Ці висновки підкреслюють **глобальний тренд до посилення регулювання криптовалют** з метою забезпечення фінансової стабільності, протидії відмиванню коштів та підтримки інновацій у цифровій економіці.

<https://www.elliptic.co/resources/global-crypto-regulation-landscape-2024>

## Жінки та організована злочинність: Від пасивних ролей до активного спротиву



Документ «The Missing Piece of the Puzzle: Women and Organized Crime» досліджує роль жінок у **транснаціональній організованій злочинності**, зосереджуючись на **трьох ключових аспектах**: участь жінок у злочинних угрупованнях, вплив злочинності на них та їхню роль у боротьбі з цими явищами. Автори наголошують на важливості **гендерно-чутливого підходу** до розробки політик у сфері боротьби з організованою злочинністю та **описують бар'єри**, з якими стикаються жінки в різних контекстах — як у злочинних мережах, так і в системах правосуддя та реагування. Документ акцентує увагу на **складній динаміці між експлуатацією та участю жінок у злочинах**, а також на **необхідності залучення жінок до формування політик для підвищення ефективності боротьби з організованою злочинністю**.

### Ключові висновки:

#### 1. Жінки як учасниці організованої злочинності

- **Роль жінок у злочинних угрупованнях часто недооцінюється** через стереотипи, що обмежують їх до ролей жертв або допоміжних фігур. Насправді жінки можуть займати різні позиції — від виконавців до лідерів злочинних мереж.
- **Жінки часто залучені через соціальні та економічні обставини**, зокрема бідність, соціальну маргіналізацію та вплив кримінальних середовищ.
- **Стереотипи у правоохоронній системі** ускладнюють виявлення участі жінок у злочинних схемах. Внаслідок цього вони можуть отримувати або надмірно жорсткі покарання, або навпаки залишатися непоміченими, що знижує ефективність боротьби з організованою злочинністю.

- **Частина жінок потрапляє у злочинність примусово:** наприклад, вони використовуються як кур'єри наркотиків, бо менш підозрілі для правоохоронців, або як вербувальниці для торгівлі людьми, де їм вдається легше завоювати довіру жертв.

## 2. Вплив організованої злочинності на жінок

- **Гендерно-обумовлене насильство** поширене серед жінок, пов'язаних з організованими злочинними групами. Це включає фізичне, сексуальне та психологічне насильство, а також експлуатацію в умовах домашнього насильства та сексуальної торгівлі.
- **Жінки стають жертвами тиску та експлуатації через дискримінацію** у сферах зайнятості та освіти, що робить їх вразливими до торгівлі людьми та інших форм злочинної експлуатації.
- **Злочинні ринки, де домінують чоловіки,** поглиблюють нерівність, сприяючи маргіналізації жінок і обмежуючи їхні економічні можливості. У результаті, вони часто змушені працювати в низькооплачуваних або неофіційних секторах, таких як хатня робота або секс-робота.
- **Патріархальні норми та обмежений доступ до ресурсів** посилюють вплив злочинності на жінок, що призводить до ще більшої соціальної вразливості та втрати економічної незалежності.

## 3. Жінки як агенти протидії організованій злочинності

- **Жінки відіграють ключову роль у зміцненні стійкості громад.** Вони часто є рушійною силою локальних ініціатив із запобігання злочинності, хоча їхній внесок залишається малопомітним та недооціненим.
- **Жінки можуть вносити унікальні перспективи** у формування політики й реагування на злочинність завдяки своїм знанням та досвіду, що часто ігноруються у традиційних структурах безпеки.
- **Недостатня представленість жінок у правоохоронних структурах** та у процесах прийняття рішень знижує ефективність боротьби з організованою злочинністю, адже політика формується без врахування гендерних аспектів.
- **Жіночі організації та громадські ініціативи відіграють ключову роль** у підтримці жертв та сприяттві реінтеграції колишніх правопорушників, проте вони стикаються з фінансовими та інституційними обмеженнями.

## 4. Важливість гендерно-чутливого підходу в політиці протидії злочинності

- **Відсутність даних із розподілом за гендером** про роль жінок у злочинності ускладнює формування адекватної політики та сприяє поширенню стереотипів. Необхідне навчання правоохоронців та судових органів гендерній чутливості.
- **Гендерно-орієнтовані програми мають враховувати конкретні потреби жінок.** Це включає реабілітаційні програми для жінок, що постраждали від злочинів, а також заходи для запобігання повторного залучення їх у злочинність.
- **Гендерні питання потребують більшої уваги в міжнародних дискусіях,** таких як Конференція сторін Конвенції ООН проти транснаціональної організованої злочинності. Це сприятиме не лише боротьбі з організованою злочинністю, а й зменшенню гендерної нерівності.
- **Посилення участі жінок у процесах прийняття рішень та їх економічна підтримка** допоможе створити більш ефективні механізми протидії злочинності. Це включає виділення фінансування для жіночих організацій та створення безпечного середовища для їхньої діяльності.

## 5. Ризики та бар'єри для жінок у боротьбі з організованою злочинністю

- **Дискримінація та домагання в правоохоронних органах** обмежують можливості кар'єрного росту жінок і знижують їхню участь у боротьбі зі злочинністю.



- **Фінансові обмеження та гендерна дискримінація** впливають на роботу жіночих ініціатив, особливо у громадах, які найбільше потерпають від організованої злочинності.
- **Запровадження антизлочинних політик без урахування гендерних аспектів** може мати негативні наслідки для жінок, сприяючи масовим арештам, поліцейському насильству та зниженню доступу до соціальних послуг.

## 6. Рекомендації для політиків та міжнародної спільноти

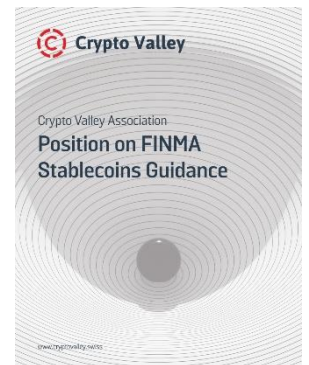
- **Потрібно розвивати гендерно-чутливу політику** в боротьбі з організованою злочинністю, яка враховує роль жінок як у злочинних групах, так і в заходах протидії.
- **Необхідно сприяти більшій участі жінок** у процесах прийняття рішень, забезпечуючи їхній доступ до ресурсів та можливостей для впливу на політику.
- **Міжнародні організації повинні підтримувати жіночі ініціативи** та забезпечувати їх інтеграцію в національні та глобальні стратегії боротьби зі злочинністю.
- **Забезпечення гендерної рівності в правоохоронних структурах** сприятиме більш ефективній боротьбі зі злочинністю та покращить якість правосуддя.

Ці висновки підкреслюють необхідність всебічного гендерного підходу до боротьби з транснаціональною організованою злочинністю, що сприятиме як безпеці, так і соціальній рівності.

<http://surl.li/lpfofq>

## Позиція Crypto Valley Association щодо керівництва FINMA про стейблкоїни

Документ є **звітом** Асоціації Crypto Valley у відповідь на публікацію FINMA, яка встановлює нові вимоги до емітентів стейблкоїнів та банків, що надають гарантії. Ці вимоги викликали занепокоєння у криптоспільноті, адже вони суттєво **ускладнюють діяльність централізованих емітентів стейблкоїнів у Швейцарії**. Асоціація розкритикувала FINMA за відсутність консультацій з галуззю та невідповідність підходу міжнародним стандартам, що може підірвати конкурентоздатність Швейцарії як лідера криптовалютного ринку.



### Ключові висновки:

#### 1. Посилення вимог до ідентифікації користувачів

FINMA зобов'язує **ідентифікувати всіх власників стейблкоїнів**, включаючи тих, хто отримує токени через вторинні транзакції. Це означає необхідність контролю не лише на етапі первинної емісії, але й під час будь-якого подальшого переказу токенів між користувачами. Вимоги виходять за рамки стандартів FATF та практик інших ключових юрисдикцій, таких як **ЄС, США, Сінгапур, Гонконг та Японія**, що створює **надмірні регуляторні обмеження** для ринку стейблкоїнів у Швейцарії.

#### 2. Надмірна централізація та технологічні обмеження

FINMA вимагає використання **контрактних та технологічних інструментів для обмеження можливості переказів стейблкоїнів**. Це фактично змушує емітентів створювати централізовану платформу для обліку всіх гаманців користувачів, що **суперечить природі децентралізованих блокчейнів**. Такий підхід підриває **основний принцип розподілених реєстрів**, де транзакції повинні здійснюватися без централізованого контролю. **Технічно це нереально** для стейблкоїнів, випущених на публічних блокчейнах.

#### 3. Розширення регуляторних інтерпретацій

У своїй комунікації FINMA **розширює трактування поняття «тривалих ділових відносин»** (ст. 4 п. 1 б Антилегалізаційної постанови) таким чином, що будь-який емітент стейблкоїнів автоматично

стає фінансовим посередником. Це **перевищує звичайні регуляторні норми** та вимагає **додаткових гарантій від банків** на покриття ризиків при конвертації стейблкоїнів у фіатну валюту. Така інтерпретація **не відповідає принципам регуляторного підходу FINMA**, що потребувала б або випуску циркуляра, або **зміни нормативно-правових актів** для обґрунтування цих нових вимог.

#### 4. Ризик підриву ринкової конкурентоздатності

Через нові регуляторні обмеження **централізованим емітентам стейблкоїнів стане складніше працювати у Швейцарії**. Це може призвести до **відтоку бізнесу** та проектів у інші юрисдикції з менш суворими вимогами. Натомість **децентралізовані стейблкоїни залишаються поза сферою впливу** цієї регуляції, що створює **нерівні умови на ринку** для різних видів стейблкоїнів.

#### 5. Інноваційні перешкоди та ризик втрати лідерства Швейцарії

Впровадження регуляторних нововведень без попередніх консультацій з учасниками ринку, включаючи Crypto Valley Association, **підриває принципи прозорості та співпраці** (передбачені ст. 7 Закону про FINMA). **Відсутність діалогу** з індустрією може **послабити позиції Швейцарії як глобального лідера у криптосекторі** та інноваціях, оскільки жорсткі вимоги ускладнюють запуск нових проектів та продуктів.

#### 6. Неприйнятність централізації для публічних блокчейнів

Зобов'язання емітентів **створювати централізовану базу даних для управління транзакціями** суперечить фундаментальним принципам технології блокчейну, **де операції здійснюються на основі peer-to-peer мереж без централізованого контролю**. Це може поставити під сумнів технічну реалізованість використання стейблкоїнів на таких блокчейнах та змусить емітентів шукати інші рішення або юрисдикції.

#### 7. Обмежена сфера застосування нових правил

Вимоги FINMA застосовуються лише до **тих стейблкоїнів, що містять зобов'язання емітента конвертувати токени у фіат**. Це суттєво звужує охоплення законодавства, але водночас створює **додаткові перешкоди для централізованих проєктів**.

#### 8. Висновок та рекомендація Crypto Valley Association

Crypto Valley Association висловлює жаль з приводу **відсутності консультацій з галуззю** перед запровадженням нових вимог та закликає до **більш зваженого підходу** у регулюванні, який враховує технологічні реалії та відповідає міжнародним стандартам. Асоціація наголошує на необхідності **сприяти інноваціям та підтримувати конкурентоздатність** Швейцарії як криптосфери.

<https://members.cryptovalley.swiss/news/2192539>

## Безпрецедентне зростання нерегулярної міграції через Туніс: Причини, наслідки та нові виклики

Дослідження "Tunisia: Irregular migration reaches unprecedented levels" аналізує зростання нерегулярної міграції з Тунісу в 2023 році, акцентуючи увагу на ролі Тунісу як основного пункту відправлення для мігрантів, які прямують до Європи.

Цей звіт надає детальний огляд нелегальної міграції, мереж контрабанди людей, впливу внутрішньої політики Тунісу та кризи мігрантів, що спровокувала збільшення кількості незаконного перетину кордону. Крім того, дослідження підкреслює посилення міграційних потоків через Туніс



з сусідніх країн, таких як Алжир і Лівія, на фоні загострення політичних, економічних та соціальних проблем у самій країні.

### Ключові моменти

#### Зростання нерегулярної міграції:

- У 2023 році Туніс обігнав Лівію як основний пункт відправлення мігрантів, які намагаються дістатися Італії. Близько 97 306 мігрантів прибули до Італії з Тунісу за рік, що втричі більше, ніж у 2022 році.
- Основну частину зростання забезпечили іноземні мігранти, переважно з країн Західної Африки та Судану, що стали довгостроковими резидентами Тунісу або прибули з сусідніх країн, таких як Алжир та Лівія.

#### Зміни в мережах контрабанди:

- Спостерігалось ускладнення екосистеми контрабанди людей. Збільшилася кількість незалежних мігрантів, які самостійно організовували перетини кордону без участі контрабандистів, що називається "самостійною контрабандою".
- Поряд із традиційними мережами контрабандистів, що оперують вздовж узбережжя, почали з'являтися мережі, які використовують дешеві човни для перевезень мігрантів, що підвищує ризики для їх життя.

#### Політична та соціальна криза у Тунісі:

- Внутрішні кризи в країні, такі як економічна депресія, безробіття та нестача ресурсів, стимулювали збільшення бажання мігрантів залишити країну.
- Уряд Тунісу посилив контроль на кордонах та здійснив масові примусові переміщення мігрантів на кордон з Лівією та Алжиром. Ці дії супроводжувалися численними випадками насильства з боку правоохоронців.

#### Різка посилення політики щодо мігрантів:

- У лютому 2023 року президент Тунісу зробив різкі заяви проти мігрантів із Субсахарської Африки, що спричинило масові арешти, виселення та звільнення мігрантів з роботи, погіршуючи умови їх перебування.
- Влада також почала частіше застосовувати примусове виселення мігрантів, у тому числі шляхом використання насильства. Це призвело до суттєвого зростання кількості мігрантів, які намагалися втекти з країни.

#### Зростання міграційних потоків з Алжиру та Лівії:

- Відбувся значний приріст мігрантів, які прибували до Тунісу через сухопутні кордони з Алжиром і Лівією. Особливо різке зростання потоку спостерігалось з квітня 2023 року через конфлікт у Судані та важкі умови життя в Лівії.

### Висновки

Дослідження підкреслює, що Туніс у 2023 році зіткнувся з безпрецедентним зростанням нелегальної міграції, що вказує на подальший погіршення внутрішньої політичної та економічної ситуації в країні. Незважаючи на посилення контролю на кордонах, міграційні потоки продовжують збільшуватися, а контрабанда людей набуває нових форм. Політичні рішення Тунісу, зокрема посилення репресій щодо мігрантів, лише ускладнюють ситуацію і сприяють подальшому зростанню потоків міграції в Європу через Туніс.

<http://surl.li/ifzbpv>

# РЕКОМЕНДОВАНІ МАТЕРІАЛИ

## Баррі Сіл: Король контрабанди



Захоплюючий фільм, який, окрім історії про шпигунство та торгівлю наркотиками, торкається тем, дуже актуальних для тих, хто працює у сфері комплаєнсу та відмивання коштів.

Фільм заснований на реальних подіях і розповідає історію Баррі Сіла, пілота, який у 1980-х роках виявляється залученим у складну мережу незаконних угод і таємних операцій, працюючи як на ЦРУ, так і на Медельїнський картель. У ньому показано, як Сіл обробляє величезні суми брудних грошей, використовуючи класичні методи відмивання коштів, які залишаються актуальними й сьогодні, наприклад купівля предметів розкоші та використання офшорних рахунків.

Для тих, хто залучений до сфериПВК, фільм пропонує інтригуючі роздуми про складність управління незаконними коштами і про те, як відмивання коштів тісно пов'язане з геополітичними проблемами, міжнародною торгівлею людьми та таємними операціями.

Прекрасний приклад того, як кіно може пролити світло на виклики, з якими ми щодня стикаємося в нашій професії.

<https://www.netflix.com/tn-en/title/80121192>

## Новий епізод подкасту від RUSI: "Еволюція сучасного відмивання коштів"

У цьому епізоді Том Кітінг, директор Центру фінансів та безпеки при RUSI, разом із журналістом розслідувачем Джеффом Вайтом обговорюють найгостріші виклики сучасної кіберзлочинності та відмивання коштів. Ключові теми — це використання криптовалют у незаконних схемах, зломи, організовані Північною Кореєю, а також співпраця злочинців через кілька юрисдикцій, що ускладнює роботу правоохоронних органів.



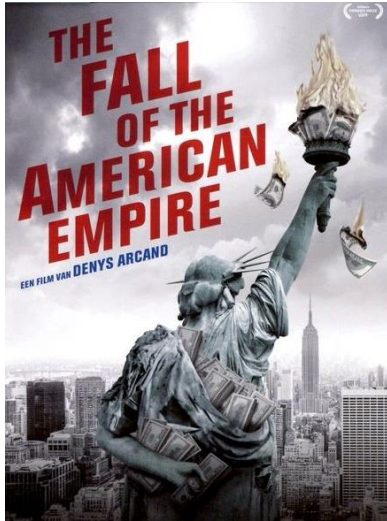
🚧 В епізоді розглядаються такі важливі питання, як рекрутинг "мулів" для відмивання коштів, еволюція ринку тіншових інтернет-майданчиків, таких як Silk Road та Hydra, та як кіберзлочинці змінюють стратегії, щоб залишатися непомітними для закону.

💡 **Чому це важливо?** Випуск актуальний для тих, хто цікавиться кібербезпекою, боротьбою з фінансовими злочинами та роллю криптовалют у сучасній економіці. Темі кіберзлочинності, відмивання коштів та транснаціональних злочинних схем, як показує кейс "Evil Corp", мають дедалі більший вплив на світову безпеку. Тому розуміння цих процесів та інструментів, які використовуються злочинцями, є ключем до ефективної боротьби з фінансовими злочинами.

<http://surl.li/hsoatd>

## Падіння Американської імперії

Фільм, який, хоч і не заснований на реальних подіях, пропонує багато роздумів про ключові проблеми, з якими ми стикаємося в нашій сфері: відмивання коштів і корупція у фінансовій системі.



Історія розповідає про П'єра-Поля, молодого інтелектуала, який випадково заволодів двома речовими сумками, наповненими готівкою, після невдалого пограбування. Незважаючи на те, що гроші походять із злочинного джерела, їх не можна використовувати без попереднього «очищення». Щоб не бути спійманим, П'єр-Поль об'єднується з колишнім ув'язненим, який має фінансовий досвід, щоб розробити схему відмивання. У фільмі демонструється використання офшорних рахунків, компаній-оболонок та інших механізмів, які зазвичай використовуються для «очищення» незаконних грошей.

Фільм підкреслює важливу роль, яку відіграють банки та фінансові консультанти у сприянні потоку незаконного капіталу, піднімаючи етичні проблеми, які є основою нашої щоденної роботи.

За допомогою захоплюючої розповіді він критикує співучасть певних учасників фінансової системи та економічну нерівність, що виникає в результаті.

Це чудовий варіант перегляду для роздумів над проблемами реального світу, з якими ми стикаємось у процесі боротьби з відмиванням коштів та забезпечення доброчесності фінансового сектору.

<https://megogo.net/ua/view/3959681-padinnya-amerikansko-imperi.html>

# ІНШІ НОВИНИ

## Побудова спільного бачення фінансів і безпеки між Британією та Європою



Стаття обговорює критичну необхідність поглиблення співпраці між Великою Британією та ЄС у питаннях фінансової безпеки після Brexit, оскільки обидві сторони зіштовхуються з новими глобальними викликами, такими як економічний вплив Китаю, агресія Росії та загрози з боку південних країн. Основна увага приділяється координації зусиль у протидії відмиванню коштів, фінансуванню тероризму, санкціям і боротьбі з дезінформацією. Співпраця залишається важливою для захисту міжнародної фінансової системи від ризиків і підтримки

стабільності. Особливо підкреслюється, що можливе повернення Дональда Трампа до влади може ускладнити цю співпрацю, враховуючи його політику, що раніше спонукала до ізоляціонізму та зменшення участі в міжнародних питаннях. Це, у свою чергу, створює ризики для ефективності фінансових санкцій і глобальної безпеки.

Крім цього, йдеться про те, що без тісної координації Великої Британії та ЄС у сфері фінансової розвідки та розслідування фінансових злочинів, існує ймовірність зростання злочинної активності, особливо в умовах складної політичної та економічної ситуації. Тому відновлення чи розширення альянсів, зокрема у фінансовій сфері, є ключовим кроком у протидії спільним загрозам.

<http://surl.li/ogjdub>

## Ілюзія кохання: Як міжнародні шахраї виманюють мільйони у американців через інтернет-схеми

Стаття "Inside the 'hustle kingdom, where overseas scammers prey on Americans online" від CBS News розповідає про масштабну проблему шахрайства з інтернет-романами, яка особливо поширена серед шахраїв із Західної Африки, зокрема з Гани.



Ця стаття розкриває функціонування шахрайських схем, в яких африканські шахраї ("Yahoo boys") використовують соціальні мережі та онлайн-платформи для знайомств, щоб обманювати американських громадян, найчастіше літніх людей, маніпулюючи їхніми емоціями і виманюючи великі суми грошей.

### Ключові моменти

- **Масштаб проблеми:** Стаття наголошує на тому, що в 2023 році американці втратили понад 10 мільярдів доларів через різні види шахрайства, що на 14% більше, ніж у 2022 році. Ці втрати не лише фінансові, але й емоційні для багатьох жертв, особливо для літніх людей.
- **Організація шахрайських схем:**

Шахраї працюють в "підпільних кімнатах" у Гані, де за допомогою соціальних мереж, таких як Instagram та платформи для знайомств, вони видають себе за білих американських жінок. Вони "будують відносини" з чоловіками, після чого виманюють у них гроші.

Для створення довіри використовують як підроблені профілі, так і голосові дзвінки або відеодзвінки, для яких наймають жінок, щоб обман виглядав переконливіше.

- **Наслідки для жертв:**

Жертви, такі як 92-річна американка Рут, втратили сотні тисяч доларів. У її випадку, шахраї переконали її купити золоті злитки і передати їх кур'єрам. Лише після того, як її банківські рахунки були повністю спустошені, вона зрозуміла, що стала жертвою шахрайства.

- **Роль банків та регулюючих органів:**

Більшість банків опинилися під тиском через нездатність ефективно протистояти такому шахрайству. Хоча банки часто підозрюють шахрайські операції, вони змушені дотримуватися побажань клієнтів. Це створює правову та етичну дилему: чи можуть банки запобігати транзакціям, якщо клієнт наполягає на їх виконанні.

У статті також наведені судові позови проти великих банків, таких як Schwab і Citibank, через їхню нездатність запобігти значним втратам для клієнтів. Наприклад, сім'я Рут подала позов проти Schwab, стверджуючи, що банк міг зробити більше, щоб захистити її заощадження.

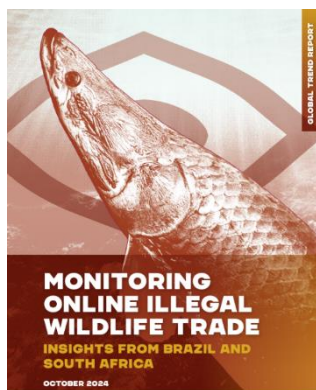
- **Позиція шахраїв:** Деякі шахраї, які брали участь у розслідуванні CBS, пояснюють свою діяльність складними умовами життя в Гані. Вони зазначають, що шахрайство стало їхнім єдиним способом виживання, зважаючи на бідність та відсутність перспектив для молодих освічених людей.
- **Вплив на фінансові системи:** Гана є однією з основних країн, куди направляються великі міжнародні грошові перекази, які за останнє десятиліття зросли на 140%. Однак частина цих коштів пов'язана зі злочинними схемами, що збагачують шахраїв.

## Висновки

- **Загроза для громадян:** Шахрайство з інтернет-романами стало великою загрозою для американських громадян, особливо літніх людей, які легко піддаються емоційній маніпуляції.
- **Необхідність регулювання:** Існує нагальна потреба у вдосконаленні системи регулювання банківських операцій для захисту клієнтів від шахрайства. Банки повинні знайти баланс між захистом інтересів клієнтів і дотриманням законодавчих норм.
- **Роль урядів:** Влада має забезпечити кращу координацію між банками, урядовими установами та правоохоронними органами, щоб ефективно боротися з міжнародними схемами шахрайства.
- **Соціально-економічні проблеми:** Для таких країн, як Гана, де шахрайство стало частиною економіки для багатьох молодих людей, необхідно створювати нові економічні можливості, щоб запобігти зростанню злочинності серед населення.

<http://surl.li/echdnl>

## Моніторинг незаконної торгівлі дикими тваринами через інтернет: Аналіз ринків Бразилії та Південної Африки



Дослідження "Monitoring Online Illegal Wildlife Trade" за жовтень 2024 року від Global Initiative Against Transnational Organized Crime аналізує незаконну торгівлю дикими тваринами в Бразилії та Південній Африці через інтернет-платформи.

Дослідження охоплює період з травня по липень 2024 року і спрямоване на виявлення основних тенденцій незаконної торгівлі захищеними видами тварин, а також розкриває нові механізми моніторингу цієї діяльності через інтернет. Основна увага приділяється двом видам нелегальної торгівлі: пірауку (в Бразилії) та використанню частин тварин для традиційної медицини в Південній Африці.

- **Глобальна система моніторингу:** Дослідження впроваджує Глобальну систему моніторингу (GMS), яка використовує національні хаби даних для збору інформації про оголошення незаконної торгівлі тваринами через інтернет. Хаби знаходяться в країнах, де цей ринок є найбільш значущим. Дослідження надає глибокий аналіз оголошень, виявлених у Бразилії та Південній Африці.
- **Піратський ринок у Бразилії:** Піраруку — велика прісноводна риба, яка піддається значному незаконному вилову через високий попит на її м'ясо і продукти. Ринок піраруку розглядається через призму його тісних зв'язків із торгівлею наркотиками. Дослідження розкриває зв'язок між незаконною торгівлею піраруку та контрабандою кокаїну.
- **Традиційна медицина в Південній Африці:** В Південній Африці зростає незаконна торгівля частинами тварин для традиційної медицини. Дослідження виявляє 61 оголошення, пов'язане з продажем частин тварин, таких як шкіра тигра, шкура леопарда та інші, через Facebook.
- **Тенденції ринку незаконної торгівлі тваринами через інтернет:**
  - **Соціальні медіа є головною платформою для торгівлі захищеними видами тварин:** 78% оголошень про продаж тварин розміщено на таких платформах, як Facebook.
  - **Ринкові концентрації:** Хоча ринки здаються роздробленими, є окремі види (піраруку, африканський сірий папуга), на яких домінують декілька продавців.
  - **Концентрація продавців:** Більшість оголошень опубліковані невеликою кількістю продавців, часто з фальшивими профілями, що дозволяє їм обходити регулювання.
- **Незаконна торгівля тваринами та насильство:** Торгівля піраруку та іншими дикими тваринами пов'язана з насильством у Бразилії, що підтверджується випадками вбивств активістів, які боролися проти цієї практики.

## Висновки

- **Посилення правозастосування:** Для боротьби з незаконною торгівлею тваринами через інтернет необхідно посилити правозастосування та співпрацювати з національними хабами моніторингу для отримання актуальних розвідданих.
- **Соціальні медіа як основна платформа:** Зростання використання соціальних медіа для незаконної торгівлі дикими тваринами вимагає пріоритетної уваги з боку правоохоронців та регуляторів.
- **Підтримка традиційних спільнот:** У Південній Африці необхідно інтегрувати традиційних цілителів у заходи з охорони дикої природи, пропонуючи заміники тваринних частин у культурних практиках.
- **Зв'язок з торгівлею наркотиками:** Взаємозв'язок між торгівлею тваринами та контрабандою наркотиків у Бразилії вимагає комплексного підходу до розслідувань та боротьби з організованою злочинністю.

Це дослідження демонструє складність і масштаб проблеми незаконної торгівлі дикими тваринами, підкреслюючи важливість скоординованих заходів для боротьби з цією глобальною загрозою.

<http://surl.li/rkznhf>

## Глобальний бум шахрайства в електронній комерції: виклики, ризики та нові загрози

Дослідження, представлене International Coalition Against Illicit Economies (ICAIE) і опубліковане на платформі OCCRP, висвітлює глобальне зростання шахрайства у сфері електронної комерції (e-commerce). Воно показує, що шахрайство має місце приблизно в 20% світових онлайн-продажів щороку, що приносить злочинцям трильйони доларів прибутку.





У звіті наголошується, що контрафактні товари складають \$4,5 трлн із загальних \$20 трлн, які були згенеровані від електронної комерції в 2023 році. Це робить онлайн-торгівлю контрафактними товарами більш прибутковою, ніж наркотрафік чи торгівля людьми, які мають суворіші покарання.

### Ключові моменти:

- **Масштаб шахрайства:** Шахрайство в електронній комерції охоплює близько 20% світових онлайн-продажів, що еквівалентно трильйонам доларів щороку. Зокрема, піратські та контрафактні товари складають значну частку цього ринку.
- **Контрафактні товари:** Згідно з ICAIE, продаж підробок в інтернеті приносить більше доходів, ніж такі серйозні злочини, як торгівля наркотиками чи людьми. Це обумовлено тим, що для таких злочинів передбачені суворіші покарання, а продаж контрафактів є менш ризикованим і більш привабливим для злочинців.
- **Технологічні чинники:** Розвиток мобільних технологій сприяє зростанню шахрайства. Зростання використання смартфонів, доступ до глобальної фінансової системи та мобільні додатки (як-от WeChat і криптовалютні гаманці) полегшують процес відмивання грошей і обхід банківських систем. Також злочинці використовують програми для конвертації валют, які можуть допомогти приховати джерела коштів.
- **Криптовалюти:** З розвитком криптовалют, які з'явилися за останні 15 років, їх почали широко використовувати у злочинній діяльності, зокрема в електронній комерції. Зростання числа криптовалют, таких як Bitcoin, спрощує обхід фінансових регуляцій і дозволяє анонімізувати транзакції.
- **Законодавчі ініціативи:** Звіт наголошує на важливості законодавчих змін, які намагаються впоратися з цією проблемою. У США було запропоновано кілька законопроектів, таких як SHOP SAFE Act, який вимагає від онлайн-продавців перевірки автентичності своїх товарів, та Combating Cross-Border Financial Crime Act 2023, що передбачає посилення боротьби з транскордонними фінансовими злочинами, включаючи відмивання грошей.

### Висновки

Звіт підкреслює, що глобальна цифрова економіка і, зокрема, сфера електронної комерції, стають дедалі більшою ареною для шахрайства та відмивання коштів. Злочинці адаптуються до нових технологій, таких як мобільні додатки, криптовалюти і цифрові платіжні платформи, щоб уникнути виявлення. Одночасно регуляторні органи намагаються наздогнати ці зміни, але без швидких законодавчих кроків і посилення контролю за електронною комерцією, ця сфера залишатиметься привабливим інструментом для незаконної діяльності.

<http://surl.li/wumwxp>

# ДЛЯ ЗАГАЛЬНОГО РОЗВИТКУ

## Міфи про криптоплатежі



Інфографіка розглядає основні міфи, пов'язані з криптовалютами, та надає дані, що спростовують ці міфи на основі актуальних досліджень. Вона покликана розвіяти хибні уявлення щодо використання криптовалют у повсякденних транзакціях.

Перший міф стверджує, що криптовалюти переважно використовуються для незаконної діяльності, наприклад, для відмивання коштів. Проте, статистика від Chainalysis показує, що частка незаконних транзакцій з криптовалютами значно нижча, ніж зазвичай вважається — у 2023 році цей показник склав лише 0,34% від загального обсягу транзакцій.

Другий міф полягає в тому, що криптовалютні транзакції займають багато часу та є ненадійними. У відповідь на це документ стверджує, що більшість транзакцій у біткоїнах та ефірі проводяться менш ніж за 10 хвилин, а використання рішень другого рівня ще більше прискорює процес.

Третій міф стосується волатильності криптовалют, що робить їх непридатними для щоденних транзакцій. Однак, стейблкоїни (stablecoins), такі як USDC, прив'язані до долара США і мінімізують ризики волатильності, забезпечуючи надійність у повсякденних платежах.

Четвертий міф заявляє, що криптовалютні транзакції небезпечні, і шахрайство є поширеним явищем. Насправді, блокчейн забезпечує високу безпеку транзакцій, оскільки вони зашифровані та майже неможливі для зміни після верифікації.

П'ятий міф полягає в тому, що криптовалютні платежі не широко прийняті серед торговців. Документ наводить приклади того, як понад 15,000 підприємств у всьому світі вже приймають біткоїни, а кількість крипто-дружніх торгових точок постійно зростає.

Таким чином, документ показує, що криптовалютні платежі безпечні, швидкі та все більше приймаються у глобальному масштабі, спростовуючи популярні міфи та надаючи інформацію для більш об'єктивного погляду на криптовалютні транзакції.

<http://surl.li/dwgvub>

## Сірий список

«Сірий список» — це юрисдикції, які перебувають під посиленним моніторингом Групи розробки фінансових заходів протидії відмиванню грошей (FATF) через стратегічні недоліки в їхніх системах з протидії відмиванню коштів та фінансуванню тероризму.

Країни потрапляють до цього списку, якщо вони мають недоліки у своїх системах ПВК/ФТ, але вони не настільки серйозні, як у тих, кого внесено до чорного списку, що викликає найвищий рівень занепокоєння. Ці юрисдикції повинні здійснити певні дії, щоб їх вилучили з сірого списку.



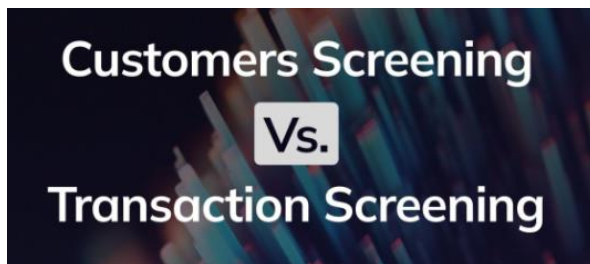
Ці країни активно співпрацюють із FATF, щоб усунути ці недоліки, але все ще підлягають посиленому контролю, поки вони повністю не виконають рекомендації FATF.

Перебування в «сірому списку» може призвести до посилення труднощів для цих країн у доступі до глобальної фінансової системи та може призвести до підвищення вимог до належної обачності з боку фінансових установ.

Список регулярно оновлюється FATF на основі прогресу кожної країни у зміцненні системи ПВК/ФТ.

<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

## Який підхід до реалізації програми з ПВК є найкращим: перевірка ризиків клієнта чи моніторинг транзакцій?



Для початку необхідно зазначити, що обидва підходи важливі, але в деяких випадках один підхід може мати перевагу над іншим.

Перевірка клієнтів під час започаткування ділових відносин є основою заходів з ПВК для фінансових установ та інших секторів, які регулюються нормами ПВК/ФТ. Це необхідно для оцінки

ризиків відповідно до ризик-орієнтованого підходу. Перевірка на предмет статусу PEP, підсанкційних установ, несприятливих згадок у медіа та включення до списків терористів дає початкове розуміння потенційних ризиків, пов'язаних із клієнтами.

Ця початкова оцінка ризиків допомагає установам ефективно розподіляти ресурси для подальшої належної перевірки конкретних клієнтів або навіть для зниження ризиків у випадках, коли фінансові установи мають низьку схильність до ризику.

З іншого боку, моніторинг транзакцій насамперед виявляє незвичайні моделі транзакцій, наприклад ті, що перевищують певні порогові значення або залучають осіб із високим ризиком, як-от ті, що підпадають під експортний контроль.

Чи існує ситуація, коли постачальники фінансових послуг можуть надавати пріоритет перевірці ризиків клієнта під час реєстрації над моніторингом операцій?

З точки зору комплаєнсу з ПВК/ФТ і ризик-орієнтованого підходу, перевірка ризиків клієнта під час започаткування ділових відносин повинна не тільки мати пріоритет, але й вважатися життєво важливою.

Наприклад, РЕГЛАМЕНТ (ЄС) 2024/886 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ ТА РАДИ від 13 березня 2024 року містить конкретні вказівки, щоб постачальники платіжних послуг віддавали пріоритет перевірці під час започаткування відносин із клієнтами:

«Через природу миттєвих кредитних переказів провайдери (PSP) не можуть перевірити протягом необхідного короткого терміну ці позначені транзакції, і, як наслідок, вони відхиляються... Щоб забезпечити більшу юридичну визначеність, підвищити ефективність комплаєнсу провайдерів в контексті миттєвих кредитних переказів у євро та запобігти непотрібним перешкодам у надсиланні та отриманні миттєвих кредитних переказів, PSP повинні періодично, принаймні щодня, перевіряти, чи є їхні користувачі фізичними або юридичними особами, які підпадають під цільові фінансові обмежувальні заходи, і більше не повинні застосовувати моніторинг операцій у цьому конкретному контексті».

Ключовий висновок: постачальники платіжних послуг, чий бізнес-моделі покладаються на миттєві перекази, можуть вибрати більше ресурсів для перевірки ризиків клієнтів під час започаткування з ними ділових відносин, а не зосереджуватися виключно на моніторингу транзакцій.