# Методологічний бюлетень

Серійний номер: МінФін-AML-2025-12

Березень 2025

“Ми - це те, що ми робимо постійно”

Арістотель

**Мета**

Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі починаючи з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для суб'єктів первинного фінансового моніторингу (СПФМ), регуляторів та правоохоронних органів.

Включає актуальні дані про нові методи та схеми ВК і ФТ, що дозволяє СПФМ адаптувати свої процедури моніторингу та контролю.

Для регуляторів та правоохоронних органів є інструментом для розробки ефективних стратегій боротьби з ВК, включаючи навчання та координацію дій між різними установами для забезпечення належної співпраці та обміну інформацією.

## Звіти міжнародних організацій та окремих юрисдикцій

### Простіша та швидша Європа[1]


Документ, представлений Європейською Комісією, визначає стратегічну мету на 2024-2029 роки – спростити та пришвидшити регуляторне середовище ЄС, забезпечуючи ефективніше впровадження політик. Він наголошує на необхідності зменшення адміністративного навантаження на бізнес, державні установи та громадян, підвищення конкурентоспроможності Європи та адаптації нормативно-правових актів до сучасних викликів. Основний акцент робиться на тому, що регуляторне середовище має бути не лише високоякісним, але й ефективним, пропорційним і простим у застосуванні.

Документ починається з аналізу поточного стану нормативно-правової бази ЄС. Автори визнають, що накопичення регуляторних вимог протягом років призвело до надмірної складності та ускладненого впровадження норм, що обмежує економічний потенціал ЄС. Як наслідок, компанії стикаються з адміністративними бар'єрами, а державні органи – з

[1] https://commission.europa.eu/document/download/8556fc33-48a3-4a96-94e8-8ecacef1ea18_en?filename=250201_Simplification_Communication_en.pdf

труднощами у впровадженні політик. Основна мета Єврокомісії – створити більш передбачуване та зручне для бізнесу середовище, зменшити фрагментацію єдиного ринку та покращити впровадження норм у країнах-членах.

Одним із ключових напрямків реформи є спрощення існуючих норм та покращення їх імплементації. Документ передбачає "стрес-тест" усього законодавства ЄС для виявлення дублюючих та застарілих норм, а також заходи з покращення імплементації політик. Для цього передбачається зміцнення співпраці з державами-членами, розширення використання цифрових інструментів та підвищення адміністративної спроможності органів влади.

Щодо механізмів спрощення, Комісія планує запровадити нові цілі зі зменшення адміністративного навантаження, зокрема скорочення звітності на 25% для всіх компаній та на 35% для малого та середнього бізнесу. Передбачено впровадження "Omnibus"-пакетів, що містять комплексні зміни до законодавства в таких сферах, як сталий розвиток, цифрові технології, інвестиції та сільське господарство. Також планується створення Європейського бізнес-гаманця, що спростить управління регуляторними вимогами.

Для забезпечення швидшого та ефективнішого прийняття норм Комісія запроваджує новий підхід до законодавчого процесу, який включає:

- Посилення оцінки впливу нових норм на бізнес та конкурентоспроможність.
- Детальніший аналіз економічних наслідків змін до законодавства під час його прийняття.
- Інтеграцію цифрових рішень у нові нормативні акти.

Окрему увагу приділено взаємодії з державами-членами. Європейська Комісія планує покращити діалог із національними урядами, підтримувати їх у впровадженні законодавства та застосовувати більш оперативні механізми вирішення порушень. Очікується проведення "перевірки реальності", що передбачає консультації з представниками бізнесу та громадянського суспільства для виявлення проблем у застосуванні норм.

Документ також акцентує увагу на необхідності оновлення багаторічного фінансового плану ЄС для покращення доступу до фінансування та зменшення бюрократичних процедур. Пропонується спрощення правил виділення коштів для забезпечення ефективнішого впровадження політик ЄС.

Загалом, ініціатива Європейської Комісії спрямована на підвищення ефективності регуляторного середовища, усунення бюрократичних перешкод і посилення імплементації політик. Це повинно сприяти зростанню економіки ЄС, стимулювати інновації та забезпечити відповідність європейського законодавства сучасним реаліям.

**Висновки:**

- **ЄС скорочуватиме адміністративне навантаження на бізнес** – зменшення звітності на 25% для всіх компаній та на 35% для МСП дозволить підприємствам витрачати менше ресурсів на бюрократію та більше на розвиток.
- **Будуть впроваджені нові "Omnibus"-пакети** – масштабні реформи у сферах цифровізації, сталого розвитку та інвестицій спростять бізнес-процеси та усунуть дублювання норм.
- **Посилена підтримка держав-членів у впровадженні законодавства** – покращений діалог, консультації та цифрові рішення дозволять уникнути фрагментації єдиного ринку.
- **Європейська Комісія проведе повний "стрес-тест" законодавства** – перегляд чинних норм виявить застарілі чи надмірно складні регуляції та дозволить їх усунути або адаптувати.

## Пропоновані регуляторні технічні стандарти в контексті відповіді EBA на Заклик Європейської Комісії щодо надання консультацій щодо нових мандатів AMLA[2]


Документ Європейського банківського органу (EBA) є відповіддю на запит Європейської комісії щодо розробки проекту регуляторних технічних стандартів (RTS) для нового законодавчого режиму ЄС у сфері боротьби з ВК/ФТ. Основною метою цих стандартів є гармонізація підходів до управління ризиками, оцінки відповідності, контролю за фінансовими установами та посилення санкційних механізмів у межах нового органу – AML Authority (AMLA).

Документ складається з кількох ключових секцій, які окреслюють підходи до оцінки ризиків, нагляду за фінансовими установами, процесів належної перевірки клієнтів (CDD) та застосування санкційних механізмів. Основні запропоновані зміни спрямовані на уніфікацію регуляторних вимог у всіх державах-членах ЄС, мінімізацію регуляторного арбітражу та посилення ефективності нагляду.

У частині, що стосується оцінки внутрішніх та залишкових ризиків фінансових установ, EBA пропонує запровадження єдиної методології для всіх регуляторів у межах ЄС. Ця методологія включає три основні кроки:

1. Оцінка внутрішніх ризиків – визначення рівня ризику установи за чотирма категоріями (низький, середній, значний, високий).
2. Оцінка якості систем контролю – класифікація рівня якості системи з ПВК/ФТ на основі автоматизованого підходу.
3. Оцінка залишкового ризику – визначення реального рівня загроз, які залишаються після врахування контрольних механізмів.

Методологія оцінки використовуватиме автоматизовану систему балів із можливістю коригування на основі національних особливостей, проте з обмеженнями для мінімізації суб'єктивного впливу. Цей підхід спрямований на усунення розбіжностей між підходами національних регуляторів, що призведе до підвищення ефективності нагляду з ПВК/ФТ та спрощення процедур для фінансових установ.

Наступним ключовим аспектом є підхід до відбору фінансових установ для прямого нагляду з боку AMLA. Відповідно до нової системи, під безпосередній контроль AMLA підпадатимуть ті фінансові групи та установи, які здійснюють діяльність щонайменше у шести країнах ЄС. Основні критерії відбору включають:

- Обсяги транзакцій та кількість клієнтів у кожній країні, що допоможе виключити фіктивну присутність установ у різних юрисдикціях.
- Рівень ризику установи, визначений відповідно до нової методології оцінки ризиків ВК/ФТ.

Цей підхід дозволить AMLA зосередити нагляд на найбільш ризикових суб'єктах, мінімізуючи регуляторне навантаження на установи з низьким ризиком.

Документ також приділяє значну увагу налагодженню процесів CDD. Відповідно до нових RTS, AMLA встановлюватиме єдині вимоги до CDD для всіх фінансових установ у ЄС, що включатиме:

[2] https://www.eba.europa.eu/sites/default/files/2025-03/9bc83e61-e9a1-4e91-93de-2af8325e0182/Consultation%20Paper%20on%20Response%20to%20Call%20for%20Advice%20new%20AMLA%20mandates.pdf

- Збір та перевірку даних про клієнтів – використання незалежних та надійних джерел інформації.
- Спрощену (SDD) та посилену (EDD) перевірку клієнтів – чітке визначення критеріїв для різних рівнів оцінки ризиків.
- Використання електронних ідентифікаційних засобів – запровадження вимог щодо eIDAS-комплаєнтних рішень для онлайн-верифікації клієнтів.

Особливу увагу приділено питанням санкцій та правозастосування. Нові правила передбачають чіткі критерії для визначення рівня порушень законодавства з ПВК/ФТ та застосування санкцій, адміністративних заходів і періодичних фінансових стягнень (PePPs).

Основні зміни включають:

- Визначення чотирьох рівнів серйозності порушень.
- Запровадження єдиної методики визначення розміру штрафів та адміністративних заходів.
- Використання PePPs як інструменту примусового виконання вимог з ПВК/ФТ, що є новим механізмом для багатьох юрисдикцій ЄС.

Загалом, запропоновані регуляторні зміни спрямовані на підвищення ефективності нагляду з ПВК/ФТ, усунення розбіжностей у підходах різних країн ЄС та створення єдиної системи ризик-орієнтованого регулювання фінансового сектору. Це сприятиме зміцненню механізмів виявлення та запобігання фінансовим злочинам, зниженню регуляторного арбітражу та забезпеченню більш ефективного функціонування AMLA як центрального органу нагляду.

**Висновки:**

- **ЄС запроваджує єдину методологію оцінки ризиків ВК/ФТ** – автоматизована система балів допоможе стандартизувати підходи регуляторів, що підвищить ефективність нагляду та мінімізує ризики розбіжностей між країнами.
- **AMLA здійснюватиме прямий нагляд за найбільш ризиковими фінансовими установами** – до нагляду будуть відібрані компанії, що працюють у шести або більше країнах ЄС та мають високий рівень ризику ВК/ФТ.
- **Єдині правила CDD забезпечать однаковий рівень AML-комплаєнсу у всіх країнах ЄС** – нові вимоги усунуть фрагментацію та розбіжності у процесах KYC/CDD.
- **Санкційні механізми будуть посилені** – нові стандарти передбачають чіткі критерії оцінки порушень AML-законодавства, що гарантує ефективне та пропорційне застосування штрафів і адміністративних заходів.

## Посилення фінансової безпеки України: ключові виклики та шляхи реформування системи протидії фінансовим злочинам[3]


Документ, підготовлений Центром фінансової доброчесності (CFI), є ґрунтовним аналізом ключових викликів та необхідних реформ у сфері протидії фінансовим злочинам в Україні. У ньому розглядається вплив війни на фінансову систему країни, а також виклики, пов'язані з впровадженням міжнародних стандартів боротьби з відмиванням коштів (ПВК) та фінансуванням тероризму (ФТ). Публікація ґрунтується на аналізі офіційної документації, таких як звіти MONEYVAL, план Ukraine Facility та результати експертних інтерв'ю, проведених у 2024 році.

Документ починається з аналізу контексту, в якому опинилася Україна. Ще до початку повномасштабного вторгнення РФ країна стикалася з

[3] https://cfi-ua.org/strengthening-ukraines-fight-against-financial-crime/

труднощами у виконанні стандартів FATF. Однак війна суттєво загострила проблеми фінансової безпеки, одночасно створивши унікальне вікно можливостей для реформ. Масштабні фінансові вливання від міжнародних партнерів, включаючи допомогу та кредити на відбудову, вимагають безпрецедентного рівня прозорості та підзвітності. Питання фінансової доброчесності набуває особливої ваги у світлі майбутньої відбудови України, яка передбачає багатомільярдні трансакції, що можуть стати мішенню для корупції та фінансових зловживань. Одним із головних викликів залишається баланс між забезпеченням відкритості фінансових потоків та безпековими обмеженнями, які з'явилися під час війни, такими як закриття публічних реєстрів.

У документі аналізуються основні недоліки поточної системи боротьби з фінансовими злочинами. Однією з ключових проблем є відсутність ефективного механізму державно-приватного партнерства (PPP) у сфері протидії відмиванню коштів. Успішні міжнародні практики демонструють, що тісна взаємодія державних органів з приватним сектором суттєво підвищує ефективність моніторингу підозрілих фінансових операцій. В Україні наявні ініціативи у сфері PPP (наприклад, Українська мережа доброчесності та комплаєнсу – UNIC), але вони орієнтовані переважно на боротьбу з корупцією, а не на фінансові злочини. Важливо розробити єдине бачення державно-приватного партнерства, створити правові механізми для обміну інформацією між фінансовими установами та правоохоронними органами, а також використати міжнародний досвід таких ініціатив, як австралійська Fintel Alliance.

Ще одним суттєвим викликом є відсутність повноцінного регулювання ринку віртуальних активів. Україна займає шосте місце у світі за рівнем використання криптовалют, і їхня роль в економіці значно зросла після початку війни. У 2022 році було ухвалено закон «Про віртуальні активи» (№2074-IX), але він так і не набув чинності через нерозв’язані питання оподаткування. Два альтернативні законопроєкти щодо регулювання криптоактивів перебувають у Верховній Раді, проте міждержавні та міжвідомчі дискусії гальмують їхній розгляд. Відсутність чіткої регуляторної політики створює ризики використання криптовалют для ухилення від санкцій, фінансування тероризму та інших незаконних операцій. Крім того, відсутність механізму ліцензування постачальників послуг, пов’язаних з віртуальними активами (VASPs), посилює загрози фінансових зловживань. У документі наголошується на необхідності ухвалення законодавства, яке чітко визначатиме регулятора ринку, запровадження реєстру VASPs та використання «регуляторних пісочниць» для тестування механізмів нагляду.

Також розглядається проблема недостатнього нагляду за визначеними нефінансовими установами та професіями (DNFBPs), такими як адвокати, аудитори, рієлтори та дилери коштовностей. Незважаючи на розширення законодавства у 2019 році, регуляторний контроль за цими секторами залишається слабким. MONEYVAL ще у 2017 році вказав на те, що Україна не відповідає 28 Рекомендації FATF, і без удосконалення підходів до нагляду цей недолік буде збережений у майбутніх оцінках. Важливим кроком є впровадження ризик-орієнтованого підходу до контролю DNFBPs, активізація навчальних програм та координація між різними регуляторними органами.

Документ також висвітлює проблему зростання використання «грошових мулів» – фізичних осіб, які, усвідомлено чи ні, беруть участь у схемах з переказу незаконних коштів. Останнім часом через такі схеми проходять мільярди гривень, що створює загрози як для фінансової стабільності України, так і для її міжнародної репутації. Для боротьби з цим явищем Національний банк України запровадив обмеження на одноразові P2P-перекази, а банки уклали меморандум про співпрацю в ідентифікації підозрілих клієнтів. Однак ці заходи є лише частковими рішеннями. Необхідно посилити процедури KYC, удосконалити обмін інформацією між банками та розглянути можливість криміналізації діяльності «грошових мулів».

Останньою, але не менш важливою проблемою є слабкість механізму цільових фінансових санкцій (TFS). Україна веде активну санкційну політику проти росії, проте відстає у сфері боротьби з фінансуванням розповсюдження зброї масового знищення. MONEYVAL ще у 2017 році вказав на недостатню імплементацію санкцій проти Ірану та брак чітких процедур заморожування активів. У документі рекомендується надати Держфінмоніторингу провідну роль у координації санкційної політики, підвищити обізнаність про загрози, пов'язані з ФРЗМ, та забезпечити законодавчу відповідність 6 і 7 Рекомендації FATF.

**Висновки:**

- Україна потребує ефективної моделі державно-приватного партнерства (PPP) для боротьби з фінансовими злочинами.
- Нагальним є законодавче врегулювання ринку віртуальних активів (ВА), оскільки його нерегульований статус створює значні ризики.
- Фінансові розслідування в Україні потребують кардинального перегляду та впровадження чітких методологічних стандартів.
- Боротьба з «грошовими мулами» має стати пріоритетом, оскільки ця проблема набирає загрозливих масштабів.

Загальний висновок документа підкреслює, що Україна має унікальну можливість здійснити глибоку реформу своєї фінансової системи, зробивши її більш стійкою та прозорою. Для цього необхідно не лише забезпечити технічну відповідність міжнародним стандартам, а й впровадити ефективні механізми їхньої реалізації. Виконання цих рекомендацій дозволить Україні не лише зміцнити фінансову безпеку, а й підвищити рівень міжнародної довіри та залучити більше інвестицій у процес післявоєнної відбудови.

## Приватно-правові аспекти токенізованих CBDC: виклики, можливості та перспективи правового регулювання[4]


Документ, підготовлений експертами МВФ у березні 2025 року і досліджує приватно-правові аспекти цифрових валют центрального банку (CBDC), що базуються на токенах. Основна увага приділяється питанням власності, передачі прав, використання таких активів у фінансовій системі, їх взаємодії з традиційними банківськими операціями, а також потенційним юридичним ризикам та необхідності реформ у приватному праві. Документ ґрунтується на аналізі правових особливостей цифрових активів у різних юрисдикціях та пропонує концептуальну основу для розробки правової інфраструктури, яка забезпечить ефективну інтеграцію CBDC у світову економіку.

У вступі зазначається, що цифрові валюти центральних банків є наступним кроком у розвитку грошей після готівкових і безготівкових форм. Хоча ідея CBDC вже не є новою, більшість дискусій зосереджені на публічно-правових аспектах, тоді як приватне право залишається недостатньо розробленим. У цьому контексті документ досліджує, як токенізовані CBDC можуть функціонувати у приватному праві та які виклики вони створюють для правової

[4] https://www.imf.org/en/Publications/fintech-notes/Issues/2025/03/14/Private-Law-Aspects-of-Token-Based-Central-Bank-Digital-Currencies-565165

системи. На момент написання звіту понад 90% центральних банків у світі розглядали можливість випуску CBDC, а деякі (Багамські острови, Нігерія, Ямайка) вже запустили такі ініціативи. Однак для того, щоб CBDC могли повноцінно функціонувати в економіці, необхідно врегулювати такі питання, як правовий статус цифрового токена, його власність, передача, взаємодія з банками та міжнародна правова відповідність.

Один із головних викликів полягає у визначенні правової природи токенізованого CBDC. Документ аналізує можливі підходи до класифікації, зокрема чи слід розглядати його як гібридний актив (аналог банкнот або цінних паперів), нову категорію майнових прав чи чистий нематеріальний актив. У деяких юрисдикціях (наприклад, у США, Великій Британії, Ліхтенштейні, Швейцарії) вже розроблено спеціальне законодавство для цифрових активів, що може стати основою для регулювання CBDC. Однак у більшості країн питання власності на токенізовані цифрові активи залишається відкритим. Якщо CBDC розглядатиметься як гібридний актив, то він може отримати правові характеристики, аналогічні цінним паперам або традиційним банкнотам, що дозволить встановити правила їх передачі та захисту. Якщо ж CBDC буде визначено як унікальний нематеріальний актив, знадобиться розробка окремих законодавчих норм для регулювання його використання та передачі.

**Висновки:**

- **Чітка правова кваліфікація токенізованого CBDC є критично важливою**
  - Країни мають вирішити, чи буде CBDC розглядатися як новий клас активів, гібридний актив, чи нематеріальна власність.
  - Від цього залежить правовий режим передачі, забезпечення прав власності та захист добросовісних набувачів.
- **Необхідно забезпечити правовий захист власників CBDC при використанні фінансових посередників**
  - Повинні бути чітко визначені права власності користувачів на токени у випадку банкрутства банку чи зберігача.
  - Розробка механізмів аналогічних до захисту клієнтів у сфері брокерських послуг.
- **Юридичний статус реєстрів та гаманців має бути врегульований**
  - Чи визнаються реєстри (DLT/блокчейн) як офіційні записи власності?
  - Чи можуть цифрові гаманці виконувати функції довірчого зберігача (custodian), і які наслідки це має для власників?
- **Міжнародне право повинно адаптуватися до CBDC для забезпечення їх правової сумісності у транскордонних платежах**
  - Необхідні міжнародні угоди щодо статусу CBDC, зокрема у рамках UNIDROIT та Гаазької конференції з міжнародного права.
  - Врегулювання питань екстериторіальної юрисдикції у разі транзакцій між країнами.

Наступний розділ документа розглядає, як власність на токенізовані CBDC може бути засвідчена та захищена. Тут важливу роль відіграють цифрові реєстри (ledger) та гаманці. Традиційно право власності на активи може бути підтверджене через реєстрацію у певному юридично визнаному реєстрі. У випадку токенізованих CBDC питання полягає у тому, чи має цифровий реєстр або блокчейн визнаватися офіційним джерелом інформації про власність. Є два можливі підходи: реєстр може мати конститутивну функцію (тобто тільки запис у ньому створює право власності) або лише індикативну (тобто може бути використаний як доказ, але не єдиний механізм встановлення прав). У разі якщо власники CBDC зберігають їх через фінансових посередників, важливо, щоб вони не втрачали своїх прав на актив у випадку банкрутства такого посередника.

Далі розглядаються механізми передачі CBDC між власниками. У традиційній фінансовій системі гроші передаються через банківські рахунки, а їхні власники

захищені відповідним законодавством. Для токенізованих CBDC принципи передачі ще не сформовані. Важливим є питання правового захисту добросовісного набувача, а також визначення моменту остаточного переходу власності. У разі використання блокчейн-технологій юридичний статус запису про транзакцію має бути чітко визначений: чи є запис у реєстрі остаточним підтвердженням угоди, чи можуть існувати механізми оскарження?

Документ також аналізує, як CBDC взаємодіють із традиційною банківською системою. Чи можуть вони вважатися депозитами, як це відбувається з коштами на рахунках у комерційних банках? Чи можуть CBDC бути передані у заставу або використані для кредитування? Однією з головних проблем є захист користувачів у разі банкрутства зберігача. Якщо CBDC зберігаються через фінансових посередників, чи буде їхній власник мати пріоритетні права у процедурі банкрутства? У деяких країнах такі механізми вже працюють для цінних паперів, але чи можуть вони бути застосовані до CBDC?

Окремий розділ присвячений міжнародному приватному праву. Оскільки CBDC можуть використовуватися у міжнародних транзакціях, виникає питання, яке право буде застосовуватися у разі спорів. Наприклад, якщо громадянин однієї країни зберігає CBDC, емітовані центральним банком іншої країни, через міжнародного посередника, яка країна буде мати юрисдикцію у разі конфлікту? Документ підкреслює необхідність міжнародних угод щодо статусу CBDC та можливість адаптації чинних норм для цінних паперів або криптовалют до нових умов.

Завершальний розділ аналізує необхідність реформ у приватному праві. Оскільки більшість чинного законодавства не передбачає регулювання токенізованих CBDC, необхідно або створювати нові правові категорії, або адаптувати чинні норми. Досвід таких країн, як Швейцарія та Франція, показує, що можливий варіант, коли CBDC прирівнюється до цінних паперів у питаннях власності та захисту прав інвесторів. Водночас інші країни можуть піти шляхом створення спеціальних законів для цифрових активів.

У підсумку документ МВФ наголошує на тому, що для успішного впровадження CBDC необхідно розробити комплексний правовий підхід, який забезпечить їхню правову визначеність, захист користувачів та інтеграцію у банківську систему. Також потрібні міжнародні механізми регулювання, оскільки цифрові валюти центральних банків матимуть транскордонний вплив.

## Загрози ядерній безпеці: як незаконний обіг радіоактивних матеріалів підриває глобальну стабільність[5]

Публікація від UN News висвітлює проблему незаконного обігу ядерних і радіоактивних матеріалів, яка залишається серйозною загрозою для міжнародної безпеки. За даними Міжнародного агентства з атомної енергії (IAEA), у 2024 році було зафіксовано майже 150 випадків незаконного або несанкціонованого поводження з такими матеріалами. Хоча загальна кількість інцидентів залишається відносно стабільною порівняно з попередніми роками, аналітики наголошують на тому, що навіть окремий випадок потрапляння радіоактивних матеріалів до рук зловмисників може призвести до катастрофічних наслідків. Три з цих випадків були безпосередньо пов’язані з контрабандою або навмисним використанням у злочинних цілях, тоді як у 21 інциденті правоохоронці не змогли визначити, чи була присутня кримінальна складова.

[5] https://news.un.org/en/story/2025/02/1160656

Особливе занепокоєння викликає зростаюча загроза, пов'язана із забрудненими промисловими матеріалами, такими як металеві труби та інші вироби, що містять радіоактивні речовини та випадково потрапляють у промислові ланцюги постачання. Це свідчить про серйозні проблеми з утилізацією ядерних відходів у ряді країн і водночас демонструє ефективність детекторних систем, які змогли виявити ці матеріали. Експерти IAEA наголошують, що така ситуація вимагає вдосконалення механізмів виявлення та контролю за радіоактивними речовинами в промисловості.

Ще одним критично важливим аспектом ядерної безпеки є транспортування таких матеріалів. За останні десять років 65% усіх зареєстрованих крадіжок ядерних і радіоактивних речовин сталися саме під час їх перевезення. Ядерні матеріали широко використовуються в медицині, промисловості та наукових дослідженнях, що робить їх об'єктом підвищеної уваги з боку злочинних угруповань. Основна проблема полягає у великій кількості осіб та організацій, що беруть участь у процесі транспортування, що створює значні прогалини у безпеці. Експерти наголошують, що необхідно вжити додаткових заходів щодо захисту таких вантажів, зокрема посилити контроль за маршрутом перевезень, впровадити системи моніторингу та підвищити рівень підготовки персоналу.

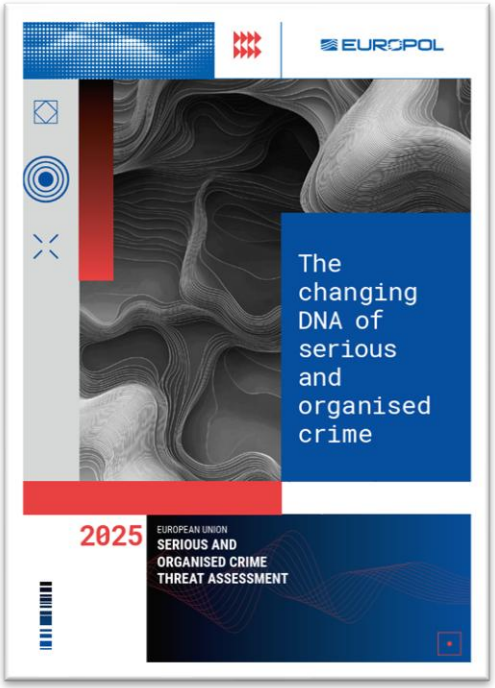
Міжнародне співробітництво відіграє ключову роль у боротьбі з незаконним обігом ядерних матеріалів. IAEA веде спеціальну базу даних ITDB, в якій фіксуються всі виявлені інциденти. Проте, у 2024 році звіти надали лише 32 з 145 країн-учасниць IAEA, що свідчить про недостатню залученість багатьох держав до глобального моніторингу та контролю. Враховуючи динаміку змін у сфері ядерної безпеки, агентство закликає держави посилити заходи контролю, особливо у сфері транспортування, промислового використання та утилізації радіоактивних матеріалів. Відсутність повноцінної глобальної системи обміну інформацією про такі інциденти значно ускладнює боротьбу з незаконним обігом і створює ризики для міжнародної безпеки.

Загалом, звіт підкреслює, що незаконний обіг ядерних матеріалів є не лише кримінальною проблемою, а й викликом глобальній системі безпеки, який вимагає комплексних заходів для мінімізації ризиків. Основними напрямками, що потребують негайного посилення, є контроль за промисловими радіоактивними відходами, захист ядерних матеріалів під час транспортування та розширення міжнародної співпраці у сфері моніторингу та запобігання загрозам.

Висновки:

- **Необхідність зміцнення заходів безпеки при транспортуванні ядерних матеріалів -** Посилення контролю, впровадження обов'язкових супутникових трекерів та удосконалення логістичних процедур.
- **Покращення механізмів ідентифікації та запобігання контамінованим матеріалам у промислових ланцюгах -** Розширення обов'язкових перевірок радіаційного забруднення на митницях і підприємствах, що працюють із металами.
- **Посилення міжнародної координації у боротьбі з незаконним обігом ядерних матеріалів -** Розширення участі держав у програмі ITDB від IAEA та впровадження нових протоколів обміну інформацією.
- **Розширення звітності та обов'язкової реєстрації інцидентів серед усіх держав-учасниць IAEA -** Запровадження суворішої відповідальності за відсутність звітності про випадки незаконного обігу та створення глобальної бази даних щодо загроз у цій сфері.

## ДНК організованої злочинності змінюється -- EU-SOCTA 2025 [6]




Європейська оцінка загроз серйозної та організованої злочинності EU-SOCTA 2025 є найдетальнішим та найбільш далекоглядним дослідженням сучасного кримінального ландшафту в ЄС. Основний висновок цього звіту полягає в тому, що "ДНК організованої злочинності змінюється" – злочинні мережі еволюціонують разом зі світом, адаптуючись до нових умов, використовуючи передові технології та реагуючи на глобальні кризи. Це перетворення має три ключові складові: злочинність дестабілізує суспільство, активно розвивається в цифровому просторі та отримує нові можливості завдяки штучному інтелекту й іншим проривним технологіям.

Одним із найважливіших викликів, які виділяє звіт, є подвійний дестабілізуючий ефект організованої злочинності. Вона не лише послаблює верховенство права, політичну стабільність і соціальну згуртованість, а й стає невід'ємною складовою гібридних загроз. Глобальні кризи, включно з війною Росії проти України, політичною напруженістю в інших частинах світу, економічною нестабільністю та цифровими трансформаціями, сприяють розширенню впливу злочинних угруповань. Ці мережі не лише отримують фінансовий зиск, а й можуть бути використані для досягнення геополітичних цілей держав або гібридних загроз.

Сучасна злочинність все більше живиться в онлайн-просторі, що робить її менш залежною від фізичних кордонів. Інтернет став не просто інструментом для координації злочинних операцій, а й основним середовищем їх здійснення. Кіберзлочини, онлайн-шахрайство, торгівля наркотиками через даркнет, відмивання грошей за допомогою криптовалют – все це свідчить про нову цифрову реальність злочинності. Широкомасштабні шахрайські схеми, такі як інвестиційні афери, фальсифікація товарів і підробка фармацевтичної продукції, завдають удару не лише по громадянах, а й по бізнесу та державним фінансам. Водночас криптовалюти, децентралізовані фінансові платформи (DeFi) та технології блокчейну ускладнюють ідентифікацію кінцевих бенефіціарів злочинних активів. Цифровий простір також використовується для вербування молодих виконавців, які стають частиною злочинних схем, часто навіть не усвідомлюючи масштаб їхньої діяльності.

Важливим аспектом є роль штучного інтелекту та нових технологій у прискоренні розвитку злочинних угруповань. Використання генеративного штучного інтелекту та мовних моделей дає можливість створювати переконливі шахрайські повідомлення, автоматизувати атаки на банківські системи, а також розповсюджувати фейки та дезінформацію. Голосові копії, deepfake-відео та підроблені цифрові особи використовуються для фінансового шахрайства, маніпуляцій та навіть політичного впливу. Квантові технології та криптографія майбутнього також можуть змінити правила гри у сфері злочинності: «зберігай зараз – зламай пізніше» – таку стратегію використовують злочинні угруповання, накопичуючи зашифровані дані з метою їх подальшого розшифрування, коли технології дозволять це зробити.

Важливим напрямом діяльності злочинних угруповань є фінансова злочинність та відмивання коштів. Від традиційних схем, які включають використання готівки та підставних компаній,

[6] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

злочинці переходять до складних фінансових операцій через криптовалюти, анонімні гаманці та офшорні структури. Відмивання грошей все частіше здійснюється через децентралізовані біржі, де транзакції можуть бути анонімними та захищеними від традиційного контролю фінансових установ. Професійні «відмивачі» коштів надають послуги різним злочинним групам, використовуючи методи «laundering-as-a-service», що дозволяє будь-якій особі приховати незаконні доходи.

Окремим викликом є зростання насильства, пов'язаного з організованою злочинністю. Портові міста Європи стають осередками збройних конфліктів між конкуруючими наркокартелями, а онлайн-інструменти використовуються для вербування виконавців насильницьких злочинів. Злочинні мережі активно використовують «violence-as-a-service» – модель, за якою можна замовити фізичну розправу, залякування або знищення опонентів, не виходячи з тіні. Окрему загрозу становлять молоді виконавці, які через соціальні мережі залучаються до злочинної діяльності та швидко радикалізуються.

Крім того, важливу роль у сучасному кримінальному середовищі відіграє корупція, яка є головним інструментом, що дозволяє злочинним мережам функціонувати. Йдеться не лише про підкуп чиновників, суддів чи правоохоронців, а й про корупцію у цифровій сфері, що включає злам урядових систем, крадіжку конфіденційних даних та маніпуляцію інформацією. Новою загрозою стає поява «корупційних брокерів», які спеціалізуються на підкупі високопосадовців та посадових осіб у державних і комерційних структурах.

Ще одним ключовим аспектом є взаємодія організованої злочинності з державами та гібридними загрозами. Деякі держави активно використовують кримінальні мережі для дестабілізації ЄС. Наприклад, контрабанда мігрантів використовується як інструмент тиску на європейські країни, а кіберзлочини застосовуються для саботажу критичної інфраструктури або

**Висновки:**

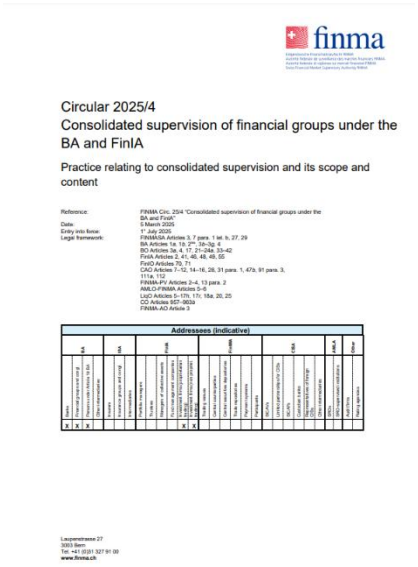
- **Фінансова злочинність та відмивання коштів стають цифровими та невидимими -** Організовані злочинні мережі активно використовують криптовалюти, DeFi-платформи та технології блокчейну для приховування незаконних фінансових потоків. Лише 2% кримінальних доходів у ЄС конфіскуються, що свідчить про необхідність посилення механізмів фінансового контролю та міжнародної співпраці у сфері протидії відмиванню коштів.
- **Штучний інтелект і нові технології радикально змінюють злочинність -** Злочинці використовують генеративний ШІ для створення шахрайських схем, deepfake-маніпуляцій та автоматизованих атак. Квантові технології можуть у майбутньому загрожувати кібербезпеці, дозволяючи зламувати зашифровані дані. Необхідні нові регуляторні підходи для контролю ШІ та цифрових злочинів.
- **Корупція залишається фундаментальним інструментом злочинності -** Злочинні мережі все частіше використовують "корупційних брокерів", які виступають посередниками між бізнесом, державними структурами та криміналом. Цифрові платформи та фінансові технології дозволяють здійснювати анонімні хабарі через криптовалюти, що значно ускладнює викриття корупційних схем.
- **Організована злочинність та гібридні загрози все більше переплітаються -** Деякі держави використовують злочинні угруповання як інструмент гібридної війни, застосовуючи їх для дестабілізації ЄС через кібер-атаки, контрабанду наркотиків, торгівлю людьми та ухилення від санкцій. ЄС має посилити координацію між правоохоронними органами та розвідкою для протидії цим загрозам.

викрадення конфіденційних даних. Це свідчить про все більшу роль злочинних мереж у глобальних геополітичних конфліктах.

У підсумку, EU-SOCTA 2025 наголошує, що для протидії сучасній злочинності ЄС повинен не лише розвивати законодавчі механізми, а й активно впроваджувати цифрові технології для боротьби з фінансовими злочинами, посилювати міжнародну співпрацю та змінювати підхід до конфіскації злочинних активів. Організована злочинність вже не є локальною проблемою – вона діє глобально, швидко адаптується і використовує найновіші технології для досягнення своїх цілей.

# Регулювання

## Консолідований нагляд за фінансовими групами[7]


finma

Circular 2025/4
Consolidated supervision of financial groups under the BA and FinIA

Practice relating to consolidated supervision and its scope and content

Addressees (indicative)

Цей циркуляр Швейцарського управління з нагляду за фінансовими ринками (FINMA), який набирає чинності з 1 липня 2025 року, детально регламентує практику консолідованого нагляду над фінансовими групами відповідно до Закону про банки (BA) та Закону про фінансові інституції (FinIA). Метою документа є уточнення сфери застосування, методології та змісту нагляду за фінансовими групами з метою виявлення системних ризиків, підвищення стабільності ринку та ефективного впровадження стандартів ПВК/ФТ на рівні груп.

Документ визначає, що консолідований нагляд застосовується до фінансових груп, у складі яких перебувають банки, компанії з торгівлі цінними паперами або інші установи, зазначені у статті 1b BA. Його мета — забезпечити повний контроль за групою як єдиним економічним суб'єктом, незалежно від юридичної форми окремих компаній. FINMA надає пріоритет саме консолідованому нагляду, а не альтернативним заходам, таким як заходи "ринг-фенсингу" (організаційна, фінансова або функціональна ізоляція окремих підрозділів), які можуть застосовуватися лише у виняткових випадках, наприклад, за відсутності ефективного іноземного нагляду над материнською компанією.

Обсяг нагляду визначається на основі оцінки економічної єдності, фактичного або юридичного обов'язку надавати підтримку, а також фінансової активності компанії. У документі уточнено, що активність у фінансовому секторі включає не тільки ліцензовані дії, але й інші форми участі у фінансовому посередництві, зокрема лізинг, факторинг, операції з платіжними токенами або зберігання цінних паперів. Відтак, навіть компанії, які формально не мають статусу фінансової установи, можуть підпадати під консолідований нагляд, якщо мають істотні фінансові зв'язки з рештою групи.

FINMA також класифікує різні типи структури фінансових груп — від класичної ієрархії з материнською компанією до холдингових структур, атипових договірних об'єднань та підгруп іноземних фінансових груп. У кожному випадку оцінюється рівень впливу на інші компанії групи, а також ризики, що можуть виникати внаслідок організаційних, фінансових чи кадрових взаємозв'язків.

[7] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2025-04-20250305.pdf?sc_lang=en&hash=F556F70A1A6F58F3F188F398E846DA81

Особливе місце в циркулярі посідає зміст консолідованого нагляду, який поділяється на якісні та кількісні елементи. Якісні включають вимоги до корпоративного управління, систем внутрішнього контролю, управління ризиками, а також впровадження стандартів ПВК/ФТ у масштабах усієї групи. Крім того, всі члени управлінських органів мають відповідати критеріям "fit and proper", а також бути чітко розмежовані за наглядовими функціями. Визначено обов'язок призначення незалежного зовнішнього аудитора для всієї групи, який має бути погоджений з FINMA.

Кількісні елементи включають консолідовані вимоги до достатності капіталу, ліквідності, розподілу ризиків, звітності про процентний ризик, а також ведення звітності за міжнародними стандартами (IFRS, US GAAP або Швейцарські банківські стандарти). У випадках, коли до складу групи входять компанії, які є несуттєвими з точки зору нагляду, FINMA може звільнити їх від кількісних вимог, проте не від якісних.

Циркуляр також встановлює чітку межу між сферою консолідації для фінансової звітності та для наглядових цілей. Наприклад, навіть якщо компанія не входить до складу консолідованої звітності відповідно до бухгалтерських стандартів, вона все одно може підпадати під нагляд, якщо має економічні або правові зв'язки з рештою групи.

Загалом, документ формує ґрунтовну основу для всебічного, скоординованого нагляду за фінансовими групами, з акцентом на регуляторну прозорість, інтегровану оцінку ризиків та нагляд за дотриманням норм ПВК/ФТ у межах всієї корпоративної структури.

**Висновки:**

- **Консолідований нагляд FINMA поширюється не лише на банки, але й на будь-які компанії, які здійснюють фінансову діяльність та мають економічні або правові зв'язки з групою**, навіть якщо вони не є ліцензованими установами — це вимагає перегляду групової структури на предмет потенційних ризиків.
- **Заходи "ринг-фенсингу" застосовуються лише у виключних випадках і не можуть замінити повноцінний консолідований нагляд**, що підкреслює необхідність структурної відповідності вимогам до прозорості взаємозв'язків в середині групи.
- **Фінансові групи зобов'язані впровадити на груповому рівні стандартизовані політики ПВК/ФТ**, з урахуванням внутрішнього контролю, управління ризиками та системи незалежного аудиту, що гарантує охоплення усіх учасників групи.
- **FINMA залишає за собою право звільняти від кількісних вимог лише несуттєві компанії**, проте якісні вимоги (наприклад, щодо ПВК/ФТ) залишаються обов'язковими — тому фінансовим групам необхідно проводити детальний внутрішній аналіз на відповідність критеріям "суттєвості" та підтримувати відповідну документацію.

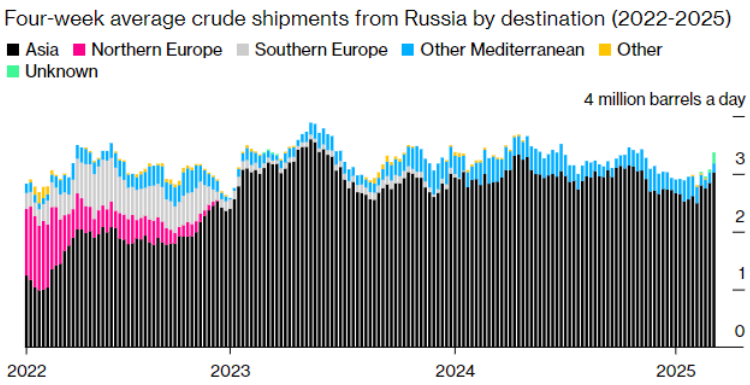
## Санкції

### Російські нафтові потоки зросли через руйнацію санкцій США[8]

Російський нафтовий експорт демонструє стрімке зростання, що може свідчити про послаблення ефективності санкцій США. За даними Bloomberg, обсяги експорту сирої нафти з усіх російських портів за чотири тижні до 9 березня зросли на 300 тисяч барелів на день, що є найбільшим приростом з січня 2023 року. Загальний обсяг постачання досяг 3,37 млн барелів

[8] https://www.bloomberg.com/news/articles/2025-03-11/russia-s-oil-exports-surge-in-sign-us-sanctions-starting-to-crumble

на день, що є максимальним показником з листопада 2024 року. Відновлення активності танкерів, які понад рік перебували в простої через санкції, дозволило Москві відновити обсяги поставок, зокрема через головний тихоокеанський порт.




Санкції США проти російського нафтового танкерного флоту, які мали обмежити можливості Москви продавати нафту та фінансувати військові операції, почали давати збої. Незважаючи на те, що адміністрація Джо Байдена у січні 2025 року запровадила нові обмеження, додавши до санкційного списку ще 161 судно, що спочатку суттєво скоротило російський нафтовий експорт, останні дані свідчать про адаптацію РФ до санкційного режиму. Росія продовжує використовувати тіньовий флот танкерів, які належать маловідомим компаніям за межами юрисдикції західних держав, що дозволяє їй уникати обмежень, пов'язаних із західними страховими та фінансовими послугами.

Постачання нафти з Арктичного регіону зазнало суттєвих змін після введення санкцій у січні: якщо раніше близько 60% арктичної нафти йшло до Індії, то після 10 січня не було зафіксовано жодного випадку офіційного постачання. Натомість частина цих вантажів перенаправляється в обхідними маршрутами – деякі судна здійснюють приховані перевантаження в Аравійському морі біля узбережжя Оману, а їхні кінцеві пункти призначення, ймовірно, знаходяться в Китаї. Щонайменше 15 мільйонів барелів нафти, завантаженої в Арктиці після посилення санкцій, залишаються на морі, що свідчить про складнощі з її реалізацією. Деякі арктичні танкери вказані як такі, що прямують до сирійського порту Баніас, проте фактична доставка ще не відбулася.

У Тихоокеанському регіоні ситуація також нестабільна. Лише 8 з 22 танкерів, що транспортували нафту з проекту "Сахалін-1" після введення останнього раунду санкцій, були успішно розвантажені. Деякі судна завантажили нафту у резервуарах в порту Яншань неподалік Шанхаю – ці резервуари не підключені до основних нафтопереробних потужностей Китаю, що може вказувати на спроби приховати походження сировини перед її подальшим продажем.

Російський нафтовий експорт також стикається зі складнощами під час розвантаження. Наприклад, супертанкер, що перевозив 2 мільйони барелів нафти з Сахаліну, не зміг розвантажитися у двох китайських портах – Янтай та Дунцзякоу, а зрештою вирушив у порт Хуандао. Подібні труднощі можуть бути пов’язані із загостренням регуляторного контролю з боку китайських державних органів, які намагаються уникнути потрапляння під вторинні санкції.

Тим часом у Чорному морі та Балтійському регіоні ситуація залишається неоднозначною. Постачання через порт Новоросійськ скоротилися після нещодавнього сплеску активності, проте обсяги відвантаження з Приморська та Сахаліну залишаються високими. У Туреччині, яка є єдиним великим європейським покупцем російської нафти, імпорт скоротився – найбільший нафтопереробний завод країни Tüpraş припинив закупівлі, побоюючись санкцій США.

Хоча вартість експорту російської нафти у тиждень до 9 березня впала на 80 мільйонів доларів (на 5%) і склала 1,44 мільярда доларів, чотиритижневий середній показник доходів продовжує зростати, що свідчить про довгострокову ефективність тіньових схем обходу санкцій. Зростання доходів та збільшення обсягів перевезень вказує на те, що Росія змогла частково компенсувати втрати та поступово послаблює вплив західних санкцій, використовуючи альтернативні канали та нових партнерів.

Зміна політичного курсу у Вашингтоні може додатково послабити санкційний режим. Дональд Трамп, який повернувся на посаду президента США, вже натякнув на можливість перегляду обмежень, що створює потенційну перспективу для подальшого відновлення нафтового експорту Росії. Якщо такі зміни відбудуться, вони можуть ще більше підірвати санкційний механізм, створюючи для Москви вікно можливостей для нарощування доходів від нафти.

## Звіти окремих інституцій та експертів

### Стан та перспективи FinTech у Швейцарії: аналіз Swiss FinTech Study 2025[9]


Дослідження, підготовлене Інститутом фінансових послуг у місті Цуг (IFZ), надає глибокий аналіз екосистеми фінансових технологій у Швейцарії та Ліхтенштейні, висвітлюючи її поточний стан, ключові тенденції та майбутні перспективи. У 2024 році в регіоні діяли 511 FinTech-компаній, що свідчить про певну стабілізацію ринку, оскільки зростання становило лише 1% порівняно з попереднім роком. Це може вказувати на насичення ринку в Швейцарії, тоді як Ліхтенштейн демонструє позитивну динаміку. Фінансування FinTech-сектору знизилося вдвічі порівняно з піковим 2022 роком і становило лише 300 млн CHF, що відображає зміну інтересу інвесторів.

Основні категорії продуктів включають платежі, депозити та кредитування, управління інвестиціями та банківську інфраструктуру. Використовувані технології охоплюють великі дані, штучний інтелект, розподілені реєстри (DLT) та квантові обчислення. Найбільше компаній працює у сфері управління інвестиціями (201 компанія) та банківської інфраструктури (185 компаній). Географічно основними FinTech-хабами є Цюрих (187 компаній), Цуг (125 компаній) та Женева (49 компаній). Цуг і Женева демонструють найшвидше зростання FinTech-компаній за період 2015–2024 років, тоді як у Цюриху спостерігається певне насичення ринку.

Висновки:

- Ризик стагнації FinTech-сектору у Швейцарії
  - Незначне зростання компаній та різке падіння фінансування вказують на ризик насичення ринку.
  - **Рекомендація:** диверсифікувати бізнес-моделі та залучати міжнародні інвестиції.
- Стійке зростання сектора Sustainable FinTech:
  - Кількість компаній, орієнтованих на ESG-фінансування, зросла на 84% за два роки.
  - **Рекомендація:** розширення державної підтримки та інвестицій у технологічні рішення для зеленої економіки.
- Глобалізація швейцарських FinTech-компаній:
  - 81% компаній працюють на міжнародному рівні, що свідчить про зростаючу конкуренцію.
  - **Рекомендація:** активне просування на нові ринки та співпраця з міжнародними регуляторами.
- Впровадження ШІ та DLT у фінансові сервіси:
  - Big Data, AI та блокчейн активно інтегруються у фінансові продукти.
  - **Рекомендація:** підготовка до регуляторних змін та інвестиції в інноваційні технології.

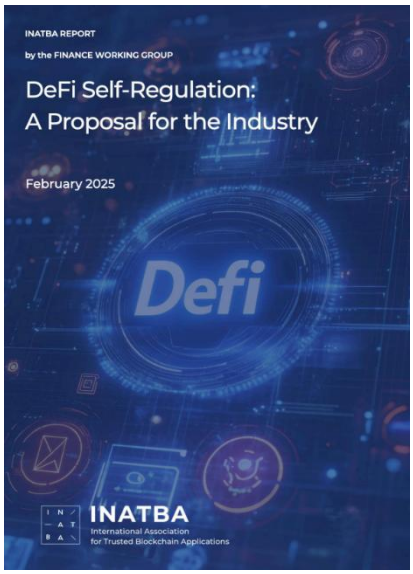
[9] https://www.handelszeitung.ch/sites/default/files/media/document/ifz_fintech_studie_2025.pdf

З точки зору бізнес-моделей, 58% компаній орієнтовані на B2B, тоді як B2C займає лише 6%. Зростає орієнтація на міжнародні ринки: 81% компаній працюють на глобальному рівні. Основні моделі монетизації включають SaaS (36%) та комісійну модель (31%), тоді як реклама та продаж даних поступово зникають. FinTech все більше інтегрується з InsurTech (46 компаній) та RegTech (63 компанії). Стійкий FinTech є швидкозростаючим напрямком: кількість компаній у цьому сегменті зросла на 84% за два роки, використовуючи ESG-аналітику та блокчейн-рішення для зеленої фінансової екосистеми.

Ринок криптоактивів у Швейцарії залишається активним, однак з'являються нові виклики, пов'язані з регулюванням. Впровадження штучного інтелекту у фінансовий сектор змінює бізнес-моделі, зокрема в автоматизованому управлінні активами. Частка жінок у керівництві FinTech-компаній повільно зростає, але становить лише 13% серед керівників та 9% у раді директорів, що значно нижче, ніж у традиційних банках.

Загалом, дослідження підкреслює необхідність адаптації FinTech-компаній до нових викликів, диверсифікації бізнес-моделей, залучення міжнародних інвестицій та впровадження інноваційних технологій для забезпечення сталого розвитку галузі.

## Майбутнє DeFi: Як саморегулювання може стати альтернативою традиційному фінансовому контролю[10]




Документ є комплексним дослідженням, яке аналізує ризики та перспективи саморегулювання у сфері децентралізованих фінансів (DeFi). Його автори висвітлюють ключові виклики, які постають перед індустрією, зокрема у сфері відповідності регуляторним вимогам, фінансової стабільності, безпеки смарт-контрактів та управління децентралізованими організаціями. Документ також містить пропозиції щодо механізмів, які можуть допомогти DeFi-протоколам стати більш стійкими до загроз без втручання традиційних фінансових регуляторів.

У вступній частині наголошується на важливості DeFi як нової парадигми фінансів, що пропонує автоматизовані, прозорі та глобально доступні фінансові послуги без залучення традиційних посередників. Водночас швидкий розвиток індустрії призводить до появи нових ризиків, серед яких вразливість смарт-контрактів, централізація управління, ризики ліквідності та регуляторна невизначеність. Автори підкреслюють, що традиційні підходи до фінансового регулювання не відповідають децентралізованій природі DeFi, що створює потребу у впровадженні саморегуляторних механізмів.

У подальшій частині документа розглядаються основні поняття, що стосуються DeFi, його відмінностей від централізованих фінансових послуг (CeFi) та традиційної фінансової системи (TradFi). Окремо аналізується поняття «справжньої децентралізації», що включає параметри, такі як структура управління, механізми голосування, розподіл токенів, контроль за оновленням смарт-контрактів, рівень залежності від централізованих платформ і джерел даних. Автори звертають увагу, що більшість сучасних DeFi-протоколів лише частково децентралізовані, що створює певні ризики для їх користувачів.

[10] https://inatba.org/wp-content/uploads/2025/02/SubWG3-Output-Web3-Self-Regulatory-Analysis-and-Proposal-2.pdf

Значна увага приділяється аналізу ризиків у DeFi. Вони класифікуються на стратегічні, операційні, фінансові та нові ризики, які виникають у зв'язку з використанням інноваційних технологій. Документ містить порівняльний аналіз ризиків DeFi та TradFi, демонструючи, що хоча деякі загрози є спільними для обох систем (наприклад, репутаційні ризики та ризик концентрації капіталу), інші є унікальними для DeFi, такі як ризик уразливостей смарт-контрактів, маніпуляції цінами через MEV, вразливості мостів між блокчейнами та можливість внутрішніх атак через централізоване управління DAO. Також зазначено, що ряд ризиків, характерних для TradFi, таких як шахрайство з боку співробітників, недобросовісні бізнес-практики та проблеми з ліквідністю, у DeFi значно знижені або відсутні через прозорість і автоматизовану природу смарт-контрактів.

Документ висуває пропозицію щодо впровадження саморегуляції DeFi, яка дозволить зберегти фінансову стійкість індустрії без необхідності запровадження надмірного державного контролю. До основних заходів саморегулювання пропонуються адміністративні, бізнес-орієнтовані, технічні та додаткові заходи безпеки. До адміністративних належать механізми звітності у реальному часі, стандарти запобігання конфлікту інтересів, правила розмежування активів користувачів і операційних рахунків протоколів. Бізнес-орієнтовані заходи передбачають впровадження зрозумілих політик управління протоколами та розкриття інформації про ключових стейкхолдерів. Технічні заходи зосереджені на забезпеченні безпеки DeFi-протоколів через стандартизовані аудити смарт-контрактів, регулярний аналіз ризиків і застосування механізмів запобігання шахрайським діям. Додатково пропонується створення єдиної платформи для моніторингу ризиків DeFi, яка дозволить аналізувати фінансову стійкість проєктів, їхню відповідність стандартам саморегулювання та рівень децентралізації.

**Висновки:**

- **DeFi потребує саморегуляції для забезпечення фінансової стабільності та уникнення надмірного державного контролю.** Регулювання повинно бути сфокусоване на централізованих посередниках, а не на самих DeFi-протоколах, щоб зберегти інноваційність галузі.
- **Впровадження прозорої фінансової звітності у реальному часі зменшить ризики шахрайства та забезпечить довіру до DeFi-протоколів.** Для цього необхідно створити індустріальний стандарт моніторингу фінансового стану децентралізованих платформ.
- **Ризики DeFi значно відрізняються від ризиків TradFi, і їх слід регулювати окремо.** Впровадження регуляторного принципу «ті ж ризики – ті ж правила» може бути хибним, оскільки DeFi має інші механізми управління ризиками.
- **Потрібно створити стандартизовані механізми аудиту смарт-контрактів та управління безпекою.** Це допоможе запобігати атакам на протоколи, маніпуляціям із цінами та шахрайським схемам у DeFi.

Документ також містить пропозиції щодо вдосконалення політики регулювання DeFi. Автори наголошують, що регуляторні зобов'язання повинні бути зосереджені на централізованих посередниках, таких як он-та офф-рампи, криптобіржі та зберігачі активів, а не на самих децентралізованих протоколах. Також вони пропонують розробку спеціальної категоризації DeFi-протоколів за рівнем їхньої децентралізації, щоб забезпечити адаптивний підхід до їх регулювання. Запропоновані ініціативи включають запровадження стандартів аудиту смарт-контрактів, використання Zero-Knowledge технологій для забезпечення приватності та механізмів блокування підозрілих транзакцій на рівні централізованих платформ.

У підсумку документ підкреслює, що DeFi має значний потенціал для створення більш прозорої, доступної та ефективної фінансової системи. Проте для того, щоб ця система була життєздатною, необхідне впровадження чітких стандартів

саморегулювання, які дозволять зменшити ризики без обмеження інновацій. Автори наголошують, що хоча DeFi на сьогодні є молодою індустрією з низкою викликів, у майбутньому розвиток технологій і правильне впровадження саморегуляторних механізмів дозволять значно знизити ризики, пов'язані з безпекою, регуляторною відповідністю та фінансовою стабільністю.

## Як технології формують майбутнє ексклюзивних брендів[11]


Звіт розглядає глибокий вплив технології блокчейн на індустрію розкоші, зосереджуючись на прозорості, автентифікації та інноваційних способах взаємодії з клієнтами. Автори досліджують, як сучасні споживачі змінюють свої вимоги, змушуючи бренди шукати нові рішення для збереження довіри та ексклюзивності. Блокчейн пропонує унікальні можливості для створення цифрових паспортів товарів, перевірки автентичності через децентралізовані системи та розвитку токенізованих програм лояльності.

Одним із ключових аспектів дослідження є розгляд блокчейну як засобу забезпечення довіри до брендів розкоші. Традиційно такі компанії будували свій статус на ексклюзивності та ручній майстерності, проте сучасний клієнт очікує більшої прозорості. Статистика свідчить, що 87% споживачів хочуть знати про походження товарів, а 66% готові платити більше за екологічно відповідальні продукти. Блокчейн дає змогу задовольнити ці вимоги завдяки незмінним записам про походження матеріалів, умови виробництва та екологічну відповідність продукції.

Другою вагомою проблемою, яку вирішує блокчейн, є боротьба з підробками. Фальсифіковані товари завдають індустрії розкоші збитків у мільярди доларів, а контрафактний ринок, за прогнозами, досягне 81 мільярда доларів до 2026 року. Блокчейн-технології, такі як цифрові сертифікати автентичності та інтеграція QR-кодів або NFC-чипів у вироби, дозволяють клієнтам перевіряти оригінальність продукції безпосередньо з мобільних пристроїв. Глобальні ініціативи, зокрема Aura Blockchain Consortium, створені LVMH, Prada та Cartier, впроваджують такі рішення в масштабах усієї індустрії. Крім того, деякі бренди, як-от Richemont, використовують блокчейн для миттєвої реєстрації інтелектуальної власності, що значно скорочує ризик плагіату.

Ще одним напрямком, у якому блокчейн трансформує індустрію, є персоналізація клієнтського досвіду. Сучасний ринок розкоші все більше орієнтується на глибоку взаємодію зі споживачем, пропонуючи йому не просто продукт, а ексклюзивний досвід. За допомогою блокчейну бренди створюють токенізовані програми лояльності, які дозволяють клієнтам отримувати унікальні бонуси, що можуть бути використані в будь-якій точці світу. Це усуває регіональні обмеження традиційних програм винагород. Деякі бренди йдуть ще далі, запроваджуючи NFT-членства, що відкривають доступ до закритих заходів, приватних показів колекцій та спеціальних пропозицій.

NFTs також змінюють концепцію ексклюзивності у розкоші. Проєкти, як-от Tiffany & Co. з NFTiffs, створюють нову категорію цифрових предметів розкоші, що поєднують реальні вироби та цифрові активи. Водночас Hublot у партнерстві з Takashi Murakami використовує NFT як механізм доступу до ексклюзивних годинників, а Hennessy інтегрує NFT у колекційні випуски коньяку. Однак не всі ініціативи були успішними — наприклад, Porsche зіткнулася з

[11] https://media.licdn.com/dms/document/media/v2/D4D1FAQHZA0v7kriV0w/feedshare-document-pdf-analyzed/B4DZVheqzfG8Ac-/0/1741097244033?e=1743638400&v=beta&t=q1lbDxd2RyCEmgW6Th7riCULMDIq__wEDZTVLiTs0zI

нерозумінням ринку через недосконалу комунікацію своїх NFT-пропозицій. Це підкреслює важливість стратегічного підходу до інтеграції блокчейн-рішень.

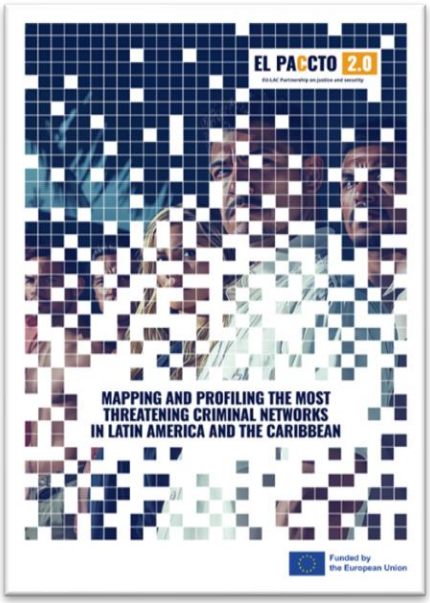
На тлі технологічних можливостей, звіт також аналізує виклики, що постають перед брендами при впровадженні блокчейну. Серед основних бар'єрів — висока вартість реалізації та потреба в освітній роботі зі споживачами. Незважаючи на очевидні переваги технології, багато клієнтів усе ще не повністю розуміють її функціональні можливості. Це вимагає від брендів активної комунікації щодо переваг блокчейну у контексті автентифікації та довіри. Іншою складністю є регуляторна невизначеність, оскільки закони щодо блокчейн-активів значно відрізняються у різних країнах.

У підсумку звіт робить висновок, що блокчейн — це не просто технологія, а стратегічний інструмент, який визначає майбутнє розкоші. Він допомагає зберігати ексклюзивність, водночас адаптуючи бренди до нової реальності цифрового світу. Найуспішнішими стануть ті компанії, які зможуть гармонійно інтегрувати блокчейн у свою бізнес-модель, зберігаючи баланс між традиційною майстерністю та інноваційними технологіями.

**Висновки:**

- **Прозорість і автентифікація є критично важливими для брендів розкоші.** Використання цифрових паспортів товарів (DPPs) підвищує довіру клієнтів та додає конкурентну перевагу.
- **Блокчейн — ефективний інструмент боротьби з підробками.** Впровадження NFT-сертифікації, NFC-чипів та QR-кодів у кожному виробі дозволяє клієнтам перевіряти його справжність.
- **NFT і токенізація відкривають нові моделі взаємодії з клієнтами.** Бренди можуть продавати токенізовані ексклюзивні пропозиції, такі як VIP-доступ до заходів або участь у спеціальних колекціях.
- **Ключем до успіху є кооперація та стандартизація.** Спільні ініціативи, такі як Aura Blockchain Consortium, дозволяють брендам зменшувати витрати на впровадження та створювати єдині стандарти прозорості.

## Тіньові імперії: Як злочинні мережі Латинської Америки загрожують безпеці Європи [12]




Документ є всебічним дослідженням, що аналізує сучасний ландшафт організованої злочинності в Латинській Америці та Карибському регіоні (ЛАК) та її зв'язки з Європою. Підготовлений у межах програми EL PACCTO 2.0 у співпраці з InSight Crime та European Multidisciplinary Platform Against Criminal Threats (EMPACT), звіт досліджує 28 найвпливовіших кримінальних мереж, які відіграють ключову роль у нелегальній економіці регіону, використовуючи як класичні форми організованої злочинності, так і новітні методи діяльності.

В останні роки спостерігається стрімке зростання співпраці між латиноамериканськими злочинними групами та європейськими кримінальними структурами. Головними сферами їхньої незаконної діяльності є контрабанда наркотиків, торгівля золотом, нелегальний видобуток корисних копалин, торгівля людьми та відмивання коштів.

[12] https://elpaccto.eu/wp-content/uploads/2025/02/ENG_Mapping-and-profiling-HRCN_LAC_Vpages.pdf

Злочинні організації з ЛАК дедалі активніше використовують мережевий підхід до своєї діяльності, де замість жорстко централізованих картелів функціонують високоспеціалізовані кримінальні суб'єкти, які взаємодіють у гнучких партнерствах. Це дозволяє злочинцям легко адаптуватися до правоохоронного тиску та підтримувати стабільні канали постачання незаконних товарів.

Методологія дослідження ґрунтується на багатовимірному аналізі, що враховує історію розвитку злочинних груп, географію їхньої діяльності, основні джерела доходу, внутрішню структуру, реакцію державних органів, рівень контролю над місцевими громадами, а також взаємозв'язки з міжнародними кримінальними мережами. Також у дослідженні розглянуто роль жінок та гендерний аспект у злочинних організаціях. Особливу увагу приділено зміні операційних моделей кримінальних угруповань, які тепер усе частіше покладаються на брокерів, фінансових посередників, корупційні зв'язки у правоохоронних органах, юридичну підтримку та цифрові технології для приховування незаконних операцій.

Документ містить детальні профілі 28 найбільш активних злочинних мереж, серед яких як великі транснаціональні структури на зразок картелю Sinaloa, Jalisco New Generation Cartel (CJNG) та Familia Michoacana, так і менші групи, що спеціалізуються на певних аспектах злочинної діяльності, наприклад, Roger Khan Network у Гаяні, яка здійснює операції з незаконного обігу наркотиків і відмивання грошей через офшорні рахунки. Окремі злочинні групи, такі як Cartel of the Suns у Венесуелі, діють у тісному зв'язку з корумпованими урядовими структурами, використовуючи державні ресурси для підтримки наркоторгівлі та нелегального експорту природних ресурсів.

Аналіз показує, що багато злочинних мереж ЛАК функціонують за принципом субпідряду, коли основні картелі делегують виконання окремих операцій меншим групам. Це зменшує ризик втрат у разі арештів або операцій правоохоронних органів, оскільки загальна структура залишається гнучкою. Наприклад, Gulf Cartel (CDG) та Los Huistas у Гватемалі все частіше залучають сторонні організації для транспортування наркотиків через Центральну Америку до Мексики та США, що ускладнює їхнє відслідковування та ліквідацію.

Значна частина документу присвячена аналізу змін у маршрутах наркотрафіку. Традиційні маршрути через Карибський регіон залишаються важливими, проте злочинці дедалі частіше використовують нові транзитні шляхи через Африку, особливо через Гвінею-Бісау, Малі та Нігерію, що дозволяє переправляти наркотики з Південної Америки до Європи, минаючи традиційні правоохоронні

**Висновки:**

- **Боротьба з нелегальними фінансовими потоками та відмиванням коштів.** Необхідно посилити контроль над підставними компаніями, особливо в зонах офшорного фінансового регулювання. Впровадження суворіших стандартів KYC (Know Your Customer) та EDD (посилена перевірка клієнта).
- **Посилення міжнародної координації у правоохоронній сфері.** Спільні операції між Європолом, правоохоронними органами Латинської Америки та фінансовими регуляторами. Використання AI та Big Data для виявлення мережевого аналізу злочинних фінансових потоків.
- **Боротьба з корупцією у державних органах.** Розробка міжнародних антикорупційних механізмів для контролю впливу злочинних угруповань на політичні структури. Санкції проти високопосадовців, пов'язаних із картелями.
- **Адаптація стратегії боротьби з кримінальними мережами до нових реалій.** Врахування децентралізованої природи злочинності та націлення не тільки на великі картелі, а й на фінансові брокерів, адвокатів, бухгалтерів, які їх обслуговують. Підвищення рівня безпеки для свідків і захист викривачів корупції.

механізми. Крім того, роль Бразилії та Уругваю як експортних хабів для наркотиків значно зросла, що змушує країни ЄС переглядати свої підходи до боротьби з трансконтинентальною наркоторгівлею.

Корупція в державних органах є однією з головних причин процвітання кримінальних мереж. У багатьох країнах ЛАК злочинці досягають стратегічного контролю над правоохоронними структурами, використовуючи хабарі, погрози або насильство. Венесуела, Мексика, Гондурас і Колумбія залишаються найвразливішими до проникнення кримінальних структур у державний апарат. Наприклад, у Венесуелі, за даними звіту, Cartel of the Suns тісно пов'язаний із високопосадовими військовими та урядовими чиновниками, що дає йому змогу контролювати великі обсяги наркотрафіку без загрози втручання державних органів.

Документ також звертає увагу на економічні наслідки діяльності злочинних угруповань. Їхня активність не тільки сприяє поширенню насильства, а й має руйнівний вплив на економічний розвиток регіону. Масштабне відмивання коштів через офшорні компанії, корумповані банки та криптовалютні біржі спотворює фінансові ринки та ускладнює притягнення інвестицій. За даними Europol, 86% європейських кримінальних мереж використовують підставні компанії для легалізації доходів, що свідчить про системну проблему глобального масштабу.

Підсумовуючи, документ окреслює ключові напрями боротьби з транснаціональною злочинністю. Серед основних рекомендацій – посилення міжнародної координації між правоохоронними органами ЛАК та ЄС, запровадження жорсткіших механізмів фінансового моніторингу, створення спеціалізованих антикорупційних підрозділів для боротьби з проникненням злочинців у державний апарат, а також удосконалення механізмів відстеження нелегальних фінансових потоків через криптовалютні транзакції та офшорні рахунки.

Звіт є важливим аналітичним інструментом для урядів, фінансових розвідок та міжнародних організацій, які працюють над нейтралізацією загроз, що походять від високоризикових злочинних мереж. Він не тільки детально описує поточний стан організованої злочинності в ЛАК, а й дає чітке розуміння того, як саме ці структури адаптуються до змін у глобальній правоохоронній та фінансовій політиці.

# ВНУП

## Ризики фінансування розповсюдження зброї масового знищення (ФР) та заходи для їх мінімізації

Фінансування розповсюдження зброї масового знищення є однією з критичних загроз для глобальної безпеки, і роль визначених нефінансових установ та професій, у запобіганні цьому ризику стає все більш значущою. ВНУП можуть ненавмисно стати інструментами для фінансування розповсюдження. Саме тому їхня здатність впроваджувати ефективні заходи з оцінки ризиків, виявлення підозрілих операцій і дотримання режиму санкцій має першорядне значення.

### Основи ризику ФР для ВНУП

Фінансування розповсюдження включає забезпечення фінансових ресурсів, економічних активів або інших засобів для підтримки програм, пов'язаних з розробкою, виробництвом або транспортуванням зброї масового знищення (ЗМЗ). ЗМЗ охоплює ядерну, хімічну та біологічну зброю, а також засоби її доставки. Зловмисники можуть використовувати легальні структури для приховування своїх операцій, включаючи офшорні компанії, трасти, підставні фірми або складні фінансові та торговельні механізми.

### ВНУП можуть бути залучені в такі процеси:

- Юридичне оформлення та управління компаніями – створення підставних компаній або складних корпоративних структур, які приховують кінцевих бенефіціарів.
- Торгівля нерухомістю – використання дорогих об'єктів нерухомості для приховування руху коштів або їх легалізації.
- Операції з дорогоцінними металами та камінням – купівля та продаж високоліквідних активів для переведення коштів.
- Бухгалтерські та фінансові послуги – надання консультативних та аудиторських послуг для компаній, що можуть бути причетні до ФР.

Зважаючи на це, ВНУП зобов'язані проводити оцінку ризиків ФР у своїй діяльності, ідентифікувати червоні прапорці та вживати заходи належної перевірки клієнтів (CDD) та посиленої перевірки (EDD).

### Оцінка ризику ФР у діяльності ВНУП

ВНУП повинні проводити системну оцінку ризиків ФР, яка включає:

- Ідентифікацію загроз – осіб, організацій та юрисдикцій, які можуть використовувати ВНУП для фінансування розповсюдження.
- Визначення вразливостей – факторів, що можуть сприяти обходу санкцій та використанню сектору ВНУП у злочинних схемах.
- Оцінку наслідків – потенційного використання коштів або активів для незаконного придбання чутливих технологій і матеріалів.

Основні джерела ризику охоплюють географічні, клієнтські та продуктові чинники. Наприклад, робота з клієнтами з високоризикових юрисдикцій, відсутність прозорої структури власності або використання компаній, які можуть бути пов'язані з підсанкційними особами, збільшує ризик ФР.

### Зобов'язання ВНУП щодо санкцій та ЦФС (Цільових фінансових санкцій)

Окрему увагу слід приділити дотриманню режиму цільових фінансових санкцій, встановлених ООН та місцевими регуляторами. ВНУП повинні забезпечувати:

- Перевірку клієнтів та транзакцій на відповідність санкційним спискам (особливо щодо Росії, Північної Кореї, Ірану та пов'язаних з ними осіб).
- Заморожування активів осіб, які потрапляють під санкції.
- Неможливість надання фінансових чи нефінансових послуг особам або компаніям, що перебувають під санкціями.

### Механізми протидії ФР у ВНУП

Щоб ефективно зменшити ризики ФР, ВНУП мають впровадити такі заходи:

- Запровадження політик та процедур боротьби з ФР, інтегрованих у загальну політику ПВК/ФТ.
- Здійснення CDD з фокусом на кінцевих бенефіціарних власниках (КБВ) та джерелах фінансування.
- Здійснення EDD для клієнтів із високим ризиком – включає детальну перевірку фінансових потоків, бізнес-діяльності та зв'язків із підсанкційними юрисдикціями.
- Моніторинг транзакцій – особливо у випадках великих, незвичайних або нестандартних операцій.
- Обов'язкове звітування про підозрілі транзакції (STR) до відповідних державних установ.
- Постійне навчання персоналу для підвищення обізнаності щодо схем ФР, червоних прапорців та змін у законодавстві.

### Червоні прапорці ФР у ВНУП

ВНУП мають звертати увагу на наступні сигнали потенційної участі у ФР:

- Робота з клієнтами із підсанкційних юрисдикцій (Росія, Іран, Північна Корея).
- Нетипові або надто заплутані корпоративні структури, які не мають очевидного економічного обґрунтування.
- Використання компаній-посередників у країнах, які не є кінцевими місцями доставки товарів.
- Невідповідність між діяльністю компанії та видами товарів, що імпортуються/експортуються.
- Використання підроблених або змінених торгових документів.
- Часті транзакції через рахунки третіх осіб без логічного економічного обґрунтування.

**Висновки:**

- **ВНУП повинні інтегрувати оцінку ризиків ФР у свої процедури ПВК/ФТ.** Це означає розробку спеціальних політик, зосереджених на виявленні та мінімізації ризиків, пов'язаних із ФР.
- **Належна перевірка клієнтів (CDD) та виявлення кінцевих бенефіціарів (КБВ) є критичними.** ВНУП повинні проводити належну перевірку клієнтів, особливо тих, хто здійснює міжнародні торгові операції.
- **Обов'язковий моніторинг та звітування про підозрілі операції (STR).** ВНУП мають впроваджувати системи контролю та вчасно повідомляти регуляторів про будь-які підозрілі фінансові потоки.
- **Тренінги та підвищення кваліфікації персоналу є необхідними для ефективної протидії ФР.** ВНУП мають інвестувати у навчання своїх співробітників, щоб вони могли ідентифікувати червоні прапорці та реагувати на загрози ФР.

Таким чином, ефективна боротьба з ФР вимагає всебічного підходу, який включає оцінку ризиків, моніторинг транзакцій, перевірку клієнтів та активну співпрацю з регуляторами. ВНУП, будучи частиною системи фінансового контролю, мають безпосередню відповідальність за запобігання використанню їхніх послуг в контексті здійснення незаконної діяльності.

## Інші новини

### Тіньові ставки: Як нелегальний онлайн-гемблінг захоплює Європу [13]

Документ є результатом масштабного журналістського розслідування, що висвітлює проблеми стрімкого зростання онлайн-гемблінгу в Європі та його тіньової складової. Незважаючи на привабливий образ індустрії, який формується через агресивні маркетингові кампанії, бонусні пропозиції та спонсорство спортивних заходів, реальна картина значно похмуріша. За лаштунками цього багатомільярдного бізнесу ховається відсутність належного регулювання, офшорні рахунки, ухилення від судових рішень та зростаюча соціальна криза, пов'язана з ігровою залежністю.

[13] https://www.investigate-europe.eu/themes/investigations/shady-bets-europe-gambling-industry

За останні п’ять років доходи онлайн-гемблінгу в Європейському Союзі зросли на понад 200%, сягнувши приблизно 20–21,2 мільярда євро, проте ці цифри відображають лише офіційний сектор. Насправді значна частина цього ринку залишається в тіні, працюючи через нелегальні платформи, які не мають необхідних ліцензій та діють через офшорні юрисдикції. Розслідування виявило велику мережу таких сайтів, які отримують мільйони відвідувань щомісяця, попри заборони та численні судові позови. Такі платформи не тільки залишають гравців без жодного захисту, але й сприяють ухиленню від податків та відмиванню коштів.

Окрему увагу в документі приділено ролі Мальти, яка стала ключовою юрисдикцією для гемблінгових компаній у Європі. Законодавство країни дозволяє операторам уникати судових рішень інших держав, фактично роблячи її безпечним притулком для великих гемблінгових корпорацій. Завдяки сприятливому регулюванню та мінімальному контролю з боку ЄС, Мальта створила умови, за яких компанії можуть уникати фінансових та правових наслідків своєї діяльності, незважаючи на тисячі скарг від постраждалих гравців по всій Європі.

Ще одним важливим аспектом, висвітленим у документі, є відсутність загального європейського регулювання у сфері онлайн-гемблінгу. Експерти Всесвітньої організації охорони здоров’я називають ситуацію «диким заходом», оскільки кожна країна ЄС має власний підхід до регулювання, що ускладнює боротьбу з нелегальними операторами та мінімізує можливість захисту споживачів. Відсутність єдиних правил дозволяє великим гральним корпораціям використовувати прогалини у законодавстві та продовжувати працювати навіть там, де їх діяльність заборонена.

Окремо документ розкриває проблему, пов’язану з негативними соціальними наслідками зростання онлайн-гемблінгу. Дослідження, опубліковане у The Lancet, наголошує на необхідності розглядати гемблінг як загрозу громадському здоров’ю, на рівні з алкоголем та тютюном. Безконтрольна діяльність операторів сприяє зростанню залежності серед молоді та вразливих категорій населення, а маркетингові стратегії гральних компаній активно експлуатують психологічні тригери, що стимулюють користувачів до азартних ставок. Водночас відсутність належного контролю та механізмів соціальної відповідальності операторів означає, що величезні прибутки, які вони отримують, не використовуються для фінансування програм боротьби з ігровою залежністю чи підтримки постраждалих.

Крім того, у звіті міститься інформація про те, як великі фінансові установи, такі як Mastercard і Visa, пов’язані з нелегальними гемблінговими сайтами, сприяючи обігу коштів у цій тіньовій сфері. Використання анонімних платіжних методів, таких як криптовалюти та офшорні рахунки, значно ускладнює моніторинг транзакцій, що

**Висновки:**

- **Відсутність єдиного регулювання в ЄС сприяє зростанню нелегального ринку** - Брак загальноєвропейських норм дозволяє гемблінговим компаніям використовувати правові прогалини, працюючи через офшорні юрисдикції та ухиляючись від відповідальності.
- **Мальта стала головним центром захисту гемблінгових компаній** - Місцеве законодавство фактично блокує виконання судових рішень інших країн ЄС, дозволяючи операторам уникати фінансових санкцій та зобов’язань перед споживачами.
- **Гемблінгова індустрія посилює фінансові злочини та відмивання коштів** - Використання офшорних рахунків, криптовалют і міжнародних платіжних систем, таких як Visa та Mastercard, сприяє незаконним фінансовим потокам.
- **Азартні ігри стали серйозною загрозою для суспільного здоров’я** - Відсутність ефективного контролю та агресивні маркетингові стратегії сприяють зростанню ігрової залежності, особливо серед молоді та вразливих груп населення.

створює сприятливі умови для фінансових злочинів, включаючи відмивання коштів та ухилення від податків.

Таким чином, дослідження демонструє масштабну проблему, що потребує негайного втручання як на рівні окремих держав, так і на рівні ЄС. Відсутність ефективного контролю призводить до поглиблення кризових явищ у суспільстві, від фінансових злочинів до загострення проблем громадського здоров'я. Розслідування чітко показує, що без єдиної європейської стратегії, посиленого фінансового моніторингу та жорсткішого регулювання реклами та платіжних механізмів, ситуація лише погіршуватиметься.

## Жінка визнає себе винною у шахрайській схемі з обману сім'ї Елвіса Преслі [14]

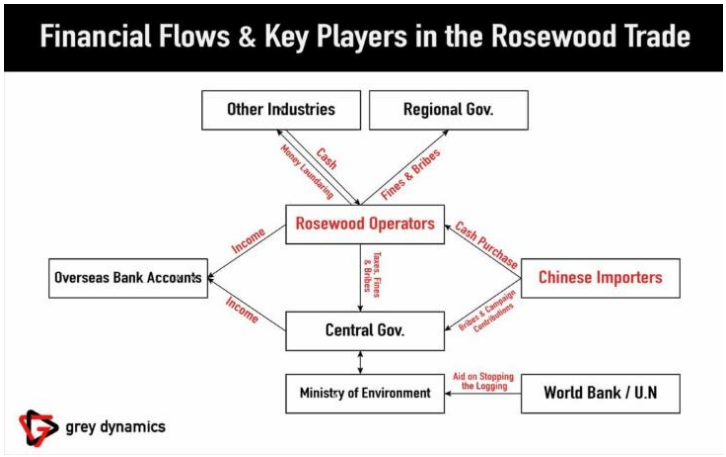
Прес-реліз Міністерства юстиції США, датований 25 лютого 2025 року, який детально описує визнання вини Ліси Джанін Фіндлі, 53-річної мешканки міста Кімберлінг-Сіті, штат Міссурі, у справі про шахрайську схему, спрямовану на обман сім'ї Елвіса Преслі та спробу заволодіння їхньою власністю — маєтком Graceland у Мемфісі, штат Теннессі. У документі зазначається, що Фіндлі організувала складну аферу, в рамках якої вона намагалася провести фіктивний продаж Graceland, використовуючи підроблені документи, фальшиву компанію та сфабриковані судові позови. Її схема базувалася на неправдивому твердженні, що дочка Елвіса Преслі, яка вже померла, нібито заклала Graceland як заставу за кредит, який не був погашений. Погрожуючи вилученням маєтку та його продажем на аукціоні, Фіндлі вимагала від сім'ї Преслі виплати значної суми для "врегулювання" вигаданої заборгованості. Ця зухвала спроба шахрайства мала на меті не лише фінансову вигоду в мільйони доларів, а й позбавлення сім'ї культової спадщини, пов'язаної з Елвісом Преслі.

Фіндлі визнала свою провину за одним пунктом обвинувачення у поштовому шахрайстві — злочині, який у США класифікується як федеральний і передбачає суворе покарання. Її вирок призначено на 18 червня 2025 року, і вона може бути засуджена до максимального терміну в 20 років ув'язнення. Остаточне рішення про покарання ухвалить федеральний суддя Західного округу Теннессі, враховуючи рекомендації федеральних настанов щодо винесення вироків та інші законодавчі фактори. Розслідування справи проводили Поштова інспекційна служба США (USPIS) та ФБР (офіс у Нешвіллі), що підкреслює залучення кількох федеральних агентств до розкриття цього злочину. Прокуратуру представляють співробітники Відділу боротьби з шахрайством Кримінального підрозділу Міністерства юстиції, а також помічник прокурора Західного округу Теннессі, за підтримки інших юристів, які брали участь у розслідуванні та підготовці справи.

[14] https://www.justice.gov/opa/pr/woman-pleads-guilty-scheme-defraud-elvis-presleys-family

## Для загального розвитку

### Техніки ВК: Відмивання коштів на основі торгівлі Палісандром[15]




Незаконна торгівля палісандром – це не лише екологічний злочин. Це також головний фактор відмивання грошей і навіть фінансування тероризму. Ця багатомільярдна індустрія процвітає завдяки корупції, ухиленню від сплати податків і фінансовій таємниці.

Злочинні мережі використовують слабке законодавство, щоб інтегрувати прибутки від незаконної вирубки в офіційну економіку, використовуючи компанії-оболонки, офшорні рахунки та TBML.

Як працює схема:

1. Оператори палісандрового виробництва, які часто підтримуються злочинними компаніями, незаконно збирають захищену деревину. Вони ухиляються від правил лісового господарства та вирубують величезну кількість палісандру, переважно в Африці та Південно-Східній Азії.
2. Щоб забезпечити безперебійну роботу, вони підкуповують чиновників регіональної влади, сплачуючи хабарі, щоб отримати дозволи на перевезення.
3. Заготовлене рожеве дерево потім оптом продається китайським імпортерам, які часто купують за готівку, щоб уникнути банківської перевірки. Потім ця готівка повертається назад у злочинну мережу.
4. Незаконні доходи від продажу рожевого дерева потім відмиваються через кілька каналів:
   - Частина грошей надсилається на закордонні банківські рахунки, де інтегрується в інші підприємства або використовується для фінансування додаткової незаконної діяльності.
   - Частина спрямовується в інші галузі, приховуючи походження коштів через законні бізнес-операції.
   - Деякі кошти надходять до центральних державних установ під виглядом податків, надаючи легітимності транзакціям, одночасно зміцнюючи корупцію в офіційних структурах.
5. Центральна влада, збираючи доходи від цієї діяльності, також сприйнятлива до корупції. Хабарі та внески на виборчі кампанії гарантують, що політика залишається сприятливо налаштованою до незаконних операцій з лісозаготівлі.
6. Тим часом міжнародні організації, такі як Світовий банк та ООН, надають допомогу, щоб зупинити незаконну вирубку. Однак через системну корупцію частина цієї допомоги привласнюється або не має значного впливу.

Червоними прапорцями щодо відмивання коштів у торгівлі рожевим деревом можуть бути:

- Великі готівкові операції в мережах поставок деревини

[15] https://www.thetelegraphandargus.co.uk/news/24980520.fowler-oldfield-four-guilty-266m-money-laundering-plot/

- Використання компаній-оболонок для приховування права власності на лісозаготівельний бізнес
- Розбіжності між задекларованим і фактичним експортом деревини
- Виплати публічним діячам у країнах високого ризику
- Часті перекази коштів на офшорні банківські рахунки, пов’язані з лісозаготівельними компаніями

Найкращі методи боротьби з цією схемою:

- Посилена належна перевірка секторів високого ризику, таких як деревина та лісозаготівля
- Посилення систем моніторингу торгівлі для виявлення шахрайства з рахунками
- Підвищення прозорості бенефіціарної власності лісозаготівельних компаній
- Транскордонне співробітництво для відстеження незаконних фінансових потоків, пов’язаних із екологічними злочинами

## Запрошуємо до обговорення

1. Чи готові суб’єкти приватного сектору в Україні до впровадження повноцінного державно-приватного партнерства (PPP) у сфері ПВК/ФТ? Які бар’єри найбільше перешкоджають співпраці з державою?

2. Чи є сьогоднішні механізми KYC достатніми для боротьби з феноменом "грошових мулів"? Які технології та алгоритми верифікації могли б стати ефективнішими?

3. Чи мають ВНУП в Україні належну обізнаність та ресурси для виконання своїх зобов’язань з ПВК/ФТ на практиці? Які формати навчання чи підтримки могли б бути ефективними?

4. Які переваги і ризики несе з собою концепція токенізованих CBDC для національної фінансової системи?

5. Чи мають місце у вашій практиці випадки спроб обходу санкцій через використання криптовалют? Як ви реагуєте на них і які інструменти виявилися найефективнішими?

6. Чи достатньо міжнародної координації в боротьбі з незаконним обігом радіоактивних матеріалів? Які конкретні функції могли б взяти на себе органи влади в цій сфері?

7. Як слід адаптувати методики виявлення та розслідування фінансових злочинів в умовах, коли організована злочинність активно співпрацює з гібридними загрозами, використовуючи криптовалюти, DeFi, фіктивні компанії та молодь як "грошових мулів"?

8. Чи існують у вашій практиці приклади того, як злочинні мережі діють як проксі для зовнішніх державних або недержавних акторів? Які інструменти виявилися найбільш ефективними при спробах розплутати такі схеми?

## Контактуйте щодо цього документу з Міністерством фінансів України:


- **Email:** AML_Bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-12


Бюлетень є волонтерською розробкою методологічної команди Міністерства фінансів України відповідно до частини 8 статті 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

Щоб отримати доступ до інших Методологічних Бюлетенів – перейдіть за посиланням [офіційний веб-сайт Міністерства фінансів].