Методологічний бюлетень

Серійний номер: МінФін-AML-2025-07

Лютий 2025

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

Фармацевтична злочинність у ЄС: як підроблені ліки загрожують здоров'ю, економіці та безпеці [1]

Звіт Europol є ґрунтовним дослідженням проблеми фармацевтичної злочинності, яка становить значну загрозу як для здоров'я населення, так і для економічної стабільності фармацевтичної галузі в ЄС та за його межами. Документ детально описує способи, якими організовані злочинні угруповання використовують вразливості фармацевтичного ринку для незаконного прибутку, завдаючи шкоди легітимному бізнесу та підриваючи довіру до медичної системи.

Основним об'єктом фармацевтичної злочинності є інтелектуальне піратство та підробка ліків, які включають субстандартні, неправильно марковані або повністю фальсифіковані медичні засоби. Така продукція або не містить активних речовин, або ж містить небезпечні для здоров'я інгредієнти. Зростаючий попит на медичні препарати, особливо в умовах дефіциту та обмеженого

[1] https://www.europol.europa.eu/publications-events/publications/threat-of-pharmaceutical-crime-in-eu-and-beyond

доступу до ліків, створює сприятливі умови для незаконного ринку, яким активно користуються злочинні організації.

Звіт наголошує, що фармацевтична злочинність має глобальний характер і підтримується добре організованими злочинними мережами. Ці угруповання функціонують за принципами бізнес-структур, з чітким розподілом ролей та широкою мережею посередників. Серед ключових злочинних процесів звіт виділяє виробництво підроблених ліків, організоване як у невеликих підпільних лабораторіях у країнах ЄС, так і на великих підприємствах в Азії та Туреччині. У таких виробництвах не дотримуються жодних стандартів безпеки, що створює ризики не лише для кінцевих споживачів, але й для екології через небезпечні відходи.

Окремий акцент зроблено на інфільтрації злочинців у легальний ланцюг постачання лікарських засобів. Часто справжні ліки потрапляють у нелегальний обіг через корумпованих співробітників аптек, лікарень, логістичних компаній та фармацевтичних підприємств. Крадіжки ліків можуть відбуватися на будь-якому етапі – від виробництва до транспортування та реалізації в аптеках. Одним із найпоширеніших методів отримання легальних ліків є фальсифікація рецептів, що дозволяє злочинцям отримувати великі партії препаратів для подальшого перепродажу або незаконного використання.

У звіті підкреслюється, що онлайн-продажі та соціальні медіа стали основними каналами розповсюдження нелегальних ліків. Даркнет, тимчасові вебсайти, соціальні мережі та месенджери використовуються злочинцями для продажу підроблених препаратів, що значно ускладнює їхнє відстеження правоохоронними органами. Онлайн-реклама фальшивих ліків часто маскується під законні пропозиції, а маркетинг здійснюється через впливових осіб у соціальних мережах, які пропагують такі товари як "натуральні добавки" або "альтернативну медицину".

Серед основних категорій лікарських засобів, що піддаються фальсифікації та нелегальному продажу, звіт виділяє антиконвульсанти, синтетичні опіоїди (зокрема фентаніл і трамадол), протиракові препарати, засоби для лікування еректильної дисфункції, антидіабетичні засоби (особливо семаглутід), гормональні та стероїдні препарати, анальгетики, снодійні та антивірусні засоби. Однією з нових тенденцій є різке зростання нелегального попиту на семаглутід, який призначений для лікування діабету, але масово використовується людьми для швидкої втрати ваги. Це створює штучний дефіцит препарату, який злочинці використовують для завищення цін на чорному ринку.

Europol зазначає, що боротьба з фармацевтичною злочинністю потребує міжнародної співпраці та координації зусиль правоохоронних органів, регуляторів, фармацевтичної індустрії та технологічних компаній. Успішним

Висновки:

- **Фармацевтична злочинність зростає через високий попит та низькі ризики для злочинців:** необхідне посилення кримінального переслідування, посилення покарань за розповсюдження підроблених ліків та розширення міжнародної співпраці.
- **Соціальні медіа та даркнет є основними каналами збуту нелегальних ліків:** необхідна тісніша співпраця між правоохоронними органами та великими технологічними компаніями для моніторингу та блокування нелегальних продажів.
- **Підроблені ліки загрожують громадському здоров'ю та створюють глобальні ризики:** державам слід посилити контроль за імпортом лікарських засобів та покращити систему відстеження оригінальності препаратів.
- **Кримінальні групи використовують корупцію та інфільтрацію в легальні бізнеси для нелегальної діяльності:** необхідно впровадити ефективні механізми перевірки та контролю у фармацевтичному секторі, включаючи антикорупційні заходи.

прикладом є Операція SHIELD, яка об'єднала правоохоронні органи 30 країн і призвела до масштабних вилучень нелегальних медичних препаратів. Такі операції є важливим інструментом у боротьбі з фармацевтичною злочинністю, проте проблема залишається гострою через високий попит на нелегальні ліки.

Звіт завершується аналізом перспектив розвитку фармацевтичної злочинності. Очікується, що в майбутньому ця проблема лише загострюватиметься через постійне зростання попиту на медичні препарати, особливо ті, що використовуються для схуднення, покращення фізичних можливостей та рекреаційного вживання. Навіть попри посилення законодавства, злочинці продовжуватимуть знаходити способи обійти систему, використовуючи корупцію, технології та анонімні онлайн-канали продажу.

Europol наголошує, що ефективна боротьба з фармацевтичною злочинністю вимагає поєднання жорстких законодавчих заходів, посилення контролю за ланцюгом постачання, технологічного моніторингу онлайн-платформ та міжнародного співробітництва. Лише скоординована відповідь на цю загрозу зможе мінімізувати ризики для здоров'я громадян, економіки та безпеки суспільства загалом.

Фінансовий слід фентанілу: як відмиваються мільйони від торгівлі синтетичними опіоїдами [2]

Документ, підготовлений FINTRAC, є стратегічним аналітичним дослідженням, спрямованим на виявлення схем відмивання коштів, отриманих від незаконного виробництва, поширення та продажу синтетичних опіоїдів, зокрема фентанілу. Цей документ замінює минуле попередження 2018 року та містить оновлені індикатори ризику, засновані на аналізі фінансових транзакцій, звітів про підозрілі операції та інформації від правоохоронних органів.

Фентаніл та інші синтетичні опіоїди спричинили серйозну кризу передозувань у Північній Америці, що посилюється через їхню високу летальність і швидке поширення на чорному ринку. За оцінками, близько 80 000 осіб щорічно помирають через опіоїдну залежність, що стало причиною активізації міжнародного співробітництва у боротьбі з незаконним обігом наркотиків та супутнім фінансовим злочинами. FINTRAC спільно з партнерами реалізує ініціативу Project Guardian, метою якої є підвищення обізнаності про проблему відмивання доходів від синтетичних опіоїдів та покращення механізмів ідентифікації відповідних фінансових потоків.

Документ містить глибокий аналіз методів фінансування незаконного виробництва фентанілу та його розповсюдження. Раніше основний шлях потрапляння фентанілу до Північної Америки пролягав через імпорт з Китаю, проте останніми роками злочинні організації в Канаді, США та Мексиці почали самостійно виробляти синтетичні опіоїди, використовуючи прекурсори, які ввозяться з Азії. Діяльність цих організацій координується через міжнародні злочинні мережі, які використовують підставні компанії, онлайн-платформи, криптовалютні транзакції, а також нелегальні лабораторії, що працюють під прикриттям фармацевтичних, хімічних або харчових підприємств.

FINTRAC ідентифікував основні методи відмивання коштів, пов'язаних із незаконним обігом синтетичних опіоїдів. Виявлено, що ключові фінансові операції включають використання

[2] https://fintrac-canafe.canada.ca/intel/operation/iso-osi-eng

дрібних грошових переказів (тактика "cash smurfing"), а також активне застосування криптовалют, зокрема Bitcoin, Ethereum, Tether та USD Coin, які використовуються для розрахунків із постачальниками прекурсорів і наркотиків у "даркнеті". Віртуальні активи дозволяють злочинцям обходити традиційні фінансові системи, ускладнюючи виявлення підозрілих транзакцій. Окремо наголошується на залученні онлайн-гемблінгу, де кошти, отримані від продажу наркотиків, відмиваються через ставки та виграші на азартних платформах, зокрема через платіжні процесори в Канаді, Великій Британії та Мальті.

Документ аналізує маршрути руху коштів у процесі відмивання, включаючи схеми транзитних переказів через рахунки третіх осіб (номіналів), операції з обготівковування та використання офшорних зон. Ідентифіковано основні регіони, які відіграють ключову роль у виробництві та розповсюдженні фентанілу. Основними точками зосередження виробництва залишаються Британська Колумбія та південні регіони Онтаріо, а зростання активності мексиканських картелів у Канаді свідчить про розширення транснаціональної торгівлі наркотиками.

Документ також містить рекомендації для фінансових установ щодо ідентифікації підозрілих транзакцій та клієнтських профілів, які можуть бути пов’язані з незаконним обігом синтетичних опіоїдів. FINTRAC надає конкретні індикатори підозрілих операцій, зокрема різкі та нелогічні зміни в транзакційній активності, часті міжнародні перекази на рахунки, пов’язані з хімічними компаніями в Китаї, Індії або Східній Європі, використання криптовалютних міксерів та платформ P2P, а також значні обсяги операцій через платіжні процесори, пов'язані з онлайн-казино.

Окрему увагу приділено схемам нелегального виробництва фентанілу, в яких залучаються лабораторії, що офіційно працюють у сфері фармацевтики, харчових добавок або сільськогосподарської хімії, але фактично використовуються для синтезу наркотиків. FINTRAC виявив випадки використання віртуальних адрес для доставки прекурсорів, оренди складів і лабораторій через номінальних осіб, а також транзиту хімічних речовин через посередників у Гонконгу, Сінгапурі та Південній Кореї.

Висновки:

- **Необхідність підвищеної уваги до віртуальних валют:** Віртуальні валюти (наприклад, Bitcoin, Ethereum) використовуються для закупівлі прекурсорів наркотиків та для переміщення коштів через кордони. Встановлення ліній моніторингу таких транзакцій допоможе виявити фінансові потоки, пов'язані з нелегальним обігом синтетичних опіоїдів.
- **Інтеграція методів виявлення відмивання коштів через криптовалютні обміни:** Підозрілі операції, пов'язані з криптовалютними біржами та змішуванням транзакцій, повинні бути предметом пильного контролю. Фінансові установи повинні навчатися відрізняти звичайні фінансові операції від тих, що можуть бути пов'язані з незаконними активностями.
- **Фокус на підозрілі банківські транзакції та бізнеси, що використовуються для відмивання коштів:** Підозрілі рухи коштів через підконтрольні особи, використання підставних компаній та часті великі транзакції через онлайн-казино або псевдозаконні підприємства є чіткими індикаторами нелегальної діяльності.

Розподіл синтетичних опіоїдів здійснюється через чітко організовані логістичні маршрути. Виявлено, що транспортні компанії, які працюють з готівкою, можуть використовуватися для перевезення наркотиків, а підставні фірми забезпечують покриття для нелегальної торгівлі. Для мікротрафікерів (дрібних дилерів) особливу роль відіграють поштові та кур’єрські сервіси, що дозволяють відправляти невеликі партії наркотиків споживачам, маскуючи їх під звичайні товари.

Окрім викладення фактів і схем, документ містить рекомендації для суб'єктів фінансового моніторингу, зокрема щодо посилення аналітики транзакційних даних, використання штучного інтелекту для відстеження аномальних патернів, а також посилення міжнародної співпраці між фінансовими установами та правоохоронними органами для обміну інформацією про відмивання коштів, пов'язаних з наркотрафіком. FINTRAC підкреслює важливість інтеграції цих знань у ризик-орієнтований підхід до фінансового моніторингу, оскільки саме аналіз сукупності факторів, а не поодиноких індикаторів, дозволяє виявляти складні схеми відмивання коштів.

Загалом, цей аналітичний звіт є важливим інструментом для виявлення зв'язків між фінансовими потоками та незаконним виробництвом синтетичних опіоїдів, пропонуючи конкретні механізми для вдосконалення фінансового моніторингу та боротьби з цим видом злочинності.

Революція у боротьбі з шахрайством: нові регуляторні механізми та санкції у соціальній сфері Великої Британії [3]

Документ, опублікований 20 січня 2025 року Комісією з азартних ігор Великої Британії (Gambling Commission), є офіційним попередженням щодо виявлення випадків використання ліцензованого ігрового програмного забезпечення на нелегальних ринках. Основна проблема, на яку звертає увагу регулятор, полягає в тому, що казино-ігри, створені або розповсюджені ліцензованими постачальниками, з'являються на вебсайтах, які не мають відповідного дозволу для обслуговування британських споживачів. Це порушує правові норми, оскільки такі ринки є нерегульованими і не забезпечують відповідного рівня захисту гравців. Зокрема, нелегальні оператори можуть цілеспрямовано залучати вразливі групи споживачів, у тому числі тих, хто самостійно заблокував собі доступ до азартних ігор через систему GAMSTOP.

Комісія підкреслює, що нелегальні вебсайти часто не дотримуються вимог щодо соціальної відповідальності та боротьби з відмиванням коштів (AML), що значно підвищує ризики шахрайства, витоку персональних даних та несправедливих ігрових практик. Тому регулятор закликає всю індустрію азартних ігор та її партнерів вжити заходів для мінімізації цих ризиків. Окрему увагу в документі приділено постачальникам ігрового контенту, які працюють за схемою Business-to-Business (B2B) і створюють або розповсюджують ігри для казино. Виявлено, що деякі треті сторони, які отримали право розповсюджувати ліцензовані ігри, порушують контрактні угоди та передають програмне забезпечення нелегальним операторам.

Комісія зазначає, що відповідальність за такі порушення лежить як на нелегальних операторах, так і на ліцензованих постачальниках, які не забезпечують належного контролю за своїми бізнес-партнерами. Якщо такі випадки будуть виявлені, Gambling Commission може визнати дії ліцензіата недбалими, що потенційно поставить під загрозу його власну ліцензію. Тому операторам рекомендується активно перевіряти свої комерційні зв'язки та негайно розривати відносини з будь-якими контрагентами, які залучені до нелегального розповсюдження продуктів.

Документ також вказує на важливість співпраці з регулятором. Ліцензіати, які виявлять факти незаконного використання свого контенту, зобов'язані не лише припинити такі порушення, але й повідомити Комісію, надавши чіткий план дій для усунення проблеми. Регулятор наголошує,

[3] https://www.gamblingcommission.gov.uk/news/article/industry-warning-notice-licenced-software-appearing-on-illegal-market/

що такі повідомлення повинні містити конкретні заходи щодо запобігання повторенню ситуації. Водночас Gambling Commission анонсує посилення заходів контролю, включаючи проведення тестових покупок (test purchasing), щоб перевірити, чи ліцензовані оператори та постачальники виконують свої зобов'язання перед регулятором.

Документ закликає всіх учасників ринку продовжувати моніторинг ситуації та повідомляти про будь-яку нелегальну діяльність, яка може загрожувати британським споживачам. Для цього Комісія надає контактну інформацію для надсилання повідомлень про підозрілі випадки, включаючи можливість анонімного звернення через спеціальний портал.

Таким чином, документ підкреслює серйозність проблеми витоку ліцензованого контенту на нелегальний ринок і встановлює чіткі вимоги до операторів та постачальників. Він наголошує на необхідності посилення контролю за бізнес-партнерами, тісної взаємодії з регулятором та готовності вживати оперативних заходів у разі виявлення порушень. Gambling Commission дає зрозуміти, що буде застосовувати суворі санкції до компаній, які не забезпечують відповідного рівня відповідальності, що потенційно може призвести до втрати ліцензії або інших серйозних наслідків.

Висновки:

- **Ліцензовані оператори мають посилити контроль за бізнес-партнерами.** Переглядати та моніторити діяльність третіх сторін, особливо реселерів програмного забезпечення, використовувати внутрішні механізми аудиту для виявлення нелегального використання контенту.
- **Оператори, які не усувають витоки своїх ігор на нелегальні ринки, ризикують втратити ліцензію.** Комісія може застосовувати жорсткі санкції до компаній, які не контролюють своїх контрагентів. В разі виявлення порушень необхідно негайно інформувати регулятора та демонструвати заходи для вирішення проблеми.
- **Нелегальні ринки становлять значний ризик для гравців та регульованого ринку Великої Британії.** Нелегальні оператори не забезпечують відповідального гемблінгу та не мають ефективних заходів захисту гравців. Вони можуть використовувати слабкі AML-процедури, що підвищує ризик фінансування злочинності та тероризму.
- **Gambling Commission активізує заходи з моніторингу та розслідувань.** Планується використання методів тестових покупок (test purchasing), запроваджено гарячу лінію для повідомлення про нелегальне використання ліцензованих продуктів.

Технології підвищення конфіденційності для цифрових платежів[4]

Документ є технічним дослідженням, підготовленим Банком міжнародних розрахунків (BIS), що аналізує технології захисту приватності у цифрових платежах. Він розглядає напруженість між конфіденційністю, аудиторськими вимогами та технічними обмеженнями у фінансових операціях, а також досліджує поточні та перспективні технології для забезпечення приватності.

Документ починається з аналізу зростаючої ролі цифрових платежів та ризиків, пов'язаних із розкриттям персональних фінансових даних користувачів. У сучасних умовах цифрові транзакції часто збирають, зберігають та аналізують великі обсяги даних, що робить користувачів

[4] https://www.bis.org/publ/work1242.pdf

вразливими до комерційного монетизування, державного нагляду та кібератак. Автори зазначають, що технологічний прогрес, зокрема штучний інтелект та квантові обчислення, можуть ще більше загострити ці загрози, роблячи нинішні методи захисту застарілими.

Описується таксономія приватності, яка розділяє технології на "м'які" (soft privacy) та "жорсткі" (hard privacy). М'яка приватність базується на політиках доступу до даних, запроваджених фінансовими установами, що можуть змінюватися залежно від законодавчих вимог. Жорстка приватність ґрунтується на криптографічних механізмах, що запобігають доступу до даних навіть для постачальників послуг. Цей підхід є більш безпечним, але може ускладнити виконання законодавчих вимог щодо боротьби з фінансовими злочинами.

Ключовою напруженістю є баланс між приватністю, прозорістю та вимогами правоохоронних органів. У документі показано, що існує три основні групи зацікавлених сторін: користувачі, що цінують приватність; правоохоронні органи, які прагнуть мати доступ до фінансових даних для розслідувань; комерційні структури (банки, платіжні системи, BigTech), які монетизують дані користувачів. У зв'язку з цим у документі досліджується компроміс між конфіденційністю та аудитом, розглядаючи існуючі технологічні підходи до їх поєднання.

Автори надають детальний огляд технологій, що сприяють підвищенню конфіденційності цифрових платежів, включаючи:

Висновки:

- **Сучасні системи цифрових платежів мають низький рівень приватності, що створює ризики витоку персональних фінансових даних користувачів.** Рекомендується розробляти криптографічні механізми, які дозволяють обмежити зберігання та використання таких даних.
- **Технологічні рішення, такі як Zero-Knowledge Proofs, гомоморфне шифрування та анонімні цифрові підписи, можуть значно покращити конфіденційність транзакцій.** Проте їх масштабованість залишається технічною проблемою, що потребує подальших досліджень.
- **Компроміс між приватністю та аудитом може бути досягнутий шляхом поєднання "м'якої" приватності з "жорстким" аудитом.** Наприклад, частина транзакцій може бути зашифрована, але розкрита за чітко визначеними правилами (наприклад, при досягненні певних порогів або при виявленні підозрілої поведінки).
- **CBDC та інші цифрові форми грошей повинні враховувати питання приватності з самого початку їхнього проєктування.** Використання технологій захисту конфіденційності дозволить зберегти баланс між прозорістю фінансової системи та захистом прав громадян.

- Докази з нульовим розголошенням (Zero-Knowledge Proofs, ZKP) – дозволяють підтвердити наявність певної інформації без її розкриття.
- Гомоморфне шифрування (Homomorphic Encryption, HE) – дозволяє виконувати операції з зашифрованими даними без їх розшифрування.
- Розподілені схеми обміну секретною інформацією (Secret Sharing, Multi-party Computation, MPC) – розподіляють контроль над даними між кількома сторонами для запобігання несанкціонованому доступу.
- Анонімні цифрові підписи (Ring Signatures, Blind Signatures) – дозволяють зберігати анонімність при верифікації транзакцій.
- Технології довірених середовищ виконання (Trusted Execution Environments, TEEs) – забезпечують безпечне зберігання ключів та обробку конфіденційних даних.
- Метрики конфіденційності (k-anonymity, Differential Privacy) – методи, що мінімізують ризик ідентифікації користувачів у великих масивах даних.

Також у документі оцінюється можливість поєднання жорсткої та м'якої приватності у цифрових платежах. Автори пропонують чотири сценарії:

1. М'яка приватність та м'який аудит – нинішня модель, що дозволяє правоохоронцям отримувати доступ до даних через судові запити.
2. М'яка приватність та жорсткий аудит – автоматизований моніторинг ризиків та обов'язкова звітність про великі транзакції.
3. Жорстка приватність та жорсткий аудит – впровадження криптографічних механізмів для умовної анонімності транзакцій.
4. Жорстка приватність та м'який аудит – система, де платежі є повністю зашифрованими, але можуть бути розкриті за визначеними умовами.

Автори зазначають, що існує суттєва прогалина у впровадженні технологій захисту приватності у цифрових валютах центральних банків (CBDC). Деякі проєкти, такі як GNU Taler та BIS Project Tourbillon, пропонують потенційні технічні рішення, проте вони ще потребують подальшої перевірки та доопрацювання.

Документ завершується висновком, що для створення ефективних систем цифрових платежів з балансом між приватністю та аудитом необхідні нові технологічні розробки. Автори наголошують, що цифрові платіжні системи мають бути розроблені з урахуванням таких аспектів:

- Мінімізація збереження конфіденційних даних.
- Використання криптографічних механізмів контролю доступу.
- Чіткі правила доступу для правоохоронних органів.
- Впровадження технологій автоматизованого моніторингу для виявлення зловживань.

Регулювання

Революція у боротьбі з шахрайством: нові регуляторні механізми та санкції у соціальній сфері Великої Британії [5]

Новий законопроєкт Public Authorities (Fraud, Error & Recovery) Bill, представлений урядом Великої Британії, є найбільш масштабною ініціативою боротьби з шахрайством у сфері соціальних виплат за останнє покоління. Основна мета законодавчих змін – суттєве зменшення фінансових втрат, пов’язаних із шахрайством та помилками у системі соціального забезпечення, які наразі оцінюються у £10 мільярдів на рік. Документ передбачає впровадження нових санкцій щодо осіб, які ухиляються від повернення незаконно отриманих коштів, а також значне розширення повноважень державних органів у сфері розслідування та стягнення заборгованості.

Одна з найбільш дискусійних новацій законопроєкту – можливість позбавлення водійських прав осіб, які отримали соціальні виплати незаконно та відмовляються повертати борг. Відповідно до положень законопроєкту, Департамент праці та пенсій (DWP) зможе звертатися до суду з клопотанням про тимчасове позбавлення права на керування транспортними засобами терміном до двох років у випадку, якщо заборгованість перевищує £1,000, а всі попередні

[5] https://www.gov.uk/government/news/biggest-fraud-crackdown-in-a-generation

вимоги про погашення боргу було проігноровано. Важливим регуляторним принципом у застосуванні цього заходу є його пропорційність та обґрунтованість – уряд наголошує, що першочерговим способом стягнення залишатимуться добровільні угоди про повернення коштів, а санкції застосовуватимуться лише у разі систематичної відмови від виконання зобов'язань.

Значні зміни відбудуться у сфері розслідувань фінансових злочинів, пов'язаних із соціальними виплатами. Законопроєкт передбачає надання розширених слідчих повноважень співробітникам DWP, що дозволить їм звертатися до суду з проханням про обшуки та вилучення майна осіб, підозрюваних у шахрайстві. Це включає можливість конфіскації електронних пристроїв, таких як смартфони та комп'ютери, для збору доказів у кримінальних розслідуваннях. Уряд аргументує такі нововведення необхідністю модернізації підходу до виявлення та запобігання шахрайству, оскільки злочинці використовують все більш складні схеми приховування незаконних доходів.

Крім цього, новий закон надасть DWP право запитувати виписки з банківських рахунків осіб, які мають значну заборгованість перед державою, але не перебувають у категорії соціальних отримувачів або офіційно працевлаштованих у системі PAYE (Pay As You Earn). Це дозволить виявляти випадки, коли боржники мають кошти для повернення незаконно отриманих виплат, проте навмисно уникають розрахунків із державою. Однак, важливим регуляторним обмеженням є те, що DWP не отримає прямого доступу до банківських рахунків громадян, а лише право вимагати виписки через судові запити.

Окремий акцент зроблено на боротьбі з шахрайством, яке мало місце під час пандемії COVID-19. Уряд пропонує подвоїти строк позовної давності для цивільних позовів, пов'язаних із незаконним отриманням державної допомоги, збільшивши його з 6 до 12 років. Це рішення продиктоване тим, що велика кількість незаконних виплат відбувалася у надзвичайних умовах, коли контроль за розподілом коштів був ослаблений, а розслідування подібних випадків потребують більше часу через складність збору доказової бази. Також нові повноваження, надані Public Sector Fraud Authority, передбачають можливість вилучення коштів безпосередньо з банківських рахунків осіб, викритих у масштабному шахрайстві з COVID-фондами.

Для підвищення ефективності нових заходів уряд планує запровадити механізми незалежного нагляду та звітності, а також спеціальні Кодекси практики, які визначатимуть чіткі межі використання нових інструментів. Працівники DWP, які отримають додаткові повноваження, пройдуть спеціальну підготовку, що забезпечить правомірне та пропорційне застосування нових заходів щодо порушників. Додатково планується залучення банків до активнішого

Висновки:

- **Радикальне посилення відповідальності за шахрайство у соціальній сфері** - введення таких покарань, як позбавлення водійських прав, дозволяє зробити санкції більш відчутними для шахраїв і сприятиме поверненню коштів державі.
- **Розширення повноважень DWP у розслідуванні шахрайства** - Департамент отримає нові оперативні механізми для виявлення та переслідування шахраїв, що дозволить швидше припиняти незаконні схеми.
- **Повернення незаконно отриманих виплат, зокрема з COVID-фондів** - завдяки продовженню строків розслідування на 12 років уряд зможе повернути мільярди фунтів, що були розтрачені через шахрайство під час пандемії.
- **Збільшення прозорості та ефективності державних витрат** - нові механізми дозволять оптимізувати соціальні виплати, мінімізувати помилки у виплатах та запобігти майбутнім втратам бюджету.

моніторингу фінансової поведінки осіб, які отримують соціальні виплати, щоб попереджати шахрайство ще на ранніх стадіях.

Таким чином, новий законопроєкт передбачає комплексну реформу у сфері боротьби з шахрайством у соціальному забезпеченні, спрямовану на посилення відповідальності порушників, надання державним органам розширених слідчих повноважень та удосконалення механізмів контролю за соціальними виплатами. Уряд позиціонує ці заходи як необхідний крок для захисту коштів платників податків, створення більш справедливої системи соціального забезпечення та підвищення ефективності витрачання державних ресурсів.

Санкції

Санкції ЄС проти Росії 2025: поточний стан, перспективи та виклики[6]


BRIEFING

European Parliament

EU sanctions against Russia 2025: State of play, perspectives and challenges

SUMMARY

In response to Russia's illegal and unprovoked full-scale invasion of Ukraine in February 2022, the European Union swiftly adopted unprecedentedly tough sanctions, in close cooperation with partners including the United States, the United Kingdom, Canada, Australia and Japan. The rapid succession of 15 packages of EU sanctions adopted since then have resulted in an unparalleled set of measures targeting Russian political elites and key sectors of the Russian economy. New sanctions have also been adopted against Belarus, Iran and North Korea in response to their involvement in Russia's war of aggression. Furthermore, in 2024 the EU adopted two new regimes of sanctions, addressing human rights violations and repression in Russia (May 2024), and responding to Russia's destabilising activities ('hybrid attacks') abroad (October 2024).

The unprecedented nature of the sanctions imposed on Russia, in scale and scope, has created new implementation challenges. Member States and EU institutions have renewed efforts to improve the enforcement of sanctions and to close loopholes to prevent circumvention, including reinforcing cooperation with third countries. A specific anti-circumvention tool was included in the 11th package of sanctions (June 2023), followed by additional measures in the successive packages, including those to counter Russia's 'shadow fleet'. Furthermore, a newly adopted EU directive (April 2024) obliges the EU Member States to introduce minimum criminal offences and penalties for violating and circumventing EU sanctions. It also aims to improve cross-border cooperation on investigations, prosecutions and sentencing of EU sanctions violations.

Since Russia's illegal annexation of Crimea and Sevastopol in 2014, the European Parliament has been a vocal advocate of severe sanctions. It has unequivocally condemned Russia's unjustified aggression against Ukraine, demanded broader and better-enforced sanctions and called for the confiscation of Russian assets frozen by the EU to pay for Ukraine's reconstruction. Parliament has demanded a full review of more centralised EU-level oversight of sanctions implementation and a full ban on liquefied natural gas (LNG) imports, among other measures.

This briefing updates and complements a previous briefing published in September 2023.

IN THIS BRIEFING

- EU sanctions on Russia: State of play (January 2025)
- Other developments in 2024: Two new sanctions regimes and an EU directive on the violation of sanctions
- Challenges and perspectives for 2025

Документ від Європейської парламентської дослідницької служби (EPRS) надає детальний аналіз поточного стану санкцій ЄС проти Росії у 2025 році, їхню еволюцію, виклики та перспективи подальшого посилення. Основна увага приділяється ефективності санкцій, запровадженню нових обмежень у 2024 році та заходам щодо боротьби з обходом санкцій. Документ також висвітлює перспективи майбутньої політики ЄС у цьому напрямку.

Санкції ЄС проти Росії розпочалися у 2014 році після анексії Криму, але їхній безпрецедентний масштаб було досягнуто після повномасштабного вторгнення Росії в Україну у лютому 2022 року. За цей час ЄС ухвалив 15 пакетів санкцій, які включають як секторальні обмеження (фінансові, торговельні, енергетичні), так і індивідуальні заходи (замороження активів, візові заборони). Санкції охоплюють близько 2400 фізичних та юридичних осіб, включаючи керівництво РФ, пропагандистів, військових командирів та бізнесменів, які підтримують агресію.

У 2024 році ЄС прийняв два нові санкційні режими: за порушення прав людини в Росії (у відповідь на репресії та загибель Олексія Навального) та за дестабілізуючі дії Росії за кордоном ("гібридні атаки"), що включає інформаційні маніпуляції, кіберзагрози та саботаж. Також у квітні 2024 року ЄС ухвалив директиву, яка криміналізує порушення санкцій, встановлює мінімальні стандарти покарання та покращує співпрацю між державами-членами у розслідуванні випадків обходу санкцій.

Одним із ключових викликів стало зростання обсягів обходу санкцій через треті країни, такі як Казахстан, Туреччина, ОАЕ та Китай. У відповідь ЄС посилив контроль за експортом до країн посередників, ввів механізми заборони реекспорту чутливих товарів та почав цілеспрямовано накладати санкції на посередників, що сприяють обходу санкцій.

Економічні санкції продовжують завдавати серйозних збитків економіці Росії. Санкції охоплюють понад 54% експорту та 58% імпорту між ЄС та РФ, що призвело до скорочення обсягів торгівлі на 75%. Рубль втратив майже 25% вартості, інфляція в РФ зросла до 9,5%, а ключова процентна ставка досягла 21%. Водночас Росія продовжує отримувати прибутки від продажу зрідженого природного газу (LNG) до ЄС, що викликало нові дискусії щодо

[6] https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/767243/EPRS_BRI(2025)767243_EN.pdf

необхідності повної заборони імпорту російського LNG та інших критично важливих товарів, таких як алюміній, нікель та добрива.

Одним із найгостріших питань залишається використання заморожених російських активів. У травні 2024 року ЄС затвердив використання надлишкових прибутків від заморожених активів РФ на підтримку України. До кінця 2024 року ЄС направив Україні перший платіж у розмірі 1,5 млрд євро. G7 досягла угоди щодо використання цих активів для надання Україні позики у 50 млрд доларів США.

На перспективу 2025 року ЄС розглядає нові заходи, включаючи посилення санкцій проти російських металів, подальше закриття лазівок у фінансових операціях, удосконалення механізмів контролю та розширення санкцій на ядерний сектор РФ. Також обговорюється можливість створення центрального органу санкційного контролю на рівні ЄС за аналогією з американським OFAC.

Висновки:

- **Посилення санкційного режиму та контроль за обходом.** У 2024 році ЄС запровадив нові санкційні режими щодо порушень прав людини та гібридних атак РФ, а також новий правовий механізм боротьби з обходом санкцій, що передбачає кримінальну відповідальність.
- **Значний економічний тиск на РФ.** Санкції призвели до падіння торгівлі між ЄС та РФ на 75%, ослаблення рубля та економічних труднощів, проте РФ адаптується через альтернативні маршрути торгівлі та збільшення військових витрат.
- **Використання заморожених активів РФ на користь України.** ЄС та G7 погодили механізм використання прибутків від заморожених активів Росії для надання Україні фінансової допомоги у розмірі 50 млрд доларів США.
- **Перспективи нових санкцій.** ЄС розглядає можливість запровадження повного ембарго на російський LNG, алюміній, нікель та добрива, а також удосконалення санкційної політики через створення єдиного наглядового органу на рівні ЄС.

Великобританія та Канада наклали санкції на Білорусь через фальсифікацію виборів[7]

Великобританія та Канада запровадили нові санкції проти Білорусі у відповідь на фальсифікацію президентських виборів, що відбулися 26 січня 2025 року. Ці вибори були широко засуджені міжнародною спільнотою через відсутність прозорості та придушення опозиційних голосів.

Санкції спрямовані проти дев'яти фізичних осіб, включаючи голову Центральної виборчої комісії Білорусі Ігоря Карпенка, а також керівників пенітенціарних установ та правоохоронних органів, відповідальних за порушення прав людини та придушення політичної опозиції. Крім того, під санкції потрапили три оборонні компанії Білорусі, які підтримують урядові дії, спрямовані на обмеження свобод та придушення інакодумства.

Запроваджені санкції передбачають фінансові обмеження, заморожування активів, заборону на поїздки та обмеження на ведення бізнесу з іноземними державами. Ці заходи мають на меті чинити тиск на білоруське керівництво з метою поваги до прав людини та політичних свобод.

[7] https://regtechtimes.com/severe-sanctions-strike-belarus-uk-and-canada/

Варто зазначити, що ці санкції є частиною скоординованих міжнародних зусиль, спрямованих на підтримку демократичних процесів у Білорусі та засудження дій уряду, які порушують основні права та свободи громадян.

Звіти окремих інституцій та експертів

Таємна угода: Як Росія продала Саудівській Аравії зброю на 2,2 млрд євро, обходячи міжнародні санкції [8]

Звіт, опублікований OCCRP, висвітлює масштабний витік внутрішніх документів, що свідчать про продаж Росією зенітно-ракетних комплексів «Панцир-С1М» Саудівській Аравії на загальну суму 2,2 мільярда євро. Контракт, підписаний ще у квітні 2021 року, продовжує діяти навіть після введення жорстких міжнародних санкцій проти російського оборонного комплексу у 2022 році через повномасштабне вторгнення РФ в Україну. Аналіз витоку засвідчує, що постачання деяких компонентів здійснювалося у 2023 році, що вказує на фактичне продовження військово-технічної співпраці між Москвою та Ер-Ріядом.

Згідно з викритими документами, схема фінансування угоди передбачала перерахування коштів через російську державну компанію Рособоронекспорт, яка потім передавала їх виробникам озброєнь, серед яких Роселектроніка – дочірнє підприємство концерну Ростех. Перша оплата в розмірі 326 мільйонів євро була здійснена в серпні 2021 року. Однак витік не містить доказів подальших транзакцій після травня 2022 року, хоча угода має діяти до 2026 року. У документі також зазначено, що Росія змогла забезпечити постачання спеціальних транспортних засобів, які використовуються для перевезення систем протиповітряної оборони, що є прямим порушенням санкційних обмежень.

Попри те, що Саудівська Аравія офіційно не приєдналася до санкційних режимів США та ЄС щодо російського оборонного сектора, експерти попереджають про ризики вторинних санкцій проти саудівських компаній та осіб, які співпрацюють із підсанкційними російськими підприємствами. Особливо це стосується можливості застосування закону CAATSA, який дозволяє США запроваджувати обмеження щодо будь-яких іноземних компаній, що ведуть справи з російським військово-промисловим комплексом.

Ще одним важливим аспектом угоди стала домовленість про локалізацію виробництва на території Саудівської Аравії. Документи містять детальний 69-сторінковий план, згідно з яким передбачалося будівництво навчального центру площею 15 000 м² у Джидді для підготовки персоналу, а також створення заводу для збирання комплексів «Панцир-С1М» та боєприпасів. Угода щодо заводу планувалася до підписання у другій половині 2022 року, проте відсутність подальших даних у витоку не дозволяє підтвердити її фактичне виконання. Експерти висловлюють сумніви щодо здатності Росії забезпечити спільне виробництво через санкційні обмеження на імпорт критичних компонентів для оборонної промисловості.

Геополітичні наслідки цієї угоди також є надзвичайно значущими. Саудівська Аравія офіційно підтримала резолюцію ООН щодо виведення російських військ з України та пообіцяла 400

[8] https://www.occrp.org/en/scoop/sanctioned-russian-firms-sold-2b-air-defense-system-to-saudi-arabia-leaked-documents-show

мільйонів доларів гуманітарної допомоги Києву, однак водночас утримувалася від голосування за більшість рішень щодо агресії РФ. Розслідування вказує на зв'язок між постачанням зброї та голосуванням деяких країн на міжнародних майданчиках, що підтверджує використання Кремлем військових контрактів як інструменту дипломатичного тиску.

Окрему стурбованість викликає можливість витоку інформації про американські системи ППО Patriot, які Саудівська Аравія придбала у США. Документи містять згадки про візити російських військових делегацій на саудівські військові бази, що потенційно могло надати РФ доступ до технічної документації та принципів роботи цих систем.

Таким чином, викриття цієї угоди демонструє не лише фактичне порушення санкційного режиму, але й стратегічну політику Росії, яка використовує продаж озброєнь як інструмент міжнародного впливу, економічної підтримки та обходу обмежень. Виявлені факти можуть мати серйозні політичні та правові наслідки для Саудівської Аравії, а також стати підставою для подальшого посилення санкційного тиску на російський оборонний сектор.

Революція у боротьбі з шахрайством: нові регуляторні механізми та санкції у соціальній сфері Великої Британії [9]

Документ, опублікований Королівським об'єднаним інститутом оборонних досліджень (RUSI), аналізує новий підхід Великої Британії до боротьби з організованою злочинністю у сфері нелегальної міграції через запровадження спеціального санкційного режиму. Автори досліджують, чи може цей підхід стати ефективним інструментом у протидії злочинним мережам, які заробляють мільярди на контрабанді людей.

Прем'єр-міністр Великої Британії Кір Стармер та міністр закордонних справ Девід Леммі оголосили про створення першого у світі автономного санкційного режиму, спрямованого виключно на протидію незаконній міграції шляхом блокування фінансових потоків, які живлять діяльність злочинних угруповань. Головний механізм впливу полягає в заморожуванні активів осіб і структур, пов'язаних з контрабандою людей, та обмеженні їхньої здатності використовувати глобальну фінансову систему для отримання прибутків. Ця ініціатива є частиною ширшого підходу Великої Британії до використання санкцій у боротьбі з корупцією, порушеннями прав людини та кіберзлочинністю, але тепер акцент зміщено на боротьбу з міграційною злочинністю, яка останнім часом набула масштабного характеру.

Організована злочинність у сфері нелегальної міграції є високоорганізованою мережею, яка діє у багатьох юрисдикціях і використовує складні фінансові механізми для переказу коштів, що значно ускладнює її відстеження. За оцінками, щорічний обсяг прибутку від контрабанди мігрантів становить не менше 10 мільярдів доларів, а з огляду на зростання примусової міграції через війни, економічну нестабільність та політичні кризи, ця цифра постійно зростає. У 2023 році зафіксовано рекордну кількість нелегальних перетинів кордону в Європі з 2016 року, що ще раз підтверджує зростаючий попит на такі злочинні «послуги». Нелегальна міграція не лише створює ризики для національної безпеки, а й стає джерелом багатьох інших видів злочинності, зокрема торгівлі людьми, трудової та сексуальної експлуатації, а також наркоторгівлі.

[9] https://www.rusi.org/explore-our-research/publications/commentary/new-frontier-organised-immigration-crime-and-uk-sanctions

Однією з головних проблем у фінансових потоках нелегальної міграції є використання неформальних платіжних систем, таких як hawala. Ця система дозволяє переказувати кошти без банківських операцій, використовуючи мережу посередників, що працюють на довірі. У випадку міграційної злочинності такі схеми функціонують наступним чином: мігрант або його родичі передають гроші hawala-посереднику, який зберігає кошти до завершення міграційної операції, а потім передає їх злочинному угрупованню через аналогічного посередника в іншій країні. Завдяки анонімності та відсутності регулювання ця система широко використовується для фінансування нелегальної міграції, а також для відмивання коштів, фінансування тероризму та ухилення від санкцій.

Запроваджений санкційний режим має потенціал створити серйозні перешкоди для функціонування цих схем, але залишається багато невирішених питань. Наприклад, санкції Великої Британії діятимуть лише на тих осіб та компанії, які мають активи або операційну діяльність, що підпадає під британську юрисдикцію. Однак основні фінансові транзакції, пов'язані з нелегальною міграцією, відбуваються у країнах Близького Сходу, Північної Африки та Азії, де санкційний вплив Лондона обмежений. Це ставить під сумнів ефективність нових заходів, якщо вони не будуть підтримані ширшою міжнародною співпрацею, особливо з боку Європейського Союзу.

Також залишається відкритим питання щодо того, хто саме підпадатиме під санкції: чи це будуть лише ключові організатори контрабанди, чи також дрібні посередники, які забезпечують її логістику? Крім того, міграційна злочинність має складну структуру, що включає постачальників човнів, перевізників, корумпованих прикордонників і навіть соціальні мережі, які використовуються для вербування мігрантів. Неясно, чи зможуть санкції охопити весь цей спектр учасників злочинного бізнесу.

Ще одним ризиком є надмірне сподівання на ефективність санкцій. Історія міжнародних санкцій демонструє, що їхня результативність часто є обмеженою через складність контролю за виконанням обмежень, можливість обходу через підставних осіб або компанії, а також недостатню координацію між державами. Приклад санкцій проти Росії показав, що хоча вони створюють економічний тиск, вони не завжди здатні змінити поведінку підсанкційних осіб або зупинити злочинні процеси.

У підсумку, автори наголошують, що санкції можуть бути дієвим інструментом лише за умови їхньої інтеграції в ширший комплекс заходів, таких як посилення фінансового моніторингу, міжнародна співпраця у сфері обміну даними, більш жорсткий контроль над неформальними фінансовими системами та активна боротьба з корупцією в країнах, де базуються ключові угруповання, що займаються нелегальною міграцією. Без цих додаткових кроків санкції ризикують залишитися політичним жестом, який не принесе реального впливу на злочинні мережі, що експлуатують вразливих мігрантів.

Висновки:

- **Санкції можуть бути дієвим інструментом** боротьби з організованою злочинністю у сфері незаконної міграції, але лише за умови їхнього поєднання з іншими заходами (законодавчими, правоохоронними, фінансовими).
- **Hawala та інші неформальні фінансові системи відіграють ключову роль у фінансуванні злочинності,** оскільки вони дозволяють анонімні перекази коштів і уникають традиційного банківського контролю.
- **Відсутність міжнародної координації,** особливо з боку ЄС, може значно знизити ефективність санкцій Великої Британії.
- **Високі очікування щодо санкцій можуть не виправдати себе** через складність правоохоронного механізму та історичну неефективність подібних заходів у боротьбі з іншими видами організованої злочинності.

Інші новини

Кататумбо у вогні: Війна за кокаїновий центр Колумбії та крах мирного процесу [10]

Стаття висвітлює ескалацію насильства в регіоні Кататумбо, що розташований у північно-східній Колумбії та є ключовою точкою для виробництва та транспортування кокаїну. Ця територія історично була ареною конфліктів між різними незаконними збройними формуваннями, а остання хвиля насильства розгорнулася між Національною визвольною армією (ELN) та 33-м фронтом дисидентів колишніх Революційних збройних сил Колумбії (FARC). Конфлікт спричинив загибель щонайменше 80 людей та змусив понад 11 000 мешканців покинути свої домівки.

Кататумбо є стратегічним регіоном для наркоторгівлі, оскільки на його території розташовані великі плантації коки, зокрема близько 44 000 гектарів у муніципалітеті Тібу. Контроль над цим регіоном визначає розподіл потоків наркотрафіку до сусідньої Венесуели, яка довгий час слугувала притулком для колумбійських партизанів. Саме боротьба за контроль над цими територіями та ресурсами стала ключовою причиною протистояння між ELN та дисидентами FARC.

Раніше між цими угрупованнями існував певний баланс сил. У 2022 році вони досягли де-факто угоди про розподіл сфер впливу, що дозволило їм уникнути прямої конфронтації. Проте, як застерігали правозахисники та місцеві жителі, цей хиткий мир був вкрай нестабільним. У 2023 році вже з'являлися попередження про можливий зрив домовленостей, оскільки обидві групи використовували перемир'я для зміцнення своїх позицій у регіоні. В листопаді 2024 року Офіс Омбудсмена Колумбії повідомив про зростання рівня насильства, викрадень, рекрутування дітей та пропагандистських кампаній, які здійснювали обидві сторони.

Безпосереднім приводом для бойових дій став інцидент у Тібу, коли була вбита родина, що займалася ритуальними послугами. Ця подія має особливе значення, оскільки власники похоронних бюро часто виконують важливу роль у конфліктних зонах, допомагаючи ідентифікувати загиблих та організовувати поховання. ELN заявила, що 33-й фронт відповідальний за вбивство, що й стало приводом для розгортання військової кампанії. Проте незалежні розслідування та витоки з урядових структур свідчать про те, що саме ELN могло вчинити цей злочин, оскільки родина, ймовірно, порушила їхні накази щодо поводження з тілами загиблих бойовиків 33-го фронту.

ELN, прагнучи розширити свій контроль над кордоном з Венесуелою, використала цей інцидент як привід для масштабного наступу. Важливим контекстом є той факт, що після демобілізації FARC у 2016 році ELN поступово посилила свій вплив у регіоні, знищивши або витіснивши конкурентів, таких як Народна визвольна армія (EPL) та сили самооборони Гайтаністів Колумбії (AGC). Останнім значним конкурентом для них залишався 33-й фронт. Протягом останніх років ELN звинувачувала цю групу у співпраці з урядом, що є класичною тактикою для виправдання атак, зокрема проти цивільного населення.

[10] https://insightcrime.org/news/renewed-war-for-colombia-cocaine-center/

Ескалація насильства в Кататумбо стала потужним ударом по мирній стратегії уряду Колумбії «Total Peace». Президент Густаво Петро, який раніше прагнув до переговорів з ELN, після початку бойових дій в регіоні оголосив про припинення мирних переговорів. Це рішення було очікуваним, оскільки ELN уже в серпні 2024 року здійснила напад на військову базу в Арауці, що тимчасово зупинило переговори. Попри спроби відновити діалог у листопаді 2024 року, події в Кататумбо зробили будь-яке примирення малоймовірним.

Варто також зазначити, що ELN діє не лише в Кататумбо. Група веде бойові дії в інших регіонах Колумбії, зокрема в департаменті Чоко, де вона бореться проти AGC, а також у Болівари та Антіокії. В цих зонах ELN навіть уклала ситуативні союзи з іншими FARC-дисидентами, що робить їхню тактику дуже гнучкою та регіонально варіативною. Однак ескалація конфлікту в Кататумбо може вплинути на ці союзи, оскільки 33-й фронт також є частиною ширшої коаліції дисидентів. Таким чином, загострення протистояння може мати значні наслідки не лише для самого Кататумбо, а й для всієї Колумбії.

Додатковий фактор, який впливає на розвиток подій, – це політична ситуація у Венесуелі. Президент Ніколас Мадуро, який є довготривалим союзником ELN, щойно переобрався на новий термін після спірних виборів. Це створює сприятливі умови для ELN, оскільки режим Мадуро надає їм можливість використовувати територію Венесуели як тилову базу, що ускладнює спроби колумбійської влади нейтралізувати їхній вплив.

Таким чином, конфлікт у Кататумбо має кілька рівнів. З одного боку, він є наслідком боротьби між двома угрупованнями за контроль над наркотрафіком. З іншого боку, він відображає більш глобальні виклики для Колумбії, такі як неефективність мирного процесу, складність нейтралізації незаконних збройних формувань та вплив зовнішніх факторів, зокрема Венесуели. Враховуючи ці обставини, найближчим часом слід очікувати подальшого загострення ситуації, яке може мати не лише внутрішньоколумбійські, а й міжнародні наслідки.

Висновки:

- **Зростає ризик подальшої дестабілізації регіону -** Конфлікт між ELN та 33-м фронтом має потенціал до подальшої ескалації, що може призвести до нових масових переміщень населення та гуманітарної кризи.
- **ELN посилює свій контроль над наркотрафіком -** Група використовує хаос, щоб закріпити домінування в Кататумбо та отримати ключові маршрути постачання кокаїну через Венесуелу.
- **Мирні переговори перебувають під загрозою -** Відновлення конфлікту демонструє слабкість політики «Total Peace», що вимагає перегляду урядової стратегії щодо незаконних збройних формувань.
- **Посилення міжнародного спостереження та тиску -** Оскільки ситуація безпосередньо впливає на глобальні маршрути наркотрафіку, міжнародні організації можуть збільшити санкційний тиск на пов'язані з ELN суб'єкти та уряди, що їх підтримують.

Відмивання коштів через нерухомість[11]

Документ досліджує ризики відмивання коштів через ринок нерухомості, зокрема у таких ключових фінансових центрах, як Дубай, Лондон, Мілан, Дублін і Лос-Анджелес. Основна увага

11 https://www.canva.com/design/DAGRwbaOQG4/DGoCYJiyx_2VIqfp3_HWqA/view?utm_content=DAGRwbaOQG4&utm_campaign=designshare&utm_medium=link2&utm_source=uniquelinks&utlId=hcd57d2fbc6#1

приділяється схемам використання елітної нерухомості для легалізації незаконних доходів, включаючи анонімні корпоративні структури, офшорні трасти.

Перший розділ аналізує загальні ризики у сфері нерухомості, зазначаючи, що цей сектор є привабливою мішенню для відмивання коштів через слабке регулювання, відсутність прозорості у володінні активами та високий попит на інвестиційну нерухомість. Європейський Союз посилює заходи контролю шляхом впровадження нових директив, які зобов'язують агентів з нерухомості проводити ретельну перевірку клієнтів (CDD) та повідомляти про підозрілі транзакції.

Окремий розділ присвячений ринку нерухомості в Європі у 2024 році. Спостерігається зростання вартості житла у більшості країн ЄС, що спричинило занепокоєння щодо доступності житла для населення та можливих фінансових маніпуляцій. Інвестори переорієнтовуються на такі сегменти як студентське житло та готелі, що свідчить про зміну пріоритетів у секторі. Водночас, приплив іноземного капіталу та комерційної нерухомості сприяє збільшенню ризиків, пов'язаних із незаконними фінансовими потоками.

У розділі, присвяченому Мілану, розкрито, як організована злочинність використовує місцевий ринок нерухомості для легалізації незаконних доходів. Складні корпоративні структури та недостатній контроль за власниками компаній дозволяють відмивати великі суми грошей. Одним із вирішень цієї проблеми пропонується створення відкритих реєстрів кінцевих бенефіціарів та посилення нормативних вимог щодо прозорості транзакцій.

Дубай постає як один із найбільш ризикових ринків нерухомості з точки зору відмивання коштів. Привабливість емірату для тіньових фінансових потоків пояснюється лояльним регуляторним середовищем, відсутністю вимог до фінансової звітності та активним будівництвом елітного житла. Наведено приклади, коли злочинні групи використовували дубайську нерухомість для легалізації коштів, отриманих від наркоторгівлі та фінансового шахрайства. Деякі інвестори, як-от Рафаеле Імперіале, прямо пов'язані з міжнародними злочинними мережами. Уряди кількох країн, зокрема Франції та Пакистану, вимагають екстрадиції підозрюваних, однак співпраця ОАЕ у цій сфері є обмеженою.

Документ також аналізує ситуацію у Лондоні та Дубліні, де спостерігається активне

Висновки:

- **Ринок нерухомості є ключовим інструментом для відмивання коштів через складні корпоративні структури, офшорні компанії та анонімні транзакції**. Важливо запроваджувати суворіші вимоги до прозорості власності та фінансових потоків.
- **Дубай, Лондон, Мілан і Дублін залишаються найбільш вразливими до використання нерухомості для легалізації коштів**. Їх привабливість пояснюється слабким регулюванням, високим попитом на нерухомість та доступністю фінансових інструментів, що маскують походження коштів.
- **ЄС посилює контроль за ринком нерухомості через нові регуляторні вимоги, включаючи обов'язкову перевірку клієнтів та звітність про підозрілі транзакції**. Це має стати орієнтиром для інших юрисдикцій у боротьбі з фінансовими злочинами.
- **Реконструкційні проекти після природних катастроф і для великих подій (як-от Олімпійські ігри) є високоризиковими з точки зору використання з метою ВК.** Влада повинна забезпечити прозорість процесів та ефективний моніторинг залучених фінансових ресурсів.

будівництво житла, значний рівень порожніх квартир та постійне зростання цін, що може свідчити про використання нерухомості для відмивання коштів. Експерти наголошують на важливості запровадження суворішого контролю за угодами купівлі-продажу елітної нерухомості, аби уникнути ризику фінансових зловживань.

Окремий розділ присвячений Лос-Анджелесу, де після масштабних лісових пожеж спостерігається зростання спекуляцій на ринку нерухомості та використання фондів реконструкції для відмивання коштів. Крім того, підготовка міста до Олімпійських ігор 2028 року може створити додаткові можливості для проникнення організованої злочинності в будівельний сектор через недостатній контроль та швидке освоєння інвестиційних потоків.

Російського олігарха в Німеччині підозрюють в ухиленні від санкцій[12]

Згідно з інформацією, німецькі правоохоронні органи розпочали масштабне розслідування щодо 58-річного російського олігарха Романа Абрамовича за підозрою у порушенні законів про зовнішню торгівлю та можливий обхід санкцій. Розслідування веде Генеральна прокуратура федеральної землі Гессен за підтримки інших правоохоронних органів.

У рамках розслідування в місті Оберзульм на півдні Німеччини було заарештовано чотири розкішні автомобілі загальною вартістю кілька мільйонів євро: два Bugatti Chiron, Lamborghini Reventón та Mercedes CLK GTR. Ці транспортні засоби більше не можна продавати, здавати в оренду або використовувати як заставу.

Крім того, обшуки були проведені на віллі XIX століття під назвою Leitenschlössl, розташованій у Гарміш-Партенкірхені. Під час обшуків конфісковано кілька цінних творів мистецтва, включаючи картини відомих європейських художників та рідкісні скульптури. Хоча власником вілли офіційно значиться люксембурзька компанія Parados Limited, слідчі підозрюють, що кінцевим власником є Абрамович.

Прокуратура вважає, що Абрамович міг порушити закони про зовнішню торгівлю, не задекларувавши ці високовартісні активи, що є обов'язковим, особливо для осіб, на яких накладено міжнародні санкції. У разі доведення вини йому загрожує штраф або ув'язнення терміном до одного року.

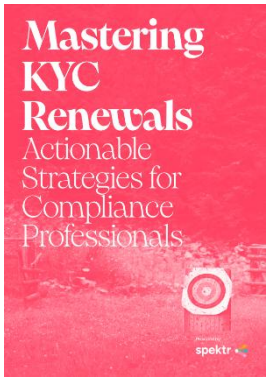
Адвокати Абрамовича заперечують будь-які правопорушення, стверджуючи, що їхній клієнт не є кінцевим власником ні вілли, ні автомобілів.

Для загального розвитку

Оновлення KYC[13]

Документ є детальним керівництвом для фахівців з комплаєнсу щодо оновлення KYC (Know Your Customer), зосередженим на вдосконаленні процесів перевірки клієнтів. Автори наголошують, що процеси оновлення KYC часто недооцінюються через їхню рутинність і трудомісткість, проте

[12] https://regtechtimes.com/oligarch-abramovich-suspected-of-sanction-evasion/#google_vignette
[13] https://media.licdn.com/dms/document/media/v2/D4E1FAQHeilZxGuAIig/feedshare-document-pdf-analyzed/B4EZT7B_ILGgAY-/0/1739378404970?e=1740614400&v=beta&t=fR6D0w4VuHQpamKtOXEk8q7XVvb1mhk7ApHDwM04Y6U



вони є критично важливими для підтримки точних клієнтських профілів, виявлення змін у факторах ризиків та забезпечення відповідності зростаючим регуляторним вимогам.

Оновлення KYC слугують не лише для дотримання регуляторних норм, а й для покращення досвіду клієнтів, мінімізації ризиків шахрайства та посилення фінансового моніторингу. У документі розглянуто ключові виклики, що супроводжують процес оновлення KYC, а також запропоновано низку практичних рекомендацій для оптимізації цього процесу.

Документ висвітлює ключові виклики та стратегії для ефективного оновлення KYC у фінансових установах. Оновлення KYC є безперервним процесом підтримки актуальних клієнтських даних, що допомагає виявляти потенційні ризики та забезпечувати відповідність регуляторним вимогам. Основними проблемами в процесі оновлення є застарілі або неповні дані, роз'єднані процеси у різних системах і посилений регуляторний тиск, що вимагає такої ж ретельності перевірок, як і на етапі початкового KYC.

Для вдосконалення оновлення KYC рекомендується інтегрувати його у процес онбордингу, централізувати збереження даних, регулярно перевіряти їхню актуальність та застосовувати ризик-орієнтований підхід. Автоматизація відіграє ключову роль у підвищенні ефективності, зокрема через використання аналітичних інструментів, автоматизованого збору даних із реєстрів та штучного інтелекту для виявлення потенційних ризиків і зменшення хибних спрацювань. Структурований підхід до оновлення дозволяє оптимізувати робочі процеси, зменшити навантаження на комплаєнс-команди та забезпечити ефективне управління ризиками у фінансових установах.

Практичні рекомендації для оновлення KYC:

1. Вдосконалення процесу збору та перевірки даних

- Використання актуальних реєстрів: інтеграція з місцевими бізнес-реєстрами для автоматичного оновлення змін у власності або статусі компаній.
- Автоматизовані нагадування клієнтам: надсилання запитів на оновлення інформації через автоматизовані платформи для мінімізації людського фактора.
- Запровадження "динамічного KYC": відстеження змін клієнтських профілів у режимі реального часу, а не періодичні перевірки за фіксованими інтервалами.

2. Централізація та уніфікація процесів

- Створення єдиного сховища даних: використання спеціалізованих платформ для KYC, які забезпечують доступність всієї необхідної інформації.
- Упорядкування джерел даних: використання структурованого підходу до оновлення клієнтських записів, щоб зменшити дублювання та помилки.

3. Використання ризик-орієнтованого підходу

- Гнучкі графіки оновлень: частіші перевірки для клієнтів із підвищеним ризиком та мінімальне втручання для низькоризикових клієнтів.
- Аналіз змін у ризикових профілях: оцінка впливу нової інформації на рівень ризику клієнта та відповідне коригування частоти оновлень.

4. Автоматизація та використання ШІ

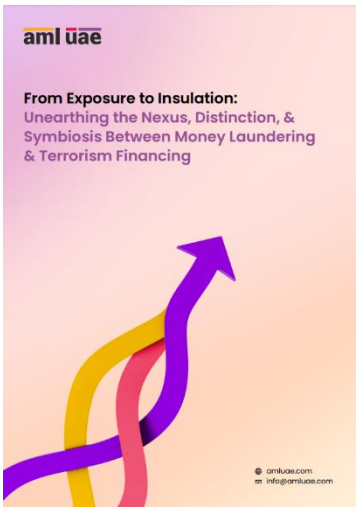
- Інтеграція з ШІ-системами: для автоматичного аналізу даних та виявлення потенційних ризиків.

- Застосування аналітичних панелей: для відстеження ефективності оновлень KYC та виявлення вузьких місць у процесі.

5. Постійний перегляд ефективності процесів

- Квартальні ревізії оновлень: перегляд підходів до KYC з урахуванням змін у регуляторному середовищі.
- Персоналізоване навчання для комплаєнс-команд: підвищення кваліфікації спеціалістів у сфері фінансового моніторингу та боротьби з фінансуванням тероризму.

Від викриття до ізоляції: виявлення зв'язку, відмінності та симбіозу між відмиванням коштів і фінансуванням тероризму[14]



Документ є комплексним дослідженням взаємозв'язку, відмінностей і взаємозалежності між відмиванням коштів та фінансуванням тероризму. Він має на меті поглибити розуміння цих процесів серед фахівців у сфері протидії фінансовим злочинам та покращити глобальні зусилля щодо мінімізації відповідних ризиків. У першій частині документ містить визначення ВК та ФТ, детально описує їхні процеси та пояснює, чому важливо розрізняти ці явища для ефективної протидії.

Процес відмивання коштів традиційно складається з трьох стадій: розміщення, розшарування та інтеграції. Розміщення передбачає введення незаконних коштів у фінансову систему через дрібні внески, обмін валют або покупку товарів високої вартості. Розшарування – це створення складних фінансових потоків для приховування джерела коштів, що включає транскордонні перекази, використання підставних компаній та торгівлю високовартісними активами. Інтеграція завершує цикл ВК, коли очищені кошти знову потрапляють у легальну економіку через інвестиції або бізнес-діяльність.

Фінансування тероризму, хоча має схожість із ВК, має суттєві відмінності, оскільки його мета полягає у фінансуванні терористичних операцій, а джерела можуть бути як законними (благодійні внески, пожертви), так і незаконними (торгівля зброєю, наркотиками, контрабанда). Процес фінансування тероризму включає чотири етапи: залучення, збереження, переміщення та використання коштів. Залучення може відбуватися через фіктивні благодійні фонди, криптовалютні операції або тіньові фінансові структури. Збереження передбачає накопичення активів у безпечних місцях, таких як офшорні рахунки або криптовалютні гаманці. Переміщення коштів часто здійснюється через грошові перекази, використання кур'єрів або електронні платіжні системи. Використання ресурсів безпосередньо спрямоване на здійснення терористичних атак, закупівлю зброї, матеріально-технічне забезпечення та вербування учасників.

Документ детально розглядає взаємозв'язок між ВК та ФТ, пояснюючи, як ці явища можуть використовувати спільні методи та канали для досягнення своїх цілей. Відмивання коштів може бути використане для приховування джерел фінансування тероризму, а терористичні групи можуть залучати кошти через ті самі механізми, що й організовані злочинні групи. Однією з ключових точок перетину є використання підставних компаній, торгівлі високовартісними

[14] https://amluae.com/wp-content/uploads/2025/02/From-Exposure-to-Insulation-Unearthing-the-Nexus-Distinction-Symbiosis-Between-Money-Laundering-Terrorism-Financing.pdf

активами, комплексних фінансових транзакцій та відмивання коштів через торгівлю (TBML) для пересування капіталу без викриття кінцевого бенефіціара.

Серед глобальних заходів боротьби з ВК та ФТ у документі розглядаються роль міжнародних організацій, таких як ФАТФ (FATF), ООН, Вольфсберзька група, Егмонтська група, які сприяють обміну інформацією між країнами, виробленню нових методів виявлення та протидії фінансовим злочинам. Документ наголошує на важливості співпраці між державами, запровадженні єдиних стандартів моніторингу транзакцій, застосуванні технологічних рішень для автоматизації комплаєнс-процесів та аналітики даних.

Також розглядаються основні виклики, пов'язані з боротьбою з ВК/ФТ, зокрема поява нових типологій, розриви в регуляторному контролі між країнами, недотримання міжнародних стандартів, брак кваліфікованих кадрів та низька обізнаність нефінансового сектору щодо ризиків. Окремо наголошується на зростаючій ролі віртуальних активів та необхідності посилення регулювання діяльності постачальників послуг у сфері цифрових фінансів.

Висновки:

- Глобальні механізми протидії ВК/ФТ мають бути посилені шляхом гармонізації регуляторних стандартів та активнішої взаємодії між державами, фінансовими установами та міжнародними організаціями.
- Відмивання коштів та фінансування тероризму використовують схожі інструменти, зокрема підставні компанії, відмивання коштів через торгівлю та віртуальні активи, що вимагає єдиного підходу до моніторингу та виявлення підозрілих операцій.
- Сучасні виклики, такі як криптовалютні транзакції та нові типології ВК/ФТ, потребують впровадження автоматизованих аналітичних рішень та штучного інтелекту для ефективної обробки великих масивів даних.
- Брак професійних кадрів у сфері ПВК/ФТ/ФР залишається критичною проблемою, що потребує активного розвитку освітніх програм, підвищення рівня кваліфікації та залучення технологічних рішень для підвищення ефективності моніторингу.

Документ завершується рекомендаціями щодо зміцнення систем фінансового моніторингу через впровадження ризик-орієнтованого підходу, автоматизацію моніторингу підозрілих транзакцій, підвищення кваліфікації працівників, зміцнення міжнародної співпраці та сприяння обміну інформацією між державами та приватним сектором.

Документ є цінним джерелом інформації для регуляторів, банків, правоохоронних органів та фінансових установ, які прагнуть розробити ефективні стратегії протидії фінансовим злочинам та мінімізувати ризики, пов'язані з ВК/ФТ.

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-2025-07

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].