Методологічний бюлетень

Серійний номер: МінФін-AML-2025-42

Жовтень 2025

“Роби все, що в твоїх силах. Більше не може зробити ніхто”

Джон Вуден

Мета

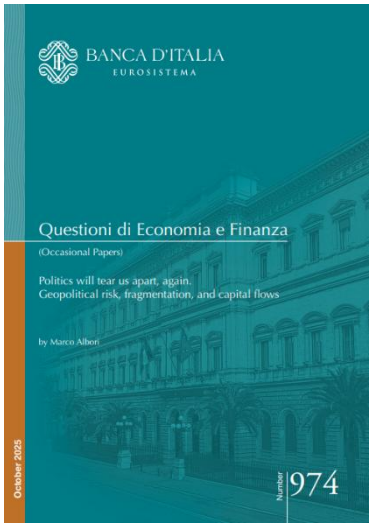
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

Містить 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

Геополітичний ризик, фрагментація та потоки капіталу [1]



Представлений огляд ЦБ Італії узагальнює емпіричні дослідження, які вивчають, як геополітичний ризик та фінансова фрагментація впливають на транскордонні потоки капіталу. Основна теза полягає в тому, що геополітичні фактори — як раптові події, так і структурні політичні розбіжності — змінюють міжнародне інвестування через процеси скорочення та перерозподілу за принципом вирівнювання (alignment-based reallocation).

Геоекономічна фрагментація визначається як багатовимірний, політико-орієнтований процес, що може спричинити розворот глобалізації, тоді як Геополітичний Ризик (ГПР) — це загроза, реалізація та ескалація несприятливих подій, пов'язаних з війнами, тероризмом або напруженістю між державами. У фінансовій сфері фрагментація проявляється в тому, що країни у політично

[1] https://www.bancaditalia.it/pubblicazioni/qef/2025-0974/QEF_974.pdf?language_id=1

узгоджених блоках активніше здійснюють кредитування та запозичення між собою, одночасно зменшуючи свою експозицію до контрагентів у конкуруючих блоках.

Вплив геополітичного ризику.

ГПР, вимірюваний переважно за новинним індексом GPR, провокує "втечу в безпеку" (flight to safety) та скорочення міжнародних потоків капіталу. Цей вплив є гетерогенним: просунуті економіки зазвичай менш чутливі і можуть навіть відчувати збільшення припливу капіталу, тоді як ринки, що розвиваються (EME), є більш вразливими до раптових зупинок і перерозподілу. Наприклад, зростання глобального ГПР зменшує як припливи, так і відтоки, але сильніший негативний ефект спостерігається в EME, де знижуються прямі інвестиції (FDI), портфельні інвестиції та інші інвестиції. Навпаки, приплив FDI до просунутих економік може зростати, оскільки багатонаціональні фірми перенаправляють інвестиції у безпечніші юрисдикції.

Дослідження підтверджують, що ГПР на рівні країни стримує FDI в EME, а інвестори США виводять кошти з EME у відповідь на зростання там ГПР, але не з провідних економік. Важливим пом'якшуючим фактором є інституційна якість та належне управління (governance) у країні-отримувачі, що частково захищає її від відтоку капіталу, особливо для EME. Крім того, виявлено ефект контагію (зараження), коли зростання ГПР в одній EME призводить до зменшення експозиції американських інвесторів до сусідніх EME.

Геополітичний ризик не лише прямо впливає на потоки, але й посилює міжнародну трансмісію інших шоків, зокрема, він збільшує негативний вплив Невизначеності Економічної Політики (EPU) на потоки капіталу і зміцнює передачу монетарної політики через кордони, безпосередньо пригнічуючи транскордонне банківське кредитування. Глобальні банки США, реагуючи на ГПР, зменшують транскордонне кредитування країн із високим ризиком, але зберігають присутність через іноземні філії, що, своєю чергою, може призводити до внутрішніх побічних ефектів на кредитування.

Висновки:

- **Геополітичний ризик як мультиплікатор фінансового ризику:** Необхідно інтегрувати індикатори ГПР (наприклад, індекс GPR) у моделі оцінки ризиків, оскільки ГПР не лише прямо впливає на потоки, а й посилює негативний вплив інших джерел нестабільності, таких як невизначеність економічної політики або жорсткість монетарної політики, що вимагає динамічного коригування лімітів експозиції та капітальних вимог.
- **Пріоритизація "вирівнювання" (alignment) належної перевірки:** Оцінка країни та контрагента має включати аналіз їхньої політичної відстані та приналежності до геополітичних блоків. Це особливо критично для інвестицій у стратегічні сектори та для операцій з EME, які є найбільш вразливими до фрагментації та подальшого скорочення капіталу.
- **Посилений моніторинг кінцевого інвестора:** Оскільки політично віддалені країни часто використовують офшорні юрисдикції для маскування справжнього походження капіталу, необхідно максимально посилити зусилля щодо ідентифікації кінцевого інвестора/власника для всіх транскордонних операцій, щоб запобігти обходу санкцій або відстежити "непряме" фінансування між конкуруючими блоками.
- **Використання інституційної якості як буфера ризику:** При роботі з EME їхня інституційна якість (наприклад, показники WGIs) повинна розглядатися як ключовий фактор пом'якшення ризику, оскільки сильніше управління істотно зменшує негативний вплив геополітичної напруги та політичної відстані на FDI та портфельні потоки.

Вплив політичних розбіжностей (Фрагментація та вирівнювання).

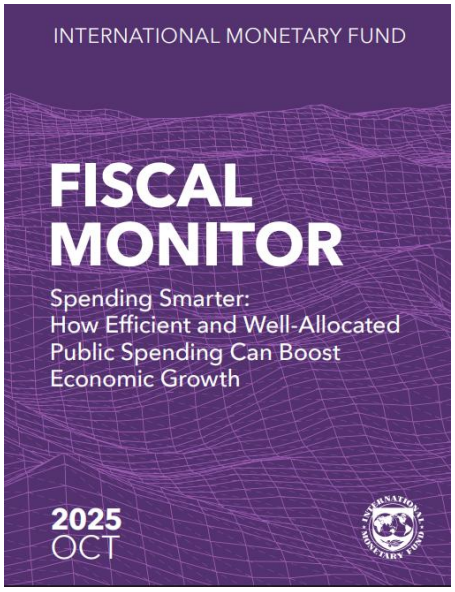
Політична відстань, вимірювана через Ideal Point Distance (IPD) на основі голосувань у ГА ООН, стає все більш визначальною для міжнародних інвестицій. Зростання геополітичної відстані систематично корелює зі зменшенням транскордонних операцій, причому цей ефект найбільший для FDI, а менш виражений для портфельних інвестицій.

Ефект фрагментації посилився з 2018 року на тлі напруженості між США та Китаєм, а також після вторгнення Росії в Україну. Зокрема, після вторгнення крос-блокові FDI та портфельні активи скоротилися. Геополітичні розбіжності найбільш суттєво впливають на інвестиції у стратегічні сектори та на інвестиції, що прямують до EME. Єврозона також демонструє чутливість до політичного вирівнювання, спрямовуючи вихідні FDI переважно до геополітично узгоджених країн, таких як США ("friend-shoring").

Незважаючи на зростаючу політичну дистанцію, інвестиції можуть продовжувати надходити до політично віддалених країн, але часто через посередницькі юрисдикції. Це особливо стосується FDI в Китай, де використання даних про кінцевого інвестора (ultimate investor data) робить негативний зв'язок між політичною відстанню та FDI статистично незначущим, на відміну від даних про безпосереднього інвестора (immediate investor data). Це підкреслює проблему використання офшорних фінансових центрів (OFCs) для маскування справжнього походження та призначення інвестицій, що є викликом для емпіричного аналізу та моніторингу.

EME загалом виявилися значно більш геоекономічно вразливими, ніж провідні економіки, особливо щодо фінансових зобов'язань (банківські та портфельні зобов'язання). Водночас, країни, які підтримують більш збалансовану геополітичну позицію (connector countries), можуть відчувати менш виражену трансмісію шоків глобального фінансового циклу. Вплив політичної близькості поширюється навіть на відносно спокійні періоди, оскільки банки та фонди коригують свої рішення після виборів, що збільшують ідеологічну відстань від США.

Розумніші витрати: як ефективні та добре розподілені державні витрати можуть стимулювати економічне зростання [2]



Представлений документ Міжнародного Валютного Фонду є глибоким дослідженням, яке пропонує відповідь на один з ключових викликів сучасної глобальної економіки: як стимулювати стійке економічне зростання в умовах уповільнення продуктивності праці, значного фіскального тиску через зростаючі борги та підвищені потреби у витратах на оборону, старіюче населення та економічний розвиток. Автори свідомо зміщують фокус з простого нарощування обсягів державних видатків на їхню якість, розкриваючи стратегію "розумних витрат". Ця стратегія стоїть на двох фундаментальних опорах: алокативній ефективності, тобто свідомому перерозподілі бюджетних коштів на користь сфер, що мають доведений потенціал для стимулювання зростання (public investment, education, health, and R&D), та технічній ефективності, що полягає у максимізації віддачі та результатів від кожного витраченого долара.

Центральна теза дослідження полягає в тому, що уряди більшості країн світу мають значний, часто недооцінений, потенціал для прискорення економіки саме через оптимізацію цих двох

[2] https://www.imf.org/en/Publications/FM/Issues/2025/10/07/fiscal-monitor-october-2025

аспектів. Аналіз виявляє тривожну тенденцію в структурі глобальних державних витрат: вони не є оптимально налаштованими на зростання. Зокрема, частка державних інвестицій у загальній структурі витрат у світі знизилася до 18%. Наприклад, у розвинених економіках вона впала з 13% до 11% у період з 1995-2009 до 2010-22 років, а на ринках, що розвиваються (без урахування Китаю), – з 22% до 20%. Водночас витрати на заробітну плату в державному секторі залишаються надзвичайно високими, складаючи в середньому близько 25% від загальних видатків у розвинених країнах та 28% на ринках, що розвиваються. Ця ситуація поглиблюється існуванням значних премій у заробітній платі держслужбовців порівняно з приватним сектором (в середньому 13% на ринках, що розвиваються), що може спотворювати ринки праці.

Для кількісної оцінки технічної неефективності документ вводить поняття "розривів в ефективності" (efficiency gaps). Ці розриви показують, наскільки країни далекі від "фронтиру виробничих можливостей" — тобто від рівня, на якому працюють найефективніші держави. Масштаб цих розривів вражає: в середньому, країни могли б отримувати на 30-40% більше віддачі ("value for money"), просто впровадивши найкращі світові практики. У розрізі груп країн ці розриви становлять близько 31% у розвинених економіках, 34% на ринках, що розвиваються, та 39% у країнах з низькими доходами. Найбільш критичною є ситуація у сферах державних інвестицій та науково-дослідних і дослідно-конструкторських робіт (НДДКР).

Висновки:

- **Пріоритет — зміцнення інституцій для підвищення ефективності.** Фундаментальною передумовою для отримання віддачі від державних витрат є якість управління. Аналіз прямо пов'язує низький рівень корупції, сильне верховенство права та ефективні практики управління державними інвестиціями з вищою ефективністю витрат. Таким чином, практична дія полягає не просто у збільшенні фінансування певних секторів, а в першочерговому впровадженні прозорих процедур відбору проєктів, контролю за їх виконанням та боротьбі з корупцією.
- **Систематичні огляди витрат є доведеним інструментом оптимізації.** Документ наголошує, що регулярне проведення оглядів державних витрат — це ефективний механізм для виявлення неефективних програм та створення фіскального простору. Рекомендація полягає в інституціоналізації таких оглядів та їх інтеграції в щорічний бюджетний процес. Як показує досвід Словаччини, це дозволяє ідентифікувати потенційну економію до 7% від загальних витрат та успішно скорочувати надлишкові витрати, зокрема на заробітну плату в державному секторі, вивільняючи ресурси для пріоритетних інвестицій.
- **Максимальний економічний ефект досягається через подвійну стратегію.** Найважливіший результат, який демонструє моделювання, полягає в тому, що економічні вигоди максимізуються лише при одночасному застосуванні двох підходів: перерозподілу коштів у продуктивні сфери (інфраструктура, людський капітал) та підвищенні ефективності їх використання. Інвестування без підвищення ефективності призводить до марнування ресурсів, оскільки вигоди в неефективних середовищах є мінімальними. Наприклад, покращення ефективності державних інвестицій на 10 % може збільшити віддачу від їхнього зростання на 1.4% ВВП протягом десятиліття.

Дослідження переконливо доводить, що першопричиною низької ефективності є слабкість державних інституцій. Емпіричний аналіз підтверджує, що країни з нижчим рівнем корупції, сильнішим верховенством права та більш ефективними процесами управління державними інвестиціями систематично демонструють вищу ефективність витрат. Наприклад, підвищення контролю над корупцією на одне стандартне відхилення асоціюється зі зростанням ефективності

витрат на освіту на 3.5 відсоткових пункти. Додатковим суттєвим бар'єром на шляху реформ є "жорсткість" (rigidity) державних витрат — наявність юридичних, контрактних та інституційних зобов'язань, які обмежують здатність уряду оперативно змінювати структуру бюджету. У розвинених економіках приблизно третина всіх видатків є "жорсткими", що значно ускладнює перерозподіл коштів на користь пріоритетних напрямків.

Найбільш вагомою частиною доповіді є моделювання потенційних економічних дивідендів від реформ. Результати показують, що перерозподіл лише 1% ВВП від непріоритетних державних витрат (наприклад, загальних адміністративних послуг) до інвестицій в інфраструктуру може збільшити обсяг виробництва на 1.5% у розвинених економіках та на 3.5% на ринках, що розвиваються, у довгостроковій перспективі. Ще більший потенціал мають інвестиції в людський капітал (освіта та охорона здоров'я): аналогічний маневр може призвести до зростання ВВП на 3% та 6% відповідно.

Однак ключовий, фундаментальний висновок дослідження полягає в тому, що ефективність діє як мультиплікатор цих вигод. Реформи з перерозподілу коштів дають максимальний ефект лише в середовищі з високою якістю управління. Аналіз показує, що у країнах з високоефективними державними інвестиціями (на рівні 75-го процентилю) віддача від їх збільшення становить близько 8% ВВП за 10 років, тоді як у країнах з низькою ефективністю (25-й процентиль) вона є статистично незначущою. Більше того, поступове закриття існуючих "розривів в ефективності" може саме по собі забезпечити додаткове зростання ВВП на 1.5% у розвинених країнах та від 2.5% до 7.5% на ринках, що розвиваються. Таким чином, документ доводить, що шлях до сталого зростання в сучасному світі лежить не стільки через пошук додаткових ресурсів, скільки через мудре та ефективне управління вже наявними.

Звіти окремих інституцій та експертів

Нарко-економіка та нова карта кримінальної геополітики Близького Сходу [3]

Аналітична стаття від OCCRP розкриває масштабну еволюцію найбільшого синтетичного наркотичного бізнесу у регіоні після краху режиму Башара аль-Асада. Це не просто історія про наркоторгівлю — це приклад того, як держава, що колись контролювала кримінальний ринок, поступово перетворила його на децентралізовану, самовідтворювану економічну систему, яка продовжує існувати поза рамками політичної влади.

Каптагон, амфетаміновий стимулятор, що колись виготовлявся як медичний препарат у Європі, став у Сирії символом війни та корупції. Режим Ассада, ізольований міжнародними санкціями, побудував на ньому повноцінну фінансову піраміду виживання, у якій армія, спецслужби та кримінальні угруповання контролювали кожен етап — від виробництва до транзиту. Після його падіння система не розвалилася — вона мутаційно адаптувалася, перейшовши до регіональної форми організації. Замість централізованих лабораторій — сотні невеликих мобільних хімічних пунктів, замість державного нагляду — мережі автономних «кураторів» із числа колишніх військових і бізнесменів, що тепер працюють на приватні картелі.

[3] https://www.occrp.org/en/feature/captagon-drug-networks-adapt-and-survive-in-middle-east-after-assads-fall

У 2024–2025 роках розслідувачі OCCRP, ARIJ та SIRAJ виявили, що основні маршрути контрабанди каптагону тепер проходять не лише через Ліван і Йорданію, а й через Туреччину, Іракський Курдистан та Перську затоку. Хоча перехідний уряд Сирії публічно заявив про "повну ліквідацію виробництва", факти на місці свідчать протилежне: замість фабрик — тисячі пересувних лабораторій, замість системи контролю — гнучка кримінальна інфраструктура. Саме тому, як підраховують експерти New Lines Institute, у 2025 році обсяг незаконного виробництва залишається на рівні понад $5 млрд, що перевищує довоєнні показники.

У Латакії, Дамаску, Дераа та Хомсі правоохоронці регулярно фіксують "зачистки", що перетворилися на медіа-шоу. Після кожної гучної операції виникає нова хвиля лабораторій — тепер ще більш мобільних і розосереджених. Влада звітує про мільйони вилучених пігулок, але експерти визнають: реальна кількість виробленого каптагону у десятки разів більша, і лише 10–15% потрапляє у статистику.

Головною причиною стійкості цього бізнесу є соціальна база. Війна залишила після себе покоління людей без роботи, доходів і майбутнього. Для них виготовлення або транспортування каптагону — не злочин, а єдиний засіб виживання. У районах, зруйнованих війною, він став і валютою, і продуктом, і засобом контролю — наркотик, що знеболює бідність. Саме тому каптагон часто називають "таблеткою бідності". У деяких селах виробництво наркотику стало сімейною справою — від підлітків до літніх людей.

Регіональна географія злочину також змінилася. Ліван і надалі залишається ключовим центром виробництва, але тепер до процесу долучилися йорданські, іракські та курдські кримінальні структури, які створюють спільні лабораторії у прикордонних зонах. За даними UNODC, у 2025 році у Йорданії було вилучено понад 200 мільйонів пігулок, але обсяги трафіку залишилися стабільними. Це означає, що виробництво стало саморегульованим ринком, який не потребує державного патронажу — він живе на логіці прибутку та безкарності.

Водночас спостерігається нова тенденція — "європеїзація" каптагону. У Туреччині, Болгарії, Італії й навіть Німеччині з'являються докази того, що у припортових містах відкриваються невеликі лабораторії, пов'язані із сирійськими та ліванськими діаспорами. У 2024 році на півдні Німеччини вилучено понад 3 млн пігулок, замаскованих під партію знеболювальних. Це доводить, що європейський чорний ринок поступово інтегрується в ближньосхідну наркоекономіку, і спроби локалізувати проблему лише в межах Сирії вже безглузді.

Каптагон перетворився на політичний інструмент і джерело впливу. Колишні військові еліти використовують його для фінансування приватних армій, місцевих адміністрацій і навіть політичних партій. Таким чином формується "тіньова держава", у якій

Висновки:

- **Необхідно створити регіональний координаційний центр** із боротьби з синтетичними наркотиками під егідою UNODC, який об'єднає Сирію, Ліван, Йорданію та Ірак у спільну систему обміну розвідданими та хімічного моніторингу прекурсорів.
- **Держави Близького Сходу мають розробити спільний механізм контролю за фармацевтичним імпортом** із Китаю та Індії, щоб запобігти незаконному ввезенню прекурсорів, які живлять каптагонову індустрію.
- **Боротьба з виробництвом каптагону повинна доповнюватися соціальними програмами у зонах ризику** — альтернативною зайнятістю, освітою та медичними програмами для молоді, яка стає робочою силою картелів.
- **Міжнародні фінансові розслідування мають відстежувати тіньові потоки коштів**, що надходять від торгівлі каптагоном, і запроваджувати санкції проти осіб, пов'язаних із "експортом війни через наркотики".

наркотик виконує роль бюджету, що живить нові центри сили. Цей феномен нагадує кланову економіку у Колумбії після падіння Медельїнського картелю, де зруйнована централізація породила безліч дрібних, але агресивних груп.

Особливо небезпечним є зростання транснаціонального виміру. Лабораторії отримують прекурсори з Китаю, Індії та навіть Східної Європи. За ланцюгами поставок стоять легальні хімічні компанії, які маскують поставки під фармацевтичні потреби. Це дозволяє картелям діяти у напівлегальній зоні, використовуючи лазівки міжнародного контролю за прекурсорами.

На цьому тлі боротьба з каптагоном дедалі більше нагадує боротьбу з ідеєю, а не з речовиною. Поліцейські рейди не змінюють логіку злочину, бо вона вбудована в економічну реальність регіону. У зоні, де рівень безробіття перевищує 60%, а держава втратила легітимність, наркотик став замінником соціального контракту. Він годує, фінансує й навіть об'єднує спільноти, що живуть поза законом.

Якщо тенденція збережеться, Близький Схід ризикує стати новим аналогом Південної Америки 1980-х років, де наркотики не лише збагачують злочинців, а й визначають політику, фінанси та міжнародні відносини. Після падіння режиму Ассада каптагон перестав бути "сирійською проблемою" — він став символом виживання поствоєнної економіки, що підживлює нестабільність у всьому регіоні.

У підсумку, каптагон — це не просто наркотик, а дзеркало соціальної руїни. Він показує, що навіть після падіння диктатур злочинна система може не лише вижити, а й еволюціонувати, створивши нову форму тіньового капіталізму, де наркотик стає політичним інструментом, а кримінал — основою державності.

Як російський нікель продовжує живити зелену економіку Заходу [4]

Розслідування Global Witness розкриває системну брехню, яка стоїть за фасадом «зеленого переходу» Європи — парадоксальну ситуацію, коли стратегічні метали для кліматичної трансформації фактично фінансують російську воєнну економіку. Йдеться про масштабну схему постачання російського нікелю на ринки ЄС і США через "санкційну шпарину" у Фінляндії, що дозволяє металу з «Норильського нікелю» (Nornickel) — компанії, контрольованої олігархом Володимиром Потаніним, близьким до Кремля — легально потрапляти до західних виробників акумуляторів, електромобілів і сталі.

Після вторгнення росії в Україну Захід обмежив експорт нафти, газу та нафтопродуктів, але нікель, титан і паладій залишилися поза санкційними списками — з огляду на їх критичну роль для «зеленої» промисловості. Ця прогалина створила величезну сіру зону, яку російські корпорації перетворили на стратегічний канал надходжень. Згідно з даними Global Witness, лише за 2024 рік у ЄС імпортовано російського нікелю на 1,3 мільярда доларів, більшість через фінське підприємство Norilsk Nickel Harjavalta Oy — дочірню компанію Nornickel, розташовану у місті Хар'явалта, неподалік Гельсінкі.

Механізм обходу санкцій виглядає простим, але юридично бездоганним. Російська руда доставляється до Фінляндії через залізничний пункт Вайніккала, далі переробляється у вигляді

[4] https://globalwitness.org/en/campaigns/transition-minerals/sanctions-gap-lets-russian-mined-nickel-flow-to-western-markets/

нікелевих брикетів або катодів, і таким чином отримує нову "юридичну ідентичність" — походження з ЄС. Американські санкції, запроваджені у квітні 2024 року, не поширюються на товари, "суттєво перероблені" у третіх країнах, а Європейський Союз досі не ухвалив аналогічних обмежень. У результаті нікель із російського Заполяр'я легально потрапляє до США, ЄС і навіть Японії, фактично підживлюючи російську металургійну галузь.

Згідно з митними даними, проаналізованими Global Witness, у період із квітня по вересень 2024 року до Фінляндії прибуло понад 18 тисяч тонн російського нікелю. Далі метал постачався через німецькі порти Гамбург і Бремен до США, де його купували Traxys (Люксембург), TMP Metals (США) та Umicore (Бельгія) — компанії, що спеціалізуються на акумуляторах для електромобілів. Цей ланцюг дозволяє Nornickel не лише зберегти, а й розширити частку на світовому ринку — понад 20% світового виробництва нікелю, який є критично важливим елементом для акумуляторів і сталі.

Розслідування Global Witness доводить, що саме Harjavalta стала "санкційним буфером" Європи, адже підприємство не входить у санкційні списки, попри те що його власник Потанін — під санкціями США, Канади та Великої Британії. Усі платежі за сировину і продукцію йдуть через дочірні офшорні структури в Швейцарії, на Кіпрі та у Великій Британії, які формально не порушують обмежень. Таким чином, система побудована так, що жодна ланка формально не винна, але всі вони спільно підтримують російський воєнний бізнес.

Особливо показово, що Фінляндія, новий член НАТО і голосний критик російської агресії, стала транзитною артерією російських металів. Державні компанії, як-от Fortum і Finnish Minerals Group, на словах декларують «повне розмежування з росією», проте на практиці вони інтегровані в ту саму логістичну інфраструктуру — залізничні, енергетичні й портові маршрути, які використовує Harjavalta. Фінська влада визнає, що підприємство є "надто значущим для економіки", аби його закрити, — і це фактично робить країну ключовим посередником між Кремлем і Заходом.

Це створює глибокий моральний і геополітичний парадокс. ЄС одночасно декларує лідерство у боротьбі зі зміною клімату та фінансує режим, який веде війну, спираючись на токсичні видобувні галузі. Нікель, що лежить в основі електромобільних батарей, добувається у Норильську — місті, побудованому на кістках політв'язнів ГУЛАГу, де рівень забруднення атмосфери перевищує 10-кратні норми ВООЗ, а викиди діоксиду сірки щороку сягають понад 1,25 мільйона тонн. У 2020 році там сталася одна з найбільших екологічних катастроф сучасності — розлив 21 тисячі тонн дизельного палива у річку Амбарна, проте компанія уникла реальної відповідальності.

Спроба Nornickel "відбілити імідж" через зелені звіти, сертифікацію ESG та участь у кліматичних форумах — класичний приклад "зеленого камуфляжу" (greenwashing). За словами експертів Arctida, російські корпорації масово використовують «зелену риторику» як засіб легалізації токсичного капіталу. У результаті, Європа отримує "чисту" сировину з брудних джерел, перекладаючи екологічні й етичні витрати на інші народи й території.

Проблема набуває ще гострішого звучання, якщо врахувати, що нікель — це не лише питання клімату, а й питання безпеки. Росія заробляє на ньому мільярди доларів, які конвертуються у виробництво зброї, утримання репресивного апарату та фінансування війни. Парадокс полягає в тому, що Європа намагається звільнитись від російського газу, але потрапляє у залежність від російського металу.

Ситуація з "санкційною діркою" показує структурну вразливість європейської політики: Енергетичні санкції працюють, а мінеральні — буксують. Нафтогазовий тиск був політичним, а металургійний — технологічним: без нікелю, паладію, титану й платини не працюватимуть європейські заводи акумуляторів, вітряки й електромобілі. Але така "реалістична" логіка

створює етичну пастку, у якій фінансова стабільність ЄС прямо залежить від порушення його власних цінностей.

У політичному вимірі ця історія демонструє непослідовність Заходу у санкційній архітектурі. Поки США, Велика Британія та Канада обмежили імпорт стратегічних металів, ЄС залишається останнім безпечним ринком для російського нікелю. У цьому контексті ініціатива Європейського акта про сталу корпоративну належну перевірку (CSDDD) виглядає радше декларацією, ніж інструментом: під тиском промислового лобі Брюссель зменшує обсяг зобов'язань компаній перевіряти ланцюги постачання та відповідати за порушення прав людини. Таким чином, санкції перетворюються на політичний ритуал — гучний, але неефективний.

Висновки:

- **Європейський Союз має терміново закрити "фінське вікно" для російського нікелю**, ухваливши санкції, аналогічні американським і британським, аби припинити непряме фінансування військової економіки РФ.
- **Необхідно створити єдиний європейський реєстр походження стратегічних металів** (Nickel & Cobalt Traceability Registry), що дозволить відстежувати ланцюг постачання від шахти до кінцевого виробника та виключити "брудні" ресурси.
- **Європейські компанії повинні нести юридичну відповідальність за закупівлю сировини,** що сприяє фінансуванню авторитарних режимів, відповідно до принципів ESG і нового корпоративного законодавства ЄС.
- **Україні слід ініціювати в рамках ЄС та FATF створення окремої категорії санкцій проти металургійних активів,** що прямо чи опосередковано підтримують російську військову індустрію, щоб посилити глобальну санкційну узгодженість.

Найбільш цинічний аспект — це парадокс "зеленої революції", яка фактично тримається на ресурсах авторитарних держав. Європейські виробники електромобілів, прагнучи мінімізувати вуглецевий слід, насправді збільшують "етичний слід", спираючись на метал, добутий у регіонах із рабською працею, екологічною катастрофою й воєнним фінансуванням. У цьому сенсі російський нікель — це нова нафта XXI століття, лише замаскована під "зелену".

Якщо Європейський Союз прагне реальної незалежності, він має закрити "фінські шлюзи" російського експорту, запровадити повне ембарго на металургійну продукцію кремля, створити єдиний реєстр походження стратегічних металів і розвивати власні потужності з переробки у партнерстві з демократичними країнами. Інакше "зелений перехід" ризикує стати не шляхом до сталого майбутнього, а маршем у бік токсичної залежності, де екологія і геополітика переплелися у смертоносному вузлі з грошима москви.

Рекомендовані матеріали та події

Дебати: Санкції не працюють як інструмент зовнішньої політики [5]

Дебати розкривають глибокі та суперечливі аспекти застосування обмежувальних заходів у сучасній геополітиці. Основна дискусія розгортається навколо тематики: «Санкції не працюють як інструмент зовнішньої політики». Зміст дебатів є критично важливим для фахівців із фінансового моніторингу, оскільки він прямо стосується ефективності інструментів, що використовуються для заморожування активів, торговельних ембарго та заборон на поїздки.

[5] https://www.youtube.com/watch?v=5xjdDzIylrg

Дебати висвітлюють два протилежні погляди: з одного боку, санкції є необхідним і працездатним інструментом, що накладає значні економічні та фінансові витрати; з іншого боку, вони є неефективним "політичним театром", який не досягає своїх кінцевих зовнішньополітичних цілей і завдає шкоди цивільному населенню.

Позиція "Санкції працюють" (Едвард Лукас, Том Кітінг). Прихильники цієї позиції наголошують, що санкції працюють, якщо визначити "працюють" як здатність змінювати поведінку або накладати значні, вимірювані економічні витрати. Том Кітінг підкреслює, що санкції активно виконуються в глобальній фінансовій системі: банки по всьому світу — від Лондона та Нью-Йорка до Сінгапуру та Сеула — постійно блокують транзакції та заморожують активи, що свідчить про їхній глобальний вплив, зумовлений контролем Західних столиць над фінансовою системою. Як переконливий доказ їхньої ефективності наводяться випадки іммобілізації 300 мільярдів доларів Центрального банку Росії у 2022 році та 70 мільярдів доларів Центрального банку Лівії у 2011 році. Санкції також зіграли центральну роль, змусивши Іран сісти за стіл переговорів щодо ядерної угоди у 2015 році, обмеживши його експорт нафти та доступ до міжнародної фінансової системи. На індивідуальному рівні санкції США проти транснаціональної організованої злочинності (так звані Kingpin sanctions) призводять до "Muerta Civil" (громадянської смерті) цільових осіб, унеможливлюючи їхню ділову активність та роблячи їх токсичними. Едвард Лукас додає, що цільові санкції, такі як режим Магнітського, порушують клімат безкарності, не дозволяючи катам і шахраям вільно подорожувати та відмивати вкрадені гроші через західні банки. Хоча санкції не є чарівною паличкою, вони є важливим інструментом, який, зокрема, скоротив доходи Росії від експорту викопного палива на половину (з 1 мільярда доларів на день до півмільярда).

Позиція "Санкції не працюють" (Ієн Прауд, Ребекка Гардінг). Опоненти стверджують, що санкції є неефективними, оскільки вони не досягли своїх найважливіших зовнішньополітичних цілей, визначених у законодавстві — припинення дестабілізуючих дій Росії в Україні та запобігання повномасштабному вторгненню. Ієн Прауд, який сам санкціонував близько половини британських санкцій проти Росії, зазначає, що Росія стала найбільш підсанкційною країною у світі (понад 20 000 санкцій), проте війна триває, а Україна повністю залежить від зовнішньої допомоги. З його досвіду, 92% індивідуальних санкцій на обмеження поїздок, накладених Великою Британією на громадян Росії, були спрямовані проти осіб, які ніколи не відвідували Велику Британію і не планували цього. Ідея про те, що олігархи, активи яких були конфісковані (наприклад, Роман Абрамович), повстануть проти Путіна, є "фантазією". Натомість, кожна нова хвиля санкцій лише підтверджує в очах пересічних росіян пропагандистський наратив Путіна про ненависть Заходу до Росії, що збільшує його внутрішню політичну підтримку. Ребекка Гардінг підходить до питання з економічної точки зору, заявляючи, що санкції ефективні лише у 34% випадків, де цілі чітко визначені та вимірювані. Головний недолік полягає в тому, що санкції "мілітаризують торгівлю", що призводить до непередбачуваних наслідків, таких як зростання цін на енергоносії та продовольство, які шкодять західним економікам і посилюють популістські настрої. Більше того, санкції стимулюють Росію та інші країни шукати альтернативи доларовій системі, використовуючи китайську міжбанківську платіжну систему (CIPS) та цифрові активи/Bitcoin для обходу обмежень.

Особливу увагу приділено стратегічним імплікаціям:

1. Проблема "Виходу" (Off-ramp): Критики зазначають, що більшість режимів санкцій не мають чітко визначеного "виходу" — умов, за яких обмеження будуть зняті, що підриває їхню дипломатичну ефективність як інструменту примусу до зміни поведінки. Це розглядається як провал зовнішньої політики, а не самого інструменту.
2. Розмивання цілей та "Сигналізація": Виникає суперечка щодо того, чи є санкції інструментом примусу, чи лише інструментом "сигналізації" (signaling) — демонстрацією геополітичної позиції. Критики вважають, що якщо санкції використовуються лише для "сигналізації" без досягнення конкретного впливу, вони не можуть вважатися ефективним інструментом зовнішньої політики.
3. Гуманітарні та Супутні Ризики: Було піднято гостре питання про вимірювання супутної шкоди, яку санкції завдають цивільному населенню, що живе в авторитарних режимах (на прикладі Сирії та Росії). Ця шкода не лише не досягає цілі зміни режиму, але й посилює владу диктаторів через пропаганду.

У кінцевому підсумку, хоча опоненти визнали, що санкції можуть працювати в окремих випадках, прихильники стверджували, що санкції є необхідним, хоча й недосконалим, інструментом у ширшому наборі інструментів (tool-box) зовнішньої політики. Фахівці з ПВК/ФТ повинні враховувати, що санкції, як форма економічної сили, продовжують використовуватися навіть не західними країнами (Індією, Китаєм), і є проявом економічної та політичної могутності.

Цифрові фінанси в ЄС: орієнтування в нових технологічних тенденціях та революції штучного інтелекту [6]

Даний документ, який є збірником статей, підготовленим у рамках EU Supervisory Digital Finance Academy (EU-SDFA). Основний зміст роботи зосереджений на всебічному вивченні впливу цифровізації та штучного інтелекту (AI) на фінансовий сектор Європейського Союзу, охоплюючи макротенденції, регуляторні зміни, можливості та системні ризики.

Звіт підкреслює, що впровадження AI у фінансовому секторі відбувається з безпрецедентною швидкістю, що зумовлено значним зростанням обсягів даних, збільшенням обчислювальної потужності та прогресом у технологіях, таких як глибоке навчання та генеративний AI. Хоча AI пропонує значні переваги, такі як підвищення операційної ефективності, оптимізація обслуговування клієнтів, покращення управління ризиками, включаючи більш точну оцінку кредитоспроможності та виявлення шахрайства, його широке використання також створює нові та посилює вже існуючі ризики для фінансової стабільності.

Ключовим аспектом регуляторного ландшафту ЄС є його проактивний підхід, спрямований на створення чітких "правил гри" для стимулювання інновацій, а не лише реакції на них. У цьому контексті документ детально описує ключові регуляторні ініціативи, що формують сферу цифрових фінансів, такі як MiCA (щодо ринків криптоактивів), DORA (щодо цифрової операційної стійкості, застосування якої розпочнеться з січня 2025 року), AI Act (перша у світі комплексна правова база для AI) та пакет FiDA/PSD3 (для відкритого доступу до фінансових даних та

[6] https://cadmus.eui.eu/entities/publication/ddecfb8d-061d-5a69-8559-0e88b7fb1c85

модернізації платіжних послуг). Зазначається, що використання AI у фінансовому секторі, наприклад, для оцінки кредитоспроможності фізичних осіб або ризиків у сфері страхування життя та здоров'я, класифікується як високоризикове згідно з AI Act, що накладає суворі вимоги щодо управління ризиками, прозорості та аудиту.

З погляду фінансових ризиків та нагляду, використання AI породжує системні загрози, які вимагають постійного моніторингу. До них належать ризик концентрації, спричинений надмірною залежністю фінансових установ від обмеженої кількості великих сторонніх постачальників (насамперед BigTechs) хмарних та AI-послуг; ризик взаємозв'язку та стадної поведінки, коли використання подібних AI-моделей, навчених на ідентичних даних, може призводити до корельованих рішень у всьому фінансовому секторі, посилюючи волатильність та ризик флеш-крахів; а також операційний ризик, посилений кіберзагрозами, здатністю генеративного AI створювати реалістичні діпфейки та загальною вразливістю системи до єдиної точки відмови. Надзвичайно важливим є ризик моделі, зокрема "проблема чорного ящика", коли складність моделей глибокого навчання робить їхні рішення непрозорими, що ускладнює пояснюваність та аудит, а також ризик упередженості, вбудованої у навчальні дані, що може призвести до дискримінаційних результатів у кредитуванні чи страхуванні.

У контексті експертизи ПВК/ФТ/ФР, документ підтверджує, що інструменти SupTech (наглядові технології), які використовують AI, є критично важливими для регуляторів. Зокрема, рішення SupTech застосовуються для посилення нагляду у сфері ПВК/ФТ/ФР (AML/CFT/CPF), дозволяючи використовувати розширену аналітику даних для оцінки ризиків та контрольних механізмів піднаглядних суб'єктів. Приклади включають застосування мережевого аналізу для відстеження переказів коштів у юрисдикції з високим ризиком та використання машинного навчання для аналізу внутрішніх контрольних систем банків. Однак, Національні компетентні органи стикаються з внутрішніми бар'єрами у впровадженні SupTech, такими як обмеження бюджету, залежність від застарілих IT-систем та, що найбільш важливо, нестача кваліфікованих людських ресурсів та навичок у сфері AI та аналізу даних.

Нарешті, документ порушує питання геополітики цифрових фінансів (цифровий суверенітет, технологічна перевага) та впливу AI на сталість (ESG). Хоча AI може сприяти управлінню ESG-ризиками (наприклад, оцінка кліматичних ризиків), значне енерго- та водоспоживання, необхідне для навчання генеративних моделей, створює власні екологічні ризики, які фінансові установи мають враховувати у своїх непрямих викидах (Scope 3).

Інші новини

Штучний інтелект у злочинах: як Бразилія стала полігоном для шахрайства [7]

Аналітична стаття від Insight Crime розкриває, як технологічний прогрес у Бразилії, що мав стати двигуном цифрової модернізації, перетворився на нову арену для злочинців, озброєних штучним інтелектом. За останні два роки країна стала одним із найнебезпечніших цифрових просторів Латинської Америки: згідно з офіційними оцінками, лише у 2024 році громадяни втратили понад 54 мільярди доларів унаслідок кібершахрайств, а третина населення зазнала прямих або непрямих атак. Бразилія, де 86% громадян мають доступ до інтернету та понад 217 мільйонів смартфонів перебувають в активному обігу, створила ідеальне середовище для синтезу технологічних інновацій і злочинної винахідливості.

[7] https://insightcrime.org/news/ghost-riders-and-deepfake-doctors-inside-brazils-ai-driven-crime-surge/

Особливо небезпечною стала поява Pix — державної системи миттєвих платіжів, яка стала зручним інструментом як для користувачів, так і для злочинців. Вона дозволяє перекази між рахунками за секунди, без банківських комісій, що в поєднанні з відсутністю ефективного моніторингу створило платформу для масштабного відмивання коштів. Більшість злочинних схем у Бразилії сьогодні так чи інакше обертаються навколо Pix, який став "цифровою артерією" кримінальної економіки. Згідно з даними Центробанку, система обробляє понад 6 мільярдів транзакцій щомісяця, і саме швидкість її роботи робить неможливим оперативне реагування правоохоронців.

Однією з найрезонансніших схем стали "Примарні водії Uber" у Ріо-де-Жанейро. Шахраї використовували генеративні моделі штучного інтелекту, щоб створювати фейкові обличчя, підробляти посвідчення та обходити біометричну перевірку платформи. Далі AI-боти бронювали поїздки між фіктивними пасажирами та "водіями", накручуючи вартість маршруту, після чого гроші миттєво переводилися через Pix на підставні рахунки. За даними слідства, лише один злочинець таким чином заробив понад $136 000 менш ніж за пів року. Схема виявилася настільки масштабною, що Uber змушений був створити окрему внутрішню команду цифрової безпеки, яка аналізувала транзакції за допомогою машинного навчання — перший прецедент співпраці між приватною платформою та поліцією у сфері AI-злочинності.

Інший вид шахрайства — "фейкові лікарі. Злочинці генерували обличчя лікарів, створювали підроблені документи та реєстрували фіктивні профілі у державній системі цифрової ідентифікації Gov.br. Ці "AI-лікарі" відкривали банківські рахунки, отримували доступ до кредитів і навіть використовували державні пільги. Група діяла в кількох штатах — Сан-Паулу, Пара, Еспіріту-Санту — і, за оцінками поліції, відмила щонайменше $130 000 за три місяці. Особливість злочину полягала в тому, що AI навчився не лише створювати візуально переконливі обличчя, але й імітувати поведінку реальних людей — їхню манеру писати, голос, медичну лексику. Це означає, що майбутнє шахрайство може перестати бути "технічним" і стати повністю персоніфікованим, коли AI фактично "краде" особистість.

Адвокат і кіберексперт Гільєрме Гуейрос зазначає, що слабкість системи KYC (Know Your Customer) в Бразилії створює основну передумову для цих злочинів. Банки мають обов'язок перевіряти клієнтів, але часто покладаються на застарілі механізми верифікації, не здатні виявити штучно згенеровані обличчя або синтетичні документи. Судова система також не встигає реагувати: запити на розкриття банківської інформації тривають місяцями, тоді як перекази через Pix відбуваються миттєво.

Не менш небезпечним є феномен керованого фішингу. Група під назвою PINEAPPLE створила десятки фальшивих сайтів урядових установ, клони державних порталів і мобільні додатки, які ідеально імітували оригінальні сторінки податкової служби та міністерств. Вони використовували генеративні AI-платформи для автоматичного створення контенту, дизайну й навіть чат-ботів для "консультацій". Після введення даних користувачами — номерів ідентифікації, банківських реквізитів, PIN-кодів — інформація потрапляла до злочинців, які знімали кошти через Pix. У 2024 році лише ця група ошукала понад 10 000 осіб на загальну суму понад $160 000.

Компанія Zscaler ThreatLabz, яка відстежує кіберзагрози, виявила нову генерацію таких шахрайських платформ: вони використовують AI для SEO-оптимізації, тобто автоматично просуваються на перші позиції у пошуку Google. Це означає, що навіть досвідчені користувачі можуть потрапити на фішинговий сайт, не підозрюючи підробку. Ця еволюція кіберзлочинності створює "ефект довіри за замовчуванням" — люди сприймають технологічно досконалий сайт як справжній, бо він виглядає "занадто добре, щоб бути фейком".

Сукупність цих тенденцій доводить: Бразилія перетворюється на тестовий полігон для злочинних інновацій, де штучний інтелект використовується не як допоміжний інструмент, а як

центральний елемент злочинної моделі. Шахраї більше не потребують складного програмування чи технічних знань — достатньо скористатися відкритими AI-сервісами, які можуть створити документи, згенерувати відео або підробити голос. Злочини стали масовими, дешевими і безособовими, а масштаби їх розповсюдження перевищують можливості правоохоронних органів навіть у найбільш розвинених штатах.

Автор статті Брюс Кей зазначає, що найглибша проблема полягає не лише у злочинах, а у психологічній трансформації суспільства, яке втрачає здатність відрізняти справжнє від фальшивого. Люди починають довіряти алгоритмам більше, ніж інституціям, і саме ця довіра стає головною зброєю злочинців. AI перестає бути технологією — він стає культурним інструментом маніпуляції.

Золото диктатури: як кримінал та армія побудували тіньову державу у Венесуелі [8]

Стаття від Mongabay розкриває глибину системного зрощення між державою, організованою злочинністю та міжнародними ринками у масштабній схемі незаконного видобутку золота, яка стала фундаментом для виживання режиму Ніколаса Мадуро.

Згідно з доповіддю Financial Accountability and Corporate Transparency (FACT) Coalition, понад 86% золота у Венесуелі видобувається нелегально, а більшість цього металу — близько $4,4 мільярда щороку — контрабандою виходить за межі країни. Йдеться не просто про тіньову економіку, а про повноцінну державну злочинну систему, у якій військові, політики та кримінальні угруповання діють як частини одного фінансового механізму, що підміняє собою державний бюджет.

Після падіння нафтових доходів у 2014 році режим Мадуро опинився на межі колапсу. Відповіддю стало створення у 2016 році Гірничої дуги Оріноко (Arco Minero del Orinoco) — офіційно задекларованого проєкту “економічного відродження”. Ця зона, що охоплює 12% території країни (близько 112 тис. км²), стала епіцентром масового нелегального видобутку золота, діамантів і міді, під контролем армії, кримінальних структур і місцевих “золотих баронів”. Замість модернізації економіки ця “реформа” створила мафіозну державу, у якій Міністерство оборони контролює шахти, а державні банки — обіг контрабандного золота.

У цій схемі ключову роль відіграє Національна армія Болівару (FANB). Офіцери отримують “квоти на видобуток” і дозволи на експлуатацію шахт в обмін на політичну лояльність. Вони керують робітниками, які працюють у нелюдських умовах по 14–16 годин на день без будь-яких засобів захисту. За доступ до шахт стягується “військовий податок” — від 10 до 20% прибутку. Фактично золото стало паралельною валютою венесуельської влади: ним платять за імпорт, зброю, політичну підтримку й утримання внутрішніх силових структур.

Сама структура контролю над регіоном нагадує феодальну систему, де кожна зона підпорядковується “команданте” — місцевому військовому, який має власну “армію”, контролює повітряні злітні смуги, карає непокірних і веде переговори з угрупованнями. За межами державного апарату діють транснаціональні кримінальні формування — зокрема колумбійська Ejército de Liberación Nacional (ELN), Segunda Marquetalia (відгалуження колишніх

[8] https://news.mongabay.com/2025/10/amid-venezuelas-illegal-gold-heist-are-armed-groups-gangs-elites-report-says/

ФАРК), Tren de Aragua та Primeiro Comando da Capital (PCC) із Бразилії. Вони ділять між собою родовища, займаються рекетом, торгівлею людьми, контролюють дороги й постачання палива.

Те, що починалось як "економічна альтернатива", перетворилось на мілітаризований бізнес, у якому золото стало еквівалентом наркотиків, а його транспортування — справжнім "золотим коридором". Золото вивозять дрібними партіями — човнами через Амазонку, літаками до Колумбії та Гайани, або через офіційні канали, підробляючи документи про "державне походження". Часто на нього оформлюють "сертифікати чистоти", які дозволяють безперешкодно експортувати його до Туреччини, Панами чи Об'єднаних Арабських Еміратів. Далі воно зливається із законним золотом і потрапляє у глобальні фінансові потоки. Таким чином, злочинна діяльність у джунглях Амазонії інтегрується у ланцюги поставок міжнародних банків і ювелірних брендів.

Соціальні наслідки цієї "золотої лихоманки" — трагічні. За даними Amazon Conservation Association, від початку роботи "Гірничої дуги" знищено понад 23 000 гектарів лісів, а у водах басейну Оріноко концентрація ртуті перевищує допустимі норми у 40 разів. Річки, що живлять десятки поселень корінних народів, стали токсичними. Жінки з племен Пемон і Каріб змушені працювати у шахтах або піддаються сексуальній експлуатації, а діти — працювати на промиванні золота. Рівень насильства у регіоні зріс утричі, а державні органи влади практично зникли. У деяких районах діє "кримінальний кодекс" замість конституції, де вбивства й катування — звична частина покарання за непослух.

За межами Венесуели цей злочинний бізнес перетворився на транснаціональну схему відмивання грошей. Через офшори Панами, карибських островів, Туреччини та ОАЕ золото легалізується через мережі компаній-прокладок. Аналітики Global Financial Integrity (GFI) зазначають, що лише у 2022 році у США було ввезено понад $350 млн "підозрілого" золота із джерел, що не відповідають сертифікації LBMA. Часто воно продавалося через торгові компанії, пов'язані з урядом Венесуели або афілійованими банками.

Одним із головних факторів, що дозволяє цій схемі існувати, є правова прогалина в міжнародному праві: незаконний видобуток золота не класифікується як "predicate offence" для переслідування за відмивання коштів. Це означає, що компанії, які купують "золото з конфліктних зон", можуть уникнути відповідальності, якщо формально доведуть його "переробку". Саме тому аналітики FACT Coalition закликають США та ЄС запровадити глобальну систему простежуваності походження золота (gold traceability) — аналог фінансового моніторингу, який би дозволив відстежувати кожен грам металу від копальні до кінцевого покупця.

Водночас політичний вимір цього процесу не менш важливий. Для режиму Мадуро золото — не просто джерело прибутку, а механізм виживання, який дозволяє йому обходити санкції, фінансувати армію, купувати підтримку союзників (зокрема Ірану, росії та Туреччини) і підтримувати мінімальний рівень валютних резервів. Таким чином, "золота економіка" стала частиною політичної стратегії виживання авторитаризму.

На міжнародному рівні зростає тиск на держави, що сприяють відмиванню "кривавого золота". У 2024 році FATF вперше офіційно включила незаконний видобуток дорогоцінних металів до ризиків глобального відмивання коштів, а ЄС розглядає нові механізми due diligence для компаній, які імпортують дорогоцінні метали з Латинської Америки. Однак, поки міжнародна система реагує повільно, злочинна модель Венесуели вже експортується — у Гайану, Сурінам, Болівію та навіть Конго.

Фактично ми спостерігаємо народження нового типу кримінальної державності, у якій ресурси стають замінником економіки, а насильство — способом адміністрування. У Венесуелі більше не існує межі між мафією, урядом і армією — усі вони є частинами одного "золотого ланцюга".

Це не просто історія про корупцію, а приклад деградації держави у фінансовий картель, який живиться природними ресурсами, людськими життями та безкарністю світових ринків.

Якщо ця тенденція не буде зупинена, “венесуельська модель” може стати шаблоном для інших кризових країн. Золото вже не просто дорогоцінний метал — це нова зброя у війні за виживання держав без економік, але з амбіціями імперій. І кожна ювелірна прикраса, виготовлена з такого золота, — це не лише символ розкоші, а й відбиток злочину, що триває у серці Латинської Америки.

Сполучене Королівство оголосило про перехід на єдиний санкційний список до 2026 року [9]

Уряд Сполученого Королівства офіційно оголосив про кардинальну реформу національної системи санкцій. Йдеться про перехід до єдиного, консолідованого переліку санкційних призначень. Ця ініціатива є стратегічно важливим кроком у розвитку автономної санкційної політики Сполученого Королівства після його виходу з Європейського Союзу, спрямованим на суттєве підвищення ефективності та прозорості санкційного комплаєнсу.

По суті, уряд оголосив про фундаментальну реформу своєї системи управління санкціями, яка полягає у консолідації всіх існуючих розрізнених санкційних списків в один уніфікований та всеохопний реєстр, що отримав назву "UK Sanctions List" (UKSL). Ключовою датою повної імплементації цих змін визначено 28 січня 2026 року. До цього моменту буде повністю припинено підтримку та оновлення Консолідованого списку Управління із застосування фінансових санкцій (OFSI), який наразі є основним джерелом для перевірки суб'єктів, що підпадають під фінансові обмеження. Цей перехід є прямою відповіддю на численні запити від представників бізнесу та фінансового сектору, які вказували на складнощі, пов'язані з необхідністю моніторингу кількох джерел для забезпечення повноцінного дотримання санкційних вимог. Основна мета полягає у ліквідації дублювання даних та спрощенні процедур перевірки, що дозволить організаціям більш ефективно розподіляти свої комплаєнс-ресурси.

Важливим аспектом є те, що новий єдиний список UKSL буде значно ширшим за своїм охопленням, ніж поточний список OFSI. Він включатиме не лише фінансові санкції, але й усі інші види обмежувальних заходів, що застосовуються Сполученим Королівством, а саме: імміграційні, торговельні та транспортні санкції. Таким чином, UKSL стане єдиним, централізованим та авторитетним джерелом інформації ("single source of truth") для всіх фізичних та юридичних осіб, які зобов'язані дотримуватися санкційного законодавства Сполученого Королівства. Це вимагатиме від компаній комплексного перегляду та оновлення своїх внутрішніх систем скринінгу та моніторингу, щоб вони були налаштовані на отримання даних саме з цього нового, розширеного джерела.

З технічної точки зору, перехід несе в собі значні зміни для автоматизованих систем комплаєнсу. Однією з ключових новацій є заміна ідентифікатора "OFSI Group ID", який використовується для групування записів, що стосуються однієї особи чи організації, на новий "Unique ID" для всіх суб'єктів. Ця зміна потребуватиме уваги з боку розробників програмного забезпечення та IT-департаментів, відповідальних за підтримку санкційних баз даних. Для полегшення цього переходу уряд також планує розширити формати файлів, у яких буде доступний UKSL. На додаток до існуючих форматів ODS, ODT, HTML та XML, будуть додані більш поширені у

[9] https://www.gov.uk/guidance/moving-to-a-single-list-for-uk-sanctions-designations-28-january-2026?utm_medium=email&utm_campaign=govuk-notifications-topic&utm_source=9608735c-12fd-49ac-8a46-d7a7fd2a4a1d&utm_content=immediately

фінансовій індустрії формати, такі як .csv, PDF та .txt, що дозволить забезпечити кращу сумісність з існуючими системами.

Для підготовки до цих змін, вже з липня 2024 року став доступним інструмент пошуку по списку UKSL, який надає можливість ознайомитися з його структурою та функціоналом. Уряд також запевнив, що продовжить публікувати офіційні повідомлення про всі нові санкції, розширивши цю практику не лише на фінансові, а й на всі інші типи санкцій. Ця ініціатива є логічним продовженням розбудови самостійної та зрілої санкційної системи Сполученого Королівства, яке прагне бути не лише ефективною у досягненні своїх зовнішньополітичних цілей, але й зрозумілою та зручною для сумлінних суб'єктів, що зобов'язані її виконувати. Організаціям наполегливо рекомендується не відкладати підготовчі заходи та завчасно розпочати процес адаптації своїх політик, процедур та технічних засобів до майбутніх змін, щоб забезпечити безперебійний та повний комплаєнс до встановленого терміну.

Для загального розвитку

Як нова ера інсайдерських атак формує глобальну архітектуру кіберзлочинності [10]

Коли у 2021 році з'явилося угруповання Medusa ransomware, воно швидко стало одним із найагресивніших гравців у сфері цифрового рекету. Сьогодні його атаки охоплюють понад 80 країн, включно з ЄС, США, Канадою та країнами Латинської Америки. За даними CISA, Medusa використовує модель "Ransomware-as-a-Service" (RaaS), у якій "афілійовані" партнери орендують доступ до шкідливого програмного забезпечення для атак на організації по всьому світу. Таким чином, Medusa діє як транснаціональна корпорація злочину: вона надає клієнтам інфраструктуру, шифрувальні інструменти, канали анонімного зв'язку, маркетингову підтримку (через dark web-сайти) і навіть "службу технічної підтримки", яка веде переговори про викуп.

Medusa діє за формулою подвійного шантажу — не лише блокує дані жертви, а й краде їх, погрожуючи публікацією на спеціальному Telegram-каналі або у даркнеті. У деяких випадках угруповання навіть надає "демонстраційні витоки" для підвищення тиску на компанії. Жертви отримують ультиматум: сплатити викуп у криптовалюті або спостерігати, як корпоративні секрети опиняються у відкритому доступі. Medusa націлюється на великі підприємства, школи, державні структури та медичні заклади — тобто тих, хто не може дозволити собі зупинку роботи. У результаті — збитки, які у 2024 році перевищили $500 млн лише у США, не враховуючи непрямі витрати на відновлення систем.

Та найнебезпечніше полягає у тому, що Medusa активно експлуатує людський фактор. Замість традиційного злому серверів чи фішингу, злочинці дедалі частіше намагаються купити внутрішній доступ. Вони пропонують гроші співробітникам компаній — адміністраторам, журналістам, технічним фахівцям — за надання логінів, токенів, доступу до внутрішніх VPN або хмарних систем. Саме цю стратегію нещодавно продемонстрували у випадку з журналістом BBC Джо Тайді, якому хакери запропонували відсоток від викупу, якщо він "допоможе" їм проникнути в інфраструктуру корпорації. Спершу пропозиція звучала як експеримент, але вона ідеально відображає еволюцію соціальної інженерії у добу штучного інтелекту.

[10] https://www.bbc.com/news/articles/c3w5n903447o https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

Злочинці більше не ховаються за безособовими фішинговими листами — вони ведуть персональні переговори, граючи на емоціях, фінансовій втомі чи кар'єрному тиску. Їхній підхід психологічно витончений: "Ти працюєш у великій компанії, вона не збідніє. А ти можеш заробити більше, ніж за все життя". Саме так будується "інсайдерська економіка злочину", яка розростається в темних куточках інтернету. На даркнет-форумах продаються корпоративні облікові дані з цінником від $100 до $20 000, залежно від рівня доступу. Так, у 2024 році Medusa та подібні угруповання використовували такі куплені обліковки для проникнення у фінансові установи Іспанії, медичні лабораторії США та муніципалітети Канади.

Інструменти Medusa відзначаються високим рівнем технологічності. Програмний код містить механізми автоматичного видалення резервних копій, відключення антивірусів і шифрування файлових систем у режимі реального часу. Сучасна версія включає компонент для зламу Windows Remote Desktop Protocol (RDP), через який більшість атак і відбувається. Після вторгнення Medusa залишає "readme.txt" із вимогами викупу та інструкціями для спілкування через Tor. Примітно, що група навіть надає можливість "купити час" — жертви можуть сплатити частину викупу, щоб відтермінувати публікацію вкрадених даних. Такий цинічний "сервіс" підкреслює, що ми маємо справу не з хаотичними хакерами, а з чітко структурованим бізнесом.

Водночас, як показує кейс із BBC, вразливість до кібератак більше не обмежується технологіями — вона глибоко людська. Хакери зрозуміли: найефективніший спосіб зламу — не обійти захист, а купити його власника. У статті BBC показано, що злочинці вербують потенційних "помічників" так само, як HR-менеджери шукають кадри: через Telegram, Signal або Dark Web, обіцяючи "легкі гроші" й абсолютну анонімність. Вони навіть проводять співбесіди — уточнюють посаду, рівень доступу, досвід. Звучить парадоксально, але у XXI столітті корпоративна зрада стала послугою з технічним супроводом.

Експерти з CISA та Europol підкреслюють: інсайдерська загроза — це нова передова кіберфронту. Жодна система багатофакторної автентифікації чи штучного інтелекту не зможе захистити компанію, якщо співробітник сам добровільно передає доступи. Більш того, злочинці дедалі частіше комбінують ці два підходи — спочатку купують внутрішній доступ, а потім запускають програми типу Medusa. Це створює гібридну модель атаки, де "інсайдер" виступає як "ключ", а програма-шкідник — як "зброя".

Ситуація ускладнюється тим, що ринок викупів стає дедалі більш організованим. Medusa, LockBit, BlackCat і Cl0p мають офіційні сайти у даркнеті з таблицями "жертв", строками сплати викупу, розділом FAQ і навіть "службою підтримки" з багатомовними чатами. Це перетворює кібервимагання на індустрію зі своєю економікою, рекламою та брендами.

Висновки із цих двох кейсів очевидні, але надзвичайно тривожні: глобальна кіберзлочинність перестала бути хаосом і стала

Висновки:

- **Організації мають впроваджувати системи поведінкового моніторингу та багаторівневої аналітики доступів**, щоб виявляти ознаки інсайдерської активності до того, як вона призведе до компрометації даних.
- **Необхідно обмежити довіру до людського фактора** — створюючи протоколи ротації паролів, тимчасові доступи та ізольовані середовища для критично важливих систем, щоб зменшити ризик продажу внутрішніх облікових даних.
- **Кібербезпека повинна включати етичні та психологічні тренінги** для співробітників, які допомагають формувати корпоративну культуру доброчесності й стійкість до спокус підкупу.
- **Міжнародна співпраця між державними та приватними секторами** має бути спрямована на створення спільних баз даних про злочинні кібермережі, що комбінують технічні атаки з соціальною інженерією.

системою. Її учасники не просто зламують коди — вони конструюють моделі поведінки, які експлуатують довіру. І якщо сьогодні підкуплений журналіст — лише окремий випадок, то завтра таким “посередником” може стати адміністратор енергосистеми, співробітник банку чи держслужбовець.

Держава повинна не лише впроваджувати нові технологічні протоколи, а й будувати культуру цифрової етики — навчати службовців, журналістів і технічних фахівців розпізнавати вербувальні спроби, повідомляти про підозрілі пропозиції, створювати внутрішні механізми довіри й захисту викривачів.

Ваша думка важлива!

1. Розслідування Global Witness демонструє, як «суттєва переробка» товару в третій країні дозволяє обходити санкції. На вашу думку, чи є покладання відповідальності за перевірку всього ланцюга постачання на приватний сектор (банки, компанії) реалістичним? Чи не є це передусім прогалиною на рівні міждержавних санкційних угод?
2. Дебати, представлені у бюлетені, показують полярні погляди на дієвість санкцій. З огляду на те, що Росія стала найбільш підсанкційною країною, але війна триває, де, на вашу думку, проходить межа між санкціями як інструментом тиску та санкціями як «політичним театром»?
3. Як Україна, експортер мінеральних ресурсів, має розробити власну систему прозорого моніторингу походження корисних копалин, щоб уникнути ризику формування “сірих ринків”?
4. Стаття BBC та CISA показує, що найслабшою ланкою в кібербезпеці є людина, яку можна підкупити. Чи достатньо сучасні системи внутрішнього контролю в українських компаніях та банках зосереджені на виявленні поведінкових аномалій та запобіганні саме інсайдерським загрозам, а не лише на технічному захисті периметра?
5. Як можливо застосувати підхід “пост-конфліктного відновлення через легальну економіку” для запобігання криміналізації суспільства після війни в Україні?

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-2025-42

Бюлетень є 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].