Міністерство
фінансів
України

Методологічний бюлетень AML

№47/2026



Зміст

DFSA про передовий і агентний штучний інтелект: кіберстійкість фінансового сектору у вимірах швидкості, охоплення, повноважень і довіри 3
GFIN Project Otto: як фінансові регулятори оцінюють власну готовність до квантових ризиків і квантових інновацій 7
Криптоактиви у фінансуванні політичних партій Великої Британії: видимі та приховані ризики (RUSI) 10
Критичні мінерали Африки: між геополітичним шансом і кримінальним захопленням 15
Як організована злочинність вбудовується у видобуток критичних мінералів 19
Економіка війни в Сахелі: як незаконні ринки зрощуються з конфліктом 22
Як розробити політику управління штучним інтелектом: практичні настанови ACAMS 26
Угорщина: майже 20 млн доларів готівки у справі колишнього міністра та розслідування про роль банку МКВ у транзиті російських коштів 29
Продаж курорту у Киргизстані як приклад обходу санкцій та російського впливу 31
Fraud Explained: Національне агентство з боротьби зі злочинністю Великої Британії пояснює п'ять поширених схем шахрайства 34

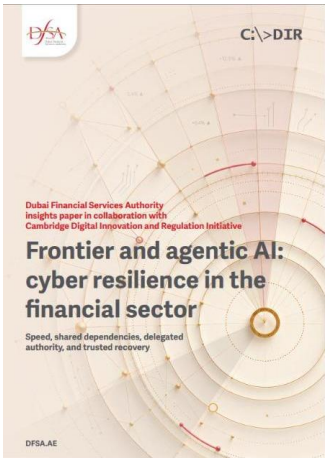


Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено для 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.

Кіберстійкість фінансового сектору у вимірах швидкості, охоплення, повноважень і довіри [1]



Управління фінансових послуг Дубая (DFSA) спільно з Кембриджською ініціативою з цифрових інновацій та регулювання (C:\>DIR) оприлюднило аналітичну доповідь про вплив передових і агентних систем штучного інтелекту на кіберстійкість фінансового сектору. Документ свідомо не встановлює нових регуляторних вимог: автори наголошують, що запропоновані аналітичні інструменти призначені для дослідження й обговорення. Методологічно це синтез публічних матеріалів, опрацьованих станом на 23 жовтня 2026 року, а не опитування чи збирання первинних даних. Автори розмежовують три типи доказів (зафіксовані зловмисні кампанії, інциденти під час оцінювання моделей і контрольовані демонстрації або гіпотетичні сценарії) та принципово утримуються від оцінок частоти інцидентів, розміру збитків чи ймовірностей. Там, де використання AI в інциденті не підтверджено, доповідь його не приписує.

Доповідь спирається на чіткі визначення. Передові моделі AI (frontier AI) розуміються як найсучасніші моделі, можливості яких можуть створювати нові або значно більші виклики для кібербезпеки, безпеки та управління. Агентний AI охоплює системи, налаштовані на досягнення цілей шляхом використання інструментів і виконання дій за різного ступеня людської участі та делегованих повноважень. Головний виконавчий директор DFSA Марк Стюард у передмові формулює регуляторну логіку документа: для наглядового органу важливо не те, що системи AI здатні робити загалом, а те, чи можуть їхні можливості суттєво вплинути на критично важливі фінансові послуги. Агентні системи додають ризику саме тому, що діють через під'єднані інструменти й за делегованими повноваженнями, тож їхні наслідки визначаються доступом і контролем довкола їхніх дій.

Перший вимір, швидкість, стосується скорочення часу на реагування. Доповідь наводить оприлюднену у 2025 році кампанію, в якій інструменти AI виконували значну частину багатоетапного вторгнення, а людські оператори залишали за собою ключові рішення; серед цілей були фінансові установи, а кількість успішних компрометацій була невеликою і без суттєвого впливу. Інститут безпеки AI Великої Британії у травні 2026 року зафіксував у контрольованих оцінюваннях швидке зростання тривалості кіберзавдань, які передові моделі виконують з

[1] https://365343652932-web-server-storage.s3.eu-west-2.amazonaws.com/files/9717/9362/3664/DFSA_Frontier_and_agentic_AI_report.pdf

успішністю 80%. Microsoft повідомила про зловмисника, що використовував агентну платформу тестування на проникнення ARTEX: у кількох випадках від вибору цілі до привілейованого доступу до хмарного середовища минало менше трьох годин, хоча це оцінка постачальника, не перевірена незалежно. Ключовий висновок розділу полягає в тому, що можливості атаки й оборони зростають у різному темпі, а застарілі системи, неповні реєстри активів і нестандартні інтерфейси сповільнюють безпечне усунення вразливостей.

Другий вимір, охоплення, присвячено спільним залежностям. Автори розрізняють концентрацію (залежність від невеликої кількості постачальників) і спільні залежності, приховані під формально різними постачальниками, які використовують ту саму модель, хмарний регіон, сервіс ідентифікації чи програмний компонент. Ілюстрацією слугує атака програми-вимагача у січні 2023 року на постачальника послуг для обробки біржових деривативів: за даними CFTC, частина клірингових учасників не змогла вчасно подати точні дані, що затримало щотижневий звіт регулятора, а окремим фірмам знадобилося до двох тижнів, щоб відновити записи про угоди. Другий постачальник не гарантує стійкості, якщо він спирається на ту саму хмару, сервіс ідентифікації чи модель, а оновлення моделі в постачальника здатне одночасно змінити поведінку багатьох робочих процесів без будь-яких змін у застосунку самої установи. Порушення можуть поширюватися через платежі, розрахунки, забезпечення, ліквідність і післяторгове обслуговування.

Третій вимір, повноваження, найбільш новаторський з методологічного погляду. Доповідь розводить три поняття: можливості моделі, доступ до систем і повноваження діяти. Передова модель може не мати жодних прав на виконання дій, тоді як менш потужний агент може мати широкий доступ, тому оцінювати їх слід разом. Запроваджено поняття «уповноваженого інсайдера»: агент здатен створити ризик, використовуючи чинні облікові дані й дозволені інструменти без участі зовнішнього зловмисника. Нелюдські облікові записи з часом накопичують дозволи, а приховані інструкції у зовнішніх даних (непряма ін'єкція запитів) можуть спрямувати агента всупереч його мандату. Звідси вимога, щоб межі дій забезпечувала цільова система, а не сама модель: платіжний мандат має визначати отримувача, суму, призначення і строк. Ролі людини (спостерігач, затверджувач, консультант, співавтор, оператор) не є щаблями зрілості, а там, де людина не здатна вчасно змістовно переглянути дію, рішенням є вужчі дозволи, автоматичні ліміти або затвердження до виконання важливої дії.

Для сфери протидії шахрайству доповідь містить окремі застереження. Автори посилаються на доповідь МВФ і Світового банку та Бангкокський план стійкості фінансових послуг до шахрайства, а серед загроз виокремлюють телефонну соціальну інженерію і видавання себе за інших осіб за допомогою синтетичних медіа. Публічні повідомлення про спроби такої соціальної інженерії щодо установ Волл-стріт, видавання себе за працівників служби підтримки та компрометацію хмарних облікових записів не підтвердили ані суттєвих збоїв, ані використання клонованих голосів, проте показали вразливі місця. Рекомендовано автентифікацію, стійку до фішингу, і незалежну перевірку через інший канал, оскільки бездоганна мова чи знайомий голос є слабким доказом повноважень. Окремо розглядаються зовнішні агенти (персональні та бізнесові), щодо яких установа має встановити, хто стоїть за агентом, кого він представляє і що йому дозволено,

що перегукується з ініціативами «Знай свого агента». Водночас доповідь прямо не аналізує заходи протидії відмиванню коштів.

Четвертий вимір, довіра, стосується відновлення. Зупинка агента не скасовує інструкцій у черзі, не відкликає облікових даних і не повертає вже виконаних змін, а збережена пам'ять і делеговані завдання можуть переносити інцидент далі. Тому механізм зупинки слід тестувати на рівні всього процесу, розмежовуючи припинення виконання, відкликання доступу, стримування наслідків і перевірку надійного стану. Відновлена доступність сервісу ще не означає звірених записів: для поновлення роботи потрібні реєстр незавершених і виконаних інструкцій, перевірені делегування та звірені результати з позиціями рахунків. Доповідь пропонує сценарії навчань (відхилення дій поза мандатом, призупинення процесу, підтримання критичних операцій, реконструкція записів, координоване поновлення) і радить структурувати внутрішні записи про інциденти за форматом FSB FIRE без запровадження нового обов'язку звітування.

Регуляторний контекст розглянуто з увагою до правового статусу документів: NIST CSF 2.0 і рамка управління ризиками AI NIST, принципи Базельського комітету щодо операційної стійкості (2021) і щодо управління ризиками третіх сторін (10 грудня 2025 року), настанови CPMI-IOSCO, остаточні «Надійні практики відповідального впровадження ШІ» FSB (15 жовтня 2026 року), наглядовий інструментарій IOSCO щодо AI на ринках капіталу (25 травня 2026 року), а також матеріали FINRA, FCA і HKMA. Підсумкова теза розділу 6 полягає в тому, що чинні рамки зберігають значення, але звичні докази вже недостатні: строк встановлення оновлень не доводить зменшення вразливості, реєстр постачальників не доводить працездатності резервних рішень, чинні дозволи не доводять, що дії залишаються в межах мандату, а відновлена доступність не доводить завершеного звіряння. Установам рекомендовано пов'язати суттєві робочі процеси з власниками, дозволами, діями, залежностями та механізмами відновлення і тестувати ці зв'язки, а органам влади проводити міжустановчий аналіз спільних залежностей і галузеві навчання з одночасних збоїв.

Висновки

Об'єктом оцінки ризику має бути робочий процес, а не модель: установам, які застосовують AI у моніторингу шахрайства, кредитному скорингу чи аналізі документів клієнтів, доцільно для кожного агента зафіксувати власника, обсяг дозволів, перелік дозволених дій, залежності від постачальників і порядок відновлення, а потім перевірити ці зв'язки на практиці, адже чинні облікові дані агента ще не гарантують, що його дії відповідають мандату.

Межі платіжних повноважень AI-агента слід забезпечувати на боці цільової системи: мандат з визначеними отримувачем, сумою, призначенням і строком має перевірятися платіжною системою незалежно від моделі; для процесів фінансового моніторингу це означає, що агент, який опрацьовує сповіщення чи документи, повинен трактувати зовнішній вміст як доказ, а не як джерело інструкцій.

Знайомий голос і бездоганна мова більше не підтверджують повноважень: зростання соціальної інженерії із синтетичними медіа вимагає автентифікації, стійкої до фішингу, та незалежних каналів підтвердження розпоряджень клієнтів і працівників, а також процедур ідентифікації зовнішніх агентів, які діють від імені клієнта.

Відновлення після інциденту має завершуватися звіреними записами: для суб'єктів первинного фінансового моніторингу цілісність історії операцій є умовою виконання обов'язків щодо звітування, тому сценарії навчань варто доповнити перевіркою того, що незавершені інструкції агентів виявлено, а записи про операції відновлено й звірено з позиціями рахунків.

Як фінансові регулятори оцінюють власну готовність до квантових ризиків і квантових інновацій [2]



Глобальна мережа фінансових інновацій (GFIN) оприлюднила інструментарій Project Otto, який було підготовлено Управлінням з фінансового нагляду Великої Британії (FCA). Партнерами проєкту стали Комісія з цінних паперів Альберти, Комісія з цінних паперів Британської Колумбії та Орган з міжнародних фінансових сервісних центрів Індії (IFSCA). Інструментарій покликаний дати регуляторам змогу оцінити власну зрілість у двох сферах: квантовій безпеці, тобто сприянні переходу фінансового сектору до практик, захищених від криптографічних загроз квантових обчислень, і квантових інноваціях, тобто розумінні нових застосувань та визначенні моменту, коли потрібні підтримка, взаємодія чи втручання. Голова GFIN і керівник напряму інновацій FCA Колін Пейн у передмові наголошує, що загроза криптографічній безпеці вимагає дій задовго до матеріалізації ризиків, а регуляторна зрілість полягає у здатності діяти ефективно тоді, коли це потрібно, а не в самому факті втручання.

Методологія ґрунтується на самооцінюванні. Опитування було відкрите з 3 червня до 31 серпня 2026 року для 85 членів GFIN, відповіді надали 25 регуляторів з Європи, Північної та Південної Америки, Близького Сходу, Азійсько-Тихоокеанського регіону та Африки. Анкета містить 42 оцінювані параметри (20 щодо безпеки і 22 щодо інновацій), згруповані за рамкою Say–Do–Engage: «Say» охоплює формулювання позицій і очікувань, «Do» означає внутрішні дослідження, підвищення кваліфікації та наглядову діяльність, «Engage» стосується взаємодії з фірмами й екосистемою. Кожен параметр оцінюється за чотирма рівнями: ситуативний (1), визначений (2), інтегрований (3) і адаптивний (4). Усі параметри мають однакову вагу, вибірка не є статистично репрезентативною, а результати є описовими і не становлять рейтингу ефективності. Показово, що жоден респондент не має середньої оцінки вище 2,57 щодо безпеки та 2,67 щодо інновацій.

Основні висновки свідчать, що зрілість у сфері безпеки та інновацій зростає синхронно: регулятори з вищою зрілістю щодо квантової безпеки зазвичай демонструють і вищу зрілість щодо інновацій, а спільними рушіями є моніторинг майбутніх тенденцій, дослідницькі програми, внутрішня експертиза і зовнішня взаємодія. Безпека переходить від усвідомлення до готовності й загалом є зрілішою за інновації. Найвищі показники має вимір «Do» в обох сферах. Участь у профільних заходах є найрозвиненішою практикою (84%, або 21 з 25 респондентів, мають рівень 2 і вище), моніторинг тенденцій і внутрішня спроможність щодо безпеки досягають 76% (19 з 25). Приблизно половина параметрів безпеки має модальну оцінку на рівні 2, і жоден не має

[2] https://thegfin.com/uploads/publications/pdf/1794890543_GFIN%20Project%20Otto%20Toolkit.pdf

модальної оцінки 3 чи 4. Натомість більшість параметрів інновацій має модальну оцінку 1, а спостереження за пілотними проєктами, «регуляторні пісочниці», тестові середовища, хакатони та транскордонне тестування розвинені найслабше, тож квантові інновації автори характеризують як етап дослідження, а не експериментування.

Для коректного порівняння регуляторів запроваджено три групи, сформовані за шістьма контекстними питаннями з вагами: модель регулювання (25%), ринковий контекст (25%), інституційний масштаб (15%), інноваційна позиція (15%), інноваційний мандат (10%) і підхід до технологічних ризиків (10%). «Адаптери» (7 регуляторів) працюють на менших або молодших ринках з вузькими мандатами й обмеженими ресурсами, їхня медіанна зрілість близька до рівня 1. «Учасники» (12) представляють усталені ринки з помітною інституційною спроможністю, їхня медіана розташована між рівнями 1 і 2. «Формувачі» (6) діють на великих впливових ринках із широкими мандатами, їхній профіль тяжіє до рівня 2, а окремі з них досягли рівня 3 за кількома видами діяльності. Автори підкреслюють, що контекст пояснює зрілість, але не визначає її: регулятори в подібних умовах можуть мати суттєво різні профілі.

Розділ про практики, що формуються, містить чотири кейси з оцінкою їх відтворюваності. Робоча група з квантових обчислень Канадських адміністраторів цінних паперів здійснила міжюрисдикційне картування можливостей і ризиків, зокрема ризику завчасного збирання зашифрованих даних для подальшого розшифрування, і має високу відтворюваність, бо не потребує формальних повноважень чи значних ресурсів. Регуляторний коледж DFSA з ризиків нових технологій поєднав брифінги експертів із закритими круглими столами регуляторів щодо взаємодії квантових ризиків, кіберстійкості та AI (висока відтворюваність). Інноваційна «пісочниця» IFSCA дала змогу спостерігати квантові експерименти з оптимізації портфеля та виявлення шахрайства (помірна відтворюваність). Наглядовий інструмент FCA PQC-QUEST, розроблений у взаємодії з Банком Англії, Органом пруденційного регулювання та Національним центром кібербезпеки, оцінює готовність фірм до постквантової криптографії за п'ятьма напрямами: управління й нагляд керівництва, пріоритизація та планування міграції, залежності від третіх сторін, виявлення та інвентаризація криптографії, готовність до тестування й моніторингу.

Практична частина пропонує регуляторам провести самоаудит за анкетою з додатка і визначити свою смугу: «позиціонування» (інновації нижче 1,50, безпека нижче 1,40), «координація» (1,50–2,00 та 1,40–1,90 відповідно) або «мобілізація» (вище 2,00 та 1,90). Порогові значення відносні до вибірки й не є універсальними орієнтирами. Для кожної смуги запропоновано дії з визначенням відповідальних функцій і очікуваних результатів. На етапі позиціонування йдеться про призначення відповідального підрозділу, формалізацію моніторингу тенденцій і картування пріоритетних фірм. На етапі координації рекомендовано заяви керівництва, необов'язкові настанови, оцінювання готовності фірм через опитування чи нагляд і публічно-приватні робочі групи. На етапі мобілізації йдеться про настанови щодо переходу на постквантову криптографію, зміни правил там, де це обґрунтовано доказами, стрес-тестування, «пісочниці» та транскордонне тестування.

Автори застерігають, що дії мають відповідати реальним регуляторним чи ринковим потребам, а нижча зрілість може відображати законний мандат або обґрунтоване судження про ризики. Колективний вимір проєкту реалізується через GFIN: спільні заходи, мережі моніторингу тенденцій, спільні дослідницькі програми, скоординовані комунікації з ринком, необов'язкові настанови та рамки найкращих практик. Для зрілих регуляторів пріоритетами названо транскордонну гармонізацію, тестування й експериментування та представлення колективних позицій міжнародним органам зі стандартизації. Сам Project Otto автори розглядають як початкову основу для тривалої міжнародної співпраці, цінність якої залежатиме від того, чи використають регулятори створені зв'язки, доказову базу та спільну рамку.

Висновки

Квантовий ризик уже сьогодні є питанням конфіденційності даних фінансового моніторингу: анкета Project Otto прямо включає до наглядової стратегії ризик «збирай зараз, розшифруй згодом», а дані належної перевірки клієнтів, відомості про кінцевих бенефіціарних власників і повідомлення про підозрілі операції мають тривалий горизонт конфіденційності, тож інвентаризація криптографії в каналах обміну такими даними має починатися вже зараз.

Інструментарій придатний для самооцінювання українських регуляторів: 42 параметри за рамкою Say–Do–Engage дають змогу Національному банку, НКЦПФР та іншим органам нагляду об'єктивно визначити свою смугу зрілості й обрати відповідні дії, з урахуванням того, що порогові значення відносні до вибірки з 25 регуляторів.

Наглядова оцінка готовності до постквантової криптографії може будуватися за моделлю PQC-QUEST: п'ять напрямів оцінювання (управління, планування міграції, залежності від третіх сторін, інвентаризація криптографії, тестування) органічно доповнюють чинні вимоги до управління інформаційною безпекою та ризиками третіх сторін.

Брак ресурсів можна компенсувати колективними форматами: кейси канадської робочої групи та коледжу DFSA мають високу відтворюваність і не потребують формальних повноважень, тому регіональні круглі столи та участь у спільних ініціативах GFIN є реалістичним способом нарощувати експертизу без створення власної дорогої інфраструктури.



Криптоактиви у фінансуванні політичних партій Великої Британії: видимі та приховані ризики [3]

Центр фінансів і безпеки Королівського інституту об'єднаних служб (RUSI) оприлюднив дослідження старшої наукової співробітниці Елізи Локгарт про вплив криптоактивів на систему фінансування політичних партій Великої Британії. Відправною точкою є стрімка зміна урядової позиції. У стратегії відновлення довіри до демократії (липень 2025 року) криптоактиви згадувалися лише один раз, у жовтні 2025 року лідер Reform UK повідомив Reuters, що партія почала отримувати криптовнески, а в березні 2026 року і Об'єднаний комітет парламенту з питань стратегії національної безпеки, і незалежний огляд Рікрофта рекомендували мораторій. Прем'єр-міністр 25 березня 2026 року оголосив, що уряд реалізує цю рекомендацію через поправки до законопроєкту про представництво народу. Водночас виник «розрив видимості»: у лютому 2026 року Виборча комісія заявила, що жодна партія не звітувала про криптовнески, а Reform UK пояснила, що криптоактиви конвертувалися в гроші стороннім провайдером ще до надходження до партії.

Автор показує, що вразливості існували задовго до появи криптоактивів. Британська система побудована на принципі допустимості донора, а не походження коштів: стаття 56 Закону про політичні партії, вибори та референдуми 2000 року вимагає від партій вжити всіх розумних заходів для встановлення допустимості донора, внески від одного джерела підлягають звітуванню, якщо перевищують 11 180 фунтів стерлінгів за календарний рік, а суми до 500 фунтів взагалі не вважаються внесками. Політичні партії не є суб'єктами вимог щодо протидії відмиванню коштів, тож не зобов'язані оцінювати ризики, проводити посилену перевірку, встановлювати джерело коштів чи джерело статків донора. За даними Transparency International UK, майже кожен десятий

[3] https://www.rusi.org/explore-our-research/publications/insights-papers/cryptoassets-uk-politics-seen-and-unseen

фунт, задекларований партіями та їхніми членами з 2001 року, надійшов із невідомих чи сумнівних джерел (загалом 115 млн фунтів), а у 2024 році під час журналістської перевірки п'ять із шести партій прийняли незаконні внески, сконструйовані для обходу законодавства про іноземне втручання.

Не менш показовою є картина правозастосування. Виборча комісія не може застосовувати слідчі повноваження щодо осіб поза межами Великої Британії, кримінальні виборчі правопорушення можуть розслідувати будь-які з 45 територіальних поліцейських служб, Національне агентство з боротьби зі злочинністю, а за наявності зв'язку з іноземною державою також спецслужби. Комісія сама характеризувала цю систему як «неузгоджену». Протягом двадцяти років після 2000 року не було жодного кримінального переслідування за порушення законодавства про політичне фінансування (перший процес відбувся у 2023 році: п'ять обвинувачених визнали провину, двох виправдано). Аналіз Spotlight on Corruption зафіксував скорочення кількості завершених Комісією розслідувань на 89% і суми накладених штрафів на 92% у 2019–2025 роках, а частка громадян, які вірять у належну реакцію органів влади на порушення, впала з 57% у 2018 році приблизно до третини у 2026 році. Криптоактиви, за висновком автора, діють як мультиплікатор, що оголює й посилює наявні системні слабкості.

Окремий розділ присвячено «криптопарадоксу». Публічні блокчейни забезпечують постійний і загальнодоступний запис транзакцій, а аналітичні інструменти дають змогу об'єднувати адреси, ймовірно підконтрольні одній особі, та відстежувати кошти значно швидше, ніж у традиційних фінансах. Проте більшість транзакцій псевдонімні, і встановлення реальної особи потребує поєднання даних блокчейну з розвідувальною інформацією з інших джерел. Змішувачі, переведення коштів між блокчейнами, анонімні монети та циклічне використання гаманців ускладнюють атрибуцію, а ці методи дедалі частіше автоматизуються за допомогою ШІ. За даними Chainalysis, обсяг криптозлочинності у 2025 році досяг щонайменше 154 млрд доларів проти 59 млрд у 2024 році. Опитані автором аналітики наголошують, що технічна простежуваність не тотожна операційній спроможності: без часу, інструментів і експертизи прозорість блокчейну не перетворюється на практичну видимість.

Дослідження вирізняє «видиме» і «приховане» використання криптоактивів. Видимими є внески безпосередньо в криптоактивах, що створюють чотири категорії вразливостей: ідентифікацію донора (блокчейн не містить ідентифікаційних даних), походження коштів (зокрема через підсанкційні біржі), оцінку вартості (вартість визначається на момент внеску, тому актив може згодом суттєво подорожчати) і дроблення внесків, яке через швидкість переказів, приховування спільного джерела та автоматизацію AI можна масштабувати, особливо з огляду на поріг у 500 фунтів. Прихованим є використання, коли внесок надходить у фіатній валюті, а криптоактиви фігурують раніше в історії транзакції: конвертацію здійснює платіжний посередник від імені партії або кошти проходять через банківський рахунок формально допустимого донора. В обох випадках і партія, і регулятор бачать звичайний грошовий внесок, якщо не проведено належної перевірки або донор сам не розкрив цю обставину.

Міжнародні приклади підтверджують реальність прихованого каналу. Напередодні парламентських виборів 2025 року в Молдові Національний центр протидії корупції провів понад 30 обшуків у справі про незаконне фінансування партії через криптоактиви. За словами посадовців, кошти, ймовірно російського походження, пропускали через незаконних провайдерів обміну криптоактивів для приховування їхнього походження, після чого конвертували в готівку, а згодом Центр виявив гаманець, через який у 2023–2025 роках пройшло понад 107 млн доларів у USDT. Уряд Великої Британії надав цій операції фінансування, інструменти блокчейн-аналітики та технічну експертизу. У самій Британії керівник Виборчої комісії у січні 2026 року повідомив про кошти, що рухаються через криптобіржі й осідають на британських банківських рахунках, а ЗМІ описали конвертацію криптовнесків польським платіжним провайдером та повернення партією коштів від продажу мем-токенів; у цих випадках порушень не стверджується, а партії заявляють про дотримання законодавства. Регуляторну проблему автор формулює так: встановлення походження внеску може залежати від інформації криптопосередників, що перебувають поза ефективною досяжністю британських органів, а імплементація стандартів FATF, зокрема правила передавання інформації (Travel Rule), істотно різниться між країнами.

Аналіз міжнародних підходів виявив три моделі. Заборона (Бразилія з 2019 року, Ірландія з 2023 року, Канада з 2026 року) рідко супроводжується вимогами перевіряти, чи не походить фіатний внесок із криптоактивів. Спектр дозволу ілюструють США: на федеральному рівні криптовнески з 2014 року прирівнюються до негрошових; у Вашингтоні їх обмежено 100 доларами з конвертацією протягом п'яти робочих днів, а Каліфорнія, заборонивши їх у 2018 році, з 2022 року допускає внески лише через зареєстрованого в Міністерстві фінансів США платіжного провайдера з процедурами KYC і конвертацією протягом двох робочих днів. Третя модель полягає в дозволі через мовчання закону, як у Японії, де у 2019 році криптовнески визнали законними, але такими, що не підлягають розкриттю. Спільна вада всіх моделей полягає в зосередженні на допустимості внеску в момент отримання, а не на його походженні.

Запропонована рамка складається з трьох етапів. «Пауза» передбачає умовний мораторій на всі криптовнески, включно з конвертованими посередником, який може бути знято лише після того, як Виборча комісія видасть обов'язкові настанови й підтвердить свою спроможність, а парламент схвалить це позитивною резолюцією. Автор звертає увагу, що законопроєкт у редакції, схваленій Палатою громад, запроваджує безстрокову заборону внесків, отриманих з 25 березня 2026 року, проте прямо не врегульовує конвертацію посередником, що діє від імені партії. «Захист» передбачає обов'язкову оцінку ризиків внесків: законопроєкт уже вимагає враховувати тип донора, історію внесків, вид і розмір внеску, але не походження коштів, тож автор пропонує явно включити походження і шляхи руху коштів, посилену перевірку великих чи ризикових внесків, зокрема з ознаками конвертації криптоактивів, і обов'язкову декларацію донора про походження значних сум (уряд взяв таке зобов'язання, однак до тексту законопроєкту воно не потрапило). Як прецедент наведено благодійний сектор, де ризик-орієнтована перевірка донорів діє щонайменше 15 років.

Етап «Підготовка» охоплює регуляторну, правозастосовну та інституційну готовність. Новий режим FCA для криптоактивів має набути чинності в жовтні 2027 року, а будь-який майбутній режим

прийняття криптовнесків, на думку автора, повинен передбачати проходження внесків через авторизованих провайдерів, обмеження анонімних монет і змішувачів, стандарти використання блокчейн-аналітики, агрегацію мікровнесків і швидку конвертацію. Автор критично оцінює право міністра вимагати перегляду настанов Комісії, що послаблює її незалежність. Комісія має отримати фахівців, ліцензії на аналітичні інструменти та повноваження витребувати інформацію в третіх осіб, але не перетворюватися на агентство блокчейн-криміналістики, тому пропонується створити поліцейський центр експертизи зі складних справ політичного фінансування. Інституційною моделлю названо австралійську Цільову групу із забезпечення доброчесності виборів, що стала постійним органом, і канадський досвід обміну типологіями з приватним сектором. П'ять рекомендацій (мораторій, перевірка походження, посилення Комісії, правозастосовна спроможність, координаційний орган із участю банків, провайдерів послуг віртуальних активів і аналітичних компаній) мають запроваджуватися пакетом, адже мораторій без реформ є «забороною без плану».

Висновки

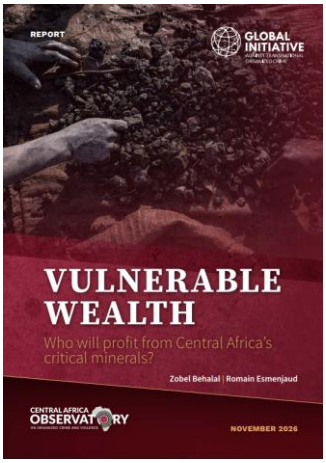
Заборона криптовнесків без перевірки походження коштів лише переміщує ризик у приховані канали: мораторій має супроводжуватися вимогою оцінювати походження і шляхи руху коштів для значних внесків, інакше конвертація криптоактивів посередником або транзит через рахунок допустимого донора залишаться непомітними для регулятора.

Політичні партії фактично приймають ризики, які в регульованому секторі покриваються належною перевіркою: для великих внесків доцільно запозичити ризик-орієнтований підхід суб'єктів первинного фінансового моніторингу (встановлення джерела коштів і джерела статків, посилена перевірка за ознаками ризику), а банкам, які обслуговують рахунки партій, враховувати ознаки конвертації криптоактивів у моніторингу.

Ключовою точкою контролю є посередник, що конвертує криптоактиви: доступ органів нагляду за політичним фінансуванням до інформації платіжних провайдерів і провайдерів послуг віртуальних активів, а також дієве виконання правила передавання інформації мають бути враховані під час формування національного регулювання ринку віртуальних активів.

Технічна простежуваність блокчейну не дорівнює операційній спроможності: досвід Молдови, де виявлено гаманець з оборотом понад 107 млн доларів у USDT, свідчить, що результат забезпечують спеціалізовані підрозділи з аналітичними інструментами та міжнародна співпраця, а не сама прозорість реєстру транзакцій.

Критичні мінерали Африки: між геополітичним шансом і кримінальним захопленням [4]



Центральна Африка, яку довго сприймали як геополітичну периферію, опинилася в епіцентрі глобальних перегонів за ресурсами, що живлять енергетичний перехід, цифрову економіку та сучасну оборону.

Демократична Республіка Конго (ДРК) є світовим лідером з видобутку кобальту й колтану, забезпечуючи понад 70% і 50% світового виробництва відповідно, а також другою у світі за видобутком міді. Габон є другим за величиною виробником марганцю на планеті, Чад видобуває сурму в регіоні Тібесті, Камерун має перспективні родовища рутилу, літію та нікелю-кобальту, а Центральноафриканська Республіка (ЦАР) володіє щонайменше 470 задокументованими мінеральними проявами, включно з колтаном, міддю, марганцем і рідкісноземельними елементами.

Попит на критичну сировину зростає стрімко: за прогнозами Міжнародного енергетичного агентства, протягом наступних 10–15 років попит на мідь зросте на 28%, а на літій більш ніж на 350%. Це перетворює центральноафриканські держави на об'єкт інтенсивної конкуренції між глобальними державами. Китай, який першим інвестував у сектор, зберігає домінантні позиції: він контролює близько 60% світового виробництва рідкісноземельних елементів, 90% їхнього розділення й очищення та 80–90% виробництва постійних магнітів, а в Центральній Африці закріпився в кобальтовому та мідному секторах ДРК і має незначні інтереси в габонському марганці.

Водночас Європейський Союз, США, ОАЕ, Японія, Саудівська Аравія та Індонезія активізували власні зусилля. ЄС уклав партнерство щодо сировини з ДРК у 2023 році, французька Eramet поглибила співпрацю з Габоном угодою 2026 року, а Японська організація з металів та енергетичної безпеки (JOGMEC) підписала мінеральну угоду з Кіншасою. ОАЕ уклали економічну угоду з ЦАР, придбали частку в провідному виробнику олова в ДРК і підписали з державною гірничою компанією ДРК угоду на 1,9 млрд доларів для розробки чотирьох копалень.

Найпомітнішим прикладом активізації є ініціативи США: після підписання мирної угоди між ДРК і Руандою в Білому домі 27 червня 2025 року Вашингтон і Кіншаса уклали стратегічне партнерство щодо критичних мінералів із преференційним доступом для американських компаній, а на початку 2026 року ДРК передала США перелік 25 пріоритетних гірничих активів, серед яких, за повідомленнями, фігурує Рубая, одне з найбільших у світі родовищ танталу, нині контрольоване підтримуваним Руандою угрупованням M23.

---

[4] https://globalinitiative.net/wp-content/uploads/2026/11/Zobel-Behalal-and-Romain-Esmenjaud-Vulnerable-wealth-Who-will-profit-from-Central-Africas-critical-minerals_-GI-TOC-November-2026-1.pdf

Для центральноафриканських держав це відкриває безпрецедентні можливості для переговорів щодо умов співпраці, залучення інфраструктурних інвестицій та створення доданої вартості. ЄС через стратегію Global Gateway і США фінансують розвиток коридору Лобіто, що з'єднує мінеральні регіони ДРК і Замбії з ангольським портом Лобіто, включно з модернізацією залізниці та відновлюваною енергетикою. Габон в обмін на підтвердження співпраці з Eramet забезпечив підтримку Французького агентства розвитку, Proparco, ЄС і Світового банку для модернізації Трансгабонської залізниці. ДРК разом із Замбією досліджує створення транскордонної спеціальної економічної зони для виробництва батарей, а в червні 2026 року заборонила експорт концентратів кобальту й міді, щоб змусити до внутрішньої переробки. Однак здатність цих партнерств забезпечити сталий розвиток критично залежить від того, чи вдасться захистити сектор від кримінальних інтересів, які вже його оточують.

Структурні вразливості регіону створюють сприятливий ґрунт для кримінального втручання. Слабке державне управління є головною з них: гірничі роботи часто ведуться в віддалених районах, де державна влада нерівномірна, а правоохоронні та регуляторні органи недофінансовані, погано контрольовані та вразливі до корупції. У Камеруні неспроможність уряду регулювати золотовидобуток призвела до разючих розбіжностей: у 2023 році країна задекларувала лише 22,3 кілограма експорту золота, тоді як ОАЕ зафіксували імпорт понад 15 тонн золота камерунського походження. У Чаді дослідження виявили обмежену операційну присутність і провали контролю в золотому секторі. У ДРК і ЦАР збройні угруповання контролюють доступ до окремих гірничих районів та експортних маршрутів і запроваджують незаконні податки на видобуток, транспортування й продаж мінералів.

Законодавча невизначеність посилює проблему: у ЦАР новий гірничий кодекс 2024 року досі не має імплементаційних положень, а закон 2023 року про токенізацію природних ресурсів запровадив паралельний механізм придбання землі (а потенційно й гірничих прав) на блокчейн-платформах, що ставить під сумнів правовий статус токенізованих активів щодо ліцензій за гірничим кодексом. У такому середовищі, де правила залежать від того, з ким маєш справу, державні агенції суперечать одна одній, а формальні й неформальні податки співіснують, відбувається своєрідний негативний відбір: відповідальні оператори, зв'язані вимогами належної обачності, утримуються від інвестицій, тоді як актори, комфортні з неформальністю, політичним посередництвом і непрозорістю, процвітають.

Особливе занепокоєння викликає те, що актори, пов'язані з непрозорими практиками в ЦАР та інших центральноафриканських державах, інвестують у новий сектор критичної сировини. Sigma Resources CAR, яка отримала дозволи на розвідку кобальту, міді, нікелю та літію в кількох районах ЦАР, контролюється Sigma Mining, що своєю чергою перебуває під контролем конгломерату ОАЕ International Holding Co, очолюваного Тахнуном бін Заєдом Аль Нахаяном, братом президента ОАЕ. Sigma Mining взяла під контроль Sigma Gold у ЦАР у червні 2023 року, саме тоді, коли компанія закуповувала золото в російської ПВК «Вагнер», зокрема з її концесії в Ндассімі, яка не повідомляє про офіційний видобуток. Того року Sigma Gold стала провідним експортером золота ЦАР, а гірничі чиновники в інтерв'ю 2024 року описували компанію як фронт «Вагнера», посилаючись на випадки політичного втручання на найвищому рівні, коли робилися спроби притягнути її до

відповідальності за володіння недокументованим золотом. Sigma Resources CAR також пов'язана з Sigma Mining Corporation у Руанді: обидві компанії зареєстрував пакистанський громадянин Саклайн Раза, який, за даними Групи експертів ООН з ДРК, був причетний до контрабанди конголезького золота з Кігалі до Дубая (Раза ці звинувачення заперечує).

Окремою критичною проблемою є слабкість запобіжних механізмів у секторі критичної сировини порівняно з високоризиковими мінералами, такими як золото, у поєднанні зі зростаючим тиском на послаблення цих механізмів. Кримінальне втручання в ланцюги постачання критичної сировини вже є реальністю: на сході ДРК торгівля колтаном давно контролюється збройними та кримінальними угрупованнями, а стрімке розширення ринку та зростаючий апетит іноземних акторів, імовірно, лише посилять і поширять ці динаміки. Звіт наголошує на зростаючому апетиті до ренти й політичних переваг серед правлячих еліт, інструменталізації організованої злочинності для геополітичних цілей та захопленні гірничих об'єктів і торговельних маршрутів кримінальними мережами; зокрема, висвітлено елітне захоплення зростаючої сурм'яної промисловості Чаду та російські «геокримінальні» активності, націлені на підтримуваний Заходом коридор Лобіто.

У підсумку, питання полягає не в тому, чи проникне організована злочинність у сектор критичних мінералів Центральної Африки, а в тому, наскільки далеко вона поширюється. Саме тому автори звіту рекомендують центральноафриканським урядам ухвалити комплексні стратегії щодо критичних мінералів, які ставлять пом'якшення ризиків організованої злочинності в центр управління сектором; закликають GABAC і FATF оновити рамки оцінки ризиків з огляду на стратегічне значення критичних мінералів і пов'язані з ними незаконні фінансові потоки; радять озброїти гірничу поліцію, митницю та підрозділи фінансової розвідки інструментами для розслідування незаконних потоків критичної сировини, посилюючи запобіжники проти корупції та кримінальної інфільтрації в самих правоохоронних органах, а також підтримувати регіональний обмін розвідувальною інформацією та спільні розслідування, спрямовані на мережі, а не лише на окремих контрабандистів.

Нарешті, уряди країн-імпортерів мінералів, відповідно до зобов'язань G7, ухвалених в Евіані, мають узгоджувати свою політичну, дипломатичну й фінансову підтримку проєктів критичної сировини в Центральній Африці з надійними стандартами управління та доброчесності. Інакше ресурсне багатство регіону, замість того щоб стати двигуном розвитку й дипломатичним важелем, ризикує перетворитися на чергову здобич для тих, хто найкраще пристосований до тіні.

Висновки

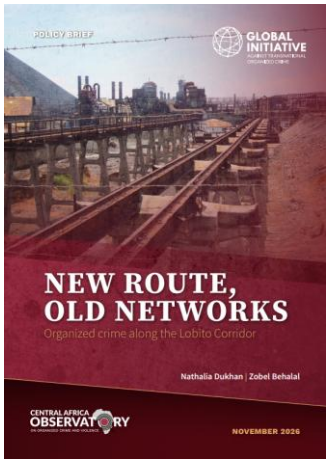
Геополітична конкуренція за ресурси. Африка стала центром глобальних перегонів за критичною сировиною, де Китай, США, ЄС, ОАЕ та інші конкурують за доступ до рідкісноземельних елементів, пропонуючи інфраструктурні та політичні ініціативи.

Структурні вразливості сприяють криміналізації. Слабке державне управління, обмежена присутність держави у віддалених гірничих районах, перешкоди формалізації дрібного видобутку та законодавча невизначеність створюють умови для корупції, контрабанди та захоплення сектору організованими злочинними мережами.

Вже задокументовані випадки кримінального втручання. У ДРК і Чаді зафіксовано злочинні практики, пов'язані з видобутком і торгівлею критичними мінералами, включно з участю збройних угруповань, політично захищених мереж і представників силових структур.

Потреба в посиленні управління та прозорості. Звіт наголошує на необхідності комплексних стратегій, що ставлять пом'якшення ризиків організованої злочинності в центр управління сектором, розкриття кінцевих бенефіціарних власників, поширення зобов'язань з протидії відмиванню коштів на трейдерів і посередників, а також узгодження підтримки країн-імпортерів із стандартами доброчесності.

Як організована злочинність вбудовується у видобуток критичних мінералів [5]



Коридор Лобіто, один із найбільших інфраструктурних проєктів у Центральній і Південній Африці, має з'єднати мідні та кобальтові копальні ДРК і Замбії з ангольським портом Лобіто, забезпечивши Заходу прямий шлях до критичних мінералів в обхід китайського домінування. ЄС мобілізував на це 2 млрд євро, загалом прихильники обіцяли понад 6 млрд доларів. Однак, як показує доповідь GI-TOC, коридор пролягає через регіон, глибоко уражений організованою злочинністю, і його безпеку неможливо відокремити від управління копальнями та прав тих, хто на них працює. Якщо нічого не зміниться, ті самі мережі, що контролюють видобуток, контролюватимуть і шлях мінералів на ринок, тобто коридор ризикує стати швидким каналом надходження мінералів сумнівного походження саме до тих ланцюгів постачання, які Європа та США прагнуть убезпечити.

Наразі коридор працює лише частково: у належному стані тільки ангольська ділянка, тоді як конголезька залізниця SNCC занепала (потяги рухаються 10–15 км/год, використовуючи менше 5% потужності), концесію на її відновлення надано лише у серпні 2026 року без фінансування, а замбійська ділянка ще не розпочата: фінансове закриття очікується лише до кінця 2027 року. Обсяги скромні: 400 тис. тонн у 2026 році проти понад 4 млн тонн міді, що виробляють обидві країни щороку. Саме період до виходу на повну потужність є вирішальним, щоб злочинні мережі не пішли за коридором.

Головний ризик зосереджений не на залізниці, а в копальнях. У Луалабі та Верхній Катанзі незаконний видобуток на промислових концесіях переріс у квазіпромислову операцію приблизно на 2 млрд доларів на рік, яку охороняють силовики, провінційна влада та політичні еліти; армія присутня на 64% обстежених кустарних ділянок, солдати стягують незаконні податки й монополізують продаж. З приблизно 200 тис. старателів (поряд з якими працюють близько 40 тис. дітей) легально працює лише меншість, а їхня продукція йде на склади з мінімальною простежуваністю. Ризик поширюється й на інші мінерали: замбійський марганець часто видобувається без ліцензій, майже половина працівників перебуває в умовах примусової праці, а руда не простежується. Оскільки незаконні обсяги змішуються з легальними, коридор надає їм легітимності, а європейські гарантії слабкі: Регламент щодо конфліктних мінералів 2017 року не охоплює мідь і кобальт, а вимоги Регламенту ЄС про батареї відкладено до серпня 2027 року.

[5] https://globalinitiative.net/wp-content/uploads/2026/11/Nathalia-Dukhan-and-Zobel-Behalal-New-route-old-networks-Organized-crime-along-the-Lobito-corridor-GI-TOC-November-2026.pdf

Наступною ланкою ризику є організовані викрадення вантажів: у липні 2025 року поблизу Тумбве викрадено партії міді вартістю близько 6 млн доларів кожна, поліція, за повідомленнями, сприяла «поверненню» за хабарі; на блокпостах між Колвезі та Касумбалесою водіїв зупиняють 10–16 разів і платять 300–1200 доларів хабарів, а вантажівки з конголезьким катодом знаходять покинутими й спорожнілими. Саме на кордонах незаконне стає легальним: через обсяги контрабанда покладається не на приховування, а на неправдиве декларування походження, ваги чи вмісту. Оцінки свідчать, що у 2000–2024 роках у вантажах кобальтового гідроксиду вивезено 2–5 тис. тонн незадекларованого урану; у червні 2026 року в ПАР вилучено 121 тонну викраденої в Замбії міді з підробленими документами. Нові обмеження ДРК (квоти на кобальт, заборона експорту концентратів) тиснуть на торгівлю в Замбію, а на кордоні Ділоло–Луау виникне новий потенційний нелегальний хаб.

Контекст стрімко змінюється: риторика енергетичного переходу поступилася безпеці постачання, а правила належної обачності пом'якшуються. Угода США–ДРК від грудня 2025 року дає американським компаніям право першої пропозиції на стратегічні активи й ставить мету спрямувати половину конголезької міді та третину кобальту через Лобіто; до списку пріоритетів потрапила Рубая, контрольована M23. Замбія відкинула прив'язку допомоги до преференційного доступу, а Кіншаса фактично обмінює мінерали на безпеку; ця модель уже дала обмежені результати на сході, де передання безпекових функцій стороннім виконавцям через патронажні мережі став рушієм насильства.

Окремий ризик виникає, коли охоронці фінансуються з доходів, які самі збирають: у ДРК гірничий компонент контракту фінансує безпековий, а гірнича «поліція» збирає доходи. Тим часом Китай уже контролює значну частину ланцюга (частки в 15 найбільших копальнях ДРК, домінування в переробці) і зміцнив східний маршрут угодою на 1,4 млрд доларів про модернізацію TAZARA. Найімовірнішим результатом стануть два конкурентні маршрути з тих самих копалень; конкуренція не демонтує злочинні економіки, а перерозподілить їх, адже мінерали сумнівного походження прямують туди, де контроль слабший.

Доповідь рекомендує: ДРК і Замбії зробити боротьбу з організованою злочинністю в гірництві пріоритетом, розслідуючи силовиків і чиновників, які прикривають незаконний видобуток, і тримаючи армію та приватних підрядників поза кустарними ділянками; дати старателям легальний шлях на ринок через прозорі аудитовані центри закупівлі; разом з Анголою захищати доходи коридору, розкриваючи пов'язані запозичення та включаючи його до національних оцінок ризиків відмивання грошей; фінансувальникам прив'язати кошти до показників доброчесності; зробити залізничні термінали пунктами простежуваності, звіряючи імпорт із експортними даними; ЄС і США застосовувати стандарти, які вони просувають, і до угод та фондів, які контролюють безпосередньо.

Висновки

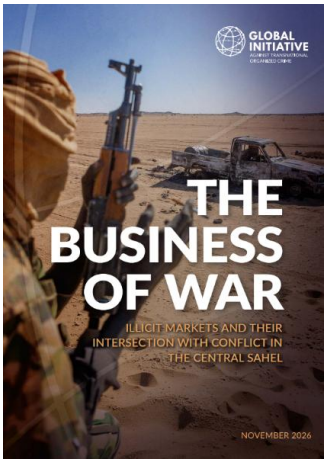
Ризик починається не з логістики, а з копальні. Незаконний видобуток на промислових концесіях ДРК, підкріплений силовиками та політичними елітами, здатен «легалізуватися» через швидкий коридор, особливо коли незаконні обсяги змішуються з легальними.

Безпека без підзвітності підживлює злочинність. Присутність армії, приватні підрядники з нечіткими мандатами та схеми, де охорона фінансується з доходів, які сама збирає, розмивають межу між незаконним покровительством і правоохоронною діяльністю.

Кордони та логістика є ключовими вразливими вузлами. Викрадення вантажів, хабарі на блокпостах і неправдиве декларування походження, ваги чи вмісту перетворюють легальний маршрут на канал для мінералів сумнівного походження.

Геополітична конкуренція не усуває, а перерозподіляє злочинні економіки. Конкуренція Лобіто з TAZARA та прив'язка фінансової допомоги до доступу до мінералів підвищують ризик, що мінерали сумнівного походження підуть туди, де контроль слабший; доброчесність слід закладати ще на етапі фінансування.

Економіка війни в Сахелі: як незаконні ринки зрощуються з конфліктом [6]



Центральний Сахель переживає період глибокої турбулентності, де політична нестабільність, екстремізм та незаконна економіка стають дедалі тісніше переплетеними. У Буркіна-Фасо, Малі та Нігері військові режими консолідували владу, але їм не вдається перетворити обіцянки відновленого суверенітету на реальну стабільність. Натомість регіон характеризується фрагментацією влади, зменшенням державного контролю над територіями та зростанням рівня насильства за участю озброєних угруповань, державних сил та їхніх допоміжних підрозділів. Це створює ландшафт, у якому межі між конфліктом, управлінням та організованою злочинністю стають дедалі менш помітними.

Звіт GI-TOC надає вичерпний аналіз того, як злочинні економіки стали центральним елементом насильства в регіоні. Дослідження показує, що як «Ісламська держава» в провінції Сахель (IS Sahel), так і «Джамаат Нусрат аль-Ислам валь-Муслімін» (JNIM) фінансують себе переважно за рахунок використання легальних та нелегальних економік, що дозволяє їм розширювати географічний обсяг операцій та ставати дедалі смертоноснішими. За даними Глобального індексу тероризму 2025 року, Сахель став епіцентром глобального тероризму, а середньорічна кількість загиблих з 2023 року більш ніж удвічі перевищує показники 2020–2023 років.

Однією з ключових тенденцій, яку висвітлює звіт, є різке відновлення економіки викрадень іноземців заради викупу. Після майже повного припинення у 2023–2024 роках, у 2025 році обидві провідні екстремістські групи реструктурували свої підходи до викрадень, що призвело до безпрецедентного зростання інцидентів. Історично JNIM домінувала в цій сфері, тоді як IS Sahel мала лише один відомий випадок викрадення іноземця у 2018 році. Однак наприкінці 2024 року IS Sahel ухвалила стратегічне рішення інвестувати в цю діяльність, створивши спеціальну команду та залучивши новобранців із кримінальним досвідом. Це стало можливим завдяки стабільному контролю над регіоном Менака в Малі, що дозволило утримувати заручників протягом тривалого часу.

Звіт зазначає, що у 2026 році IS Sahel, ймовірно, отримала десятки мільйонів доларів за звільнення американського, швейцарського та австрійського заручників, що вже робить групу зухвалішою в операціях, включаючи наступи проти JNIM. Бандити, своєю чергою, можуть отримувати від 130 000 до 350 000 євро за доставку іноземного заручника бойовикам IS Sahel, що створює потужні стимули для регіонального поширення викрадень. JNIM також значно активізувала цю діяльність, змінивши цілі. Група все частіше викрадає громадян Китаю, Індії,

[6] https://globalinitiative.net/wp-content/uploads/2026/11/The-business-of-war-Illicit-markets-and-their-intersection-with-conflict-in-the-central-Sahel-GI-TOC-November-2026.pdf

Єгипту, ОАЕ та Ірану, пов'язаних з гірничодобувними та промисловими операціями, які вважаються політично прийнятними та менш чутливими. Викрадення перетворилося на інструмент економічної війни проти малійського військового режиму: страх відлякує інвесторів і паралізує легальну економіку, а податки на промислові гірничодобувні компанії в регіонах Каєс і Сікассо є основним джерелом доходу для хунти.

Дороги стали критично важливими місцями протистояння між недержавними озброєними групами та державами. Дослідження GI-TOC 2025 року, яке охопило 350 незаконних хабів у 18 країнах, виявило, що 87% з них розташовані на або поблизу основних операційних доріг. Вимагання та рекет тісно пов'язані з контролем над пересуванням, а блокпости та «оподаткування» є поширеним механізмом отримання доходу. Більшість смертельних випадків у Західній Африці та Сахелі відбувається в межах 1 кілометра від дороги, а понад 90% атак JNIM на півдні Малі у 2025 році сталися в межах 10 кілометрів від головних національних трас.

З середини 2025 року JNIM встановила жорсткий контроль над основними дорожніми коридорами, що живлять Бамако, включаючи осі Бамако–Дакар, Бамако–Абіджан та дедалі більше Бамако–Конакрі. Блокади пального, оподаткування комерційного транспорту, викрадення водіїв та засідки на конвої перетворили ці торгові шляхи на театри економічної війни. Через ці дії JNIM чинить величезний тиск на військовий режим у Бамако. Подібна тактика застосовується і в Нігері: приблизно 70% атак IS Sahel на цивільних у 2025 році сталися в межах 24 кілометрів від шосе N1 або N23, що з'єднують Айору, Тера та Тіллабері з Ніамеєм. Регіон Тіллабері став найсмертоноснішим у Центральному Сахелі для цивільних: з 1939 зафіксованих смертей у Нігері у 2025 році майже 1300 сталися саме там.

Дрібномасштабний видобуток золота (ASGM) є основним джерелом фінансування, ресурсів та легітимності для екстремістських угруповань, водночас залишаючись критично важливим засобом існування для місцевих громад. Золоті копальні є не лише джерелом доходу, а й місцями вербування та соціального контролю. Дозволяючи видобуток, захищаючи доступ або діяльність навколо копалень, озброєні групи можуть позиціонувати себе як гаранти засобів існування, особливо там, де державні дії сприймаються як хижацькі.

Розширення JNIM на південь Малі, до регіонів Каєс і Сікассо, які є набагато важливішими для золотої економіки країни, може означати якісний стрибок у масштабах ресурсів, доступних для угруповань. Регіон забезпечує 80% національного видобутку золота. JNIM не окуповує копальні, але покладається на цивільних посередників для «оподаткування» золота. Зазвичай ці «асоціації» беруть близько 10% заробітку кожного старателя. Суми сплачуються щомісяця готівкою і варіюються залежно від розміру ділянки та доходу.

Звіт також вказує на несподіваний вплив конфлікту в Ірані у березні 2026 року, який спричинив обвал цін на золото через порушення ланцюгів постачання. Це створило вікно можливостей для міжнародних інтервенцій, спрямованих на відновлення зв'язків між громадами ASGM та державами та стимулювання надходження золота до формальних ланцюгів постачання.

Війна в Судані оживила транскордонні схеми постачання зброї, бійців, пального та засобів зв'язку. Зброя та технології дедалі більше надходять на регіональні ринки та в конфлікти, включаючи Центральний Сахель. Водночас зростаюче поширення потужних, дешевих і смертельних синтетичних опіоїдів викликає серйозне занепокоєння. У кількох прибережних країнах Західної Африки синтетичний наркотик куш (kush) містить нітазени, тобто надзвичайно потужні синтетичні опіоїди. Куш дедалі частіше фіксується на півдні Малі, і хоча тестування не проводилося, ймовірно, що склад там аналогічний.

Попри складність, перетин злочинності та конфлікту повинен залишатися пріоритетною ціллю для відповіді, оскільки він підживлює ресурси, фінансування та легітимність озброєних груп. Звіт наголошує на необхідності динамічного моніторингу незаконних економік як критичної доказової бази для визначення можливостей втручання. Використання ринкових шоків, спричинених конфліктом в Ірані, могло б дозволити пріоритезувати інтервенції в секторі ASGM, відновлюючи відносини між громадами старателів та державами.

Нарешті, зміцнення координації щодо зростаючих загроз від синтетичних наркотиків, включаючи обмін розвідданими для підтримки правоохоронних органів та раннього попередження, є критично важливим для пом'якшення шкоди. Державні сили та їхні допоміжні підрозділи також є основними учасниками насильства, і будь-яка стратегія стабілізації повинна враховувати цю складну динаміку, де економічні інтереси, політичні амбіції та кримінальні мережі утворюють нерозривний вузол.

Висновки

Зрощення економіки та насильства: Незаконні ринки (викрадення, рекет на дорогах, золото) стали основою фінансування та легітимності для озброєних угруповань, що робить їхнє відокремлення від конфлікту неможливим.

Трансформація економіки викрадень: Після затишшя 2023–2024 років відбулася реструктуризація підходів (особливо з боку IS Sahel), що призвело до різкого зростання викрадень іноземців заради викупу та залучення значних фінансових потоків.

Дороги та золото як важелі впливу: Контроль над транспортними коридорами та оподаткування видобутку золота (через місцевих посередників) дозволяють угрупованням чинити економічний тиск на держави та розширювати свій вплив без прямого захоплення територій.

Потреба в адаптивних відповідях: Ефективна протидія вимагає моніторингу ринкових змін (зокрема цінових шоків на золото) та координації зусиль із протидії новим загрозам, таким як синтетичні опіоїди, з акцентом на збереження засобів існування місцевих громад.

РЕКОМЕНДОВАНІ МАТЕРІАЛИ



Як розробити політику управління штучним інтелектом: практичні настанови ACAMS [7]

Управління штучним інтелектом за кілька років перетворилося з теоретичної концепції на практичне завдання для організацій, а кількість настанов, вебінарів і публікацій на цю тему постійно зростає. Проте більшість таких матеріалів пояснює, чому AI важливий і яких принципів слід дотримуватися, і значно менше уваги приділяє практичному етапу, коли організація має підготувати власну політику. Саме тоді постають питання: з чого почати, що має містити документ, які інструменти він повинен охоплювати і хто відповідає за його виконання.

Стаття, опублікована на платформі ACAMS, пропонує заповнити цю прогалину. Її головна теза полягає в тому, що робота має починатися не з тексту політики, а з визначення її мети. Використання чужого шаблону або тексту, згенерованого ШІ, дає документ, який формально виглядає бездоганно, але не відображає реальних ризиків організації, а отже, не застосовується в роботі. Автори радять спершу відповісти на кілька питань: навіщо створюється політика, чи є вона відповіддю на очікування регуляторів, чи має на меті встановити підзвітність, чи зумовлена тим, що AI вже настільки інтегрований у бізнес-процеси, що відсутність управління ним стала ризиком.

Відповіді на ці питання становлять основу політики, після чого доцільно спиратися на міжнародний досвід: Регламент ЄС про штучний інтелект, Стратегію цифрових стандартів Великої

[7] https://www.acams.org/en/opinion/how-write-ai-governance-policy

Британії, стандарт ISO/IEC 42001 і рамку управління ризиками NIST. Водночас ці документи не слід копіювати дослівно, оскільки законодавчий акт і внутрішня політика організації мають різне призначення.

Попри розмаїття рамок, вони мають спільне ядро, яке варто взяти за основу. Управління має бути ризик-орієнтованим, відповідальність за системи чітко визначеною, людська підзвітність має зберігатися за будь-яких обставин, контрольні заходи мають бути пропорційними ризику, а саме управління не завершується після впровадження інструменту і триває протягом усього його життєвого циклу. На думку авторів, ці п'ять принципів застосовні незалежно від юрисдикції та галузі.

Перш ніж запроваджувати контроль, організація має визначити, що саме вона контролює. Співробітники можуть по-різному розуміти поняття ШІ: для одних це Gemini та ChatGPT, для інших предиктивна аналітика, для третіх внутрішні моделі машинного навчання. Тому політика повинна чітко встановлювати, які системи охоплюються, які виключаються і чи потребують різні категорії різного підходу. Наступним кроком є інвентаризація: скільки рішень на основі AI офіційно затверджено, скільки працівників користуються публічними генеративними чат-ботами без погодження, скільки підрозділів самостійно придбали програмне забезпечення з убудованим AI і скільки наявних застосунків отримали нові функції AI після оновлень. Інвентаризація є не формальністю, а основою для виявлення дублювання, пріоритизації перевірок і формування повної картини.

Щодо питання власності на AI автори доходять висновку, що відповідальність є спільною. Бізнес-підрозділи визначають потребу, IT-підрозділ впроваджує та підтримує рішення, служба інформаційної безпеки захищає системи й дані, підрозділ із захисту персональних даних контролює обробку персональної інформації, комплаєнс тлумачить регуляторні вимоги, а управління ризиками забезпечує незалежну перевірку. Покладення всіх цих функцій на один підрозділ неминуче створює прогалини, тоді як чіткий розподіл ролей запобігає плутанині та дублюванню зусиль.

Ключовий урок європейського досвіду щодо ризиків полягає в тому, що не всі системи потребують однакової уваги: інструмент для узагальнення нарад і модель для санкційного скринінгу мають принципово різний рівень ризику. Автори пропонують просту класифікацію. До низького ризику належать інструменти продуктивності (переклад, перевірка граматики, узагальнення). Середній ризик мають системи, що підтримують операційні рішення під наглядом людини (дослідницька допомога, перевірка документів). Високий ризик притаманний системам, які впливають на рішення щодо клієнтів, підтримують виконання регуляторних обов'язків, обробляють конфіденційну інформацію або можуть спричинити фінансові втрати й репутаційні наслідки. Інтенсивність контролю має зростати разом із рівнем впливу, причому складні моделі оцінювання на початковому етапі не потрібні: прості класифікації довели свою ефективність.

Окрему увагу приділено постачальникам, оскільки багато організацій не розробляють власних моделей, а придбавають готові продукти з убудованим ШІ. Регулятори не вважають, що

відповідальність у такому разі переходить до постачальника: він відповідає за розробку і підтримку продукту, але організація залишається підзвітною за те, як продукт використовується в її середовищі. Тому належна перевірка постачальника має охоплювати аналіз того, яку функціональність AI включено, які дані обробляє модель, як її моніторять і оновлюють, чи можна скасувати її рекомендації та чи задокументовано відомі упередження. Автори розглядають такий аналіз як необхідну умову контролю ризиків, а не як надмірну формальність.

Центральним залишається питання ролі людини. Автори наголошують, що технології змінюються, а підзвітність залишається незмінною: AI може узагальнювати, формувати рекомендації та виявляти закономірності, проте не повинен замінювати людське судження там, де рішення можуть суттєво вплинути на клієнтів, працівників чи організацію. Політика має чітко визначати, хто переглядає результати роботи AI перед ухваленням рішення, чи можуть працівники оскаржити рекомендацію системи і хто несе остаточну відповідальність за рішення, ухвалене з використанням ШІ. Відповідальність при цьому завжди залишається за людьми.

Управління не завершується після впровадження. Моделі оновлюються, постачальники додають нові функції, дані змінюються, і рішення, яке два роки тому вважалося низькоризиковим, сьогодні може підтримувати зовсім інший процес. Тому регулярні перегляди є необхідністю, а організація має бути готовою реагувати на інциденти, яких неможливо повністю уникнути.

Підсумовуючи, автори визнають, що розроблення політики управління AI може видаватися складним завданням з огляду на кількість рамок, стандартів і регуляторних вимог. Водночас вони виокремлюють п'ять незмінних складових: узгодженість із бізнес-цілями, чітко визначені власність і підзвітність, пропорційність ризику, змістовний людський нагляд і безперервне вдосконалення. Успіх політики вимірюється не обсягом документа і не точністю відтворення того чи іншого стандарту, а тим, чи допомагає вона ухвалювати кращі рішення, керувати ризиками та використовувати AI на користь організації.

Угорщина: майже 20 млн доларів готівки у справі колишнього міністра та розслідування про роль банку МКВ у транзиті російських коштів [8]

За повідомленням Reuters від 14 листопада 2026 року, угорські органи влади вилучили майже 20 млн доларів готівкою в межах розслідування справи про хабарництво щодо Міклоша Сестака, який у 2014–2018 роках обіймав посаду міністра національного розвитку в уряді Віктора Орбана. Національне управління з повернення та захисту активів повідомило, що під час обшуків слідчі виявили значні суми готівки, закопані в лісах, приховані в господарських будівлях, складах і житловому приміщенні, а також у дорогому сейфі у відокремленому місці. За словами міністра фінансів Андраша Кармана, дванадцять працівників Державного казначейства протягом восьми годин перераховували кошти за допомогою лічильників банкнот. Вилучення відбулося в межах антикорупційної кампанії уряду Петера Мадяра, сформованого після квітневих виборів. Сестак заперечує порушення, його адвокат заявив місцевому виданню, що вилучена готівка не належить його клієнтові, і що у справі є інші підозрювані. Окремо під вартою за підозрою в корупції перебувають двоє колишніх міністрів і колишній голова центрального банку Дьордь Матольчі, які також заперечують свою провину.

Того ж тижня міжнародний консорціум Inside Deutsche Bank (понад 230 журналістів із 56 видань, які протягом року аналізували мільйони внутрішніх документів банку, переданих двома викривачами) оприлюднив матеріал Follow the Money про роль угорського банку МКВ у транзиті коштів, пов'язаних із підсанкційним російським олігархом Олегом Дерипаскою. МКВ у червні 2017 року придбали особи з оточення тодішнього прем'єр-міністра, зокрема мільярдер Льорінц Месарош, а аналітики Deutsche Bank у внутрішньому звіті характеризували банк як такий, що «практично контролюється» урядом. Внутрішнє розслідування Deutsche Bank під назвою Project Wingman розпочалося на початку 2019 року після скандалу з Danske Bank: на першому етапі було проаналізовано 2 864 транзакції на 667,4 млн євро, згодом обсяг зріс до понад 1,7 млрд євро, що пройшли щонайменше через 15 центральних підставних компаній, а понад половина досліджених транзакцій проходила через МКВ. Після запровадження санкцій США проти Дерипаски у квітні 2018 року обсяги операцій мережі різко зросли.

[8] https://www.reuters.com/world/hungary-recovers-20-million-cash-probe-orban-minister-2026-11-14/

Матеріали детально описують типологію мережі. Гонконзька Dempshire Corporation (зареєстрована 2011 року, ліквідована 2025 року), номінально очолювана латвійським акціонером і представлена як постачальник промислового обладнання, у січні 2017 – лютому 2020 року переказала мережі майже 160 млн євро й отримала майже 136 млн євро, оплачуючи, зокрема, чартер приватного літака, утримання нерухомості, будівельні матеріали й предмети розкоші. Yingli Trading, яку фінансова звітність «Русала» описувала як незалежного партнера, мала тісніші зв'язки з компанією (її першим директором був давній афілійований з «Русалом» менеджер) і менш ніж за рік переказала Dempshire майже 80 млн євро. Гонконзькі Versala і Sanderlyn, засновані з різницею в один день у червні 2017 року, слугували вузловими компаніями мережі. Платежі надходили французькій консьєрж-компанії (понад 1,2 млн євро), дизайнерській фірмі, що облаштовувала гірськолижний готель Дерипаски (3,8 млн євро), а компанія з Британських Віргінських Островів отримала 17 млн євро від структури, яку ЗМІ описують як посередника білоруських поставок зброї. «Русал» заявив, що Дерипаска відмовився від контролю за угодою з OFAC 2019 року.

Реакція Deutsche Bank була повільною. Ще у 2018 році внутрішній звіт фіксував корупційні, санкційні та легалізаційні ризики МКВ, формальний перегляд відносин розпочався у листопаді 2019 року, а заяви МКВ про відмову від офшорних клієнтів не підтверджувалися даними про операції. IT-системи моніторингу банку всередині установи називали «недостатніми», а повідомлення про підозрілі операції подавалися ще до розуміння масштабу мережі. Навесні 2020 року банк вирішив припинити кореспондентське обслуговування рахунків МКВ у євро та канадських доларах у Франкфурті, МКВ попросив відтермінування, і 5 червня 2020 року Deutsche Bank попередив BaFin, що раптове блокування вхідних платежів може протягом кількох днів спричинити дефіцит ліквідності в МКВ. Додаткові повідомлення до німецького підрозділу фінансової розвідки стосувалися, зокрема, семи ключових компаній, які продовжували діяти після попередніх повідомлень. Доступ МКВ до кліринґу було припинено 6 жовтня 2020 року. Commerzbank, що також мав кореспондентські відносини з МКВ, повідомив про 51 719 пов'язаних із мережею транзакцій на 678 млн євро у 2017 – квітні/травні 2020 року, близько 80% з яких ініціювали компанії, зареєстровані поза Угорщиною.

Правові наслідки виявилися обмеженими. Німецьке розслідування щодо відмивання коштів розпочалося на початку 2020 року, однак угорська прокуратура заявила, що справа не належить до її юрисдикції, і Франкфуртська прокуратура згодом закрила провадження; матеріали не свідчать про навмисне сприяння МКВ з боку угорських прокурорів. Менеджеру нерухомості Дерипаски Грему Бонем-Картеру у 2022 році висунули обвинувачення в США, але у лютому 2023 року запит на екстрадицію було відкликано. У 2023 році МКВ увійшов до складу новоствореного банку МВН. Експерт RUSI Том Кітінг звертає увагу на системну проблему кореспондентських відносин: банк-кореспондент покладається на перевірки, здійснені банком-респондентом, бачить лише частину ланцюга платежу і має обмежене уявлення про його комерційну мету, тоді як офшорна структура власності приховує, хто насправді контролює кошти. Deutsche Bank заявив, що виявив схему власним розслідуванням і повідомив про неї компетентні органи; Дерипаска, власники МКВ і МВН на запити журналістів не відповіли.



Продаж курорту у Киргизстані як приклад обходу санкцій та російського впливу [9]

Розслідування, проведене Організацією з боротьби з корупцією та організованою злочинністю (OCCRP), виявило тривожні факти навколо продажу розкішного гірського курорту «Барс», розташованого в мальовничих передгір'ях Іссик-Кульської області Киргизстану. Ця історія є не просто черговим епізодом боротьби з корупцією на пострадянському просторі, а яскравим прикладом того, як державні активи можуть використовуватися для створення складних фінансових мереж, покликаних обходити міжнародні санкції та сприяти реалізації геополітичних інтересів кремля. Курорт, який раніше належав родині відомого кримінального авторитета Камчі Колбаєва, був конфіскований державою у 2023 році, а згодом, за вельми сумнівних обставин, перейшов до рук маловідомої неурядової організації, тісно пов'язаної з російськими структурами, що перебувають під санкціями.

Ключовим елементом цієї схеми є фінансова та організаційна структура покупця. Згідно з документами, новим власником курорту стала громадська організація під назвою «Єдність народу» (Edinstvo Naroda), яка не має публічного веб-сайту чи помітної діяльності. На момент придбання об'єкта засновником організації був Саламат Чинибеков, який, за даними фінансової звітності, вніс до статутного фонду близько 13 мільйонів доларів. Примітно, що сума внеску дещо перевищує 12 мільйонів доларів, які організація сплатила державі за курорт. Походження цих коштів залишається нез'ясованим, а сам Чинибеков, який нині обіймає посаду керівника міського департаменту в регіональній столиці Каракол, відмовився відповідати на запитання журналістів. Ще більш показовим є те, що значна частина цих коштів, а саме щонайменше 1,7 мільйона

[9] https://www.occrp.org/en/investigation/kyrgyz-government-sold-mountain-resort-to-ngo-tied-to-sanctioned-russian-influence-effort

доларів, надійшла від російської організації «Євразія» (Evrazia) та її киргизької дочірньої структури «Євразія КГ».

Організація «Євразія» відома як інструмент просування прокремлівської ідеології «євразійської інтеграції» на теренах колишнього СРСР. Вона організовує освітні програми, конкурси та інші заходи, спрямовані на формування проросійського світогляду. Однак, що важливіше для розуміння контексту обходу санкцій, ця організація перебуває під санкціями Сполучених Штатів Америки та Європейського Союзу. Раніше OCCRP та молдовські партнери повідомляли, що «Євразія» брала участь у спрямуванні значних коштів до Молдови з метою забезпечення негативного результату на референдумі щодо вступу країни до ЄС у 2024 році. Уряди низки країн характеризують цю структуру як інструмент впливу Ілана Шора, молдовського олігарха-втікача, засудженого на батьківщині до 15 років позбавлення волі за шахрайство та відмивання грошей. Шор, який, за даними слідства, очолює тіньові фінансові мережі, пов'язані з кремлем, вже не вперше фігурує в контексті Киргизстану. Зокрема, платіжна мережа A7, яку він заснував разом з російським державним банком, використовує Киргизстан як транзитний вузол для переказу коштів, що також вказує на використання місцевої фінансової системи для обходу міжнародних обмежень.

Особливу увагу в розслідуванні привертає особа Саламата Чинибекова, чия біографія не відповідає масштабам фінансових операцій, які він проводить. У середині 2010-х років він працював у кафе в Караколі та на знаменитому золотому руднику «Кумтор», що підтверджується його власними публікаціями в соціальних мережах. У 2020 році він став власником компанії «Asia Tau», яка, за офіційними даними, значиться як туристична агенція, але фактично, згідно з митними деклараціями, займалася імпортом китайських деталей для друкованих плат. Крім того, у 2025 році Чинибеков ненадовго входив до ради директорів «Capital Bank», державного банку Киргизстану, який перебуває під санкціями ЄС та Великої Британії за ймовірне сприяння росії у фінансуванні війни проти України. Ці факти свідчать про те, що особа, яка формально виступає засновником ГО-покупця, може бути лише номінальною фігурою, або ж про її глибокі зв'язки з тіньовими фінансовими потоками, що проходять через підсанкційні установи.

Схема придбання курорту також викликає запитання щодо прозорості та відповідності ринковим умовам. Президент Киргизстану Садир Жапаров публічно заявив, що уряд продав курорт за 12 мільйонів доларів, що нібито вдвічі перевищує його вартість, і що ці кошти надійшли до державного бюджету. Однак розслідування OCCRP виявило, що ці твердження не відповідають дійсності. Державна служба національної безпеки (ГКНБ) Киргизстану у 2023 році оцінила курорт у 20 мільйонів доларів, що підтверджується відеоматеріалами та рішеннями Верховного суду. Таким чином, продаж за 12 мільйонів доларів фактично означає продаж за 60% від початкової оцінки, а не за подвійну ціну. Крім того, існує інвестиційна угода від лютого 2025 року, згідно з якою уряд спочатку планував передати курорт в оренду саме «Євразії КГ» за 12,1 мільйона доларів. Це свідчить про те, що російська структура була головним бенефіціаром угоди ще на етапі планування, а ГО «Єдність народу» могла бути використана як буферна ланка для приховування справжнього кінцевого власника та уникнення санкційних ризиків.

Варто звернути увагу, що президент Жапаров у своїх заявах назвав покупцем курорту місцевого бізнесмена Олексія Ширшова, який нібито вже будує гольф-поле та встановлює фунікулери. Однак журналісти не знайшли жодних документальних підтверджень того, що Ширшов є власником об'єкта. Сам Ширшов у відповіді на запит OCCRP не підтвердив і не спростував заяви президента, зазначивши лише, що не обіймає державних посад і не зобов'язаний розкривати інформацію про свій приватний бізнес. Він також заявив, що роками допомагає проєктам з розвитку економіки Киргизстану, надаючи «професійний досвід, ділові контакти та інвестиційні можливості», але не є членом керівних органів відповідних організацій. Ця заява, разом із відсутністю документальних зв'язків між Ширшовим та ГО «Єдність народу», вказує на те, що реальна структура власності може бути ще складнішою і заплутанішою, ніж здається на перший погляд.

Окремої уваги заслуговує зв'язок між засновником ГО та високопосадовцями Киргизстану. Мер міста Каракол Талантбек Іманов, який раніше обіймав посаду міністра цифрового розвитку та очолював президентське інвестиційне агентство, за даними комерційної бази SPARK, значиться співвласником компанії «Asia Tau» разом із Чинибековим. Крім того, вони разом заснували ГО «Волонтери країни», яка була створена під час пандемії COVID-19, але не веде жодної помітної діяльності. Це підтверджує існування тісних неформальних зв'язків між бізнесом, який бере участь у сумнівних фінансових операціях, та представниками місцевої влади, що створює сприятливе середовище для реалізації схем, подібних до продажу курорту «Барс». Варто зазначити, що на момент публікації розслідування курорт «Барс» залишався закритим для публіки, а офіційні особи, включаючи прес-службу президента та правоохоронців, не надали відповідей на запитання журналістів щодо розбіжностей в оцінці та кінцевого покупця.

Підсумовуючи, історія з продажем курорту «Барс» демонструє складний механізм, який може використовуватися для обходу міжнародних санкцій та легітимізації коштів сумнівного походження. Використання маловідомої ГО як покупця, фінансування якої надходить від підсанкційної російської організації «Євразія», та залучення номінальних осіб, пов'язаних з підсанкційними банками, є класичними ознаками тіньових фінансових схем.

Ця справа підкреслює необхідність посилення контролю за транскордонними фінансовими потоками та підвищення прозорості приватизації державних активів, особливо в країнах, які є важливими транзитними вузлами для російських фінансових мереж. Відсутність належної реакції з боку киргизької влади на численні запитання журналістів лише підсилює підозри щодо можливої причетності високопосадовців до цієї угоди, що становить серйозну загрозу як для економічної безпеки країни, так і для міжнародної спільноти, яка намагається протидіяти агресивній політиці кремля.



Національне агентство з боротьби зі злочинністю Великої Британії пояснює п'ять поширених схем шахрайства [10]

Національне агентство з боротьби зі злочинністю Великої Британії (NCA) запустило інформаційну кампанію Fraud Explained, мета якої полягає в тому, щоб допомогти громадянам розпізнавати тактики злочинців, помічати тривожні ознаки та захищати свої кошти, персональні дані й облікові записи. Основу кампанії становлять п'ять коротких пояснювальних відео про шахрайство на ґрунті романтичних стосунків, фішинг, видавання себе за довірені організації, інвестиційне шахрайство та шахрайство з перенаправленням платежів. Кожне відео має однакову логіку: як діє схема, за якими ознаками її розпізнати і що робити, якщо людина стала об'єктом атаки. Усі ролики завершуються порадою негайно звернутися до свого банку в разі переказу коштів, повідомити про шахрайство до служби Report Fraud і шукати додаткові матеріали за назвою урядової кампанії Stop! Think Fraud.

Шахрайство на ґрунті романтичних стосунків NCA описує як схему, де йдеться не про почуття, а про гроші. Зловмисники створюють фальшиві профілі на сайтах знайомств і в соціальних мережах, тижнями, місяцями чи навіть роками вибудовують стосунки, що здаються справжніми, і часто стверджують, що працюють за кордоном. Після здобуття довіри з'являються прохання про гроші: зламаний телефон, витрати на подорож, хворий родич, надзвичайна ситуація.

[10] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime/fraud-explained

Тривожними ознаками є уникання відеодзвінків, прохання тримати стосунки в таємниці, швидкі зізнання в сильних почуттях, перенесення спілкування за межі платформи знайомств і, зрештою, прохання про кошти. Агентство радить не надсилати гроші, не передавати банківських реквізитів і особистих документів, не інвестувати за порадою такого співрозмовника і наголошує, що потерпілий не винен у тому, що сталося.

Фішинг і видавання себе за довірені організації ґрунтуються на тиску й терміновості. У фішингових повідомленнях і дзвінках зловмисники видають себе за банк, службу доставки, податковий орган, що нібито повертає переплату, або за підрозділ протидії шахрайству, спрямовують людину на фальшиві сайти чи вимагають розкрити персональні дані. Ознаками є неочікувані запити, тривожна лексика, адреси електронної пошти чи номери телефонів, що лише нагадують справжні, і будь-які прохання повідомити логін або одноразовий код. У схемах видавання себе за інших зловмисники представляються працівниками банків, операторів зв'язку, енергопостачальних компаній чи поліції, використовують реальні відомості про жертву і вимагають негайно переказати кошти, підтвердити персональні дані, передати щось або нікому не розповідати про розмову. NCA радить припинити контакт і самостійно зв'язатися з організацією за номером з її офіційного сайту чи рахунку, оскільки справжня організація ніколи не перешкоджатиме перевірці.

Інвестиційне шахрайство, за визначенням NCA, є ретельно сконструйованим обманом, а не можливістю. Зловмисники обіцяють гарантовану дохідність через криптовалюти, схеми швидкого збагачення чи дострокове вивільнення пенсійних накопичень, використовують фальшиві сайти, підроблені рекомендації знаменитостей і агресивні прийоми продажу, створюють штучну терміновість (обмежена пропозиція, бонуси для перших інвесторів) і навіть показують фіктивний прибуток, щоб спонукати до нових вкладень. Ознаками є непрошений контакт, тиск, обіцянки високої дохідності без ризику, вимога тримати інвестицію в таємниці та затримки й відмовки при спробі вивести кошти. Агентство рекомендує перевіряти компанію в реєстрі фірм FCA, остерігатися непрошених дзвінків щодо інвестицій і пенсій, отримувати незалежну фінансову консультацію і ніколи не передавати даних для входу до пенсійних рахунків.

Шахрайство з перенаправленням платежів загрожує насамперед бізнесу та особам, які здійснюють великі платежі (купівля нерухомості, розрахунки з підрядниками й постачальниками). Зловмисники перехоплюють листування або видають себе за легітимного контрагента саме тоді, коли очікується запит на оплату, і просять переказати кошти на інший рахунок. Ознаками є неочікувані повідомлення про зміну банківських реквізитів, термінові вимоги оплати та адреси електронної пошти, що трохи відрізняються від звичних. NCA радить завжди підтверджувати зміну реквізитів телефонним дзвінком на відомий номер, не покладатися лише на електронну пошту, за сумнівів здійснювати невеликий тестовий платіж із підтвердженням його отримання та запровадити додаткові етапи погодження платежів. Для фахівців з фінансового моніторингу серія корисна як стисла довідка про предикатні злочини, доходи від яких зазвичай проходять через рахунки грошових мулів: на тій самій сторінці NCA розміщено посилання на свій сервіс прийому повідомлень про підозрілу діяльність.

Ваша думка важлива!

Які обмеження повноважень AI-агентів мають закріпити українські банки й платіжні установи, перш ніж доручати опрацювання сповіщень фінансового моніторингу?

Як має бути врегульоване фінансування політичних партій в Україні, щоб внески, конвертовані з віртуальних активів через посередників, не залишалися поза контролем НАЗК?

Які ризики для України як майбутнього члена ЄС створює залежність Європи від імпорту критичної сировини з регіонів із високим рівнем організованої злочинності?

Які ознаки в кореспондентських відносинах мають сигналізувати українським банкам, що банк-респондент обслуговує мережу підставних компаній, пов'язаних із підсанкційними особами?

Яким чином Україна та її партнери можуть удосконалити моніторинг транскордонних фінансових потоків, щоб унеможливити фінансування російських проєктів через треті країни?

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-2026-47

Архів

Бюлетень є аналітичною розробкою методологічної команди Департаменту антилегалізаційної політики Міністерства фінансів України, спрямованою на поширення кращих практик, дослідження новітніх типологій та глобальних регуляторних і правоохоронних тенденцій у сфері ПВК/ФТ/ФР. Видання призначене для підвищення інституційної спроможності всіх учасників AML системи України та сприяння ефективному управлінню ризиками ВК/ФТ/ФР з урахуванням міжнародних стандартів та актів права ЄС.

Міністерство фінансів України

AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE