Міністерство
фінансів
України

Методологічний бюлетень AML

№39/2026

Зміст

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.

Велика Британія затвердила Стратегію протидії відмиванню коштів і повернення активів на 2026–2029 роки [1]

У вересні 2026 року Міністерство внутрішніх справ (Home Office) і Казначейство Великої Британії (HM Treasury) оприлюднили Стратегію протидії відмиванню коштів і повернення активів на 2026–2029 роки. Документ підписали міністр безпеки Ден Джарвіс та економічна секретарка Казначейства Люсі Ріґбі. Стратегія має три цілі: зробити систему захисту ефективнішою і водночас простішою для добросовісного бізнесу; руйнувати мережі відмивання коштів, зокрема ті, що діють через малий бізнес на торговельних вулицях; повертати більше злочинних активів потерпілим, правоохоронним органам і державі. Досягати їх планують за трьома взаємопов'язаними напрямами: «Зосередження» (Target), «Інтеграція» (Integrate) та «Посилення спроможностей» (Empower).

Уряд оцінює масштаб загрози так: існує «реалістична можливість», що через Велику Британію, у її межах або через зареєстровані там корпоративні структури щороку відмивається понад 100 млрд фунтів стерлінгів – це близько 10% річних державних видатків. Лише доходи від окремих видів корисливих злочинів в Англії та Уельсі у 2023/24 році оцінено щонайменше в 21,9 млрд фунтів. Пріоритети Стратегії визначає Національна оцінка ризиків відмивання коштів і фінансування тероризму 2025 року. Відправна точка для вимірювання результатів – показники 2025/26 року: 3 158 випадків припинення незаконних фінансових схем (на 15% більше, ніж роком раніше), 4 085 обвинувальних вироків за відмивання коштів (+11%) і 345,3 млн фунтів повернутих активів.

На реалізацію Стратегії спрямують щонайменше 550 млн фунтів у 2026–2029 роках: 520 млн – із збору на протидію економічній злочинності (Economic Crime Levy), який сплачують суб'єкти регульованого сектору, та 30 млн – з пакета заходів для торговельних вулиць, оголошеного в бюджеті 2025 року. Ці кошти мають забезпечити понад 500 нових посад у правоохоронній і наглядовій системі. Така модель прямо пов'язує внесок приватного сектору з розбудовою державних спроможностей, а отже, створює для бізнесу підстави очікувати відчутної віддачі – насамперед у вигляді якіснішого зворотного зв'язку і меншого обсягу формальних вимог.

Найглибша інституційна зміна стосується нагляду. Кількість органів нагляду у сфері запобігання та протидії відмиванню коштів і фінансуванню тероризму скоротиться з 25 до трьох. Управління з фінансового нагляду (FCA) візьме на себе нагляд за юридичними і бухгалтерськими послугами, а також за постачальниками послуг зі створення та обслуговування трастів і компаній, яких нині наглядають переважно професійні об'єднання. Поруч залишаться Податкова і митна служба (HMRC) та Комісія з азартних ігор. Паралельно уряд проведе консультації щодо посилення наглядових повноважень: неоголошених перевірок, обшуку приміщень для виявлення готівки та посилення персональної відповідальності керівників за порушення Правил щодо запобігання відмиванню коштів (MLRs).

[1] https://assets.publishing.service.gov.uk/media/6aa950402f29b388848184ee/Anti-money_laundering_and_asset_recovery_strategy_2026-2029__web__v2.pdf

Другий ключовий блок – фінансова розвідка. У структурі Національного агентства з боротьби зі злочинністю (NCA) за підтримки FCA буде створено національну службу фінансової розвідки на засадах державно-приватного партнерства. Вона об'єднає наявні механізми обміну інформацією, зокрема Спільну робочу групу з розвідки у сфері відмивання коштів (JMLIT), а співпрацю, яка сьогодні охоплює переважно банки, поширять на постачальників послуг з криптоактивами, установи з переказу коштів та установи електронних грошей. Британський підрозділ фінансової розвідки (UKFIU) має отримати два нові законодавчі повноваження: витребовувати інформацію без попереднього дозволу суду та зупиняти фінансові операції на запит вітчизняних правоохоронних органів або іноземних партнерів – відповідно до оновлених вимог Рекомендації 40 FATF.

Окремо переглядається режим повідомлень про підозрілу діяльність. У 2024–25 році UKFIU отримав 866 616 таких повідомлень. Ще у 2025 році поріг, нижче якого банк може проводити операції за рахунком без окремої згоди правоохоронних органів (так званий запит DAML, розділ 339A Закону про доходи від злочинної діяльності 2002 року), підвищили з 1 000 до 3 000 фунтів. Тепер уряд вивчить доцільність підвищення самого порогу підозри, наприклад до стандарту «обґрунтовані підстави підозрювати». Мета – зменшити кількість малоцінних «захисних» повідомлень і вивільнити аналітичні ресурси. Водночас зміна стандарту підозри зачіпає основу всієї системи звітування, тож рішення ухвалюватимуть лише після оцінки впливу на збирання розвідувальної інформації.

Стратегія передбачає й можливе розширення периметра регулювання. Уряд проведе консультації щодо включення до сфери дії MLRs забудовників, офшорних постачальників послуг, пов'язаних з віртуальними активами, торговців антикваріатом і предметами старовини, футбольних клубів та агентів, краудфандингових платформ, що збирають пожертви, а також щодо зміни обсягу регулювання агентів з оренди нерухомості та торговців високовартісними товарами підвищеного ризику. Документ окремо наголошує: нові сектори додаватимуть лише тоді, коли це справді необхідно й ефективно для реагування на реальні ризики.

Помітне місце в Стратегії посідають криптоактиви. Документ посилається на галузеві оцінки, за якими на стейблкоїни припадає 84% обсягу незаконних транзакцій з криптоактивами у світі. Відповіддю мають стати регулювання випуску стейблкоїнів, оновлення повноважень з повернення криптоактивів, зокрема тих, що зберігаються на іноземних біржах, і дорожня карта щодо технологій посилення конфіденційності, які розривають простежувані зв'язки між транзакціями. Як приклад результативності наведено справу Столичної поліції Лондона, у якій спеціалізований підрозділ відстежив і вилучив 61 000 біткоїнів – найбільше вилучення криптоактивів у країні.

Третій практичний фокус – готівка і малий бізнес. Через підприємства на торговельних вулицях щороку відмивається щонайменше 1 млрд фунтів. Операція Machinize вже дала 2 734 обстеження приміщень, 924 затримання та понад 10,7 млн фунтів вилучених або арештованих коштів. Тепер у Home Office створюють міжвідомчий підрозділ з протидії організованій злочинності на торговельних вулицях із фінансуванням 10 млн фунтів на рік протягом трьох років. Окремо розглядається ризик внесення готівки через відділення Post Office, куди щомісяця надходить 2–3 млрд фунтів: обговорюються ліміти, відеоспостереження та цільові вимоги до ідентифікації клієнтів. Стратегія пов'язує внутрішні реформи з міжнародною роллю Великої Британії, яка головує у FATF у 2026–2028 роках і в G20 у 2027 році.

Висновки

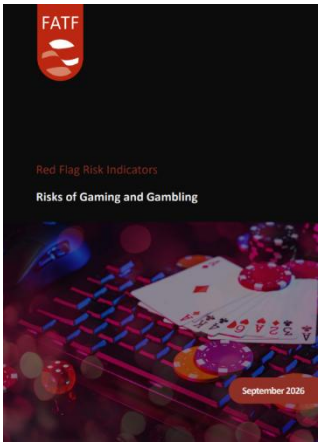
Скорочення кількості органів нагляду з 25 до трьох **свідчить, що роздрібнений нагляд** за юристами, бухгалтерами й провайдерами послуг для компаній **визнано слабкою ланкою системи**. Це аргумент на користь єдиних стандартів нагляду за незалежними професіоналами.

Право UKFIU зупиняти операції на запит іноземних партнерів відкриває підрозділам фінансової розвідки інших країн, зокрема Держфінмоніторингу, **шлях до швидшого блокування активів, виведених через британські структури**.

Підвищення порогу DAML і перегляд стандарту підозри це сигнал переходу від кількості повідомлень до їхньої якості. СПФМ варто оцінити, яку частку їхньої звітності становлять формальні «захисні» повідомлення.

Поширення MLRs на офшорних провайдерів віртуальних активів, футбольні клуби й забудовників означає, що українські компанії, які працюють із британським ринком у цих сферах, мають готуватися до вимог щодо належної перевірки клієнтів.

Червоні прапорці FATF: ризики у сфері азартних ігор та геймінгу [2]



Документ містить оновлену оцінку ризиків відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення у гральній та ігровій індустрії, а також перелік індикаторів підозрілості, призначених для операторів, наглядових органів і правоохоронних структур. Робота оновлює спільне дослідження FATF та Азійсько-Тихоокеанської групи з протидії відмиванню коштів щодо казино, проведене у 2009 році, і суттєво розширює його предметне поле. Доказову базу становлять відповіді на проєктну анкету від 80 юрисдикцій глобальної мережі FATF, письмові коментарі від 29 юрисдикцій, цільові консультації з галузевими асоціаціями, дослідниками та представниками приватного сектору, а також кейси, надані країнами. Аналіз охоплює онлайн-казино та казино у фізичних закладах, спортивні ставки та ставки на нестандартні події, інші види азартних ігор, що не належать до казино, — скретч-картки, аркади, бінго, лотереї та ігрові автомати поза межами казино, — а також онлайн-відеоігри та мобільні ігри й ризики, пов'язані з діяльністю нелегальних операторів. Окремо досліджувалися бізнес-моделі й канали надання послуг, взаємодія сектору з фінансовою системою та його перетин із цифровими платформами, зокрема соціальними мережами. Принципово важливою є методологічна ремарка авторів: FATF не запроваджує суворого визначення поняття «казино», оскільки в логіці ризик-орієнтованого підходу кожна юрисдикція самостійно оцінює власні ризики та впроваджує пропорційні їм заходи.

Основна теза оцінки полягає в тому, що гральна та ігрова індустрії за останні роки зазнали структурної трансформації і продовжують змінюватися через експансію онлайн-платформ, транскордонність, мультипродуктовість і мультиплатіжність. Гральні заклади та платформи стали частиною значно ширшої екосистеми передачі вартості з великою кількістю учасників, частина з яких узагалі перебуває поза межами національних режимів протидії відмиванню коштів і фінансуванню тероризму. Ця обставина у поєднанні з різним обсягом регулювання грального бізнесу та неоднаковим рівнем розуміння ризиків, притаманних ігровій діяльності, зумовила появу нових форм ризику. Дослідження фіксує зростання обсягів глобального ринку, поширення онлайн-платформ і накладання одна на одну платіжних моделей, коли той самий оператор одночасно приймає готівку, картки, банківські перекази, віртуальні активи, мобільні гроші та кошти через третіх осіб — посередників і сервіси переказу коштів. Водночас автори підкреслюють, що рівень і типи ризику суттєво різняться залежно від комбінації використаних платіжних методів, самої послуги та способу її надання — безпосередньо у закладі чи дистанційно.

Профіль ризиків у документі чітко диференційовано. Відмивання коштів через гральний бізнес визнано усталеним ризиком у багатьох юрисдикціях, причому найбільш експонованими вважаються казино у фізичних закладах й онлайн-казино та спортивні ставки, тоді як лотереї, скретч-картки й окремі інші неказинові форми низка країн оцінює як менш вразливі. Попри структурну схожість ігрових і гральних платформ, зокрема транскордонну клієнтську базу та подібні потоки коштів, наявні докази свідчать, що відмивання через відеоігри відбувається у менших масштабах, з нижчим рівнем складності та меншою частотою, ніж через азартні ігри. Натомість у сфері фінансування тероризму співвідношення протилежне: ризики й типології, пов'язані з гемблінгом, залишаються обмеженими та рідко фіксуються у звітності, тоді як онлайн-геймінг демонструє більше виявлених і задокументованих випадків зловживань, на що впливають соціальні та технологічні чинники цього середовища. Ризики фінансування розповсюдження зброї масового знищення в обох сегментах визнано дуже обмеженими, хоча теоретична вразливість не виключається повністю.

[2] https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/risks-of-gaming-and-gambling-2026.pdf.coredownload.pdf

Окремий блок ризиків сформовано навколо платіжних інструментів і суміжного цифрового середовища. Готівка, електронні гаманці, послуги мобільних платежів та віртуальні активи визначені як вразливі до широкого спектра схем відмивання, а різноманіття платіжних методів, які приймають онлайн-оператори, дедалі більше уможливлює швидкі, анонімні та транскордонні операції з конвертацією вартості між різними формами. Онлайн-платформи все тісніше інтегровані із соціальними мережами й іншими цифровими сервісами, що підвищує ризики: соціальні мережі використовуються для комунікації та координації протиправної діяльності, зокрема маніпуляцій результатами змагань, реклами нелегального й неліцензованого гемблінгу, вербування грошових мулів, поширення терористичної пропаганди та залучення коштів для фінансування тероризму. Зловживання послугами операторів азартних ігор в інтересах незаконних фінансових потоків тісно пов'язане з іншими злочинами — корупцією, кібершахрайством, діяльністю професійних мереж відмивання коштів та організованої злочинності. Суттєвим ризиком названо нелегальний і неліцензований офшорний гемблінг: у частині країн такий ринок конкурує з легальним або перевищує його за обсягами і продовжує зростати, приваблюючи гравців промоакціями та вищим рівнем конфіденційності. Оператори, які спеціалізуються на залученні VIP-гравців до казино, попри загальний спад цього сегмента та посилення регулювання, залишаються ризиковими через анонімність гравців і непрозору бенефіціарну власність самих посередників.

Регуляторний ландшафт оцінено як фрагментований. FATF констатує, що обсяг наглядових повноважень у сфері протидії відмиванню коштів, розподіл відповідальності між органами, ліцензійні режими та контроль допуску на ринок суттєво різняться між юрисдикціями. Такі розбіжності дають змогу операторам азартних ігор користуватися відмінностями у регулюванні, обмежують обмін інформацією між приватним і публічним секторами, ускладнюють міжнародну співпрацю та протидію нелегальній гральній діяльності, а також призводять до відставання регуляторного реагування від темпів технологічної еволюції сектору. У відповідь документ формулює низку рекомендацій для юрисдикцій, які зводяться до підвищення обізнаності та розуміння ризиків з урахуванням технологічної інтегрованості галузі й застосування ризик-орієнтованого підходу відповідно до Рекомендації 1 стандартів FATF; посилення ліцензійних і реєстраційних вимог, щоб унеможливити контроль над операторами з боку осіб, причетних до злочинної діяльності; підвищення обізнаності постачальників послуг і широкої громадськості, насамперед щодо нелегального та неліцензованого офшорного гемблінгу; зміцнення формальної й неформальної міжнародної співпраці між компетентними органами, особливо стосовно онлайн-, нелегальної та транскордонної активності; а також розвитку державно-приватних партнерств для обміну інформацією та швидкого реагування на нові й еволюційні ризики.

Другу частину документа становить перелік червоних прапорців, сформований за результатами анкетування, аналізу відкритих джерел і матеріалів інших міжнародних організацій. Автори супроводжують його принциповим застереженням: перелік не є вичерпним, а окремий індикатор сам по собі не є доказом протиправної діяльності — він лише є підставою для посиленого моніторингу та подальшого вивчення, тоді як наявність кількох індикаторів щодо одного клієнта або однієї операції вимагає поглибленої перевірки. Додатково наголошується, що частина індикаторів може відображати не злочинний намір, а проблемну гральну поведінку, причому обидва явища здатні співіснувати. Більшість наданих країнами індикаторів стосується казино у фізичних закладах і онлайн-казино та, меншою мірою, ставок; для відеоігор індикатори фіксувалися рідко, однак через спільні риси з онлайн-казино й букмекерськими платформами значна їх частина застосовна і до ігрового середовища.

Перша група індикаторів описує поведінку та профіль клієнта. У казино у фізичних закладах насторожувати мають спроби вплинути на персонал або підкупити його, щоб ігнорувати активність чи обійти належну перевірку, включно з пропонуванням чайових та інших заохочень, а також систематична взаємодія лише з одним конкретним працівником при уникненні інших. Типовою ознакою анонімізації гри є використання третіх осіб для внесення готівки в термінали, купівлі фішок або розміщення ставок, а також ситуації, коли гравець фактично діє за вказівкою іншої особи — отримує інструкції телефоном чи від присутніх у залі. До цієї ж категорії належать вимога виплатити виграш готівкою в межах порогової суми без повернення за залишком, придбання у інших відвідувачів виграшних інструментів на кшталт лотерейних квитків, ставкових квитанцій, ваучерів для внесення коштів та отримання виграшу або призових купонів із подальшим пред'явленням їх як власних, використання фішок невідомого походження та загалом нетипова або невідповідна поведінка на території закладу. В онлайн-середовищі домінують ознаки свідомого приховування особи: регулярне використання віртуальних приватних мереж, кілька пристроїв, розбіжності між заявленим місцем

проживання та фактично визначеною локацією, невідповідність IP-адреси задекларованому місцезнаходженню, збіг IP-адрес або інтернет-провайдера у кількох гравців, спроби відкрити кілька акаунтів на одне чи вигадане ім'я, невідповідність реквізитів акаунта даним платіжного інструменту, відмова пройти відеоверифікацію та спроби відновити раніше заблокований підозрілий акаунт. Окремо виділено перебування клієнта в країні, де азартні ігри заборонені, і наявність в акаунті зображень, відео або символіки, що популяризують тероризм чи насильницький екстремізм.

Спільними для обох каналів є індикатори, пов'язані з ідентифікацією, походженням коштів і санкційним ризиком. Це небажання надавати актуальні документи та спроби обійти заходи належної перевірки, часті зміни реквізитів акаунта, невідповідність банківських даних даним гравця, подання нечітких або змінених документів, використання як адреси поштової скриньки чи службового приміщення замість житлового. Сюди ж віднесено наявність статків або коштів, що не узгоджуються з профілем клієнта і не мають зрозумілого пояснення, відмову підтверджувати джерело статків і джерело коштів, а також встановлення того, що клієнт отримує дохід від міжнародної торгівлі товарами подвійного використання з підсанкційними державами — зокрема пральними машинами, автомобілями чи медичним обладнанням. Санкційна та терористична складова представлена збігами за національними й міжнародними санкційними списками, зв'язками з підсанкційною державою, групою чи особою, наявністю у відкритих джерелах інформації про належність клієнта до терористичних організацій, екстремістські погляди чи негативні згадки в медіа, ознаками підтримки певного угруповання в реєстраційних документах, адресах електронної пошти або логінах і навіть самостійним розкриттям клієнтом членства в терористичній організації. Ризиковими вважаються також перебування у юрисдикції підвищеного ризику чи запити щодо переказу коштів до неї, статус іноземного громадянина без зрозумілого зв'язку з юрисдикцією діяльності оператора, статус політично значущої особи, підвищений інтерес до внутрішніх контролів, лімітів і того, чи звітує оператор державним органам, обмін коштами між клієнтами без відомого між ними зв'язку, зв'язок клієнта зі злочинною діяльністю або наявність щодо нього правоохоронних запитів, одночасна активність у кількох закладах чи на кількох платформах без видимої ігрової мети та висловлювання екстремального характеру, зокрема наміру завдати шкоди іншим.

Друга група стосується операцій за онлайн-акаунтами. Тут ключовими сигналами є часті перекази, надходження коштів від великої кількості осіб та розподіл виплат між багатьма отримувачами, істотні зміни в характері використання акаунта — в обсягах поповнень і виведень, розмірі ставок і кількості задіяних платіжних механізмів, а також регулярні поповнення методами, що ускладнюють встановлення джерела коштів. Насторожувати має раптове велике поповнення тривало неактивного акаунта, несумісне з його історією, висока частка невдалих спроб депозиту, невідповідність профілю акаунта задекларованому джерелу коштів чи статків і зв'язок операцій із неліцензованими онлайн-операторами або організованими злочинними групами. Технічні ознаки включають відкриття кількох акаунтів під різними іменами з однієї IP-адреси чи одного пристрою, збіг фізичної адреси або контактних даних у кількох акаунтів, невідповідність телефонного номера чи поштового індексу задекларованій країні проживання, використання VPN зі зміною геолокації при кожному вході та появу нової IP-адреси, несумісної з попередньою історією, що може свідчити про перехоплення акаунта.

Третя група описує типові закономірності у здійсненні ставок і поєднує класичні схеми відмивання з ознаками маніпулювання результатами спортивних змагань. До неї віднесено витрати, що не узгоджуються з профілем клієнта, відомим рівнем доходу, професією чи місцем проживання, раптове збільшення сум або частоти ставок, скоординовану чи нетипову ставкову активність, включно з хеджуванням, ставками на всі можливі результати та систематичними програшами конкретному гравцеві у форматах P2P. Типовими є структурування депозитів на менші суми задля уникнення порогів звітності, використання ставок із короткими коефіцієнтами та інших низькоризикових механізмів для обґрунтування подальшого виведення коштів, виведення, неспівмірне з фактичною гральною активністю, регулярне отримання виграшів на суми трохи нижче ідентифікаційного порога, систематичний вибір ігор із низькою дохідністю, але зниженим ризиком і високою ймовірністю виграшу, а також обхід лімітів на прийом купюр шляхом одночасної гри на кількох автоматах. Ознаками змови вважаються стійкі пари гравців, у яких один постійно виграє, а інший програє, зокрема через ставки на обидва ймовірні результати, аномалії у форматі P2P на кшталт навмисної передачі фішок іншому гравцеві з метою прихованого переміщення коштів і неправдоподібно тривала серія виграшів, що може вказувати на використання інсайдерської інформації чи корупцію. Окремий підблок утворюють індикатори, пов'язані зі

спортивною доброчесністю: ставки осіб, причетних до відповідного виду спорту, — суддів і рефері, працівників клубів та організацій, що керують спортом, гравців, учасників змагань і тренерів; ставки на подію, результат якої згодом визнано наслідком маніпуляції; незвично великі або скоординовані за часом, вибором ринку чи сумою ставки на події, вже позначені профільними моніторинговими організаціями як потенційно «договірні». Сюди ж належать ознаки автоматизованого чи ботового розміщення ставок, великі ставки на малоймовірні результати з миттєвим закриттям позиції та ознаки штучного характеру гри, коли ставки залишаються незначними на тлі великих депозитів і виведень.

Четверта група індикаторів охоплює платіжні методи й транзакції і фактично утворює ядро ризику. Насторожувати має інтенсивне використання готівки у фізичних закладах, особливо купюр високого номіналу, готівкове поповнення цифрових акаунтів через букмекерську точку, пов'язану з дистанційним акаунтом того самого оператора, а також численні готівкові депозити протягом коротких проміжків часу, іноді з різницею в кілька секунд. Ризиковим є пріоритетне використання інструментів підвищеного ризику — віртуальних активів, передплачених карток, ваучерів та електронних гаманців, прив'язка до одного акаунта кількох платіжних методів, оформлених на різні імена, нетипові комбінації на кшталт одночасного використання кількох карток або поєднання фіатних коштів і віртуальних активів, використання електронних гаманців іноземних платіжних установ, гаманців для віртуальних активів на неліцензованих платформах і поповнення через неліцензованих чи незареєстрованих постачальників послуг переказу коштів. Найбільш показовими схемними ознаками є депозит із подальшим виведенням за мінімальної гри або взагалі без неї, спроби вивести кошти на рахунок, відмінний від джерела їх надходження, виведення за кордон, в іноземній валюті чи у віртуальних активах усупереч заявленій геолокації гравця, надходження коштів від багатьох осіб на один рахунок на банківському рахунку платформи з подальшим одним переказом на користь одного клієнта, консолідація численних дрібних депозитів із різних джерел у значно більші виведення та швидке виведення коштів на різні рахунки чи різним бенефіціарам. Доповнюють картину банківські аномалії — ознаки використання рахунків грошових мулів, високошвидкісні перекази й операції, пов'язані з юрисдикціями підвищеного ризику, рух коштів до підсанкційних юрисдикцій або з них, надходження з численних іноземних рахунків, платежі від третіх осіб без очевидного зв'язку з власником акаунта, використання кількома клієнтами одного банківського рахунку чи платіжного інструменту, часті невдалі платіжні операції, повернення коштів за операціями з кількох платіжних карток, невідповідність платіжних реквізитів реєстраційним даним, змішування гравцем фішок з готівкою та тривале зберігання значних сум на акаунті без гри. Окремо виділено систематичні спроби обійти інструменти відповідальної гри — ліміти часу, депозитів і витрат та механізми самовиключення — і регулярне досягнення денних лімітів поповнення, тобто саме ті ознаки, що можуть однаково вказувати і на умисел, і на ігрову залежність.

П'ята група індикаторів стосується характеристик продукту, платформи та самого оператора і формує окремий напрям перевірки контрагента. Базовими вразливостями визнано дистанційне гральне середовище, яке забезпечує швидкі операції та легке створення акаунтів без очної перевірки, нерегульовані й немоніторингові чати та комунікаційні функції, а також варіативну якість належної перевірки клієнтів, слабкий поточний моніторинг, неадекватні порогові значення, недостатню кількість персоналу, обмежене навчання та прогалини в обліку. Значний підблок присвячено непрозорості власності: складні, часто транскордонні структури, що приховують бенефіціарного власника й реальний контроль і здатні замаскувати причетність злочинних елементів на етапі ліцензування, використання номінальних власників, трастів і фондів, структурування часток у статутному капіталі так, щоб не перетинати порогові значення регуляторних перевірок, бенефіціарна власність осіб, які отримали громадянство за інвестиції, або осіб із подвійним громадянством з юрисдикцій зі слабкими системами протидії відмиванню коштів, а також комерційно нелогічні передачі власності, зокрема безоплатна передача прибуткового бізнесу третім особам чи придбання збиткових операторів за завищеною ціною. Ризиковими є залежність від третіх сторін і використання бренду іншого оператора без належного нагляду, контракти з постачальниками нематеріальних послуг — програмного забезпечення, маркетингу, консалтингу чи технологічних рішень — без очевидного економічного сенсу, залучення нових клієнтів через інтродюсерів та агентів, дистанційне надання послуг через агентську мережу, здійснення B2B-розрахунків у віртуальних активах і домовленості з посередниками щодо залучення VIP-гравців із високоризикових юрисдикцій. Насторожувати мають наявність у відкритих джерелах інформації про зв'язок бенефіціарних власників з організованими злочинними групами, хабарництвом, корупцією, шахрайством, у тому числі кібершахрайством, сучасним рабством чи маніпуляціями результатами змагань, розміщення платформи в юрисдикції підвищеного ризику або з послабленими заходами протидії відмиванню коштів, стрімке фінансове зростання й непояснювана прибутковість, раптові сплески доходів або

клієнтської активності поза бізнес-профілем, значні транскордонні потоки у сегменті B2B, не пов’язані з регульованою гральною діяльністю, швидка експансія в суміжні цифрові сервіси на кшталт послуг з віртуальними активами чи платіжних сервісів, обмежена онлайн-присутність із примітивними вебсайтами, часта зміна доменів, назви компанії або бренду, отримання ліцензії з подальшим тривалим періодом операційної бездіяльності та реклама платформи в юрисдикціях, де азартні ігри заборонені. Окремо названо неправомірне використання ідентифікаційних даних торговця, відоме як «фіктивні торговці», коли нелегальні оператори маскуються під легальні місцеві підприємства, щоб гральні транзакції оброблялися як звичайні роздрібні платежі, а також свідому публікацію матеріалів, що популяризують тероризм чи насильницький екстремізм.

У цілому документ демонструє зміщення центру ризику з самої гри на інфраструктуру руху коштів навколо неї. Гральний заклад або платформа дедалі рідше є замкненою точкою обслуговування і дедалі частіше виступає вузлом ширшої екосистеми передачі вартості, у якій поєднуються готівка, банківські канали, електронні гаманці, мобільні гроші, віртуальні активи, агентські мережі та цифрові платформи, причому частина учасників цієї екосистеми залишається поза периметром регулювання. Саме тому FATF наголошує не на формальному розширенні переліку індикаторів, а на здатності операторів і наглядових органів бачити зв’язки: між клієнтом і третіми особами, які за нього платять, між акаунтом і платіжним інструментом, між оператором і його реальними власниками, між легальним ринком і нелегальним офшорним сегментом, що конкурує з ним за того самого клієнта. Ефективність системи в цій логіці визначається не наявністю процедур належної перевірки як таких, а їх якістю, повнотою обліку, спроможністю верифікувати джерело коштів і статків та готовністю юрисдикцій обмінюватися інформацією достатньо швидко, щоб реагувати на транскордонні й технологічно рухливі схеми.

Висновки

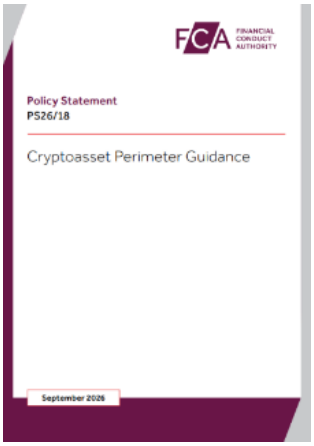
Необхідно підвищувати обізнаність і розуміння ризиків з урахуванням технологічної інтегрованості сектору та застосовувати ризик-орієнтований підхід відповідно до Рекомендації 1 стандартів FATF.

Доцільно посилити ліцензійні та реєстраційні вимоги, щоб не допустити контролю над гральними операторами з боку осіб, причетних до злочинної діяльності.

Слід підвищувати обізнаність постачальників послуг і широкої громадськості щодо ризиків, насамперед пов'язаних із нелегальним і неліцензованим офшорним гемблінгом.

Важливо зміцнювати формальну й неформальну міжнародну співпрацю між компетентними органами та розвивати державно-приватні партнерства для обміну інформацією і швидкого реагування на нові ризики.

FCA затвердило настанови щодо меж регулювання діяльності з криптоактивами (PS26/18) [3]



У вересні 2026 року Управління з фінансового нагляду Великої Британії (FCA) оприлюднило програмну заяву PS26/18 з остаточними настановами щодо меж регулювання діяльності з криптоактивами. Документ підбиває підсумки консультації CP26/13 (квітень 2026 року, 78 відгуків) і додає до Посібника з визначення меж регулювання (PERG) нову главу 18. Її завдання – пояснити ринку, кому потрібна буде авторизація FCA після 25 жовтня 2027 року, коли набудуть чинності Правила про криптоактиви 2026 року, ухвалені на підставі Закону про фінансові послуги та ринки 2000 року (FSMA). Прийом заяв на авторизацію стартує 30 вересня 2026 року, а скористатися перехідними положеннями зможуть лише ті, хто подасть заяву до 28 лютого 2027 року.

Новий режим охоплює такі види діяльності: випуск кваліфікованих стейблкоїнів у Великій Британії; зберігання криптоактивів та організацію їх зберігання; управління торговельною платформою для криптоактивів; торгівлю криптоактивами за власний рахунок і як агент; організацію угод з криптоактивами; організацію стейкінгу. Для зберігання вирішальним є «необхідний ступінь контролю» над активами: діяльність підпадає під регулювання незалежно від того, кому належить актив, якщо фірма зберігає його від імені іншої особи й контролює. Натомість повністю некастодіальні рішення, за яких провайдер такого контролю не має, до периметра не входять. Кредитування й позики криптоактивів FCA не вважає окремим видом діяльності: залежно від ролі учасника вони підпадатимуть під дозволи на торгівлю, організацію угод або зберігання.

Настанови уточнюють ключові визначення. До кваліфікованих криптоактивів не належать електронні гроші, фіатні валюти, цифрові валюти центральних банків, а також токени, які можна погасити лише в емітента й використати для придбання його товарів чи послуг. Щодо стейблкоїнів FCA зайняло чітку позицію: продукти з гібридним механізмом стабілізації, наприклад частково забезпечені активами і частково алгоритмічні, кваліфікованими стейблкоїнами не є. Розмежування між стейблкоїнами та електронними грошима регулятор винесе на окрему консультацію.

Важливо розуміти, як визначено сферу застосування. З одного боку, регулювання діє лише тоді, коли особа провадить діяльність саме як бізнес, і цей тест вужчий, ніж загальний підхід FSMA. З іншого боку, територіальні межі ширші: діяльність вважатиметься такою, що здійснюється «у Великій Британії», зокрема тоді, коли іноземна компанія надає послуги британським споживачам. Виняток для іноземних осіб (overseas persons exclusion), відомий з традиційного фінансового регулювання, на криптоактиви не поширюється. Отже, іноземні платформи, орієнтовані на британських клієнтів, мають отримати авторизацію FCA.

Для сфери запобігання відмиванню коштів найважливіший розділ – про взаємодію з Правилами щодо запобігання відмиванню коштів (MLRs). Два режими діятимуть паралельно: авторизовані фірми й далі виконуватимуть обов'язки за MLRs як оператори обміну криптоактивів або постачальники кастодіальних гаманців, але окремо реєструватися за MLRs їм не доведеться. Водночас чинні реєстрації автоматично не перетворяться на авторизацію: зареєстрованим нині фірмам потрібно буде подати заяву. FCA окремо застерігає, що виняток із Наказу про регульовану діяльність (RAO), наприклад для домовленостей, які не призводять до угоди, або для представлення клієнтів, не звільняє від MLRs, тому обов'язок реєстрації за MLRs треба оцінювати окремо.

За підсумками консультації FCA розширило роз'яснення щодо тесту «ведення діяльності як бізнесу» і територіальних меж, а також уточнило поняття послуг, які «додають вартість» під час організації угод: його не можна застосовувати

[3] https://www.fca.org.uk/publication/policy/ps26-18.pdf

відокремлено від інших обставин. Суто інформаційні або аналітичні сервіси без подальшої участі, за оцінкою FCA, навряд чи становитимуть організацію стейкінгу. Водночас прохання ринку про окремий виняток для технологічних провайдерів у сфері зберігання регулятор не підтримав: вирішальним залишається тест контролю. На початку IV кварталу 2026 року FCA планує нову консультацію щодо змін до PERG, пов'язаних із новим урядовим підзаконним актом.

Висновки

Відсутність винятку для іноземних осіб означає, що офшорні криптоплатформи з британськими клієнтами потребуватимуть авторизації FCA. Банкам, які обслуговують таких провайдерів, варто перевіряти їхній статус після 25 жовтня 2027 року.

Реєстрація за MLRs автоматично не перетвориться на авторизацію. **Фірми, які не подадуть заяву до 28 лютого 2027 року, втратять можливість скористатися перехідними положеннями**, що створює ризик і для їхніх банків-партнерів.

Звільнення від ліцензування за RAO не звільняє від обов'язків за MLRs. Комплаєнс-підрозділам слід оцінювати ці два режими окремо, а не робити висновок про один на підставі іншого.

Тест «необхідного ступеня контролю» чітко відокремлює кастодіальні послуги від некастодіальних і може стати орієнтиром для українського підходу до визначення постачальників послуг, пов'язаних з віртуальними активами.

Технології посилення приватності: можливості та виклики для правоохоронних органів [4]

Звіт підготовлений Спільним дослідницьким центром Європейської комісії (JRC) та Європолу містить прогнозну оцінку нових технологій посилення приватності (PETs) з погляду їхнього впливу на діяльність правоохоронних органів ЄС. Документ підготовлено в межах пріоритету Комісії «Нова ера європейської оборони та безпеки» та Стратегії внутрішньої безпеки ЄС 2025 року, яка передбачає надання правоохоронцям сучасних інструментів законного доступу до цифрових даних за умови дотримання фундаментальних прав. Доказову базу становлять 178 сигналів, відібраних із понад 200 зібраних у 2024 році з наукових публікацій, аналітичних звітів, патентів і проєктів ЄС, результати експертного воркшопу за участю близько 20 фахівців — юристів, науковців, представників поліції, органів влади, бізнесу та громадянського суспільства, а також сім поглиблених інтерв'ю щодо довгострокової перспективи. Автори окремо наголошують на обмеженості емпіричної бази та попередньому характері висновків.

Основна теза звіту полягає в подвійній природі PETs. Ці технології — від шифрування та анонімізації до федеративного навчання й довірених середовищ виконання — забезпечують безпечне зберігання, обробку та спільне використання даних і є основою довіри до цифрових послуг. Водночас ті самі інструменти використовуються злочинцями для приховування комунікацій, анонімізації осіб і знищення цифрових доказів без можливості відновлення. Рівень технологій корелює з рівнем злочинних груп: дрібні угруповання обходяться загальнодоступними месенджерами, серйозна організована злочинність використовує спеціалізовані зашифровані телефони на кшталт EncroChat і Sky ECC, а технічно розвинені кіберзлочинці вибудовують багаторівневу приховану інфраструктуру. З огляду на те, що цифрові дані фігурують приблизно у 85% кримінальних розслідувань, а понад половина розслідувань потребує транскордонних запитів на електронні докази, законний доступ до даних визнано одним із найкритичніших питань для європейських правоохоронців. Документ також підкреслює, що PETs не є універсальним рішенням і не замінюють правових рамок, зокрема GDPR та Директиви 2016/680.

Центральну частину звіту становить аналіз десяти технологій, визнаних експертами ключовими. Найвищий пріоритет надано виявленню діпфейків, оскільки синтетичний контент дозволяє фальсифікувати докази, здійснювати шантаж, викрадення особистих даних та обходити системи верифікації. Комунікації, стійкі до перехоплення, — децентралізовані VPN, мережа Tor, месенджери без збору метаданих і мікс-мережі — посилюють анонімність, але позбавляють правоохоронців можливості моніторингу та атрибуції дій конкретним особам. Аналіз поведінки користувачів в Інтернеті з використанням даних пристроїв Інтернету речей (IoT — фізичних пристроїв, підключених до мережі та здатних збирати й передавати дані), соціальних мереж та методів поведінкової психології., здатний підвищити точність ідентифікації підозрюваних, проте може використовуватися злочинцями для пошуку вразливих жертв і вдосконалення фішингових схем. Багаторівнева біометрична безпека підвищує надійність автентифікації, однак скомпрометовані біометричні дані неможливо замінити, а самі системи вразливі до атак із застосуванням діпфейків. Машинне навчання зі збереженням приватності дає змогу правоохоронним органам різних держав спільно навчати моделі штучного інтелекту без передачі первинних даних. До переліку також увійшли крихітні дрони на сонячній енергії, придатні як для безперервного спостереження, так і для незаконного стеження; базові аспекти штучного інтелекту, насамперед пояснюваність моделей як умова допустимості доказів у суді; навмисне введення спотворених сигналів, що загрожує достовірності сенсорних даних і може застосовуватися для підроблення доказів; довірені середовища виконання, які захищають розслідувальні дані в хмарі, але можуть приховувати шкідливе програмне забезпечення та нелегальні ринки; а також

[4] https://op.europa.eu/fr/publication-detail/-/publication/7c7edaf9-a7ba-11f1-b25c-01aa75ed71a1/language-en

людиноподібні роботи, використання яких порушує питання кібербезпеки та юридичної відповідальності за дії автономних систем.

Довгострокова частина звіту зосереджена на криптографії та суміжних технологіях. Очікувана поява квантових комп'ютерів протягом 10–15 років створює загрозу для чинних алгоритмів шифрування, а стратегія «збери зараз — розшифруй пізніше» робить перехід на постквантову криптографію нагальним уже сьогодні; можливе розходження стандартів між геополітичними блоками при цьому ускладнить доступ до цифрових доказів. Визначальною тенденцією названо також обчислення на зашифрованих даних — повністю гомоморфне шифрування, багатостороннє обчислення та докази з нульовим розголошенням, — які зміщують фокус захисту з даних під час передачі й зберігання на дані під час використання. Нині такі методи приблизно у 100 разів повільніші за звичайну обробку і застосовуються передусім у фінансовому секторі та охороні здоров'я, однак у перспективі навіть хмарний провайдер не зможе надати правоохоронцям доступ до даних, ключ від яких належить виключно власникові. Водночас ці технології відкривають нові можливості, зокрема виявлення шахрайства безпосередньо в зашифрованих масивах без доступу до окремих записів, і ставлять нове регуляторне питання: хто і які саме обчислення має право виконувати. Злочинці ж можуть застосовувати їх для створення прихованих платформ обміну інформацією та маскування платежів, пов'язаних із програмами-вимагачами. У відповідь експерти рекомендують посилювати аналіз метаданих, геолокації та комунікаційних патернів, які значно складніше приховати, ніж зміст повідомлень, адже основною проблемою для правоохоронців є не відсутність цифрових слідів, а доступ до даних, що належать приватним компаніям.

Щодо штучного інтелекту)AI) звіт фіксує його практичне застосування в поліцейській діяльності — від аналізу відеозаписів до встановлення авторів анонімних акаунтів за лінгвістичними особливостями та виявлення прихованих зв'язків у багатошарових злочинних структурах. Основною перешкодою визнано правову невизначеність щодо застосування GDPR до великих мовних моделей, яка стримує законослухняних користувачів і фактично створює перевагу для тих, хто закон ігнорує. Експерти закликають визнати, що «ідеальної приватності» не існує, визначити прийнятні пороги ризику повторної ідентифікації та враховувати ціну відмови від технологій. Квантовий розподіл ключів оцінено як надзвичайно захищений, але технічно складний і дорогий інструмент, що навряд чи стане масовою злочинною загрозою. Мережі 6G, розгортання яких очікується у 2030–2031 роках, поєднають зв'язок, вбудовану сенсорику, AI і супутникову інфраструктуру, надавши правоохоронцям багатші джерела даних, але ускладнивши відстеження доказів через постійне переміщення даних між хмарою, вузлами мережі та пристроями. Блокчейн залишається середовищем для відмивання коштів через криптовалюти, проте завдяки регулюванню постачальників послуг обміну та розвитку аналітики на основі AI відстеження таких транзакцій стає дедалі реалістичнішим; нові ризики пов'язуються із самосуверенною ідентичністю та можливою реалізацією цифрового євро на розподіленому реєстрі.

Серед контекстних факторів, проаналізованих за методологією PESTEL, ключовими визнано регуляторні ініціативи ЄС — AI Act і Акт про цифрові ринки, які можуть водночас стимулювати й стримувати інновації, технологічне суперництво США та Китаю, відставання Європи в цифровій економіці та зростання кіберзагроз: за оцінками, кіберзлочинність у 2024 році коштувала світовій економіці близько 9,5 трлн доларів США. Каталізаторами поширення PETs названо європейську та міжнародну співпрацю, зокрема пакет E-Evidence і Конвенцію ООН про кіберзлочинність, а бар'єрами — геополітичні суперечності, дефіцит ресурсів і кадрів, вигорання кіберкоманд, а також середовища даркнету й метавсесвіту, які важко піддаються регулюванню.

За результатами дослідження правоохоронним органам рекомендовано опановувати передові PETs і водночас розвивати альтернативні методи розслідування — аналіз метаданих, мережевий аналіз і агентурну роботу, готуватися до переходу на квантово-стійкі технології та адаптувати цифрову криміналістику, а також інвестувати в навчання персоналу й спільні інструменти, зокрема через репозиторій інструментів Європолу. Політикам ЄС запропоновано зменшити правову невизначеність щодо використання даних, проактивно регулювати нові технології з чіткими правилами доступу правоохоронців до даних, розвивати міжнародні стандарти та партнерства. Пріоритетами фінансування визначено технічні спроможності правоохоронних органів, дослідження у сфері кібербезпеки та криптографії, експертизу в галузі AI, цифрову криміналістику, інтероперабельність, підвищення кваліфікації не лише правоохоронців, а й законодавців, а також державно-приватні партнерства.

У цілому документ демонструє, що технологічний розвиток не так усуває можливості правоохоронців, як змінює їхній характер: у міру поширення шифрування на дані під час обробки центр ваги розслідувань зміщується від перехоплення змісту до аналізу метаданих, поведінкових патернів, транзакційних слідів і співпраці з власниками інфраструктури. Для сфери протидії відмиванню коштів це означає зростання значення аналітики зашифрованих фінансових масивів, відстеження криптовалютних потоків через регульовані точки входу та виходу і здатності систем фінансового моніторингу працювати з даними без порушення їхньої конфіденційності. Ефективність у цій логіці визначатиметься не спробами послабити захисні технології, а готовністю регуляторів, правоохоронних органів і приватного сектору заздалегідь узгоджувати правила законного доступу, інвестувати в компетенції та швидко адаптуватися до нових технологічних реалій.

Висновки

Необхідно розвивати альтернативні методи розслідування, зокрема аналіз метаданих, мережевий аналіз і агентурну роботу, а також технології аналізу зашифрованих масивів даних для виявлення шахрайства.

Доцільно вже зараз готуватися до переходу на постквантову криптографію та квантовий розподіл ключів і адаптувати методи цифрової криміналістики, зважаючи на загрозу атак за принципом «збери зараз — розшифруй пізніше» та на можливе розходження криптографічних стандартів між різними геополітичними блоками.

Слід переглянути та спростити регуляторні вимоги щодо використання даних і штучного інтелекту, чітко визначивши допустимі обчислення над зашифрованими даними, правила доступу правоохоронних органів до даних та прийнятні пороги ризику повторної ідентифікації, щоб правова невизначеність не стримувала застосування нових технологій.

Важливо спрямувати фінансування на технічні спроможності правоохоронних органів, цифрову криміналістику, експертизу в галузі штучного інтелекту та навчання як правоохоронців, так і законодавців. Також потрібно розвивати державно-приватні партнерства та спільні інструменти, зокрема через репозиторій інструментів Європолу.

Онлайн-шахрайство та фейкові вебмагазини: прогалини у захисті споживачів [5]

Дослідження, підготовлене на замовлення Комітету Європейського парламенту з питань внутрішнього ринку та захисту прав споживачів (IMCO), систематизує шахрайські практики фейкових вебмагазинів упродовж усього їхнього операційного циклу, зіставляє з ними чинний правовий і правозастосовний інструментарій ЄС та визначає структурні прогалини в охопленні, правозастосуванні й транскордонній координації. Під фейковим вебмагазином автори розуміють сайт або оголошення продавця, яке імітує легітимного онлайн-продавця, але створене для обману через підміну особи, неправдиві комерційні заяви, недоставлення товару, спотворення його характеристик або фінансову експлуатацію. Доказову базу становлять законодавчі та політичні документи ЄС, дані національних регуляторів, мережі органів із захисту прав споживачів (CPC), систем Safety Gate та eSurveillance, Європолу, Європейського банківського органу (EBA) та Європейського центрального банку (ЄЦБ), матеріали споживчих організацій, академічні й галузеві дослідження, а також шість експертних інтерв'ю. Юридичний аналіз охоплює понад десяток актів — від Директиви про недобросовісну комерційну практику (UCPD) і Директиви про права споживачів (CRD) до Акта про цифрові послуги (DSA), Регламенту про загальну безпечність продукції (GPSR), Другої платіжної директиви (PSD2) та Регламенту CPC. Наскрізно розрізняються дві моделі: автономний фейковий магазин, що повністю контролює домен, вітрину й оплату, та продавець, який здійснює шахрайські дії на маркетплейсі та який використовує довіру до платформи.

Основна теза дослідження полягає в тому, що фейкові магазини діють не поза цифровою економікою, а всередині неї, використовуючи ту саму рекламу, пошукові системи, хостинг, платіжні мережі й логістику, що й сумлінні продавці. Масштаб проблеми зростає разом з онлайн-торгівлею: у 2025 році онлайн купували 78% жителів ЄС, у 2024 році до Союзу надійшло 4,6 млрд низьковартісних посилок — утричі більше, ніж у 2022-му, а близько 45% споживачів стикалися з онлайн-шахрайством. У Німеччині від фейкового магазину за два роки постраждав кожен восьмий онлайн-покупець, у Нідерландах кількість повідомлень про шахрайство за рік зросла на 40%, а в Італії задокументовані збитки лише за перше півріччя 2024 року сягнули 114 млн євро. Якісною відмінністю від традиційного шахрайства є швидкість: магазин створюється, монетизується і замінюється за кілька днів, а після блокування ті самі шаблони, рекламні акаунти, каталоги та платіжні маршрути переносяться на новий домен. Сервіс Fakeshop-Finder зафіксував понад 60 тис. таких магазинів лише в німецькомовних країнах із приростом понад тисячу щомісяця.

Типологію побудовано навколо «шляху шахрайства», що складається з двох стадій і шести кластерів. На стадії експозиції та спонукання шахрай спершу створює синтетичну ідентичність: клонує вітрину відомого бренду, використовує домени, що відрізняються від справжніх одним символом, заявляє про статус «авторизованого реселера», зазначає віртуальні адреси, чужі реєстраційні номери та ПДВ-номери, які не проходять перевірку в системі VIES. Непрозорість щодо особи продавця тут є не випадковим порушенням, а елементом схеми: споживач має повірити в існування продавця, але після оплати продавець не мусить бути досяжним. Далі ця ідентичність отримує охоплення через довірену інфраструктуру — платну рекламу, маніпуляції пошуковою видачею та «доменне стрибання». За даними німецької федерації споживчих організацій, близько половини досліджених фейкових магазинів купували рекламу в Google або Meta, а з поданих нею як «довіреним викривачем» повідомлень про незаконну рекламу у Facebook було видалено лише близько половини оголошень. Завершальний кластер стадії — усунення перешкод до покупки через фіктивні знижки й таймери, фальшиві відгуки та оманливі запевнення на кшталт «безкоштовне повернення» чи «захист покупця». Окремо описано брашинг — розсилку непроханих посилок на адреси з викрадених баз даних для створення

[5] https://www.europarl.europa.eu/RegData/etudes/STUD/2026/772655/ECTI_STU(2026)772655_EN.pdf

«підтверджених покупок» під фальшиві відгуки. Автори наголошують, що ці техніки поширені й серед легальних продавців, тож сама їх наявність ще не відрізняє шахрая.

На стадії транзакції та шкоди найпоширенішою формою є недоставлення товару, проте показовішими є його варіанти. Затягування з постійним перенесенням строків і вигаданими митними повідомленнями розраховане на те, щоб вичерпати строк для оскарження карткового платежу (чарджбеку); тактика «порожньої коробки» створює трекінг-запис про успішну доставку, що перекладає тягар доведення на споживача; схеми «таємничих коробок» використовують рамку «сюрпризу» для відмови від претензій. Інший кластер охоплює спотворені, контрафактні та небезпечні товари: у 2024 році Safety Gate отримала рекордні 4 137 сповіщень, а окремі оператори роблять вітрини доступними лише з мобільних пристроїв, щоб обійти системи моніторингу. Найбільш чутливим для фінансового сектору є кластер фінансової експлуатації та перешкоджання засобам захисту. Він охоплює фальшиві сторінки оплати, цифровий скімінг, фішингові повідомлення після покупки, тестування викрадених карток дрібними транзакціями в межах винятків із суворої автентифікації клієнта та трикутне шахрайство, коли замовлення виконується через легального продавця за рахунок чужої картки. Сюди ж належать фальшиві адреси повернення, ухиляння від відшкодування та пастки з автоматичним продовженням підписки. Розслідування NORDIS/EDMO показало, як один оператор отримував скарги у чотирьох країнах Північної Європи, але ніде не досягав порогу для скоординованих дій, доки національні дані не об'єднали.

Аналіз правового інструментарію засвідчує, що проблема полягає не у відсутності норм, а у структурній невідповідності між припущеннями права і способом дії шахраїв. Обов'язки за UCPD, CRD чи Директивою про продаж товарів адресовані продавцю, якого можна ідентифікувати й притягнути до відповідальності, тоді як фейкові магазини спеціально руйнують цю передумову, тож першим завданням регулятора часто стає з'ясування, чи існує відповідальна особа взагалі. Для операторів із третіх країн проблема ще гостріша. Найвагомішим превентивним інструментом визнано обов'язок маркетплейсів перевіряти продавців за статтею 30 DSA, однак він діє лише за наявності контролюючого посередника і не охоплює заяви про зв'язок із брендом, а автономні магазини не проходять жодної перевірки до виходу на ринок. Обов'язки рекламних платформ, хостинг-провайдерів і реєстраторів переважно реактивні: механізм повідомлень спрацьовує вже після показу реклами, кожен новий домен того самого оператора розглядається «з чистого аркуша», а повноваження CPC щодо видалення домену реалізуються повільніше за цикл перезапуску. Навіть детально врегульовані практики, як-от фіктивні знижки та фальшиві відгуки, важко переслідувати щодо магазину, що існує кілька тижнів. Розпорошеним залишається і правозастосування між споживчими органами, координаторами цифрових послуг, органами ринкового нагляду та органами захисту даних.

Окремий висновок стосується відшкодування збитків: можливість повернути кошти залежить не від заподіяної шкоди, а від правової кваліфікації платежу та способу оплати. PSD2 гарантує повернення коштів за неавторизовані операції, проте більшість жертв фейкових магазинів авторизують платіж самостійно. Чарджбек є правилом карткових схем, а не законним правом, і не має аналога для кредитових переказів, а перевірка отримувача за Регламентом про миттєві платежі не захищає того, кого обманом змусили переказати кошти на правильно названий рахунок шахрая. Фейкові магазини цілеспрямовано скеровують покупців до незворотних методів оплати. Пакет PSD3/PSR передбачає право на відшкодування лише тоді, коли шахрай видає себе за платіжного провайдера споживача, і не охоплює типового обману з боку продавця. Перешкоджання засобам захисту розподілене між споживчим правом, механізмами врегулювання спорів на платформах і маршрутами через платіжних провайдерів, тож споживача передають від продавця до платформи, банку та регулятора без єдиного шляху ескалації.

На цій основі автори формулюють шість пріоритетних рекомендацій: зменшити залежність правозастосування від пошуку самого шахрая, перенести захист на етап до оплати, узгодити відповідальність посередників з інфраструктурою, яку вони надають, координувати правозастосування так само щільно, як скоординоване шахрайство, забезпечити, щоб відшкодування залежало від факту шахрайства, а не від способу оплати, та використовувати інформування споживачів як доповнення до структурних реформ, а не їх заміну. Частину заходів можна реалізувати без нового законодавства в межах Плану дій ЄС із протидії онлайн-шахрайству та імплементації DSA. Законодавчі зміни пропонується провести через Акт про цифрову справедливість і перегляд Регламенту CPC, заплановані на четвертий квартал 2026 року, а питання розширення захисту на жертв шахрайства з боку продавців — через положення про

перегляд PSR і технічні стандарти EBA. У довгостроковій перспективі автори пропонують сумісну перевірку продавців, коли дані, перевірені одним посередником, можуть використовувати інші, а також структурований обмін даними з доступом для дослідників. Критерій реформи має бути практичним: чи захищений споживач до оплати, чи швидше руйнується шахрайська інфраструктура і чи має жертва реальний шлях до повернення коштів.

У цілому документ демонструє зміщення фокусу протидії онлайн-шахрайству з окремого сайту на інфраструктуру, яка забезпечує його охоплення та рух коштів. Для сфери фінансового моніторингу це означає зростання ролі банків і платіжних провайдерів як одного з небагатьох досяжних елементів схеми: саме через платіжну інфраструктуру проходять кошти постраждалих, а повторне використання тих самих платіжних реквізитів різними доменами може свідчити про єдину шахрайську операцію. Ефективність протидії визначатиметься здатністю пов'язувати розрізнені скарги, платіжні дані та технічні ідентифікатори в цілісну картину і діяти до того, як оператор перезапуститься під новою адресою.

Висновки

Слід розглядати пов'язані домени, акаунти, рекламу та платіжні реквізити як одну операцію, а не як окремі сайти, і запровадити прискорену процедуру CPC для одночасного блокування всієї схеми в кількох державах ЄС.

Необхідно запровадити ризик-орієнтовану перевірку рекламодавців перед показом реклами, яка веде на онлайн-магазини, за зразком перевірки продавців маркетплейсами (стаття 30 DSA).

Доцільно оцінити поширення права на відшкодування на жертв шахрайських продавців, коли людину обманом змусили заплатити самостійно. Для цього пропонується розподіляти відповідальність між банком відправника та банком отримувача, якщо останній не забезпечив належного моніторингу рахунків.

Потрібно створити єдиний шлях звернення для споживача, який об'єднає скаргу продавцю, спір на платформі та оскарження платежу з визначеними строками. Також варто налагодити постійну взаємодію мережі CPC з Європейською радою із захисту даних.

Тіньові фінансові потоки росії: як механізм А7 обходить санкції [6]

У серпні 2026 року Національне агентство боротьби зі злочинністю Великої Британії (NCA) спільно з Національним центром економічної злочинності (NECC), Управлінням з імплементації фінансових санкцій Міністерства фінансів Великої Британії (OFSI) та Міністерством закордонних справ, у справах Співдружності та розвитку (FCDO) опублікувало екстрене попередження.

Цей документ, підготовлений у рамках діяльності Об'єднаної робочої групи з розвідки щодо відмивання грошей (JMLIT), покликаний привернути увагу фінансових установ, постачальників послуг віртуальних активів та інших підзвітних суб'єктів до нової, надзвичайно масштабної та складної схеми обходу міжнародних санкцій, яка становить серйозну загрозу цілісності світової фінансової системи. Йдеться про комерційне підприємство під назвою А7, яке, за оцінками британських правоохоронців, є не просто черговим каналом для переказу коштів, а повноцінною альтернативною системою переміщення вартості через кордони, що поєднує традиційні фіатні платежі, криптоактиви та розгалужену мережу підставних компаній і так званих «субагентів» по всьому світу.

А7 було засновано у 2024 році за підтримки двох ключових російських державних інституцій — Промсвязьбанку (ПСБ), який є санкціонованим російським банком, що підтримує військово-промисловий комплекс країни, та ВЕБ.РФ — російської державної корпорації розвитку та інвестиційної компанії. Сам ПСБ описує А7 як «унікальний механізм» для російських фізичних та юридичних осіб, а також їхніх іноземних контрагентів, який дозволяє завершувати торгові розрахунки «в умовах санкційного тиску».

Вражає те, що вже за перший рік своєї діяльності А7 заявила про проведення розрахунків на суму понад 86 мільярдів доларів США. Ця цифра сама по собі свідчить про колосальний масштаб операції, яка, за визначенням NCA, функціонує як система альтернативного переказу вартості, що переміщує кошти через кордони для клієнтів, які потребують послуг із приховування походження та призначення платежів. Важливо наголосити, що А7 та її афілійовані структури вже перебувають під санкціями Великої Британії, США та Європейського Союзу, що робить будь-яку взаємодію з ними не лише ризикованою, а й протиправною.

Ключовим елементом, який робить А7 настільки небезпечним для міжнародної фінансової системи, є його здатність успішно створювати пули ліквідності за межами росії та використовувати їх для проведення транзакцій від імені клієнтів. Історично найбільш значущим каналом для введення цієї ліквідності у світову фінансову систему були зв'язки А7 з Киргизстаном, зокрема через Торгову компанію Киргизької Республіки (TKKR), яку було ліквідовано у лютому 2026 року. За оцінками, станом на квітень 2025 року через TKKR пройшло близько 8 мільярдів доларів США.

Однак, що є критично важливим для розуміння механізму, при введенні в обіг ці кошти не мають жодного зв'язку з їхнім російським походженням. Замість цього вони асоціюються з підставними компаніями або так званими «субагентами», зареєстрованими в різних юрисдикціях по всьому світу. Ці субагенти мають місцеві банківські рахунки, підключені до ширшої банківської системи, що дозволяє переміщувати кошти між рахунками та використовувати їх для завершення

[6] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/826-necc-a7-sanctions-evasion-mechanism/file

транзакцій з міжнародними постачальниками від імені клієнтів A7, багато з яких є резидентами росії та/або перебувають під санкціями. Ці операції супроводжуються підробленими рахунками-фактурами, які виготовляє та видає сама A7, щоб створити фасад законності, що маскує основні правопорушення. Такий підхід є класичним прикладом відмивання грошей на основі торгівлі.

Незважаючи на те, що субагенти номінально розташовані в різних іноземних юрисдикціях, насправді вони контролюються особами, які перебувають всередині росії. A7 створює онлайн-присутність для своїх підставних компаній, розробляючи веб-сайти та електронні адреси, які її співробітники використовують під час спілкування з банками. Крім того, вони підтримують численні віртуальні приватні мережі (VPN), щоб співробітники могли маскуватися під осіб, які перебувають у тій самій юрисдикції, що й банківські послуги, до яких вони прагнуть отримати доступ. Це дозволяє A7 обходити традиційні правила боротьби з відмиванням грошей та перевірки клієнтів (KYC). Така тактика створює серйозні виклики для банків та фінансових установ, оскільки вимагає від них значно глибшого аналізу, ніж стандартні процедури перевірки.

Одним із найцікавіших аспектів, описаних у документі, є використання A7 фінансового інструменту, відомого як «вексель» (promissory note). Клієнти купують ці боргові розписки, які потім діють як кредитне забезпечення та покривають вартість транзакцій, які вони хочуть виконати за кордоном. Векселі дозволяють A7 відстежувати свої зобов'язання та надаються клієнтам для забезпечення дотримання російських регуляторних вимог. Водночас, пов'язуючи внутрішню та міжнародну діяльність A7 в росії, вексель приховує участь A7 у міжнародній фінансовій системі, оскільки при його погашенні не відбувається кореспондентського банківського переказу з росії. Замість цього підставна компанія здійснює начебто окрему транзакцію, супроводжуючи її підробленими документами для фінансової системи.

A7 спрямовує платежі через підставні компанії, зареєстровані в численних проміжних юрисдикціях. Ці компанії використовують складні, багаторівневі кореспондентські банківські домовленості, щоб приховати свою діяльність та уникнути виявлення. Аналіз OFSI щодо підозрюваної діяльності A7 виявив транзакції між підставними компаніями A7 та британськими бенефіціарами, які проводилися через банки в кількох проміжних юрисдикціях. Це свідчить про те, що фінансова система Великої Британії також перебуває під загрозою використання як транзитного каналу для операцій A7, що вимагає підвищеної пильності з боку британських фінансових установ.

Географія діяльності A7 не обмежується Киргизстаном. Документ зазначає, що хоча A7 переважно використовувала різноманітні киргизькі структури для доступу до міжнародної фінансової системи, останнім часом вона прагне диверсифікувати свій доступ як географічно, так і технічно. У серпні 2025 року 78% транзакцій A7 проходили через китайські юрисдикції. Крім того, A7 розширюється в Африці, відкриваючи офіси в Нігерії та Зімбабве. У Нігерії вона встановила відносини з місцевим постачальником платіжних послуг (PSP) Pilot Finance Limited, який наразі перебуває під санкціями Великої Британії і мав зв'язки з британськими, іспанськими та угандійськими фінансовими установами. Доступ до PSP надає A7 можливість ще більше приховувати походження та призначення транзакцій у міжнародній фінансовій системі, оскільки PSP може виступати посередником між субагентом та банком. Це створює додатковий рівень складності для виявлення незаконних операцій та підкреслює необхідність міжнародного співробітництва у сфері обміну інформацією.

Особливу тривогу викликає той факт, що аналіз клієнтів A7 показав, що вони представляють гравців російського військово-промислового комплексу. Це означає, що A7 може бути причетною не лише до обходу санкцій та відмивання грошей, а й до фінансування розповсюдження зброї. Більше того, її спонсор ПСБ зосереджений на підтримці російської військової промисловості. Відтак, органи нагляду, фінансові установи, постачальники послуг віртуальних активів та ВНУП повинні враховувати цю конкретну загрозу у своїх оцінках ризиків, для чого критично важливим є транскордонна співпраця щодо обміну інформацією.

Документ також наводить перелік «червоних прапорців», які можуть вказувати на зв'язок з мережею A7. Серед них:

- компанії з обмеженою історією, які здійснюють великі обсяги транзакцій з усталеними суб'єктами в, здавалося б, різних галузях;
- рахунки-фактури, що деталізують товари або послуги, які відрізняються від звичайної продукції постачальників;
- численні перекази між невідомими компаніями, що працюють начебто в різних галузях;
- обмежена інформація про власників, директорів або бенефіціарів;
- компанії, зареєстровані або такі, що діють у відомих юрисдикціях високого ризику;
- компанії з обмеженою онлайн-присутністю, веб-сайти яких містять загальні стокові фотографії та мінімум інформації про осіб, які керують компанією;
- використання VPN для проведення банківських операцій, включаючи випадки, коли компанії або їхні представники використовують VPN, які можуть збігатися з юрисдикцією, в якій вони шукають банківські послуги, але не відповідають їхньому профілю.

Жоден окремий червоний прапорець не є безумовним свідченням незаконної діяльності, але їхня сукупність має викликати серйозне занепокоєння.

У контексті протидії цій загрозі NCA закликає повідомляти про підозрілу діяльність шляхом подання звітів про підозрілі операції (SAR). Важливо також нагадати, що OFSI є компетентним органом Великої Британії з питань імплементації фінансових санкцій, і будь-яка інформація, що свідчить про заморожені активи або порушення фінансових санкцій, повинна бути негайно повідомлена OFSI.

Таким чином, опублікований документ є не просто попередженням, а глибоким аналітичним звітом, який розкриває складну, багаторівневу та добре фінансовану схему обходу санкцій, що використовує як традиційні банківські механізми, так і новітні технології для приховування російського походження коштів.

Масштаб діяльності A7, її зв'язки з російським військово-промисловим комплексом та постійна диверсифікація географії операцій роблять її однією з найсерйозніших загроз для міжнародної фінансової системи на сьогодні. Лише комплексний підхід, який поєднує регуляторні, правоохоронні та технологічні заходи, здатен ефективно протистояти цій загрозі.

Висновки

Масштаб та інституційна підтримка. А7 — це не просто тіньова схема, а повноцінна альтернативна фінансова система. За перший рік роботи А7 заявила про проведення розрахунків на суму понад 86 мільярдів доларів.

Використання векселів та фіктивних компаній. Механізм базується на використанні боргових розписок (векселів) та розгалуженої мережі підставних компаній і «субагентів» у різних юрисдикціях. Це дозволяє приховувати російське походження коштів.

Географічна диверсифікація та нові ринки. А7 активно розширює свою діяльність, виходячи за межі Киргизстану. Станом на серпень 2025 року 78% транзакцій проходили через китайські юрисдикції, також відкрито офіси в Нігерії та Зімбабве.

Загроза для військово-промислового комплексу та фінансової системи. Аналіз клієнтів А7 показав, що серед них є ключові гравці російського ВПК, що вказує на можливу причетність до фінансування розповсюдження зброї.

Бізнес на основі AI: нова операційна модель підприємств [7]

Біла книга Всесвітнього економічного форуму описує, як влаштовані та як працюють організації, що вибудовують свою операційну й бізнес-модель навколо штучного інтелекту (AI). Доказову базу становлять напрацювання понад 50 керівників компаній і підрозділів, які вже діють за принципом AI-first (підхід, за якого штучний інтелект є не допоміжним інструментом, а основою операційної моделі, процесів і ухвалення рішень компанії), а також інтерв'ю, воркшопи та консультації з понад 150 керівниками й експертами, а також інтерв'ю, воркшопи та консультації з понад 150 керівниками й експертами. Серед розглянутих кейсів — компанії з розробки ліків, фінансової інфраструктури, логістики, юридичних сервісів і кібербезпеки, зокрема Stripe, ServiceNow, Waymo, Rakuten, Indeed, Cognizant, Taktile та Ant Group. Автори виокремлюють три типи підприємств. Підприємства, що використовують AI як інструмент, застосовують його для виконання окремих завдань у межах наявних процесів. Підприємства, орієнтовані насамперед на AI, системно перебудовують процеси, ролі та повноваження щодо ухвалення рішень таким чином, щоб AI став стратегічним інструментом створення цінності. Підприємства, створені на основі AI, від самого початку будують свої продукти на основі технологій AI. Критерієм розмежування є простий тест: чи зможе підприємство функціонувати без систем штучного інтелекту. Поширення AI автори пояснюють демократизацією доступу, здатністю систем міркувати й діяти автономно, мультимодальністю та паралельним виконанням завдань. Документ позиціонується не як дорожня карта трансформації, а як опис того, як уже працюють лідери.

Основна теза полягає в тому, що AI, як свого часу електрика, дає проривний ефект лише тоді, коли організацію перебудовують навколо технології, а не додають її поверх старих процесів. Перші фабрики, які замінили парові машини електродвигунами без зміни планування, отримали лише економію на енергії, а стрибок продуктивності настав після переосмислення всього виробництва. Нині, попри глобальні інвестиції у AI понад 250 млрд доларів у 2025 році, лише 25% компаній говорять про трансформаційний ефект, а 84% не переглянули посади з урахуванням можливостей AI. Натомість результати AI-first підприємств уже помітні: цикл обробки заявок у комерційному страхуванні скоротився з 28 днів до 2,8 години, окремі команди досягають у 15 разів вищої продуктивності, а річний регулярний дохід у 100 млн доларів компанії отримують за кілька місяців замість чотирьох–восьми років.

Ядром моделі є «інтелектуальний двигун» — самопідсилювальний цикл даних, який накопичує знання організації та вдосконалюється з кожною взаємодією. Він працює через три контури. Контур швидкості прискорює експерименти: Formation Bio прогнозує успішність клінічних випробувань ще до їх початку, а ServiceNow допускає агентів AI до роботи лише після досягнення порогу виконання завдань у 80–95%. Контур масштабу перетворює AI на багатоцільову платформу: Waymo перевіряє автомобілі за 12 критеріями та понад 20 млрд миль симуляцій, BforeAI запускає нові моделі паралельно з чинними й замінює їх лише за кращих результатів, а Osmo скоротила розробку аромату з шести місяців до 60 секунд. Контур охоплення переносить здобуті можливості в нові сфери й продукти: Harvey розширився від

[7] https://reports.weforum.org/docs/WEF_The_AI_First_Operating_System_A_Blueprint_for_Operating_and_Business_Model_Innovation_2026.pdf

юридичної аналітики до податків і угод M&A, а платіжна фундаментальна модель Stripe, навчена на десятках мільярдів транзакцій, виявляє понад 95% атак із тестування карток, що на 22% краще за попередні методи. Anthropic на основі тих самих моделей послідовно створила Claude Code, який за шість місяців вийшов на 1 млрд доларів річного доходу, а згодом Claude Cowork, Claude Design і Claude for Small Business.

Другим блоком є адаптивний технологічний стек, який має бути модульним і не залежати від конкретної моделі. Автори рекомендують не замінювати одразу системи управління взаємовідносинами з клієнтами (CRM) чи системи планування ресурсів підприємства (ERP), а надбудовувати над ними рівень штучного інтелекту, який забезпечує управління процесами. Водночас вони радять контролювати рівні координації процесів та роботи з контекстом, забезпечувати доступ до власних даних через внутрішні програмні інтерфейси (API), а моделі розглядати як портфель інструментів: менші моделі — для типових завдань, передові — для складних завдань, що потребують міркування, а спеціалізовані моделі — для завдань, у яких вирішальне значення мають власні дані. Кожне прийняте, відхилене чи позначене рішення моделі має ставати сигналом для навчання, а в протидії шахрайству хибні спрацювання та виправлення аналітиків слугують розміченими даними, тоді як синтетичні сценарії атак розширюють охоплення виявлення. Контекст має збиратися в реальному часі з першоджерел із визначеною ієрархією їхньої достовірності.

Третій блок присвячено перебудові операцій. Більшість компаній досі застрягли на етапі розрізнених пілотних проєктів, які не дають накопичувального ефекту. AI-first лідери розглядають AI як капітал і спершу обирають три–п’ять пріоритетних процесів із великим обсягом повторюваних операцій, численними передачами між підрозділами та складними рішеннями, як-от обслуговування клієнтів, закупівлі, оцінювання ризиків чи врегулювання претензій. Далі для кожного завдання визначають, чи AI його автоматизує, підсилює людину чи залишається осторонь, і підбирають модель за точністю, вартістю та швидкістю відгуку: для фінансових і медичних рішень прийнятною є лише нульова помилка, для клієнтських відповідей — понад 90% точності, а виявлення шахрайства має працювати безперервно. Центральне місце посідає онтологія, тобто формалізований опис даних, правил і дозволених дій бізнесу, а також прозорість виконання з можливістю відстежити, призупинити чи скасувати дії агентів. Показовим є приклад Gamma: команда з близько 50 осіб досягла 100 млн доларів річного доходу, а валова маржа з урахуванням витрат на роботу моделей за пів року після запуску зросла приблизно з 31% до 77% завдяки постійному перерозподілу роботи між моделями й людьми.

Четвертий блок стосується взаємодії людей та AI. AI-first компанії досягають тих самих порогів доходу з уп’ятеро–вдвадцятеро меншим штатом, ніж попередні лідери ринку, що автори пов’язують із ризиком суттєвих зрушень на ринку праці. Цінність зміщується до працівників із поєднанням широкого системного мислення та глибокої галузевої експертизи, тоді як проміжний виконавчий рівень дедалі більше бере на себе AI. Окремо наголошується на ризику атрофії навичок: судження, постановку задач і роботу з винятками потрібно зберігати активними, бо їх значно важче відновити. Перехід від прототипу до надійного продукту, за оцінкою учасників воркшопу, вимагає вдесятеро більше навичок, тому ефективними визнано невеликі міжфункціональні команди до 10 осіб трьох нових типів: команди пілотування й промислового впровадження, команди, вбудовані в роботу з клієнтом, і команди безпеки AI. Орієнтирами для них є використання AI щонайменше у 50% релевантних завдань і зростання продуктивності понад 20%. Оптимальною визнано федеративну модель, за якої центральний підрозділ під керівництвом генерального директора відповідає за інфраструктуру, моделі й безпеку, а бізнес-підрозділи самостійно фінансують і впроваджують рішення, як у Rakuten з понад 70 бізнес-напрямами.

П’ятий блок присвячено створенню нової цінності на ринку. AI суттєво знижує витрати клієнтів на перехід до конкурентів, тож утримання стає головним викликом: за наведеними даними, у застосунках AI платить менше ніж один із 16 місячних підписників, що на третину гірше, ніж у звичайних застосунках. Довіра має закладатися в продукт від початку через обмеження доступу до даних, відповідність точності ставкам, показ рівня впевненості системи та можливість перевірити й відстежити результат. Автори виокремлюють п’ять моделей позиціонування AI — від функції наявного продукту до невидимої інфраструктури — та п’ять рівнів агентної комерції, від автоматичного заповнення форм до передбачення потреб. Більшість ринку нині перебуває на другому рівні, коли агент перетворює опис потреби на пошук і варіанти. Формуються три моделі володіння агентами: власний агент користувача, агент усередині екосистеми продавця чи маркетплейсу та незалежний посередник, який порівнює пропозиції різних продавців. Природною

відправною точкою для агентної комерції автори вважають сектор B2B із чіткішими правилами закупівель. Практичним інструментом документа є розширена бізнес-модель Canvas із запитаннями для кожного блоку. Керівникам радять запускати AI-first процеси паралельно з чинними та вимірювати різницю в результатах, а державним органам — уважно відстежувати вплив таких моделей на конкуренцію, зайнятість і різні групи населення.

У цілому документ демонструє, що конкурентна перевага зміщується від володіння інструментами AI до глибини його вбудовування в процеси, дані та організаційну структуру. Для сфери протидії відмиванню коштів це має подвійне значення. З одного боку, наведені приклади Taktile і Stripe показують, що AI вже застосовують для перевірки клієнтів, відсіювання хибних спрацювань і виявлення шахрайства в реальному часі, а зворотний зв'язок від аналітиків підвищує точність систем. З іншого боку, вимоги до точності, відстежуваності та людського контролю у фінансових рішеннях залишаються найвищими, тож ефективність суб'єктів фінансового моніторингу залежатиме від здатності поєднати автоматизацію з прозорим управлінням і збереженням експертного судження.

Висновки

Варто починати з трьох–п'яти пріоритетних процесів, а не з десятків розрізнених пілотів, і запускати AI-first процеси паралельно з чинними, вимірюючи різницю в результатах.

Допускати ШІ до роботи слід лише після проходження кількісних порогів, а нову модель запускати паралельно з чинною і замінювати її лише тоді, коли вона показує кращі результати.

Рішення з високими ставками в регульованих сферах потребують майже нульового рівня помилок, тому варто поєднувати правила, агентів AI та людську перевірку з повною відстежуваністю кожного кроку.

Хибні спрацювання та виправлення аналітиків потрібно використовувати як дані для навчання, що підвищує точність виявлення шахрайства з кожним циклом.

Системні вади оборонних закупівель: аналіз шахрайства в умовах війни [8]

У матеріалі авторитетного видання The New York Times, що базується на конфіденційних державних аудиторських звітах, ідеться про стійку та відтворювану модель функціонування системи оборонних закупівель в Україні в умовах повномасштабної війни. Попри те, що система закупівель значною мірою забезпечила здатність країни чинити опір, вона водночас стала джерелом системної вразливості, яка проявляється у втратах бюджетних коштів, невиконанні контрактів, завищенні цін та відсутності реальних наслідків для порушників. За оцінками внутрішніх аудитів, лише за один рік втрати від шахрайства, марнотратства та неефективного управління сягнули близько 1,2 мільярда доларів. Ці втрати не були публічними, вони накопичувалися паралельно з постійними закликами до міжнародних партнерів про надання додаткового озброєння та фінансової допомоги.

Протягом майже п’яти років бойових дій український уряд зберігає інституційну цілісність, армія чинить опір чисельнішому противнику, а поле бою зазнало революційних змін завдяки дронам і роботизованим системам. Водночас той самий процес закупівель, який дозволяє підтримувати боєздатність і фінансувати технологічні інновації, перетворився на самостійну вразливість, що впливає на внутрішню політику та довіру суспільства. Публічні скандали, відставки високопосадовців і масові протести свідчать про те, що проблема має не технічний, а системний характер.

Один із найбільш показових кейсів стосується постачання мінометних боєприпасів. У розпал активних бойових дій артилерійські розрахунки отримували снаряди, які або не вилітали з труб, або падали не детонуючи. З’ясувалося, що державне підприємство поставило армії тисячі дефектних мінометних пострілів. Пізніше суд встановив, що йшлося про 233 тисячі непридатних боєприпасів, значна частина яких мала дефектні детонатори або пороховий заряд. Керівника підприємства було заарештовано та обвинувачено у шахрайстві на суму близько 68 мільйонів доларів — вартість інспектування та заміни дефектної продукції.

Однак ключовим у цьому кейсі є не сам факт дефекту, а реакція системи. Аудитори встановили, що підприємство спочатку заявляло про відсутність спроможності виконати замовлення, але згодом, без пояснень, переглянуло свої виробничі можливості, після чого отримало контракт. Жодних доказів того, що хтось намагався перевірити реальність цих можливостей, аудит не виявив. Коли ж почали надходити дефектні боєприпаси, закупівельна агенція, за висновком аудиторів, «не зробила належних висновків». Замість санкцій підприємство отримало ще більший обсяг замовлень, зокрема контракт на постачання майже всіх 122-міліметрових артилерійських боєприпасів. Аудит не встановлює, хто саме ухвалював ці рішення і з яких мотивів. Показово, що керівник закупівельної агенції згодом пішов у відставку, а керівника підприємства було засуджено до п’яти років позбавлення волі в іншій справі — за організацію корупційної схеми з продажу вибухових речовин за завищеними цінами.

Ця схема демонструє замкнене коло: підприємство з історією порушень отримує контракт, виконує його неякісно, але замість втрати доступу до державного замовлення отримує нові, ще більші контракти. Втрати несе армія, яка не отримує боєприпасів, здатних виконувати бойові завдання, та бюджет, який витрачає кошти на неефективну продукцію.

Інший повторюваний механізм стосується закупівлі реактивних снарядів. У 2024 році закупівельна агенція оголосила тендер на сотні мільйонів доларів. На пропозицію відгукнулися три компанії, які пропонували однаковий товар — снаряди одного виробника з однієї фабрики. Різниця була лише в ціні: одна компанія пропонувала близько 4 200 доларів за одиницю, друга — 4 600, третя — 5 100. Найнижчу ціну запропонував безпосередній виробник, що

[8] https://www.nytimes.com/2026/09/06/world/europe/ukraine-war-weapons-fraud-corruption.html

передбачало пряме постачання з фабрики. Однак контракт отримав найдорожчий учасник — дочірня структура великої холдингової компанії, яка виступала посередником. Аудитори не знайшли жодного обґрунтування такого рішення, хоча попередні аудити вже застерігали від закупівель через посередників. За оцінками, це рішення додало до рахунку України близько 130 мільйонів доларів.

Цей кейс ілюструє ширшу тенденцію: держава свідомо відмовляється від прямих закупівель за нижчою ціною на користь посередницьких структур, які не додають жодної додаткової цінності, окрім зростання вартості.

Третій тип схеми стосується закупівель, які передбачають складні ланцюги посередників через політичні обмеження країн-виробників. У 2024 році закупівельна агенція мала намір придбати реактивні снаряди радянського зразка у виробника з країни, чия політика була дружньою до росії. Через це Україна покладалася на ланцюг посередників. Державний контракт уклали з українським державним брокером, який, за даними аудиторів, мав історію невиконаних контрактів. Антикорупційні органи також публічно повідомляли про розслідування щодо колишніх керівників цієї компанії за можливе розкрадання та відмивання коштів. Крім того, компанія не мала експортної ліцензії країни-виробника, а замість ліцензії подала «гарантійний лист» від військової розвідки. Аудитори зазначили, що такий преференційний підхід не мав правового обґрунтування і був застосований попри історію дефолтів компанії.

Державний брокер, у свою чергу, уклав субпідряд з американською збройовою компанією, яку очолював колишній біржовий брокер. Ця компанія мала досвід постачання українській армії та підтримуваним США повстанцям у Сирії. Загальна вартість кількох контрактів між цими структурами сягала 1,7 мільярда доларів. Однак угода почала розвалюватися. Тодішній міністр оборони прагнув виключити посередників з воєнного бізнесу і запропонував американській компанії працювати напряму із закупівельною агенцією, фактично усунувши державного брокера. Угода зірвалася, і вже на початку 2025 року державний брокер став найбільшим боржником перед агенцією із закупівель, маючи найбільше невиконаних контрактів серед усіх постачальників. Уряд подав позов про штрафи та пеню, а брокер, у свою чергу, вимагав кошти від американської компанії.

Цей кейс демонструє, як складність і непрозорість ланцюгів постачання створюють умови для взаємних звинувачень, судових позовів і втрати ресурсів, при цьому кінцевий отримувач — армія — не отримує необхідного озброєння.

Аудити охоплюють 2024 та 2025 роки і показують, що сім із десяти найбільших військових підрядників отримали нові контракти попри відкриті кримінальні провадження за шахрайство, невиконання попередніх зобов'язань або арешт керівництва за корупцію. Вісімнадцять компаній уклали угоди, попри дефолти за попередніми контрактами, а шість із них не виконали жодного контракту. Компанії отримували контракти без підтвердження спроможності постачати зброю або без відповідних ліцензій. Близько 126 мільйонів доларів було втрачено через обхід нижчих пропозицій і переплату за озброєння. Контракти укладалися без правового обґрунтування. В одному випадку компанії досі сперечаються щодо щонайменше 100 мільйонів доларів авансових платежів за угодою, яка розвалилася.

Ці втрати не були публічними, оскільки аудити мають класифікований характер і ніколи не піддавалися публічному розгляду. Незрозуміло, які саме заходи вжила закупівельна агенція у відповідь на висновки аудиторів. Керівник агенції відмовився від коментарів і згодом подав у відставку. Проблема сягає найвищих рівнів влади: минулого року корупційні розслідувачі таємно записали, як колишній бізнес-партнер високопосадовця закликав чиновників закуповувати бронежилети, які не пройшли випробування на безпеку. Розслідувачі кажуть, що ця людина втекла з України під час слідства. Сам високопосадовець не був звинувачений і заявив, що підтримує розслідування.

Експерти з антикорупції зазначають, що така практика має давню традицію. Інший колишній радник закупівельної агенції описав замкнене коло: армія не отримує необхідного, бюджет скорочується через непостачання та переплати, у результаті немає грошей на замовлення більшої кількості зброї, і немає необхідної кількості боєприпасів.

Аналіз аудитів свідчить про те, що система оборонних закупівель в Україні функціонує не як виняток із правил, а як стійка модель, у якій сигнали про порушення ігноруються, а наслідки для порушників майже відсутні. Три описані схеми

демонструють різні механізми, але спільну логіку: державні кошти витрачаються неефективно, армія не отримує необхідного, а окремі підрядники та посередники накопичують прибутки.

Проблема має системний характер і потребує не точкових покарань, а глибокої інституційної реформи, яка б усунула саму можливість відтворення цих схем. В іншому разі навіть найбільші обсяги міжнародної допомоги будуть втрачатися, не допомагаючи тим, хто на передовій захищає країну.

Висновки

Проблема має не точковий, а системний характер. Сім із десяти найбільших підрядників отримували нові контракти попри кримінальні провадження, арешт керівництва або історію невиконаних зобов'язань.

Втрати сягають мільярдних сум і залишаються непрозорими. Лише за один рік втрати від шахрайства та неефективного управління оцінюються у близько 1,2 мільярда доларів.

Посередники та завищені ціни стали нормою, а не винятком. Держава свідомо відмовляється від прямих закупівель за нижчою ціною на користь посередницьких структур, які не додають цінності, а лише збільшують вартість.

Армія платить найвищу ціну за неефективність тилу. Наслідком цих схем є не лише фінансові втрати, а й фізична нестача якісного озброєння та боєприпасів на фронті.

Як китайські злочинні синдикати поширюють свій вплив на Південну Азію [9]

Глобальна поінформованість про шахрайські організації, що базуються в Південно-Східній Азії та використовують торгівлю людьми і примусову злочинність для обману громадян у всьому світі, продовжує зростати. Однак, як зазначається в аналітичному звіті GI-TOC, головним обмеженням міжнародної відповіді на цю загрозу є тенденція розглядати проблему виключно як регіональну особливість Південно-Східної Азії. Дослідження, проведене організацією, переконливо демонструє, що китайські за походженням синдикати вже глибоко інтегрувалися в злочинні екосистеми Південної Азії, зокрема в Індії, Непалі та Шрі-Ланці, створюючи нові виклики для національної, регіональної та глобальної безпеки.

Звіт виокремлює кілька ключових моделей конвергенції між південно-азійськими, китайськими та східно-азійськими злочинними групами. Перша з них полягає у злитті транснаціональних злочинних організацій, що діють у Китаї та за його межами, з місцевими угрупованнями в Південній Азії. Ця тенденція зародилася наприкінці 2010-х років, коли китайські синдикати онлайн-гемблінгу почали мігрувати регіоном, і особливо посилилася з кінця 2025 року на тлі зростаючого міжнародного тиску на операції в Південно-Східній Азії.

Друга модель — це конвергенція між шахрайськими операціями в Південно-Східній Азії та мережами вербування й торгівлі людьми в Південній Азії. Це створює серйозну загрозу торгівлі людьми в регіоні, водночас сприяючи стрімкому зростанню залучення вихідців з Південної Азії та їхніх діаспор до кібершахрайства.

Третя модель має регіональний вимір: злочинні актори з Індії, Непалу та Шрі-Ланки дедалі частіше використовують відсутність належної транскордонної взаємодії між правоохоронними органами, регуляторами та фінансовими установами, що дозволяє їм безперешкодно вчиняти шахрайства за кордоном. Китайські синдикати відіграють у цьому процесі ключову роль, але місцеві групи адаптують їхні методики та операційні структури під власні потреби.

Історичний контекст свідчить, що китайські мережі онлайн-гемблінгу та кіберзлочинності намагалися закріпитися в Шрі-Ланці та Непалі ще близько 2018 року. У Непалі масштабне переміщення синдикатів почалося у 2019 році, ймовірно, після початку кампанії проти онлайн-гемблінгу в Камбоджі. Того ж року спільні операції Непалу та Китаю змусили багатьох злочинців переміститися до північної М'янми та Зони спеціального економічного розвитку «Золотий трикутник» на кордоні Лаосу, Таїланду та М'янми.

Попит китайських шахрайських синдикатів, що діють у Камбоджі, Лаосі та М'янмі, на молодих людей, які розмовляють англійською, зробив Південну Азію природним джерелом для вербування. Дослідження задокументувало розвиток каналу торгівлі людьми з цього регіону, починаючи з 2021 року. За оцінками GI-TOC, понад 30 000 вихідців з Південної Азії наразі утримуються в шахрайських таборах у материковій Південно-Східній Азії. Лише в Індії, за даними Міністерства внутрішніх справ, 30 000 з 73 000 індійських громадян не повернулися додому після відвідування країн Південно-Східної Азії у період з 2022 по 2024 рік, що викликає серйозне занепокоєння щодо їхнього утримання в шахрайських центрах.

---

[9] https://globalinitiative.net/wp-content/uploads/2026/09/Jason-Tower-Radha-Barooah-Criminal-convergence-Chinese-origin-scam-syndicates-and-their-reach-into-South-Asia-GI-TOC-September-2026.pdf

Серед схем, націлених на південно-азійців, поширені шахрайства з туристичними візами та працевлаштуванням. Жертв часто змушують оплачувати власну подорож до ОАЕ, Оману чи інших країн Близького Сходу, де вони в'їжджають за туристичною візою, а згодом їх переправляють до Південно-Східної Азії для примусової злочинної діяльності. З 2024 року китайські злочинні групи також використовують шахрайства з імітацією державних органів, щоб заманити шрі-ланкійців до таборів у Південно-Східній Азії. Китайські синдикати встановили міцні зв'язки з регіональними злочинними мережами в Південній Азії для торгівлі людьми. В усіх трьох країнах фіксувалися випадки, коли китайські синдикати безпосередньо наймали місцеві угруповання для вербування жертв. Подібні моделі спостерігалися і в інших країнах, причому китайські групи платили від 3250 до 5000 доларів за кожну жертву.

Окремої уваги заслуговує проблема нерегульованого онлайн-гемблінгу, який став каталізатором експансії синдикатів. Після посилення заходів проти офшорного онлайн-гемблінгу на Філіппінах у 2022 році десятки тисяч китайських громадян залишили країну. Це збіглося з швидкою лібералізацією казино-індустрії в Шрі-Ланці, яка також розпочалася у 2022 році. Інтерв'ю, проведені GI-TOC, датують прибуття китайських синдикатів онлайн-гемблінгу тим самим роком. У 2024 році влада Шрі-Ланки почала повідомляти, що китайські громадяни стають головними гравцями в країні. Стрибок туристичних прибуттів між 2023 та 2025 роками, особливо з країн, пов'язаних з індустріальними кібершахрайськими операціями, є додатковим свідченням міграції цих синдикатів. Згідно з офіційними даними, туристичні прибуття до Шрі-Ланки зросли більш ніж на 100% між 2022 та 2023 роками, а з 2023 по 2025 рік — ще на 50%. За той самий період прибуття з М'янми та Камбоджі зросли на 120% та 105% відповідно.

Повідомлення про переміщення синдикатів онлайн-гемблінгу та кібершахрайства до Шрі-Ланки з'явилися приблизно в період відкриття казино City of Dreams. Хоча це не встановлює прямого причинно-наслідкового зв'язку, це вказує на те, що розширення грального сектору підвищило привабливість країни для таких операцій. Китайськомовна платформа Bodu.co назвала відкриття казино віхою у перетворенні Шрі-Ланки на «рай для BC» (китайська абревіатура для онлайн-гемблінгу та шахрайства).

Шрі-Ланка наразі перебуває під значним ризиком перетворення на центр китайських шахрайських синдикатів, які використовують онлайн-казино та аутсорсингові компанії (BPO) для створення кібершахрайських операцій. У 2024 та 2025 роках поліція провела рейди в двох великих шахрайських центрах у районі Коломбо, заарештувавши 340 іноземців, більшість з яких — китайці. Незважаючи на ці дії та додаткові рейди у 2026 році, ті самі будівлі досі використовуються так званими «технологічними компаніями», які приймають велику кількість китайських, в'єтнамських та індонезійських громадян. Багато з цих осіб, схоже, мають зв'язки з BPO-компаніями, зареєстрованими в Port City Colombo, спеціальній економічній зоні, що викликає побоювання щодо використання пільгових політик для масштабування злочинної діяльності.

Китайські злочинні актори також використовують зростаючу мережу криптовалютних обмінників у Шрі-Ланці, які надають інструменти для переміщення коштів. Публічні Telegram-канали для китайськомовної спільноти в Шрі-Ланці стрімко зростають; один з них налічує 90 000 учасників і рекламує послуги, пов'язані з шахрайством, а також офшорні онлайн-гемблінг-сайти. Особливе занепокоєння викликає той факт, що платформа U8.com, яка раніше рекламувалася в шахрайському таборі KK Park у М'янмі, відкрила офіси в Шрі-Ланці. Рекламу U8 можна побачити на таксі та білбордах уздовж головної траси між центром Коломбо та аеропортом.

Регуляторна спроможність країн Південної Азії суттєво різниться. Індія вирізняється наявністю установ та потенціалу світового рівня для моніторингу та протидії кіберзлочинності. Індія значно сприяла боротьбі з поширенням кібершахрайства в Непалі, часто в рамках зусиль проти китайського злочинного впливу. Індійські правоохоронці у співпраці з непальською поліцією виявили розгалужену транснаціональну мережу, що включає рахунки «мулів» в Індії, які пов'язують шахрайські синдикати з Китаю та Камбоджі, що діють у Непалі, з фінансовими операціями, що сягають Дубаю. Водночас кількість зареєстрованих скарг в Індії продовжує різко зростати. Індія стикається з низкою викликів, зокрема напруженістю між юрисдикційними обмеженнями та необхідністю швидких дій. Кіберзлочинці часто діють у кількох юрисдикціях, використовуючи відмінності в правових системах. Традиційні механізми співпраці можуть тривати місяцями, а докази швидко втрачаються. Крім того, злочинці дедалі частіше використовують криптовалюти, що ускладнює традиційне відстеження.

Спроможність Шрі-Ланки боротися з кіберзлочинністю також обмежена, а правова база застаріла. Закон про комп'ютерні злочини 2007 року був ухвалений до появи криптовалют, хмарних технологій та шахрайства в соціальних мережах. Він не містить положень щодо шахрайства з цифровими активами, штучного інтелекту чи вербування через платформи. Закон про регулювання азартних ігор 2025 року є однією з найважливіших реформ, але його впровадження залишається складним завданням.

Непал стикається з подібними проблемами: Закон про електронні транзакції 2008 року, розроблений для сприяння електронній комерції, був перепрофільований як де-факто «закон про кіберзлочинність» без належного оновлення. Серед прогалин — відсутність сучасних стандартів цифрових доказів, спеціалізованих режимів для криптовалютних злочинів, положень про рахунки «мулв» та нагляду за зашифрованими платформами.

Підсумовуючи, кібершахрайство більше не можна розглядати як суто азійську проблему. Хоча індустріальні табори зосереджені в цьому регіоні, транснаціональні мережі, що ними керують, не обмежуються географічними рамками. Китайські синдикати дедалі більше пов'язані зі злочинними акторами, мережами вербування, фінансовою інфраструктурою та операціями онлайн-гемблінгу по всій Південній Азії. Індія, Непал та Шрі-Ланка зазнають впливу по-різному, але разом вони ілюструють, як шахрайська економіка стає дедалі більш транснаціональною, децентралізованою та стійкою до правоохоронного тиску. Таким чином, відповідь має бути спрямована на всю систему, а не лише на ліквідацію осередків

Висновки

Кібершахрайська індустрія більше не є суто східно-азійською проблемою: китайські за походженням синдикати активно інтегруються в злочинні та фінансові мережі Індії, Непалу та Шрі-Ланки, перетворюючи Південну Азію на новий операційний і транзитний хаб.

Понад 30 000 вихідців з Південної Азії утримуються в шахрайських таборах у Південно-Східній Азії, а китайські синдикати платять місцевим угрупованням до 5000 доларів за кожну завербовану жертву, що робить торгівлю людьми невід'ємною складовою шахрайської економіки.

Відповідь на загрозу залишається фрагментованою: замість боротьби з транснаціональною мережею в цілому держави зосереджуються на ліквідації окремих осередків, що лише змушує синдикати переміщатися до нових юрисдикцій, не порушуючи їхньої операційної спроможності.

Bloomberg: американська лобістська компанія Qorvis мала приховані зв'язки з підсанкційними нафтовими магнатами з Ірану та Росії [10]

10 вересня 2026 року Bloomberg опублікував розслідування про вашингтонську компанію Qorvis – одну з найвідоміших лобістських і комунікаційних фірм США. Протягом останнього року вона представляла сінгапурську Wellbred Capital Pte Ltd. і дубайську 2Rivers Group. За даними західних органів влади, ці компанії контролюють двоє найбільших гравців підсанкційної нафтової торгівлі: іранець Хоссейн Шамхані, батько якого був радником покійного верховного лідера Ірану, та азербайджанець Етібар Еюб, який посів помітне місце в московських трейдингових колах. Обох за останні два роки внесено до санкційних списків західних країн за незаконну торгівлю нафтою. Qorvis заперечує, що Шамхані чи Еюб були її клієнтами, і наголошує, що «не бере підсанкційних грошей». Журналісти спираються на розповіді понад десяти обізнаних осіб, зокрема колишніх працівників фірми, а також на публічні реєстри й судові документи.

Розслідування показує, як працювало прикриття. У позові про цивільну конфіскацію, поданому в березні 2026 року, Міністерство юстиції США зазначило, що Шамхані з партнерами набули контролю над Wellbred приблизно у 2019 році, щоб зберегти «бренд», який публічно не асоціювався б ні з ним, ні з Іраном. 24 серпня 2026 року Казначейство США запровадило санкції проти Wellbred. За словами трьох колишніх працівників Qorvis, фірма радила генеральному директору Wellbred Газі Абуальсауду, як пояснювати медіа і регуляторам його стосунки з Шамхані, а на закритих зустрічах у Дубаї консультувала самого Шамхані, як захистити фінансову мережу від американських регуляторів. Інший приклад – Coral Energy, ключовий трейдер російської нафти після 2022 року, яка в серпні 2024 року за участі Qorvis змінила назву на 2Rivers Group. Запроваджуючи у грудні 2025 року санкції проти Еюба, ЄС зазначив, що той заснував і очолює мережу компаній, «включно з Coral Energy (згодом 2Rivers Group)», яка контролює значну частину «тіньового флоту» Росії. У 2Rivers стверджують, що Еюб не пов'язаний з компанією з початку 2022 року.

Окреме питання – гроші. США запровадили санкції проти Шамхані та його мережі в липні 2025 року; Казначейство назвало цей пакет наймасштабнішим щодо Ірану за сім років. Проте, за словами п'яти обізнаних осіб, Qorvis і надалі отримувала платежі від структур, які, за даними органів влади, контролює Шамхані. Голова Qorvis Саманта Со визнала лише, що Wellbred «сплатила прострочені рахунки», але не уточнила, коли саме. Колишній співробітник Управління з контролю за іноземними активами (OFAC) Девід Танненбаум нагадує: за федеральним законодавством лобісти мають отримати ліцензію, щоб працювати з підсанкційною особою або приймати від неї платежі.

Розслідування торкається і впливу на санкційну політику. На початку березня 2026 року, коли через війну в Ірані ціна нафти перевищила 100 доларів за барель, керівники Qorvis, за словами джерел, запропонували високопосадовцям США послабити санкції щодо Ірану та Росії, щоб стабілізувати ринок. За кілька днів Казначейство видало короткострокові дозволи на продаж іранської та російської нафти, яка перебувала на танкерах у морі; вони діяли до початку липня. Наскільки на це рішення вплинула саме порада Qorvis, невідомо. Однак наслідок був відчутним:

[10] rusi.org/explore-our-research/publications/commentary/unfinished-business-effective-uk-anti-money-laundering-supervision

іранська нафта, яка на початку 2026 року продавалася з дисконтом 10 доларів за барель, уперше майже за чотири роки торгувалася з премією до світового еталонного сорту, що принесло мільярдні прибутки мережам, пов'язаним, зокрема, з Шамхані.

Нарешті, кейс оголює прогалину в прозорості лобіювання. Чинні та колишні посадовці США вважають, що описані відносини мали бути розкриті відповідно до Закону про реєстрацію іноземних агентів (FARA). Однак адміністрація сигналізує про обмежене застосування цього закону, а Міністерство юстиції розглядає звуження винятку для добросовісної комерційної діяльності – розмежування, яке санкційна політика часто розмиває. Група сенаторів від обох партій запропонувала зобов'язати реєструватися агентів, які діють в інтересах урядових або комерційних структур Росії, Ірану, Китаю, КНДР чи Куби, проте перспективи законопроєкту неясні. На думку експертів, м'який підхід до FARA заохочує лобістські фірми брати ризикованіших клієнтів.

Еволюція методів контрабанди та нова роль Європи у глобальному наркообігу [11]

Сучасний світ незаконного обігу наркотиків зазнає глибоких структурних змін, і однією з найбільш тривожних тенденцій останнього десятиліття стало використання рідкого кокаїну як способу приховування та транспортування заборонених речовин через легальні комерційні ланцюги постачання.

Цей метод, який ще десять років тому вважався екзотичним і поодиноким, сьогодні перетворюється на системне явище, що змушує правоохоронні органи та міжнародні аналітичні центри переглядати усталені уявлення про маршрути, технології та економіку наркотрафіку. Згідно з даними, оприлюдненими у вересні 2026 року, використання рідин для маскування кокаїну не лише зростає кількісно, але й якісно змінює роль Європи у глобальному ланцюзі постачання, перетворюючи її з переважно споживчого ринку на проміжний пункт обробки та екстракції.

Під терміном «рідкий кокаїн» розуміють не якусь окрему хімічну форму наркотику, а спосіб його підготовки до транспортування. Йдеться про порошкоподібний кокаїну гідрохлорид — кристалічну сіль кокаїну, яка зазвичай має вигляд білого порошку, — розчинений у воді, органічних розчинниках на кшталт етанолу чи ацетону, або ж у різноманітних рідинах, що містять хімічні сполуки, такі як маніт, глюкоза, целюлоза чи лактоза. Після прибуття до пункту призначення таку рідину не вживають безпосередньо; її піддають хімічному переробленню, щоб відновити кокаїн у звичній порошкоподібній формі, придатній для подальшого розповсюдження. Саме ця двоетапність — розчинення на початку маршруту та екстракція в кінці — робить метод надзвичайно ефективним для обходу традиційних систем сканування, адже рентгенівські апарати та інші пристрої, налаштовані на виявлення твердих речовин чи характерних кристалічних структур, часто виявляються безсилими перед звичайною рідиною, яка за своїми фізичними властивостями не відрізняється від шампуню, алкоголю чи побутової хімії.

Історія цього явища сягає щонайменше 2011 року, коли в Болівії було зафіксовано випадок вилучення рідкого кокаїну під час невеликої транскордонної операції. Однак протягом останніх чотирьох років географія виявлених партій різко розширилася: вантажі, що походили з Латинської Америки, були перехоплені у Франції, Хорватії, Іспанії, Ірландії та

[11] https://insightcrime.org/news/liquid-cocaine-explainer/

Нідерландах. Це свідчить про те, що метод перестав бути локальною особливістю окремих регіонів і перетворився на складову частину трансатлантичних маршрутів.

Трафік організовується двома основними способами. Перший полягає у розчиненні кокаїну в рідині-носії, яка потім маскується під звичайні споживчі товари: контейнери з-під шампуню, алкогольні напої, а також промислову продукцію — хімікати, мийні засоби, фарби, клеї та смоли. Дуже часто рідкий кокаїн змішують із легальними комерційними рідинами. Другий спосіб, відомий як імпрегнація, передбачає просочення кокаїном твердих матеріалів-носіїв: пластмас, меблевих деталей, акрилових смол, деревного вугілля, картону і навіть металів. Показовим прикладом стала операція ірландської влади на початку 2026 року, коли було вилучено фанеру, просочену рідким кокаїном, яка прямувала з Південної Америки до підпільної лабораторії в графстві Кілдер. За інформацією слідства, дерев'яні плити були занурені в рідкий кокаїн перед відправленням, а в Ірландії їх планувалося подрібнити на тирсу, з якої потім екстрагували б наркотик.

Процес хімічного приховування кокаїну, описаний в аналітичних матеріалах, має чітку послідовність етапів. Спочатку гідрохлорид кокаїну, вироблений у Південній Америці, хімічно розчиняють у рідкому розчині. Далі цей розчин приховують усередині комерційних товарів, пляшок або вантажів, після чого відправляють повітряним або морським транспортом. У країнах призначення лабораторії використовують хімічні процеси для видобутку та відновлення кокаїну: рідину розчиняють у підкисленій воді, піддають лужній обробці, осаджують, фільтрують і висушують, отримуючи кінцевий продукт. Відновлений кокаїн потім розподіляється між оптовим та роздрібним ринками. Ця схема, описана в звіті Управління ООН з наркотиків і злочинності (UNODC) за вересень 2026 року, демонструє, наскільки складним і багатоетапним став процес наркотрафіку, який тепер вимагає не лише логістичних навичок, але й глибоких знань у галузі хімії та промислової переробки.

Особливо важливим є те, що Європа в цій схемі набуває нової функції. Якщо раніше вона розглядалася переважно як кінцевий ринок споживання, то тепер вона стає проміжним пунктом обробки. Згідно з даними Європейського агентства з наркотиків (EUDA) за 2026 рік, європейські країни дедалі частіше виявляють у себе не лише готовий продукт, але й сировину та напівфабрикати, призначені для подальшої екстракції. У 2024 році шість держав-членів ЄС повідомили про ліквідацію щонайменше 42 об'єктів, пов'язаних із виробництвом, екстракцією, фасуванням або нарізанням кокаїну, порівняно з 34 у 2023 році. Ця динаміка свідчить про те, що європейські лабораторії дедалі активніше залучаються до процесу відновлення наркотику з рідких та просочених носіїв, що, у свою чергу, зменшує ризики для організаторів трафіку, адже перевезення рідини через кордон значно безпечніше, ніж транспортування готового порошку.

Трафікери постійно вдосконалюють свої методи, і використання дедалі складніших фізичних та хімічних способів приховування зростає, про що наголошується у звіті EUDA. Це стосується не лише кокаїну. Хоча й рідше, але аналогічні методи застосовуються для переміщення інших наркотиків, зокрема метамфетаміну. Під час вилучення партії метамфетаміну, що прямувала з Мексики до Австралії, австралійська федеральна поліція виявила шар метамфетаміну, введений у внутрішнє фарбування контейнера, який вони розібрали. Пізніше було знайдено промислове обладнання, призначене, за версією слідства, для екстракції наркотику в Сіднеї, у приміщенні, пов'язаному з отримувачами вантажу. Цей випадок ілюструє універсальність технології: хімічне приховування стає загальним інструментом для різних типів заборонених речовин, що ускладнює роботу митних та правоохоронних органів, які змушені реагувати на постійно еволюціонуючі форми маскування.

Таким чином, феномен рідкого кокаїну є не просто черговою тактикою контрабандистів, а відображенням глибших трансформацій у глобальній наркоекономіці. Він демонструє, як злочинні мережі адаптуються до посилення контролю на кордонах, використовуючи легальні промислові та споживчі ланцюги як прикриття, і як географія наркотрафіку стає дедалі складнішою, залучаючи нові регіони до процесів переробки та екстракції.

Для Європи це означає не лише зростання ризиків, пов'язаних із споживанням, але й необхідність перегляду стратегій протидії, адже тепер вона є не лише кінцевою точкою маршруту, але й важливою ланкою у виробничому ланцюзі, що вимагає комплексного підходу до виявлення, аналізу та ліквідації підпільних лабораторій. З огляду на постійне вдосконалення методів приховування, можна очікувати, що найближчими роками ця тенденція лише посилюватиметься, ставлячи перед міжнародною спільнотою нові виклики, пов'язані з необхідністю розробки нових технологій виявлення та координації зусиль між країнами походження, транзиту та призначення.

Китайська державна компанія постачала сировину для вуглецевого волокна російському виробнику комплектуючих для ударних дронів[12]

4 вересня 2026 року Politico оприлюднив розслідування на основі внутрішніх російських транспортних і митних документів, які зібрав київський аналітичний центр «Український центр безпеки та співпраці». Документи свідчать, що китайська державна компанія Jilin Chemical Fiber Group цього року відвантажила до 46 тонн поліакрилонітрильного джгута (PAN-прекурсора) компанії «Алабуга-Волокно» – дочірньому підприємству дивізіону композитних матеріалів UMATEX державної корпорації «Росатом». Комітет Палати представників США з питань Китаю визнав документи легітимними, а їхню автентичність підтвердив і український уряд. Документи також передано урядам Великої Британії та США.

PAN-прекурсор – основна сировина для легкого і високоміцного вуглецевого волокна військового класу. «Алабуга-Волокно» працює в особливій економічній зоні «Алабуга» в Татарстані, де серійно виробляють ударні дрони «Герань» за іранським дизайном Shahed. За оцінкою засновника Інституту науки і міжнародної безпеки Девіда Олбрайта, відвантаженої сировини вистачило б на вуглецеве волокно приблизно для 1300 таких дронів. За розрахунками українського центру, до 2030 року 89% продукції «Алабуга-Волокно» має спрямовуватися підприємствам оборонної промисловості. Сама компанія та UMATEX з 2023 року перебувають під санкціями Великої Британії, США, ЄС, України, Нової Зеландії та Швейцарії, тоді як Jilin західних санкцій наразі не має.

Особливу увагу розслідування приділяє способу маскування. Товар задекларували під митним кодом, який зазвичай застосовують до цивільних синтетичних волокон, як-от нейлону чи поліестеру, хоча правильний код ідентифікував би його як товар подвійного призначення. За даними компанії Sayari, у 2022–2025 роках жодна з підсанкційних компаній ОЕЗ «Алабуга» не імпортувала товари під кодом, який зазвичай використовують для PAN-волокна. Колишня посадовиця Казначейства США Керрі Бітсофф описує схему так: для контрольованого товару підбирають «правдоподібний код-прикриття», який потім повторюється в різних компаніях для подібних товарів. Український центр відстежив щонайменше вісім тендерів на поставки PAN-прекурсора від Jilin до «Алабуга-Волокно» з 2022 року.

«Росатом» заявив, що діє відповідно до законодавства, Jilin на запити не відповіла, а посольство Китаю у Вашингтоні назвало звинувачення спробою «очорнити» КНР і наголосило на суворому контролі за товарами подвійного використання. Колишні американські посадовці сумніваються, що державна компанія могла здійснити таку поставку без відома уряду. За словами Олбрайта, документи дають Державному департаменту США підстави запровадити санкції проти постачальника. Контекст також показовий: за даними Кільського інституту світової економіки, Китай забезпечує понад 60% компонентів, необхідних для функціонування російської армії.

[12] https://www.politico.eu/article/china-state-firm-supplies-russia-materials-kamikaze-drones/

Благодійність як фінансовий інструмент: урок про корпоративну прозорість [13]

Розслідування OCCRP розкриває історію про те, як благодійність одного з найбільших виробників залізної руди в Україні, компанії Ferrexpo, перетворилася на складний фінансовий механізм, що, за даними розслідування, використовувався для фінансування бізнес-імперії її тодішнього генерального директора та мажоритарного акціонера, який зараз знахожиться під санкціями.

Розслідування базується на раніше неопублікованому судово-економічному звіті, підготовленому українським підрозділом міжнародної аудиторської компанії Crowe. Цей звіт було замовлено новим керівництвом благодійного фонду «Квітучий край» після того, як у 2023 році контроль над організацією перейшов до громадських активістів. Згідно з цим документом, з приблизно 110 мільйонів доларів, які Ferrexpo перерахувала фонду протягом 2013–2018 років, сума близько 74 мільйонів доларів не була використана за цільовим призначенням. Це значно більша сума, ніж та, яку раніше озвучували аудитори Deloitte, які у 2018 році не змогли підтвердити цільове використання 33,5 мільйона доларів.

Схема руху коштів, описана в звіті Crowe, виглядає наступним чином: Ferrexpo перераховувала гроші на рахунки благодійного фонду «Квітучий край». Звідти кошти розподілялися між трьома підфондами, які, своєю чергою, переказували їх двом комерційним українським компаніям — «Хімреактив» та «Газотурбінні технології». Ці компанії були залучені як підрядники для надання благодійних послуг, проте, як зазначається в документі, вони не мали достатньо власних коштів на рахунках для здійснення подальших транзакцій. Протягом кількох годин або днів після отримання благодійних грошей вони переказували аналогічні суми десяткам інших місцевих компаній, що працюють у

[13] https://www.occrp.org/en/investigation/instead-of-helping-ukraines-poor-ferrexpos-charitable-donations-flowed-to-companies-associated-with-its-then-ceo

промисловому, фінансовому та оптовому секторах. Жодна з цих компаній-отримувачів не була зареєстрована як благодійна організація.

Ключовим аспектом розслідування є зв'язок цих транзакцій з підсанкційним олігархом. За даними корпоративних записів та українського державного банківського агентства (Фонду гарантування вкладів), щонайменше вісім із 43 компаній, які отримували кошти, контролювалися або частково належали йому. Ще близько двох десятків компаній, за твердженням Фонду гарантування вкладів, перебувають під контролем бізнесмена. Зокрема, компанія «Хімреактив» у 2018 році сама Ferrexpo була вказана як «пов'язана сторона», яка контролюється бізнесменом. Інша компанія, «Газотурбінні технології», у 2023 році потрапила під арешт суду, оскільки прокуратура звинуватила її основного акціонера в тому, що він був «рекрутований» як проксі-власник для утримання активів підсанкційної особи.

Окрема увага в розслідуванні приділяється транзакціям 2015 року, коли банк, що належав цьому ж олігарху, перебував у стані кризи ліквідності. Згідно з банківськими записами, отриманими OCCRP, шість компаній, які фігурують у звіті Crowe як отримувачі коштів від «Квітучого краю», переказували гроші — часто майже ідентичними сумами — на рахунки банку або іншим компаніям, які згодом робили платежі на користь цього банку. Ці перекази були позначені як погашення кредитів та інвестиції в акціонерний капітал банку. Загалом до середини лютого 2015 року кінцеві компанії в цих ланцюжках витратили близько 22 мільйонів доларів на купівлю акцій проблемного банку.

Найбільш показовим є епізод у липні 2015 року, коли з трьох підфондів «Квітучого краю» близько 26 мільйонів доларів було перераховано компаніям «Газотурбінні технології», «Хімреактив» та ще одній компанії. Того ж дня всі три компанії перерахували ці кошти фінансовій компанії «ФК Факторинг», яка, у свою чергу, того ж дня переказала 19 мільйонів доларів банку. Призначення платежу було вказано як погашення комерційного кредиту, а не благодійна діяльність. На той момент «ФК Факторинг» частково належала українській страховій компанії «Омега», яку Ferrexpo у своєму річному звіті того ж року називала такою, що перебуває під «спільним контролем» олігарха.

Важливо зазначити, що звіт Crowe не встановив, хто саме керував розподілом коштів у фонді «Квітучий край», і не називав підсанкційного олігархі відповідальним, оскільки він не обіймав жодної посади в благодійній організації. Однак новий директор фонду Олександр Кузнецов у коментарі OCCRP заявив, що, на його думку, «Квітучий край» перебував під прямим контролем підсанкційного бізнесмені з моменту створення і до 2019 року. Це твердження базується на збігу персоналій між фондом та іншими українськими бізнесами цієї особи, а також на тому факті, що деякі компанії-отримувачі коштів належали бізнесмену.

Ця історія викликає серйозні питання щодо дотримання вимог Лондонської фондової біржі та британського законодавства про розкриття інформації про «пов'язані сторони». Аудитори Deloitte ще у 2018 році зазначали «значну кількість потенційних зв'язків» навколо підсанкційного бізнесмена, але не мали достатньо доказів, щоб підтвердити, чи здійснював він контроль над фондом. Незважаючи на те, що Ferrexpo заперечує будь-який зв'язок з благодійністю олігарха, а сам бізнесмен заперечує свою причетність, зібрані OCCRP дані свідчать про складну мережу транзакцій, яка, ймовірно, використовувалася для переказу коштів від благодійного фонду до структур, пов'язаних з його бізнес-імперією, включаючи проблемний банк.

Це розслідування підкреслює важливість прозорості корпоративної благодійності, особливо коли йдеться про компанії, що котируються на міжнародних біржах, та про осіб, які мають складні корпоративні структури для управління активами.

Ваша думка важлива!

Як банкам оцінювати ризики клієнтів-VASP у перехідний період, коли одні юрисдикції вже ліцензують їх, а інші ще ні?

Наскільки ефективними є наявні в Україні інструменти для виявлення консультантів і посередників, які можуть допомагати підсанкційним особам приховувати контроль над компаніями?

Як запобігти тому, щоб молодь і люди у скрутному фінансовому становищі ставали грошовими мулами фейкових магазинів, передаючи свої банківські картки чи рахунки за винагороду?

Наскільки можлива ефективна реформа оборонних закупівель в умовах воєнного часу, коли швидкість рішень часто здається важливішою за прозорість процедур?

Як повномасштабна війна та переформатування логістичних шляхів в Україні, зокрема, зростання обсягів гуманітарних вантажів, військової допомоги та волонтерської логістики, можуть створювати нові зони для контрабанди?

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-2026-39

Міністерство **фінансів** України

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.

AML POLICY DEPARTMENT
MINISTRY OF FINANCE OF UKRAINE