Методологічний бюлетень

Серійний номер: МінФін-AML-2026-12

Березень 2026

“Не дивись на годинник – роби, як він. Рухайся далі!”

Томас Карлайл

Мета

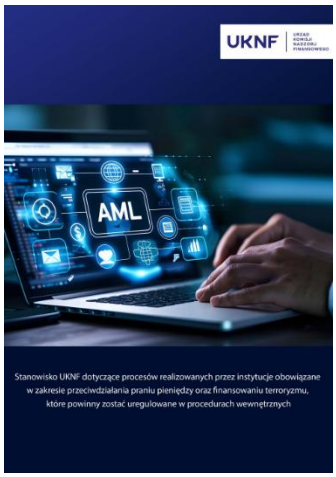
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

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

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

Звіти міжнародних організацій та окремих юрисдикцій

Трансформація наглядової парадигми: аналіз позиції Комісії з фінансового нагляду Польщі щодо ПВК/ФТ [1]



Офіційна позиція Комісії фінансового нагляду Польщі (Urząd Komisji Nadzoru Finansowego, UKNF), що глибоко та всебічно деталізує очікування регулятора щодо архітектури та функціонування систем протидії відмиванню коштів та фінансуванню тероризму (ПВК/ФТ) у піднаглядних суб'єктів, репрезентує вкрай жорстку та безкомпромісну еволюцію наглядової парадигми в межах єдиного ринку Європейського Союзу. Цей документ спрямований на остаточний і безповоротний перехід фінансових установ від формального (check-the-box) комплаєнсу до глибокої, проактивної інституційної підзвітності та персоналізації відповідальності. Методологічним та концептуальним ядром документа є імперативна вимога щодо повноцінного впровадження міжнародної моделі

[1] https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_AML_CFT_97484.pdf

«трьох ліній захисту». Ця архітектурна вимога чітко, на рівні організаційної структури розмежовує операційний ризик-менеджмент, незалежну функцію контролю та моніторингу, а також незалежне тестування ефективності системи (внутрішній аудит). Польський регулятор вимагає, щоб система внутрішнього контролю була не лише формально відповідною чинному законодавству, але й суворо, математично пропорційною до специфіки операційної діяльності, обсягів транзакцій та унікального профілю ризиків конкретної фінансової установи. Логіка UKNF недвозначно базується на тому постулаті, що управління ризиками ВК/ФТ не може розглядатися як ізольований операційний бек-офісний процес; воно має бути повністю, органічно інтегрованим у загальну стратегічну систему корпоративного управління. Цей концептуальний зсув підтверджується прямим нормативним посиланням UKNF на обов'язкові до виконання керівні принципи Європейського банківського управління (EBA/GL/2021/05) щодо стандартів внутрішнього управління, які вимагають створення спеціалізованих комітетів з питань ризиків безпосередньо на рівні наглядових рад фінансових груп та холдингів.

Особлива увага приділяється життєвому циклу процесу інституційної оцінки ризиків. Польський регулятор категорично наголошує на неприпустимості сприйняття оцінки ризиків як статичного, одноразового документа, створеного виключно для демонстрації аудиторам; це має бути безперервний, високодинамічний процес, що реагує на зміни макроекономічного середовища та клієнтської бази. Відповідно до вимог UKNF, результати оцінки ризиків, включно з усіма без винятку подальшими регулярними чи позачерговими оновленнями, повинні в обов'язковому порядку проходити процедуру формального затвердження не лише правлінням (керівним органом), але й наглядовою радою установи. Така жорстка регуляторна вимога де-факто унеможливлює небезпечну практику делегування відповідальності за прийняття критичних комплаєнс-ризиків на рівень середньої ланки менеджменту, змушуючи топ-менеджмент нести повну відповідальність за схильність до ризику. У контексті практичної імплементації, регулятор впроваджує жорсткі, математично вимірювані індикатори високого ризику, які автоматично, на рівні IT-систем, маркують ділові відносини з клієнтом як високоризикові в контексті географічного фактору.

Категорія клієнта	Критичні індикатори високого географічного ризику	Наслідок для системи ПВК/ФТ
Юридичні особи	Юридична особа, що володіє понад 50% акцій/часток клієнта, зареєстрована в юрисдикції високого ризику.	Автоматичне присвоєння найвищого балу ризику, заборона автоматичного онбордингу.
Юридичні особи	Ідентифіковані кінцеві бенефіціарні власники (КБВ) мають адресу реєстрації/проживання в юрисдикції високого ризику.	Обов'язкове застосування заходів посиленої належної перевірки (EDD) та погодження вищим керівництвом.
Юридичні особи	Клієнт здійснює систематичні операції з контрагентами, що мають реєстрацію у високоризикових країнах.	Впровадження індивідуальних сценаріїв транзакційного моніторингу для виявлення транзитних потоків.
Фізичні особи	Наявність у клієнта адреси проживання або реєстрації у високоризиковій країні.	Застосування EDD, встановлення джерела статків (SoW) та джерела походження коштів (SoF).

Категорія клієнта	Критичні індикатори високого географічного ризику	Наслідок для системи ПВК/ФТ
Фізичні особи	Здійснення систематичних переказів на користь суб'єктів або отримання коштів від осіб з високоризикових юрисдикцій.	Постійний посилений моніторинг частоти та обсягів платежів на предмет ознак ФТ або ВК.

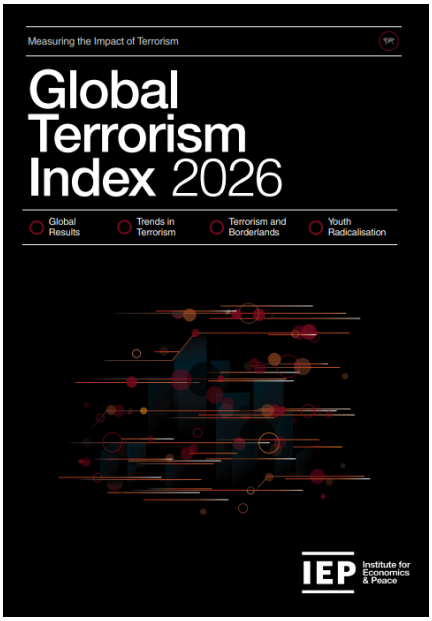
Найбільш резонансним та безпрецедентним юридичним нюансом позиції UKNF є скрупульозна деталізація правового статусу, повноважень та особистої відповідальності посадової особи, відповідальної за функцію ПВК/ФТ (AML Officer / AMLRO). Згідно з імперативними роз'ясненнями польського регулятора, внутрішні нормативні акти та політики установи повинні беззаперечно і прозоро визначати чітку архітектуру підпорядкування, межі повноважень та зону виключної відповідальності AMLRO за процеси прийняття рішень. Регулятор особливо підкреслює, що внаслідок останніх законодавчих змін у польському праві на AMLRO покладено не лише стандартні функціональні обов'язки, але й безпрецедентну за масштабами особисту фінансову відповідальність. Відтепер державний наглядовий орган наділений прямим правом накладати персональний адміністративний штраф у розмірі до 1 000 000 польських злотих (еквівалент понад 230 000 євро) не лише на членів колегіального правління установи, але й безпосередньо на AMLRO, який був персонально відповідальний за забезпечення дотримання законодавства ПВК/ФТ в установі. Ця норма безальтернативно вимагає надання такій особі статусу вищого керівництва (senior management position), що є необхідною умовою для забезпечення її абсолютної операційної незалежності від бізнес-підрозділів та гарантування безперебійного ресурсного (кадрового та технологічного) забезпечення її функції. Крім того, UKNF нагадує, що AMLRO несе не лише адміністративну, але й потенційну кримінальну відповідальність за свідоме або недбале неналежне виконання своїх статутних обов'язків. Згідно з мандатом, ця ключова посадова особа зобов'язана регулярно, на систематичній основі

Висновки:

- Впровадження концепції персональної фінансової відповідальності AMLRO (персональні штрафи до 1 млн злотих) докорінно змінює ринок праці та вимагає від фінансових установ радикального перегляду трудових контрактів, посадових інструкцій, а також обов'язкового запровадження дорогих механізмів страхування професійної відповідальності (D&O insurance) для керівників підрозділів комплаєнсу для утримання кваліфікованих кадрів.
- Імперативна вимога щодо обов'язкового залучення правління та наглядової ради до затвердження та перегляду інституційної оцінки ризиків вимагає від установ розробки глибоко адаптованих, висококонцентрованих аналітичних інформаційних систем, які б перекладали складні масиви AML-даних на мову бізнес-метрик, доступно візуалізуючи рівень ризику для топ-менеджменту.
- Чіткі параметри географічного ризику (зокрема, жорсткий поріг у 50% непрямого володіння з боку компаній з високоризикових юрисдикцій та введення критерію «систематичності» транзакцій) вимагає негайного технологічного перекалібрування автоматизованих систем скринінгу клієнтів та транзакційного моніторингу для здатності алгоритмів автоматично присвоювати найвищий бал ризику без необхідності ручного втручання та суб'єктивної оцінки аналітика.
- Жорсткі вимоги щодо інституційної незалежності «трьох ліній захисту» роблять неприпустимим суміщення функцій розробки нових бізнес-продуктів та їхнього AML-контролю в одних руках, що вимагатиме структурної та кадрової реорганізації, особливо у невеликих фінтех-компаніях (EMI/PI) та постачальниках віртуальних активів (VASP).

подавати керівному органу вичерпні, підкріплені даними звіти про поточний ландшафт ризиків та загальний рівень комплаєнсу, безпосередньо ініціювати та контролювати коригувальні дії для невідкладного усунення будь-яких виявлених під час аудитів недоліків, а також забезпечувати оперативне, безперебійне інформування органів фінансової розвідки про всі підозрілі транзакції та діяльність. Регулятор також окремо і жорстко акцентує на необхідності суворого дотримання інститутом режиму конфіденційності (anti-tipping-off rules), категорично забороняючи будь-яке, навіть непряме, розголошення клієнтам або третім особам факту передачі інформації до ПФР чи факту початку фінансового розслідування.

Децентралізація терору: Global Terrorism Index 2026 [2]



Фундаментальний звіт Global Terrorism Index (GTI) 2026, розроблений та опублікований Інститутом економіки та миру (IEP), репрезентує масштабне, концептуальне переосмислення поточної архітектури глобальної безпеки. Базуючись на великих масивах структурованих даних системи TerrorismTracker від аналітичної компанії Dragonfly, що агрегує та геолокує інформацію з відкритих джерел з січня 2007 року, методологія звіту використовує багатофакторний аналіз (із застосуванням п'ятирічних зважених коефіцієнтів) для об'єктивної оцінки впливу тероризму на 163 країни світу за чотирма індикаторами: показниками смертності, кількістю інцидентів, рівнем поранень та статистикою захоплення заручників. Фундаментальним статистичним парадоксом 2025 року, що розкривається у 13-му виданні Індексу, стало безпрецедентне в історичній перспективі падіння глобальних кількісних показників тероризму на тлі його екстремальної якісної трансформації: загальна кількість смертей у світі стрімко скоротилася на 28% (опустившись до позначки 5 582 особи), а сукупна кількість інцидентів знизилася на 22% (до 2 944 атак). Глобальне статистичне поліпшення ситуації зафіксовано у 81 країні, а середня летальність терористичних актів системно знизилася з 2,1 до 1,8 смертей на один інцидент. Причому протягом усього звітного року був практично відсутній тренд на масові мегатеракти — найбільший одиничний інцидент забрав 120 життів, що є падінням порівняно з піковими показниками попередніх років (237 у 2024 році та понад 1 100 у 2023 році). Однак цей фасадний глобальний оптимізм приховує небезпечну географічну та демографічну асиметрію: майже 70% усіх світових жертв тероризму сьогодні сконцентровано територіально лише в п'яти державах-епіцентрах (Пакистан, Буркіна-Фасо, Нігерія, Нігер та Демократична Республіка Конго). Водночас інституційний ландшафт загрози є висококонцентрованим: лише чотири домінуючі ультрарадикальні організації — «Ісламська держава» (ІД), Jamaat Nusrat Al-Islam wal Muslimeen (JNIM), «Техрік-е-Талібан Пакистан» (ТТР) та сомалійська «Аль-Шабааб» — генерують понад 70% світової смертності від терористичних актів (3 869 жертв). При цьому, на тлі загального глобального спаду, розвинені західні демократії зазнали деградації власного безпекового середовища: смертність від тероризму на Заході зросла на безпрецедентні 280% (до 57 загиблих у 2025 році), що стало прямим наслідком глибокої соціальної поляризації, сплеску антисемітизму та політичного екстремізму (про що свідчать такі резонансні інциденти, як масовий розстріл єврейських громадян на Бонді-Біч в Австралії чи таран вантажівкою в Новому Орлеані, США).

[2] https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf

Аналіз географічних зрушень доводить, що Субсахарська Африка остаточно і безповоротно закріпилася у статусі абсолютного епіцентру світового тероризму; наразі саме там розташовані шість із десяти найбільш уражених терором країн світу. Величезний, нестабільний макрорегіон Сахел сьогодні одноосібно генерує понад половину світових смертей від тероризму. Нігерія продемонструвала найбільше абсолютне світове зростання смертності (сплеск на 46%, до 750 осіб), що було жорстко каталізоване активністю угруповань ISWAP та «Боко Харам». Водночас, Південна Азія згенерувала інший тривожний феномен: Пакистан вперше в багаторічній історії Індексу посів перше місце як найбільш уражена країна світу (1 139 смертей та 1 045 інцидентів у 2025 році). Цей спалах насильства став прямим, прогнозованим геополітичним наслідком повернення режиму Талібану до влади в Афганістані у 2021 році, що спричинило безпрецедентну ескалацію транскордонної активності угруповань TTP (єдиної групи з топ-4, що показала зростання смертності) та радикальної Армії визволення Белуджистану (BLA). Ця напруга вилилася у відкритий міждержавний збройний конфлікт між Пакистаном та Афганістаном у лютому 2026 року, що створює вакуум безпеки в регіоні. Паралельно, Південна Америка (зокрема Колумбія, яка повернулася до топ-10 глобального Індексу вперше з 2013 року) згенерувала 75% усіх світових смертей від політично мотивованого тероризму. Саме тут дисидентські воєнізовані фракції FARC та ELN здійснили технологічний прорив у тактиці асиметричної війни, масово адаптувавши комерційні технології та здійснивши 77 ефективних атак із використанням безпілотних літальних апаратів (БПЛА) між 2024 та 2025 роками, прямо імплементуючи тактичний інноваційний досвід сучасної війни в Україні.

Макрорегіон / Країна	Ключові статистичні метрики та тренди	Основні драйвери та загрози
Субсахарська Африка (Сахель)	Генерує >50% світових смертей. 6 з 10 найбільш уражених країн.	Експансія афілійованих з ІД структур (ISWAP, ADF). Слабкість державних інституцій.
Пакистан (Південна Азія)	Посів **1-ше місце** у світі (1139 смертей, 1045 атак).	Транскордонні бази TTP в Афганістані. Повернення Талібану. Ескалація конфлікту.
Країни Заходу	Смертність різко зросла на **280%** (до 57 жертв у 2025 р.).	Політичний екстремізм, антисемітизм. Домінування атак «одинаків» (93%).
Близький Схід (MENA)	Історичний мінімум (падіння впливу на 15%). Смертність впала на 96% з 2015 р.	Відносне послаблення територіального контролю ІД, проте загроза ескалації конфлікту за участю Ірану залишається високою.
Південна Америка (Колумбія)	Генерує 75% політичного тероризму. Колумбія повернулася до Топ-10.	Інтеграція БПЛА-технологій (дронів) групами FARC/ELN. Злиття з наркокартелями.

Звіт IEP формалізує дві абсолютно нові критичні концепції, які визначатимуть еволюцію тероризму та протидії йому на наступні десятиліття: феномен «Прикордонних територій» та гіпершвидку, цифрову «Радикалізацію молоді». Методологія GTI 2026 чітко визначає прикордонні зони як так званий «вакуум влади», де монополія суверенної держави на легітимне насильство та правозастосування зведена до абсолютного мінімуму. Емпіричні просторові дані демонструють однозначність: 41% усіх світових терактів відбувається в радіусі 50 км від міжнародних кордонів, а 64% — у межах 100 км. Транскордонні макрорегіони

Колумбії-Венесуели, Афганістану-Пакистану та басейну озера Чад остаточно перетворилися на глобальні безпекові сірі зони, де ідеологічний тероризм органічно, взаємовигідно зрощується з транснаціональною організованою злочинністю (наркотрафіком, контрабандою зброї та людей). Концепція радикалізації молоді розкриває глибоку демографічну та технологічну кризу західних суспільств: неповнолітні та молодь до 25 років склали 42% від усіх фігурантів антитерористичних кримінальних розслідувань у Північній Америці та Європі у 2025 році (що є триразовим зростанням з 2021 року). Найбільш небезпечним висновком звіту є стиснення «часової шкали радикалізації» від кількох років ідеологічної обробки до лічених тижнів, що технологічно забезпечується на платформах соціальних мереж. При цьому психологічні та соціальні драйвери радикалізації кардинально різняться географічно: якщо на Заході 87% радикалізованих підлітків пережили психологічне насильство чи соціальну ізоляцію, то в країнах Субсахарської Африки 71% новобранців прямо вказують на систематичні, жорстокі порушення прав людини з боку самих державних силових структур як на головний, безальтернативний тригер для вступу до лав збройних екстремістських угруповань (а ще 25% вказали на тотальну відсутність економічних перспектив).

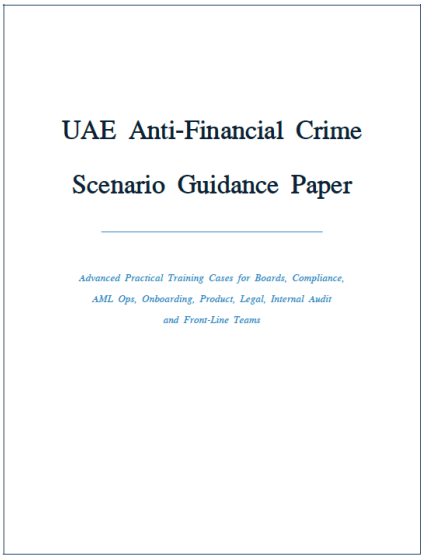
Вплив цих системних трансформацій на глобальні системи ПВК/ФТ/ФР є безпрецедентним і вимагає переоцінки існуючих парадигм. Драматичне зростання ролі «одинаків» (lone-wolf actors), які самостійно спланували та здійснили 93% усіх фатальних терористичних атак на Заході за останні п'ять років (і чиї атаки є втричі успішнішими за групові змови), повністю нівелює операційну ефективність класичного транзакційного моніторингу великих, організованих фінансових мереж та хавал. Це вимагає від фінансових установ екстреного зміщення фокусу на аналіз мікротранзакцій, використання інструментів краудфандингу та віртуальних активів. Крім того, виявлені звітом масштабні глобальні логістичні ланцюги нелегального постачання — такі як документально підтверджений канал постачання зброї від єменських повстанців-хуситів

Висновки:

- **Децентралізація ризиків ФТ вимагає від СПФМ інтеграції передових геолокаційних даних у системи скринінгу.** Особливий, посилений фокус має бути спрямований на будь-які транзакції (особливо небанківські грошові перекази, гуманітарні платежі), що надходять у "сірі" прикордонні зони країн Сахелю, Пакистану, Афганістану та Колумбії.
- **Еволюційний перехід терористичних груп (таких як FARC/ELN в Колумбії) до масового використання комерційних БПЛА створює принципово нову типологію змішаного фінансування тероризму та розповсюдження**. Підрозділи комплаєнсу великих банків повинні розширити словники моніторингу для відстеження операцій, пов'язаних із масовою закупівлею компонентів подвійного призначення (радіоелектроніка, комерційні дрони, навігаційні модулі), особливо через підставні компанії в країнах, що розвиваються.
- **Масове зростання ролі «одинаків» серед молоді в країнах Заходу (93% успішних атак) робить традиційні кількісні пороги фінансового моніторингу сліпими до таких загроз**. Необхідною є розробка нових AI-індикаторів (алгоритмів машинного навчання), які аналізують специфічні патерни мікрокредитування, донати на краудфандингових платформах, купівлю специфічних хімікатів онлайн та використання криптовалютних міксерів особами молодого віку.
- **Глибоке інституційне зрощення організованої транснаціональної злочинності та тероризму у зонах збройних конфліктів означає, що кримінальні доходи від наркотрафіку (Південна Америка) чи незаконного видобутку корисних копалин (Африка) напряму використовуються для фінансування терористичних операцій**. Це вимагає від ПФР обов'язкового поєднання традиційних індикаторів ВК та ФТ в єдині, нерозривні гібридні сценарії предикативного розслідування.

(підтримуваних Іраном) для забезпечення наступу сомалійської «Аль-Шабааб» — безальтернативно вимагають глибокого екстериторіального моніторингу торговельного фінансування та тісної координації фінансових розвідок різних континентів. Загроза інституціоналізації тероризму підкреслюється також ескалацією конфлікту за участю Ірану (після початку військової операції США та Ізраїлю в лютому 2026 року), що створює ризик остаточного перетворення іранських державних ресурсів на механізм фінансування глобальної терористичної мережі.

Управління ризиками ВК/ФТ через практичні кейси: підхід ОАЕ до навчання фінансового сектору [3]



Документ є практичним методичним посібником, спрямованим на підготовку фінансових установ, підзвітних суб'єктів та суміжних секторів до ефективного виявлення, оцінювання та реагування на ризики фінансових злочинів у системі протидії відмиванню коштів і фінансуванню тероризму. Матеріал розроблений як навчальний інструмент, що трансформує традиційні підходи до належної перевірки клієнтів і комплаєнс-контролів у реалістичні сценарії, які дозволяють перевіряти готовність організацій до складних практичних ситуацій. У вступній частині документа підкреслюється, що його метою є перехід від формального виконання вимог KYC та процедур у сфері ПВК до формування професійного судження у сфері управління ризиками фінансових злочинів. Посібник розроблений для широкого кола користувачів — членів правління та топ-менеджменту фінансових установ, працівників підрозділів обслуговування клієнтів, підрозділів комплаєнсу та фінансового моніторингу, підрозділів встановлення ділових відносин із клієнтами, юридичних департаментів, операційних підрозділів, фахівців із розробки фінансових продуктів, а також внутрішніх аудиторів і підрозділів забезпечення контролю.

Документ наголошує, що ефективна система протидії фінансовим злочинам не починається зі скринінгу санкційних списків або автоматизованих систем моніторингу транзакцій, а базується на належному корпоративному управлінні, чітко визначеній відповідальності за ризики, дисципліні прийняття клієнтів та здатності організації відмовлятися від бізнес-можливостей у випадках, коли факти або пояснення клієнта не узгоджуються між собою або не підтверджують легітимність походження коштів. У документі підкреслюється, що ключовою проблемою багатьох фінансових установ є так зване «мислення за чек-листами», коли формальна наявність документів сприймається як доказ належної перевірки клієнта, тоді як реальний аналіз ризиків і економічної сутності операцій фактично відсутній. Автори звертають увагу на те, що комерційний тиск, прагнення швидко завершити процедуру встановлення ділових відносин або укласти угоду наприкінці фінансового кварталу часто призводять до обхідних рішень, які підривають ефективність системи контролю та створюють серйозні регуляторні ризики.

У документі детально описано сучасну архітектуру системи протидії фінансовим злочинам в Об'єднаних Арабських Еміратах. Основу цієї системи становить федеральна нормативно-правова база, зокрема Federal Decree-Law No. 10 of 2025 on Combatting Money Laundering,

[3] https://media.licdn.com/dms/document/media/v2/D4D1FAQHP1VtNFldMLg/feedshare-document-pdf-analyzed/B4DZzkh1WOGQAc-/0/1773360602802?e=1774483200&v=beta&t=xvnHzS5mcwuD7hHRTFyZVN9nzCcOidmg0lkvBXcWhl0

Combatting the Financing of Terrorism and Illegal Organisations, а також Cabinet Resolution No. 134 of 2025, яка встановлює виконавчі правила реалізації цього закону. Ці акти формують базові вимоги для всіх підзвітних суб'єктів, включаючи процедури належної перевірки клієнтів, ідентифікацію бенефіціарних власників, контроль політично значущих осіб, механізми подання повідомлень про підозрілі операції, вимоги щодо внутрішніх політик і процедур, оцінку ризиків нових технологій та збереження документів. Водночас національна система доповнюється галузевими регуляторними рамками, які застосовуються різними наглядовими органами залежно від типу фінансової діяльності. До таких органів належать Центральний банк ОАЕ (CBUAE), який регулює банки, платіжні установи та фінансові компанії; Управління фінансових послуг Дубая (DFSA), що здійснює нагляд у фінансовому центрі DIFC; Орган регулювання фінансових послуг (FSRA), який виконує функції нагляду в міжнародному фінансовому центрі ADGM; Орган регулювання віртуальних активів (VARA), що регулює сектор віртуальних активів; а також регулятори ринку цінних паперів і органи, що здійснюють нагляд за визначеними нефінансовими установами та професіями. Документ наголошує, що для правильного застосування вимог ПВК/ФТ фінансові установи повинні одночасно враховувати як федеральні норми, так і специфічні правила галузевого регулятора, що застосовуються до конкретної бізнес-моделі.

Особливе місце у структурі документа займає концепція десяти ключових принципів, які визначають базові вимоги до системи комплаєнсу у сфері протидії фінансовим злочинам. Ці принципи формують основу управління ризиками та підкреслюють, що жодні комерційні інтереси не можуть виправдовувати порушення процедур належної перевірки клієнтів. Серед них виділяється правило, що без завершеної процедури CDD неможливо встановлювати ділові відносини, а також принцип, що визначення бенефіціарного власника не повинно обмежуватися лише формальним аналізом часток участі, оскільки контроль над компанією може здійснюватися через угоди акціонерів, фінансовий вплив, право призначення керівництва або інші механізми. Документ також наголошує на важливості незалежності комплаєнс-функції у прийнятті рішень щодо подання повідомлень про підозрілі операції, заборони розголошення інформації клієнту про проведення розслідування або подання повідомлення до фінансової розвідки, а також необхідності оцінки ризиків нових фінансових продуктів, каналів обслуговування та технологій до їх впровадження.

Для практичного застосування цих принципів у документі запропоновано структуровану модель реагування на підозрілі або ризикові ситуації. Ця модель передбачає п'ять послідовних етапів: стабілізацію ситуації, що включає призупинення операцій або встановлення ділових відносин у випадку виявлення ризиків; верифікацію інформації шляхом незалежної перевірки документів і даних; повторну оцінку ризику з урахуванням нових фактів; ескалацію питання до відповідних органів управління ризиками або керівництва; а також прийняття остаточного рішення з детальною фіксацією доказів, аргументації та відповідальних осіб. Автори підкреслюють, що ключовим елементом ефективного контролю є документування процесу прийняття рішень, оскільки регулятори під час перевірок оцінюють не лише результат, але й логіку та обґрунтування прийнятих рішень.

Основна частина документа присвячена аналізу двадцяти одного практичного сценарію, які відображають реальні ризики та типові помилки у сфері протидії фінансовим злочинам. Ці сценарії охоплюють широкий спектр ситуацій, починаючи від складних корпоративних структур із використанням офшорних компаній та номінальних акціонерів і закінчуючи сучасними ризиками, пов'язаними з криптоактивами, цифровими каналами обслуговування та новими технологіями. Наприклад, один із сценаріїв описує ситуацію, коли компанія намагається пройти процедуру онбордингу перед завершенням фінансового кварталу, маючи складну структуру власності через офшорні холдингові компанії, а менеджери з продажу тиснуть на комплаєнс-підрозділ із вимогою тимчасово прийняти неповний пакет документів. Документ підкреслює,

що у таких випадках правильним рішенням є зупинення процесу встановлення ділових відносин до завершення належної перевірки та встановлення реальних бенефіціарних власників.

Інший сценарій аналізує ситуацію, коли корпоративна структура побудована таким чином, що жоден акціонер формально не володіє більше ніж 25% акцій, але один із учасників фактично контролює компанію через акціонерну угоду та право призначення членів ради директорів. Документ наголошує, що у таких випадках контроль повинен визначатися не лише через формальні пороги володіння, а й через реальний вплив на управління компанією. Окремі сценарії присвячені використанню трастів і фондів для приховування бенефіціарного володіння, ризикам, пов'язаним із рахунками з об'єднаними коштами клієнтів, а також ситуаціям, коли клієнт набуває статусу політично значущої особи після встановлення ділових відносин, що потребує перегляду ризикового профілю та проведення посиленої перевірки.

Важливе місце в документі займають сценарії, пов'язані з новими технологіями та цифровими активами. Зокрема, розглядаються випадки, коли клієнти заявляють, що їхні кошти походять від інвестицій у криптовалюти, але аналіз блокчейн-транзакцій показує використання міксерів і анонімних гаманців, що може свідчити про спробу приховати походження активів. У таких випадках фінансовим установам рекомендується використовувати спеціалізовані інструменти блокчейн-аналітики, перевіряти історію транзакцій і оцінювати ризики взаємодії з непідконтрольними або анонімними гаманцями. Інший сценарій демонструє, як клієнти можуть навмисно здійснювати численні транзакції трохи нижче встановленого регуляторного порогу для уникнення вимог щодо передачі інформації про відправника і отримувача, що є типовою схемою обходу так званого правила передачі інформації про платника та отримувача під час переказу коштів (Travel Rule).

Документ також приділяє значну увагу ризикам фінансування розповсюдження зброї масового знищення та обходу санкцій, особливо у сфері торговельного фінансування. Сценарії описують ситуації, коли компанії здійснюють операції з товарами подвійного призначення через складні логістичні маршрути або використовують посередників для приховування кінцевого отримувача продукції. Автори наголошують, що у таких випадках формальна наявність документів не є достатнім доказом легітимності операції, і фінансові установи повинні аналізувати

Висновки:

- **Належна перевірка клієнта має передувати будь-яким операціям або встановленню ділових відносин.** Будь-які спроби прискорити встановлення ділових відносин через комерційний тиск або неповну документацію повинні розглядатися як порушення базових вимог ПВК/ФТ і можуть призвести до регуляторних санкцій.
- **Формальні пороги володіння не гарантують відсутності контролю над компанією.** Фінансові установи повинні аналізувати фактичний контроль через угоди акціонерів, фінансовий вплив або управлінські повноваження, застосовуючи поглиблену перевірку навіть тоді, коли частка власності кожного акціонера формально нижча за 25%.
- **Сучасні ризики ПВК/ФТ пов'язані з цифровими активами, структурованими транзакціями та новими технологіями.** Фінансові установи повинні використовувати блокчейн-аналітику, аналіз пов'язаних гаманців та контроль порогових транзакцій для виявлення спроб обходу регуляторних вимог.
- **Ефективність системи ПВК/ФТ залежить від корпоративного управління та культури комплаєнсу.** Ключові рішення — зокрема щодо подання повідомлень про підозрілі операції, заморожування активів або припинення ділових відносин — повинні прийматися незалежними комплаєнс-підрозділами, а не підрозділами обслуговування клієнтів.

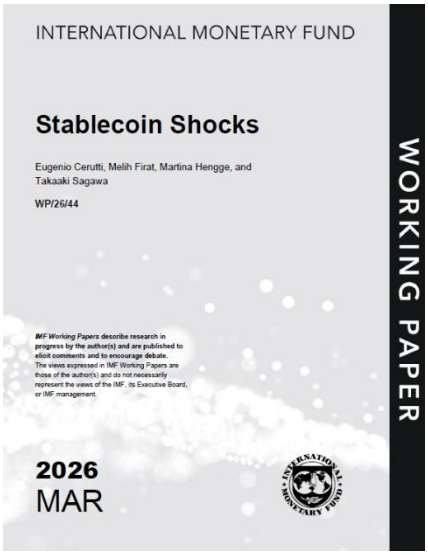
економічну логіку угоди, кінцеве використання товарів і ризики, пов'язані з контрагентами та юрисдикціями.

Окрім аналізу ризиків, документ також звертає увагу на внутрішні слабкі місця системи комплаєнсу. Наприклад, описуються ситуації, коли керівництво компанії пропонує зменшити чутливість систем моніторингу транзакцій для зменшення кількості сповіщень, або коли компанія покладається на проведення належної перевірки клієнтів іншими підрозділами групи в юрисдикціях із нижчими стандартами прозорості. У таких випадках підкреслюється, що відповідальність за дотримання вимог законодавства завжди залишається за установою, яка покладається на результати перевірки третьої сторони.

Завершальна частина документа містить довідкову таблицю ключових правових норм законодавства ОАЕ, які найчастіше застосовуються у сфері протидії відмиванню коштів і фінансуванню тероризму. Серед них — положення щодо належної перевірки клієнтів, визначення бенефіціарних власників, контролю політично значущих осіб, подання повідомлень про підозрілі операції, заборони розголошення інформації клієнту, вимог до внутрішніх систем контролю, оцінки ризиків нових технологій, ведення документації, а також правил щодо кореспондентських банківських відносин і передачі інформації у платіжних операціях. Документ підкреслює, що ефективна система протидії фінансовим злочинам повинна поєднувати нормативні вимоги з практичними механізмами прийняття рішень, здатними працювати навіть у ситуаціях високого комерційного тиску або обмеженого часу.

Таким чином, посібник формує комплексну навчальну модель, яка дозволяє фінансовим установам розвивати здатність до аналізу складних ризикових ситуацій, приймати обґрунтовані рішення щодо управління ризиками фінансових злочинів та забезпечувати відповідність вимогам сучасних міжнародних стандартів у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

Від крипторинку до державних облігацій: як зростання стейблкоїнів впливає на глобальні фінансові ринки [4]



Документ, підготовлений експертами Міжнародного валютного фонду, присвячений емпіричному дослідженню впливу розвитку ринку стейблкоїнів на традиційні фінансові ринки, насамперед на ринок державних облігацій США, валютний курс долара, фондові індекси та криптовалютний сектор. У роботі автори намагаються вирішити ключову наукову проблему сучасної фінансової економіки — визначити, чи має швидке поширення стейблкоїнів реальні макрофінансові наслідки та чи можуть вони виступати новим каналом передачі фінансових шоків між криптовалютною екосистемою та традиційною фінансовою системою.

У вступній частині дослідження автори підкреслюють, що за останні кілька років стейблкоїни стали одним із найбільш динамічних сегментів криптофінансової екосистеми. Спочатку вони використовувалися переважно як інструмент для здійснення розрахунків між криптовалютними біржами та трейдерами, однак поступово їхня функціональність розширилася і вони почали застосовуватися у міжнародних платежах, у секторі децентралізованих фінансів та у процесах токенізації фінансових активів. У роботі зазначається,

[4] https://www.imf.org/-/media/files/publications/wp/2026/english/wpiea2026044-source-pdf.pdf

що загальна ринкова капіталізація основних стейблкоїнів, насамперед Tether (USDT) і USD Coin (USDC), зросла з менш ніж 5 млрд доларів у 2019 році до понад 300 млрд доларів у жовтні 2025 року, що свідчить про їхню дедалі більшу роль у глобальній фінансовій системі. Паралельно із цим у провідних юрисдикціях почали формуватися спеціалізовані регуляторні рамки для таких інструментів, зокрема регламент MiCA у Європейському Союзі, який набув чинності у 2024 році, а також законодавча ініціатива GENIUS Act у США, ухвалена у 2025 році.

Однією з головних дослідницьких проблем, яку намагаються вирішити автори, є складність ідентифікації так званих шоків попиту на стейблкоїни. На відміну від традиційних фінансових активів, ціна стейблкоїнів майже не змінюється, оскільки вони підтримують прив'язку до базового активу (переважно долара США). Тому класичні підходи до аналізу фінансових шоків, що ґрунтуються на коливаннях цін активів, у цьому випадку не працюють. Для подолання цієї проблеми автори пропонують альтернативний підхід, який базується на аналізі змін ринкової капіталізації стейблкоїнів. Оскільки ціна стейблкоїнів залишається стабільною, зміни їхньої ринкової капіталізації фактично відображають процеси емісії та погашення токенів і, відповідно, зміни попиту на ці інструменти. Саме такі зміни автори трактують як шоки попиту на стейблкоїни.

Для ідентифікації таких шоків у дослідженні застосовано інноваційну методологію, яка поєднує кілька економетричних підходів. Передусім автори формують спеціальний наративний набір даних, що включає новинні події, пов'язані зі стейблкоїнами, починаючи з 2019 року. Для цього використовується систематичний аналіз новинних повідомлень Google News із застосуванням ключових слів, пов'язаних зі стейблкоїнами, таких як «stablecoin», «USDC», «USDT» тощо. Кожну новину було проаналізовано вручну з метою визначення того, чи є вона подією, що виникла безпосередньо всередині екосистеми стейблкоїнів і не була спричинена ширшими макроекономічними або фінансовими процесами. У результаті такого аналізу було ідентифіковано 50 ключових подій, серед яких — регуляторні заяви, партнерства між фінансовими компаніями, технологічні інновації, запуск нових сервісів або інфраструктурних рішень. До таких подій, наприклад, належали заяви керівництва Федеральної резервної системи щодо регулювання стейблкоїнів, ухвалення законодавчих ініціатив, інтеграція стейблкоїнів у платіжні системи або партнерства між великими криптовалютними платформами та фінансовими компаніями.

На основі цього набору подій автори аналізують зміни ринкової капіталізації стейблкоїнів у короткому часовому вікні після появи відповідних новин. Для цього використовується високочастотний аналіз даних, який дозволяє зафіксувати реакцію фінансових ринків протягом одного дня після події. При цьому застосовується метод гетероскедастичної ідентифікації, який дозволяє відокремити ефект саме стейблкоїн-шоку від інших факторів, що можуть впливати на фінансові ринки. Такий підхід дозволяє оцінити причинно-наслідковий вплив змін попиту на стейблкоїни на ключові фінансові показники.

Окрім короткострокового аналізу подій, у дослідженні також застосовується структурна векторна авторегресійна модель (SVAR) із зовнішніми інструментами, що дає змогу оцінити динамічні ефекти стейблкоїн-шоків у більш довгостроковій перспективі. У межах цієї моделі аналізується взаємозв'язок між змінами ринкової капіталізації стейблкоїнів та такими змінними, як дохідність короткострокових державних облігацій США, фондові індекси, індекс долара та індекси криптовалютного ринку. Для перевірки надійності отриманих результатів автори також використовують альтернативний метод ідентифікації шоків — max-share identification, який дозволяє визначати структурні шоки без використання наративного відбору новинних подій. Застосування двох незалежних методів ідентифікації шоків забезпечує високу надійність отриманих результатів і дозволяє переконатися, що виявлені ефекти не є наслідком методологічних обмежень.

Емпіричні результати дослідження свідчать про те, що зростання попиту на стейблкоїни має відчутний вплив на фінансові ринки, насамперед на ринок короткострокових державних облігацій США. Автори встановили, що шок попиту на стейблкоїни, який призводить до збільшення їхньої ринкової капіталізації приблизно на один відсоток, спричиняє зниження дохідності одномісячних казначейських векселів приблизно на 1,9 базисного пункту. Такий ефект пояснюється тим, що значна частина резервів емітентів стейблкоїнів інвестується саме у короткострокові державні облігації США. Збільшення попиту на стейблкоїни означає необхідність випуску нових токенів, що, у свою чергу, потребує збільшення обсягу резервних активів, серед яких ключову роль відіграють короткострокові казначейські папери. Відповідно, емісія стейблкоїнів створює додатковий попит на ці активи, що призводить до зниження їхньої дохідності.

Висновки:

- **Зростання попиту на стейблкоїни безпосередньо впливає на ринок державних облігацій США.** Збільшення капіталізації стейблкоїнів на 1% знижує доходність короткострокових казначейських векселів приблизно на 1,9 базисного пункту, оскільки резерви стейблкоїнів інвестуються у T-bills.
- **Стейблкоїни створюють новий канал передачі фінансових шоків між крипторинком і традиційною фінансовою системою.** Зростання їхнього використання викликає ефекти поширення на валютний ринок, криптоактиви та фондові індекси.
- **Ринки не розглядають стейблкоїни як негайну загрозу банківській системі.** Дослідження не виявило статистично значущого впливу шоків стейблкоїнів на акції банків, що свідчить про відсутність очікувань масштабної дезінтермедіації депозитів.
- **Основними бенефіціарами зростання стейблкоїнів є платіжні та криптоінфраструктурні компанії.** Акції компаній, які інтегрують стейблкоїн-платежі або пов’язані з криптовалютною інфраструктурою, демонструють позитивну реакцію на збільшення попиту на стейблкоїни.

Дослідження також демонструє, що ефекти поширюються за межі ринку державних облігацій. Зокрема, зростання попиту на стейблкоїни супроводжується помірним зниженням курсу долара США, що пов’язано з глобальною перебалансировкою інвестиційних портфелів у відповідь на зміну дохідності американських активів. Крім того, виявлено позитивний вплив на криптовалютні індекси, що пояснюється тим, що стейблкоїни часто використовуються як базовий інструмент для купівлі інших криптоактивів. Зростання їхньої пропозиції полегшує доступ до криптовалютних ринків і стимулює попит на інші криптоактиви. Водночас вплив на фондовий ринок виявився відносно обмеженим: індекс S&P 500 демонструє лише незначне зростання, яке не має істотного економічного значення.

Окремий напрям аналізу присвячений впливу стейблкоїнів на різні типи компаній. Дослідження показує, що зростання попиту на стейблкоїни позитивно впливає на компанії, які активно інтегрують їх у свою платіжну інфраструктуру. До таких компаній належать платіжні провайдери та криптовалютні платформи, зокрема PayPal, Square або Coinbase. Їхні акції демонструють статистично значущу позитивну реакцію на збільшення ринкової капіталізації стейблкоїнів. Натомість акції традиційних банків, включаючи як великі банки, так і банки спільнот, не демонструють значущих змін. Це свідчить про те, що фінансові ринки наразі не оцінюють стейблкоїни як серйозну загрозу банківській системі або як фактор, що може призвести до масштабного відтоку депозитів із банків.

У завершальній частині дослідження автори підкреслюють, що стейблкоїни поступово стають важливим елементом глобальної фінансової інфраструктури та формують новий канал передачі фінансових шоків між криптовалютною екосистемою та традиційними фінансовими ринками. З

огляду на це, регуляторні рішення щодо випуску та використання стейблкоїнів можуть мати значні макрофінансові наслідки, зокрема для ринку державних облігацій, валютних курсів і фінансової стабільності. Автори наголошують, що подальше зростання ролі стейблкоїнів у платіжних системах та токенізованих фінансових сервісах потребує більш системного моніторингу з боку регуляторів та центральних банків, оскільки їхній вплив на традиційну фінансову систему може посилюватися в міру інтеграції криптовалютних технологій у глобальну фінансову архітектуру.

Інноваційні технології у боротьбі з незаконними фінансовими потоками цифрових активів: підхід Міністерства фінансів США [5]

Аналітичний звіт Міністерства фінансів США, підготовлений на виконання вимог GENIUS Act 2025, являє собою комплексне дослідження ролі інноваційних технологій у протидії незаконним фінансовим потокам, пов'язаним із використанням цифрових активів, і водночас формує стратегічне бачення подальшого розвитку системи ПВК /ФТ у цифровій економіці.

У документі вихідною тезою є визнання того, що цифрові активи стали невід'ємною складовою глобальної фінансової інфраструктури та драйвером інновацій, однак їхні технологічні характеристики — швидкість транзакцій, глобальність, псевдоанонімність і децентралізована природа — одночасно створюють сприятливе середовище для незаконної діяльності. Міністерство фінансів США підкреслює, що ефективна протидія таким ризикам не може ґрунтуватися виключно на традиційних інструментах фінансового моніторингу, а потребує інтеграції новітніх технологій, які дозволяють працювати з великими обсягами даних, складними транзакційними структурами та новими моделями поведінки злочинців.

Значна частина звіту присвячена оцінці ризиків, пов'язаних із використанням цифрових активів у незаконних цілях. У документі фіксується суттєве зростання обсягів транзакцій у блокчейн-мережах, що супроводжується розширенням участі традиційних фінансових установ у криптоекосистемі, включаючи надання кастодіальних послуг, випуск фінансових інструментів і створення стейблкоїнів. Водночас підкреслюється, що розширення ринку супроводжується пропорційним зростанням ризиків ВК/ФТ, оскільки цифрові активи активно використовуються для переміщення незаконних доходів, фінансування злочинних мереж і обходу санкцій. Особливо небезпечними визнаються схеми, пов'язані з транснаціональними злочинними організаціями, кіберзлочинністю, кібератаками із використанням програм-вимагачів, шахрайством та діяльністю державних суб'єктів, зокрема КНДР, яка системно використовує криптоактиви для фінансування своїх військових програм.

Окремий акцент робиться на стрімкому зростанні шахрайських схем у сфері цифрових активів, зокрема інвестиційного шахрайства, яке характеризується високим рівнем організованості та використанням соціальної інженерії. У документі підкреслюється, що злочинні мережі функціонують як масштабні індустріальні структури, які використовують цифрові платформи для залучення жертв, а також спеціалізовану інфраструктуру для обробки та відмивання коштів.

[5] https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf

Значні обсяги фінансових втрат, зафіксовані у цій сфері, демонструють системний характер загрози та необхідність технологічного переосмислення підходів до її протидії.

У межах аналізу вразливостей звіт визначає ключові структурні проблеми глобальної системи регулювання цифрових активів. Центральною з них є регуляторний арбітраж, який виникає внаслідок нерівномірності або відсутності вимог ПВК/ФТ у різних юрисдикціях. Це дозволяє провайдерам послуг, пов'язаних із цифровими активами, а також злочинним суб'єктам використовувати юрисдикції з низьким рівнем контролю для здійснення операцій, які фактично пов'язані з більш жорстко регульованими ринками. Додатковим фактором ризику є складні корпоративні структури таких провайдерів, що ускладнює їх нагляд і створює прогалини у відповідальності.

Звіт також детально розглядає проблему недотримання суб'єктами ринку вимог законодавства, зокрема щодо реєстрації, ідентифікації клієнтів і виконання санкційних обмежень. Особливу увагу приділено таким інструментам, як криптовалютні кіоски, які, незважаючи на свою доступність і зручність, стали каналом для здійснення шахрайських операцій через низький рівень комплаєнсу. Це свідчить про те, що технологічна доступність без належного регуляторного контролю може значно посилювати ризики незаконної діяльності.

Критично важливим аспектом звіту є аналіз засобів ускладнення відстеження транзакцій, які використовуються для приховування походження коштів. До них належать міксери, тумблери, технології міжмережевого перенесення активів (bridging) та обміну цифрових активів (swapping), які дозволяють розривати зв'язок між первинним джерелом коштів і їх кінцевим використанням. У документі підкреслюється, що такі інструменти значно ускладнюють розслідування та відстеження фінансових потоків, особливо коли вони використовуються у комбінації з іншими технологіями, включаючи децентралізовані фінансові сервіси. Водночас наголошується, що навіть у цих умовах певні технологічні рішення дозволяють частково відновлювати транзакційні зв'язки, що підкреслює важливість розвитку аналітичних інструментів.

Важливе місце у звіті займає аналіз регуляторної архітектури США, яка базується на Bank Secrecy Act і була модернізована в межах AML Act 2020 з урахуванням розвитку цифрових активів. У документі підкреслюється, що підхід США залишається технологічно нейтральним і

Висновки:

- **Інноваційні технології стають ключовим інструментом боротьби з фінансовими злочинами у сфері цифрових активів.** Штучний інтелект, блокчейн-аналітика та цифрова ідентифікація дозволяють фінансовим установам швидше виявляти складні схеми ВК/ФТ, знижувати кількість хибних спрацювань і автоматизувати комплаєнс-процеси.
- **Штучний інтелект, блокчейн-аналітика та цифрова ідентифікація дозволяють фінансовим установам швидше виявляти складні схеми ВК/ФТ, знижувати кількість хибних спрацювань і автоматизувати комплаєнс-процеси.** Особливо значну загрозу становлять кібероперації КНДР, масштабні криптошахрайства та атаками із застосуванням програм-вимагачів, що генерують мільярдні доходи у цифрових активах.
- **Державні та організовані злочинні суб'єкти активно використовують криптоінфраструктуру.** Розмір штрафів та механізми їх стягнення повинні бути приведені у відповідність до міжнародних стандартів, щоб антиконкурентні практики стали економічно невигідними.
- **Подальша ефективність системи ПВК/ФТ залежить від інтеграції технологій і міжнародної координації.** Необхідні гармонізація стандартів, розвиток цифрової ідентичності, міжнародний обмін даними та підтримка інноваційних рішень у фінансовому секторі.

ризик-орієнтованим, що дозволяє фінансовим установам самостійно визначати інструменти виконання вимог, зосереджуючи ресурси на найбільш ризикових сегментах. Такий підхід розглядається як ключовий для забезпечення балансу між інноваціями та ефективним контролем.

Центральною частиною звіту є аналіз інноваційних технологій, які можуть суттєво посилити ефективність системи ПВК/ФТ. Зокрема, штучний інтелект розглядається як інструмент, здатний трансформувати підходи до фінансового моніторингу за рахунок автоматизації аналізу транзакцій, виявлення складних патернів і скорочення часу обробки інформації. Особливу роль відіграють генеративні моделі, які можуть працювати з неструктурованими даними, здійснювати аналіз медіа-контенту та допомагати у формуванні аналітичних висновків. Водночас підкреслюється, що використання таких технологій пов'язане з ризиками, зокрема щодо прозорості рішень, якості даних і потенційної упередженості алгоритмів.

Окремий блок присвячений цифровій ідентичності як інструменту підвищення ефективності процедур ідентифікації та верифікації клієнтів. У звіті наголошується, що сучасні рішення у цій сфері дозволяють поєднати високий рівень безпеки з мінімізацією збору персональних даних, використовуючи криптографічні механізми та біометричні технології. Розвиток цифрової ідентичності розглядається як ключовий фактор зниження рівня шахрайства та підвищення довіри до фінансової системи, особливо у контексті цифрових активів і децентралізованих фінансових сервісів.

Блокчейн-аналітика визначається як один із найбільш практичних інструментів, який уже активно використовується фінансовими установами та державними органами. Завдяки відкритості блокчейн-даних такі інструменти дозволяють здійснювати відстеження транзакцій, ідентифікацію ризикових адрес і аналіз поведінкових патернів. Це створює унікальні можливості для фінансового моніторингу, які відсутні у традиційних фінансових системах.

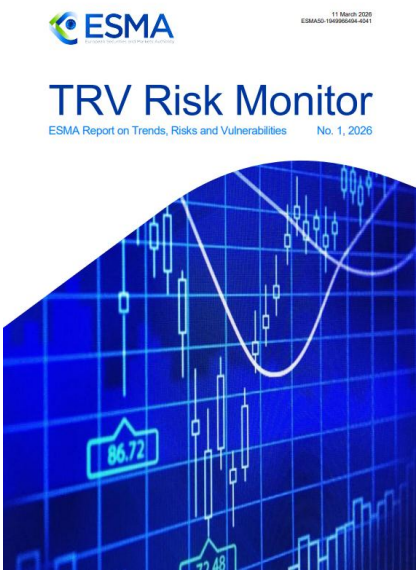
Завершальна частина звіту формує стратегічні пріоритети державної політики США у цій сфері, серед яких — підтримка впровадження інновацій у фінансовому секторі, розвиток партнерства між державою і приватним сектором, а також міжнародна координація та гармонізація стандартів. Підкреслюється, що лише комплексний підхід, який поєднує технологічні інновації, ефективне регулювання та міжнародну співпрацю, здатний забезпечити належний рівень протидії незаконним фінансовим потокам у цифровій економіці.

Таким чином, документ не лише аналізує поточні ризики та інструменти їх нейтралізації, а й формує концептуальну модель майбутньої системи ПВК/ФТ, у якій ключову роль відіграватимуть технології, здатні адаптуватися до швидко змінюваного характеру фінансових злочинів у сфері цифрових активів.

Фінансові ринки ЄС у 2026 році: ключові ризики, тенденції та вразливості за оцінкою ESMA [6]

Звіт, підготовлений Європейським органом з цінних паперів та ринків (ESMA), є комплексним аналітичним дослідженням стану фінансових ринків Європейського Союзу, яке оцінює ключові тенденції, системні ризики та структурні вразливості у сфері ринків капіталу, управління активами, фінансових інфраструктур та інноваційних фінансових технологій. Документ охоплює розвиток подій у другій половині 2025 року та на початку 2026 року і спрямований на оцінку факторів, що можуть впливати на фінансову стабільність, ефективність функціонування ринків та захист інвесторів.

[6] https://www.esma.europa.eu/sites/default/files/2026-03/ESMA50-1949966494-4041_TRV_Risk_Monitor_1_2026.pdf



У звіті підкреслюється, що глобальне фінансове середовище залишається складним і характеризується поєднанням макроекономічної невизначеності, геополітичних ризиків та структурних змін у фінансовій системі. У другій половині 2025 року світові фондові ринки досягли історично високих рівнів оцінки активів, що посилило ризики формування нестійких цінових рівнів та потенційно різких корекцій. Незважаючи на часткове зниження оцінок після короткострокових коливань, рівень ринкових оцінок залишається високим, що створює ризик поширення шоків між різними сегментами фінансових ринків. Посилення міжсекторальної взаємозалежності активів обумовлює зростання ризику ефекту фінансового зараження, який полягає у трансмісії шоків між різними сегментами фінансової системи.

Макроекономічне середовище, у якому функціонують фінансові ринки, характеризується помірними темпами економічного зростання та збереженням певних інфляційних ризиків. Прогнози міжнародних фінансових організацій свідчать, що глобальне економічне зростання у 2026 році становитиме приблизно 3,3 %, тоді як економіка Європейського Союзу демонструє слабшу динаміку. Водночас очікується, що інфляція поступово стабілізується біля цільових значень центральних банків. Однак геополітичні фактори, включаючи торговельні конфлікти, зміни у тарифній політиці та триваючі регіональні конфлікти, залишаються джерелом нестабільності. Зокрема, напруженість у торговельних відносинах між США та Китаєм, а також інші геополітичні події можуть спричиняти різкі коливання на фінансових ринках і впливати на динаміку капіталовкладень.

Суттєвим фактором ризику залишається зростання державного боргу. За прогнозами Європейської комісії, співвідношення державного боргу до валового внутрішнього продукту в Європейському Союзі може зрости з приблизно 82 % у 2024 році до близько 85 % у 2027 році. У деяких державах-членах цей показник може перевищити 100 % ВВП, що підвищує вразливість державних фінансів до змін процентних ставок і макроекономічних шоків. У США аналогічні занепокоєння пов’язані з бюджетною політикою та зростанням дефіциту бюджету. У сукупності ці фактори створюють довгострокові ризики для стабільності глобальної фінансової системи.

Аналіз ринків цінних паперів показує, що у 2025 році світові фондові індекси демонстрували значне зростання, яке значною мірою було зумовлене технологічним сектором і швидким розвитком компаній, пов’язаних із штучним інтелектом. У США зростання ринкової капіталізації технологічних компаній спричинило значну концентрацію ринку, що підвищує ризик утворення фінансових бульбашок. У Європі зростання фондових індексів також було значним, хоча менш інтенсивним, ніж у США. Особливо високі темпи зростання спостерігалися у банківському секторі, де підвищення прибутковості банків та зниження частки проблемних кредитів сприяли зростанню оцінок акцій фінансових установ. Водночас підвищення коефіцієнтів ціни до прибутку на фондових ринках сигналізує про підвищений ризик корекції у разі погіршення економічних умов або зміни очікувань інвесторів.

Ситуація на ринку облігацій характеризується відносною стабільністю, хоча певні ознаки напруженості все ж спостерігаються. Доходності державних облігацій у країнах єврозони дещо зросли, але залишаються близькими до історичних середніх значень. Водночас спреди між доходностями облігацій різних держав-членів загалом звузилися, що свідчить про відносно стабільні очікування інвесторів. Однак політична нестабільність у деяких країнах, зокрема у Франції, спричинила тимчасове підвищення доходностей державних облігацій. На

корпоративному борговому ринку спостерігається зниження кредитних спредів, що відображає високий попит інвесторів на ризикові активи.

Особливу увагу у звіті приділено ризикам, пов'язаним із розвитком ринку приватного кредитування. Цей сегмент фінансового ринку швидко розширюється і характеризується відносно низьким рівнем прозорості та високою взаємозалежністю з іншими фінансовими інститутами. Події 2025 року, зокрема фінансові проблеми окремих компаній у США, продемонстрували, що збитки у сегменті приватного кредиту можуть швидко поширюватися на інші фінансові установи. Через складні структури фінансування та використання позабалансових інструментів існує ризик, що негативні події у цьому сегменті можуть мати системний характер.

Важливою темою звіту є розвиток ринку криптоактивів. У 2025 році криптовалютний ринок пережив значне зростання, досягнувши ринкової капіталізації майже 3,9 трильйона євро. Проте у жовтні 2025 року відбулося різке падіння ринку, відоме як «flash crash», унаслідок якого ринкова капіталізація криптовалют зменшилася приблизно на 30 % протягом кількох місяців. Ця подія була спричинена поєднанням макроекономічних факторів та структурних особливостей крипторинку, включаючи високий рівень кредитного плеча та автоматичні механізми ліквідації позицій на ринку деривативів. Крім того, під час цього обвалу виявилися технічні проблеми на криптовалютних біржах, що посилило панічні настрої серед інвесторів.

Незважаючи на волатильність криптовалют, сегмент стейблкоїнів продовжує активно розвиватися. До кінця 2025 року загальна капіталізація стейблкоїнів досягла приблизно 269 млрд євро. Ці активи дедалі частіше використовуються як інструмент ліквідності та хеджування ризиків у криптовалютному секторі. Однак їх швидке зростання створює нові ризики для фінансової стабільності, оскільки резервні активи стейблкоїнів часто пов'язані з традиційними фінансовими інструментами. Таким чином, проблеми у криптовалютному секторі можуть передаватися до традиційної фінансової системи.

Звіт також детально аналізує сектор управління активами. Активи під управлінням європейських інвестиційних фондів продовжували зростати, досягнувши понад 21 трильйон євро. Проте значна частина цього зростання була зумовлена не притоком нових інвестицій, а підвищенням вартості активів унаслідок зростання фондових ринків. Важливим фактором є зростання частки американських акцій у портфелях європейських фондів, що підвищує їх залежність від динаміки фондового ринку США. У разі різкого падіння американських фондових індексів це може призвести до значних втрат для європейських інвесторів.

Висновки:

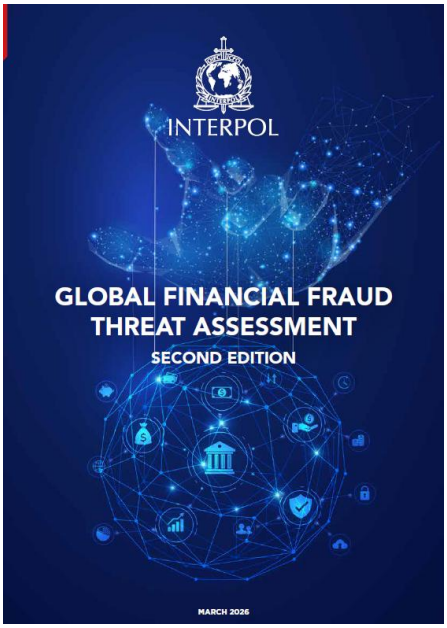
- **Завищені оцінки активів створюють ризик різких корекцій фінансових ринків.** Фінансовим регуляторам і інституційним інвесторам доцільно посилити моніторинг ринкових оцінок, особливо в технологічному секторі та сегменті AI-компаній, а також проводити регулярні стрес-тести портфелів.
- **Ринок приватного кредиту стає потенційним джерелом системних ризиків.** Необхідне посилення прозорості, регуляторного нагляду та стандартів розкриття інформації щодо структури кредитів, рейтингових оцінок і взаємозв'язків з банківським сектором.
- **Зростання ролі стейблкоїнів підвищує взаємозалежність крипто- та традиційних фінансових ринків.** Регулятори мають розробити узгоджені міжнародні правила щодо резервів, ліквідності та управління ризиками стейблкоїнів, щоб мінімізувати потенційні системні ефекти.
- **Кіберризики та залежність від критичної IT-інфраструктури стають ключовою загрозою для фінансової стабільності.** Фінансовим установам і регуляторам необхідно розширювати механізми операційної стійкості, включаючи нагляд за постачальниками ІКТ-послуг, стрес-тестування кіберризиків та підвищення стандартів інцидент-репортингу.

У сфері поведінки інвесторів спостерігається активне залучення роздрібних інвесторів до фінансових ринків, зокрема через цифрові торговельні платформи. Хоча це сприяє розширенню доступу до інвестицій, існує ризик, що недостатньо досвідчені інвестори можуть приймати необґрунтовані рішення. Важливим фактором є також вплив соціальних мереж на інвестиційну поведінку, що може призводити до формування спекулятивних бульбашок або масових коливань ринкових цін.

Окремий розділ звіту присвячений операційним ризикам та кіберзагрозам. Фінансовий сектор дедалі частіше стає мішенню кібератак, а залежність від великих технологічних постачальників послуг, таких як хмарні провайдери, створює додаткові ризики. Наприклад, збій у роботі Amazon Web Services у жовтні 2025 року вплинув на роботу кількох криптовалютних платформ і продемонстрував потенційну вразливість фінансових систем до технічних збоїв.

Крім того, у звіті розглядаються довгострокові структурні зміни у фінансовій системі, зокрема розвиток сталого фінансування, токенізації активів та використання штучного інтелекту. Хоча впровадження цих технологій поки що залишається обмеженим, вони можуть суттєво змінити функціонування фінансових ринків у майбутньому. У цілому ESMA підкреслює, що фінансові ринки перебувають у стані відносної стабільності, але накопичення структурних ризиків та зростання взаємозалежності між різними сегментами фінансової системи може призвести до швидкої ескалації фінансових потрясінь у разі виникнення несприятливих подій.

Шахрайство без кордонів: як транснаціональні мережі та штучний інтелект змінюють ландшафт фінансової злочинності [7]



Документ, підготовлений INTERPOL, є комплексним глобальним аналітичним дослідженням, спрямованим на оцінку масштабів, динаміки та ключових характеристик сучасного фінансового шахрайства у світі. Звіт ґрунтується на аналізі інформації, отриманої від держав-членів INTERPOL, міжнародних організацій, наукових установ та приватного сектору, а також на даних оперативних систем INTERPOL і матеріалах міжнародних правоохоронних операцій. Основною метою документа є формування системного уявлення про еволюцію фінансового шахрайства, визначення ключових типологій злочинної діяльності та прогнозування подальших ризиків для економічної, соціальної та безпекової сфер.

У звіті підкреслюється, що фінансове шахрайство у сучасному світі перетворилося на один із найбільш масштабних і поширених видів транснаціональної злочинності. Воно дедалі більше інтегрується у глобальні кримінальні екосистеми та часто виступає центральним елементом так званої полікримінальної діяльності, коли різні види злочинів взаємодіють між собою. Шахрайські схеми все частіше перетинаються з кіберзлочинністю, торгівлею людьми, відмиванням коштів, незаконним обігом наркотиків і навіть фінансуванням терористичних структур. Така взаємозалежність пояснюється тим, що доходи від шахрайства є одним із ключових джерел фінансування організованих злочинних мереж, які використовують складні

[7] https://www.interpol.int/Media/Documents/Publications/Financial-Crime/INTERPOL-Global-Financial-Fraud-Threat-Assessment-March-2026

фінансові та технологічні інструменти для приховування походження коштів і їх подальшого легалізування.

За оцінками, наведеними у документі, глобальні фінансові втрати від шахрайства у 2025 році досягли приблизно 442 мільярдів доларів США, що свідчить про винятковий масштаб цієї проблеми. При цьому автори звіту наголошують, що реальні втрати можуть бути значно більшими, оскільки значна частина випадків шахрайства не повідомляється правоохоронним органам. У деяких країнах, зокрема у Великій Британії, фінансове шахрайство становить значну частку усіх зареєстрованих злочинів, а в інших державах масштаби збитків вимірюються мільярдами доларів щороку.

У контексті аналізу сучасного ландшафту шахрайства особлива увага приділяється ролі цифрових технологій, які значно розширили можливості злочинців. Широке використання інтернету, соціальних мереж, мобільних платіжних систем і криптовалют створило нове середовище, у якому шахрайські операції можуть здійснюватися на глобальному рівні з мінімальними витратами. Автори звіту підкреслюють, що розвиток цифрових технологій не лише полегшив здійснення шахрайства, але й значно підвищив його масштабованість, що дозволяє злочинним групам одночасно атакувати тисячі потенційних жертв у різних країнах.

Окремий розділ документа присвячений класифікації основних типів фінансового шахрайства, які спостерігаються у глобальному масштабі. Одним із найпоширеніших видів є Business Email Compromise (BEC) — шахрайство, пов’язане з компрометацією корпоративної електронної пошти. У межах таких схем злочинці отримують доступ до електронних листувань компаній або створюють підроблені повідомлення, що імітують листи керівництва чи партнерів, з метою змусити працівників перевести значні суми коштів на підконтрольні рахунки. Подібні схеми є особливо небезпечними через високий рівень довіри до внутрішніх корпоративних комунікацій і складність їх своєчасного виявлення.

Іншим поширеним видом є шахрайство з передоплатою, що передбачає отримання передоплати за товари або послуги, які фактично не існують або не відповідають заявленим характеристикам. Такі схеми часто здійснюються через інтернет-платформи, соціальні мережі або фіктивні комерційні вебсайти. Жертви переконуються у вигідності пропозиції та здійснюють оплату наперед, після чого контакт із продавцем зникає.

Важливу роль у сучасному ландшафті фінансового шахрайства відіграють шахрайські схеми, засновані на видаванні себе за іншу особу або організацію. Злочинці можуть представлятися співробітниками банків, державних органів або технічної підтримки, використовуючи психологічний тиск, страх або терміновість для отримання доступу до фінансових даних жертв. Останнім часом поширюються нові форми такого шахрайства, зокрема так званий QR-фішинг, коли жертви сканують підроблені QR-коди, що перенаправляють їх на фішингові сайти або запускають шкідливе програмне забезпечення.

Значна частина шахрайських схем пов’язана з шахрайством, що пов’язане з неправомірним використанням персональних даних. Зловмисники отримують доступ до логінів, паролів, номерів банківських карток, біометричних даних або інших конфіденційних відомостей через фішингові атаки, злом інформаційних систем або фізичне викрадення документів. Особливо небезпечним новим явищем є шахрайство з використанням синтетичної (штучно створеної) ідентичності, коли створюються штучні цифрові особи на основі комбінації реальних і вигаданих даних. У звіті зазначається, що подібні схеми часто використовують персональні дані дітей, що може призводити до багаторічної експлуатації таких ідентичностей без виявлення.

Окрему категорію становить інвестиційне шахрайство, що передбачає залучення жертв до інвестування у фіктивні або маніпульовані фінансові проєкти. Шахраї створюють підроблені торговельні платформи або мобільні додатки, які демонструють нібито успішні інвестиції та

прибутки. На початковому етапі жертвам можуть навіть повертатися невеликі суми коштів, щоб сформувати довіру, після чого вони вкладають значно більші суми і втрачають їх повністю. Особливо поширеними є криптовалютні інвестиційні шахрайства, де використання цифрових активів значно ускладнює відстеження фінансових потоків і повернення викрадених коштів.

Серед соціально орієнтованих шахрайських схем особливе місце займає романтичне шахрайство та його сучасна еволюція — гібридні моделі, що поєднують встановлення емоційного зв'язку з жертвою та подальше залучення її до фіктивних інвестиційних операцій. У таких випадках злочинці встановлюють довготривалі емоційні контакти з жертвами через соціальні мережі або застосунки для знайомств, поступово здобуваючи довіру і переконуючи їх надсилати гроші під різними приводами. Згодом такі схеми часто поєднуються з інвестиційними пропозиціями або переходять у форму шантажу.

Важливим новим трендом є шантаж інтимними матеріалами, коли злочинці вимагають гроші, погрожуючи поширенням інтимних матеріалів. У сучасних схемах дедалі частіше використовуються штучно згенеровані зображення та та відео з використанням діпфейків, які можуть створюватися навіть без участі жертви, що значно підвищує ефективність шантажу. Звіт підкреслює, що шантаж інтимними матеріалами дедалі частіше інтегрується у складніші шахрайські схеми, наприклад поєднується з романтичними або інвестиційними шахрайствами.

Однією з найбільш тривожних тенденцій є глобальне поширення так званих шахрайські кол-центри — організованих комплексів, у яких тисячі людей змушені здійснювати онлайн-шахрайство. У багатьох випадках працівники таких центрів самі є жертвами торгівлі людьми, яких заманюють за кордон обіцянками роботи, а потім примушують здійснювати шахрайські операції. За даними INTERPOL, жертви з майже 80 різних країн були залучені до роботи в таких центрах. Спочатку такі структури зосереджувалися переважно у Південно-Східній Азії, однак поступово вони почали з'являтися і в інших регіонах світу.

Звіт також детально аналізує роль штучного інтелекту як каталізатора шахрайської діяльності. Завдяки генеративним моделям і автоматизованим системам злочинці можуть створювати переконливі повідомлення, підроблені голоси та відео, а також автоматично проводити розвідку потенційних жертв. У деяких випадках так звані «автономні системи

Висновки:

- **Фінансове шахрайство перетворилося на одну з основних форм транснаціональної організованої злочинності.** Правоохоронним органам і ПФР необхідно розглядати шахрайство не лише як окремий злочин, а як джерело фінансування інших кримінальних активностей (відмивання коштів, торгівля людьми, фінансування тероризму), що потребує інтегрованих фінансових розслідувань.
- **Штучний інтелект радикально змінює масштаби та ефективність шахрайських схем.** Необхідно впроваджувати AI-інструменти для виявлення контенту з використанням діпфейків, автоматизованих шахрайських кампаній та синтетичних ідентичностей, а також адаптувати процедури KYC і фінансового моніторингу до нових ризиків.
- **Шахрайські кол-центри та примусове онлайн-шахрайство стають глобальною кримінальною індустрією.** Ефективна протидія вимагає міжнародних операцій, обміну розвідданими та співпраці між правоохоронними органами, фінансовими установами та технологічними компаніями.
- **Основні втрати від шахрайства концентруються у криптовалютних інвестиційних схемах і соціальній інженерії.** Потрібно посилити регулювання криптоплатформ, удосконалити моніторинг транзакцій та розвивати механізми швидкого блокування коштів і міжнародного повернення активів.

AI» здатні автономно планувати та виконувати шахрайські операції — від збору інформації до визначення оптимальної суми вимагання. Поява сервісів Deepfake-as-a-Service та Fraud-as-a-Service створює новий кримінальний ринок, де інструменти шахрайства продаються або орендуються так само, як легальні цифрові сервіси.

Важливою характеристикою сучасних шахрайських мереж є їх високий рівень організації та міжнародної кооперації. У звіті зазначається, що злочинні групи часто спеціалізуються на окремих етапах кримінального процесу: одні створюють фішингові інструменти, інші здійснюють соціальну інженерію, треті займаються відмиванням коштів. Така модель дозволяє підвищити ефективність злочинної діяльності та значно ускладнює роботу правоохоронних органів.

На основі аналізу даних держав-членів INTERPOL зроблено прогноз, що у найближчі три-п’ять років глобальний рівень ризику фінансового шахрайства залишатиметься високим, а масштаби злочинної діяльності, ймовірно, продовжать зростати. Найбільш значні негативні наслідки очікуються для економічної та соціальної сфер, а також для системи безпеки, тоді як вплив на сферу охорони здоров’я та управління оцінюється як помірний.

Загалом звіт підкреслює, що фінансове шахрайство стало глобальною системною проблемою, яка потребує комплексної відповіді. Ефективна протидія можлива лише за умов активної міжнародної співпраці, обміну розвідувальною інформацією, використання сучасних технологій для виявлення шахрайства та залучення приватного сектору до спільних заходів боротьби з фінансовою злочинністю.

Тіньова фінансова система: аналіз сучасних загроз відмивання коштів [8]

Сучасний світ фінансів дедалі більше нагадує поле битви, де технологічний прогрес та витонченість злочинців вступають у пряму суперечку із зусиллями правоохоронних органів та фінансового сектору.

35-й випуск журналу "SARS in Action", офіційного видання Підрозділу фінансової розвідки Великої Британії (UKFIU), надає глибокий аналітичний зріз поточних загроз, що демонструє еволюцію злочинності. Він розкриває, як класичні шахрайські схеми набувають нової, більш небезпечної форми, використовуючи криптовалюти як інструмент та ціль, імітуючи авторитет професійних послуг і проникаючи навіть у такі, здавалося б, захищені сфери, як соціальне житло. Це видання є важливим сигналом для всіх учасників фінансової екосистеми: від пересічних громадян до керівників великих корпорацій та регуляторів, адже ціна незнання або ігнорування цих загроз вимірюється мільйонами втрачених фунтів та долями людей.

Однією з найбільш болючих, підступних та руйнівних тем, порушених у виданні, є шахрайство з перенаправленням платежів (Payment Diversion Fraud), особливо під час угод з нерухомістю. Цей вид злочину вражає саму суть довіри, на якій будуються відносини між учасниками ринку. Злочинці, діючи як невидимі маніпулятори, втручаються в комунікацію між покупцями, продавцями, юристами та рієлторами. Вони видають себе за одну зі сторін за допомогою фальшивих електронних листів, телефонних дзвінків або навіть підроблених документів, і

[8] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/799-sars-in-action-issue-35/file

перенаправляють кошти, призначені для купівлі житла — часто це депозити або залишкова сума угоди — на підконтрольні їм рахунки.

Статистика, наведена в журналі, вражає: середня сума втрат потерпілих сягає 82 000 фунтів стерлінгів. Це не просто гроші, це заощадження, які зникають в одну мить. Особливо тривожним є віковий профіль жертв — найбільш уразливою виявилася економічно активна група населення віком 30-49 років. Це люди, які найактивніше залучені до ринку нерухомості, купуючи своє перше житло або інвестуючи в більше, і саме їхня зайнятість та довіра до цифрових каналів комунікації робить їх легкою мішенню.

UKFIU, підтримуючи загальнонаціональну кампанію "Stop! Think Fraud", не обмежується лише констатацією фактів. Інформаційні бюлетені з практичними порадами щодо верифікації платіжних реквізитів були надіслані 165 000 фахівців з нерухомості — юристам та рієлторам, які є першою лінією захисту. Крім того, UKFIU активно використовує сучасні канали комунікації, такі як LinkedIn та власний подкаст, де фахівці детально розбирають методи соціальної інженерії, яку використовують злочинці. Це є свідченням розуміння того, що ефективний захист можливий лише через постійне навчання та підвищення професійної пильності, створюючи міцний бар'єр на шляху злочинних схем.

Паралельно з прямим фінансовим шахрайством розвивається не менш небезпечна тенденція — шахрайство з використанням імітації компаній (Company Impersonation Fraud). Цей метод є значно витонченішим, оскільки атакує не лише гаманці, але й саму довіру до інституційних брендів, які формувалися роками.

Журнал наводить показовий приклад злочинної схеми, націленої на жертв попередніх криптошахрайств. Злочинці, виявивши бази даних ошуканих людей, створили фейковий веб-сайт та електронні адреси, що ідеально імітували велику міжнародну аудиторську фірму. Використовуючи авторитет відомого бренду, вони запропонували потерпілим "повернути" вкрадені кошти, стверджуючи, що "слідча група" фірми нібито відстежила активи. Жертвам пропонували заповнити анкети з персональними даними та банківськими реквізитами, а потім, для більшого ефекту, починали телефонувати, тиснучи на необхідність термінової сплати "внеску за розслідування".

Цей випадок є класичним прикладом вторинного шахрайства, коли злочинці цинічно експлуатують вразливий стан людей, які вже зазнали фінансових втрат і перебувають у відчаї, чіпляючись за будь-яку примарну надію.

Окремим і надзвичайно актуальним блоком видання, що заслуговує на найпильнішу увагу, є глибокий аналіз загрози інвестиційного шахрайства з криптовалютами (Crypto Investment Fraud). Це не просто нова форма шахрайства, а системна проблема, що ґрунтується на поєднанні фінансової неграмотності населення щодо нових технологій, галасу навколо "легких грошей" у криптосфері та обіцянках надшвидкого збагачення. Злочинці створюють витончені, професійно зроблені фейкові торгові платформи, які імітують роботу реальних бірж. Жертви вкладають кошти, бачать на дашбордах, як їхні інвестиції "зростають" завдяки вдалим угодам, і не підозрюють, що всі їхні гроші давно вкрадені, а цифри на екрані — не більше ніж декорація.

Однак географія фінансових злочинів не обмежується віртуальним простором криптобірж та операціями з елітною нерухомістю. Журнал робить значний і надзвичайно важливий акцент на відносно новій, глибоко прихованій та, на жаль, недооціненій загрозі — відмиванні грошей у сфері соціального житла. Це яскравий та показовий приклад того, як організовані злочинні групи використовують будь-які, навіть найменш очевидні прогалини в регулюванні та нагляді.

Соціальне житло, створене для підтримки вразливих верств населення, може стати ідеальним прикриттям для злочинних фінансових потоків. Злочинці можуть використовувати його для фіктивної реєстрації підставних фірм, які не ведуть реальної діяльності; оплачувати оренду з

непідтверджених або явно сумнівних джерел; або використовувати самі приміщення для зберігання активів, отриманих злочинним шляхом.

Автори статті, представники самої галузі, б'ють на сполох щодо ролі професійних посередників — юристів, бухгалтерів, рієлторів, які через недбалість, небажання проводити належну перевірку або, в гіршому випадку, навмисне, сприяють легалізації злочинних доходів. Вони порушують Закон про боротьбу з відмиванням грошей (MLR) та Закон про доходи від злочинів 2002 року (POCA), що створює пряму відповідальність не лише для самих посередників, але й для житлових асоціацій, які з ними співпрацюють. Наслідки можуть бути катастрофічними: від величезних регуляторних штрафів та кримінального переслідування до непоправної шкоди репутації.

Однак найбільш тривожним сигналом, який лунає зі сторінок журналу, є парадокс: на тлі рекордної кількості Звітів про підозрілу діяльність (SARs), які подаються фінансовим сектором по всій країні, організації, що надають соціальне житло, подають їх надто мало. Це свідчить або про критично низьку обізнаність співробітників щодо індикаторів ризику, або про вкрай слабкі внутрішні контролі та процедури комплаєнсу. Така ситуація робить цілий сектор економіки "сліпою зоною" для фінансового моніторингу та надзвичайно вразливим для проникнення та експлуатації з боку організованої злочинності, що потребує негайного виправлення через посилення регулювання, навчання персоналу та впровадження ризик-орієнтованого підходу.

Висновки:

- **Еволюція загроз у бік соціальної інженерії та імітації довіри.** Злочинці дедалі частіше відходять від примітивних схем на користь багатоходових комбінацій, що базуються на використанні довіри та маніпуляціях
- **Крипто-інвестиційне шахрайство перетворилося на системну загрозу**, що завдає мільйонних збитків. Ефективна протидія потребує не лише блокування транзакцій, а й масштабних інформаційних кампаній, націлених на групи ризику та тісної співпраці з легітимними постачальниками віртуальних активів (VASPs).
- **Злочинці активно проникають у сектори, які традиційно не вважалися високо-ризиковими**, зокрема у сферу соціального житла. Недостатня обізнаність персоналу, слабкі внутрішні контролі та нехтування обов'язковою перевіркою контрагентів з боку професійних посередників створюють ідеальні умови для легалізації злочинних доходів.
- **Вирішальна різниця між "сигналом" і "зброєю".** Повідомлення про підозрілі операції є критичним інструментом для виявлення саме відмивання грошей, а не самого факту шахрайства. Ефективність системи залежить від правильної кваліфікації злочину та нерозривного поєднання подання SARs з одночасним інформуванням поліції про предикатні злочини.

Нарешті, журнал не оминає увагою міжнародний вимір боротьби з фінансовими злочинами, детально висвітлюючи діяльність Великої Британії на посаді президента в потужній мережі CARIN (Camden Asset Recovery Inter-agency Network). Цей аспект є принципово важливим, оскільки він підкреслює просту, але часто ігнорована істину: активи злочинців не мають кордонів. Вони вільно переміщуються між юрисдикціями, ховаються в офшорах, інвестуються в нерухомість по всьому світу. А отже, і протидія їм має бути глобальною, скоординованою та базуватися на міцних міжособистісних та інституційних зв'язках.

CARIN, яка відзначила своє 20-річчя, є саме таким інструментом — неформальною, але надзвичайно ефективною мережею, що об'єднує понад 60 юрисдикцій. Співпраця між підрозділами фінансової розвідки, прокуратурами та органами з розшуку активів у виявленні, заморожуванні,

арешті та конфіскації активів є критично важливою для того, щоб позбавити злочинність її фінансової основи — прибутку.

Підсумовуючи, злочинці невпинно шукають найслабшу ланку, найменш захищеного учасника фінансової екосистеми. Ефективна протидія можлива лише за умови поєднання кількох критичних факторів: вдосконалення законодавства та регулювання, тісної міжнародної координації, активного використання передових технологій для аналізу даних та, найважливіше, постійної, цілеспрямованої освіти та підвищення обізнаності як професіоналів фінансового сектору, так і пересічних громадян.

Журнал закликає до пильності, проактивності та нерозривної співпраці всіх ланок суспільства у цій невидимій, але відчайдушній боротьбі.

Звіти окремих інституцій та експертів

Технологічна мутація кримінального капіталу [9]

Дослідження «Протидія гідрі незаконних фінансів на крипторинках: захист роздрібних інвесторів та припинення експлуатації з боку ворожих урядів», опубліковане британським аналітичним центром Товариство Генрі Джексона (Henry Jackson Society, HJS) у березні 2026 року за авторством експерта Александра Браудера, є працею, що деконструює механізми інтеграції цифрових активів у глобальну тіньову та мілітаризовану економіку. Методологічним фундаментом цього звіту виступає створена автором Глобальна база даних відмивання криптовалют (Global Cryptocurrency Laundering Database, launderingdatabase.org), яка вперше у світі систематизує та агрегує 164 найбільш масштабні, резонансні та складнодоказові кейси відмивання криптоактивів, жорстко верифіковані через обвинувальні акти, судові рішення, міжнародні санкційні списки та розслідування за довгий період еволюції ринку. Загальний обсяг підтверджених незаконних коштів, які були успішно пропущені злочинцями через криптоекосистему лише в цих 164 задокументованих справах, становить 350 мільярдів доларів США. Динаміка поширення цієї технологічної загрози математично підтверджується сукупним річним темпом зростання (CAGR) кількості масштабних справ на рівні 16,5%, що перетворює відмивання криптоактивів з нішевої проблеми шахраїв на індустріалізований сектор кримінальної економіки. Концептуальна метафора «Гідри» описує феномен надвисокої, децентралізованої регенеративної здатності кримінальних мереж: ліквідація правоохоронцями одного інфраструктурного вузла (наприклад, арешт серверів даркнет-маркетплейсу чи накладення санкцій на конкретний крипто-міксер Tornado Cash) призводить до миттєвого перерозподілу кримінальної ліквідності через нові, технологічно більш досконалі, часто крос-ланцюгові протоколи. Ефективність поточних державних контрзаходів залишається критично низькою — середній рівень успішного повернення викрадених або відмитих коштів становить лише 27% (загалом конфісковано 92 млрд доларів), причому у переважній більшості справ (79% від загальної кількості), особливо тих, що пов'язані із хакерськими зломами DeFi-протоколів, показник повернення активів часто наближається до абсолютного нуля.

Дослідження HJS структурує екосистему відмивання криптоактивів за класичною, визнаною FATF триступеневою моделлю, яка була глибоко адаптована до технологічних реалій

[9] https://henryjacksonsociety.org/wp-content/uploads/2026/03/HJS-Crypto-Currency-Report-web-final.pdf

розподіленого реєстру (блокчейну). Перший, найбільш масовий етап — On-ramps (Розміщення/Вхід) — агрегує 127 млрд доларів незаконних надходжень (що з урахуванням зростання курсу криптовалют становить 307 млрд доларів у поточній вартості). Цей етап включає розміщення коштів через хакерські атаки, функціонування програм-вимагачів (ransomware), масштабні фінансові піраміди (схеми Понці) та даркнет-маркетплейси. Аналітика звіту фіксує небезпечну еволюційну мутацію тіньових ринків: на зміну класичним, відомим майданчикам стрімко прийшли так звані «ринки гарантій» (guarantee markets) на кшталт Xinbi та Haowang, які згенерували левову частку — понад 57 млрд доларів тіньових потоків. Індустріалізація злочинності вражає: створена лише у 2023 році азійська платформа Xinbi досягла обсягу у 8 млрд доларів ліквідності всього за два роки свого існування, відкрито, без приховування пропонуючи в месенджерах (Telegram) послуги з «відмивання брудних криптоактивів» для наркокартелів та торговців людьми. Другий, найтехнологічніший етап — Layering (Розшарування) — використовується криміналом для безповоротного розриву ланцюга транзакцій та знищення цифрового сліду. Традиційно на цьому етапі домінували спеціалізовані міксери (звіт ідентифікує, що 10 найбільших міксерів, таких як ChipMixer, котрий активно обслуговував операції російського ГРУ, безперешкодно обробили 9,2 млрд доларів), проте звіт HJS виявляє фундаментальний зсув у преференціях транснаціональних злочинців. Відбувся масовий, системний перехід від використання високоволатильного Bitcoin до використання стейблкоїнів (цифрових активів, прив'язаних до фіатних валют, переважно до долара США), на які сьогодні припадає 63% усіх світових незаконних криптовалютних транзакцій. Злочинці обирають стейблкоїни через їхню здатність зберігати купівельну спроможність під час тривалих циклів відмивання та наявність глобальної мережі нерегульованих обмінників. Третій, фінальний етап — Off-ramps (Інтеграція/Вихід) — є критичною точкою конвертації «очищеної» крипти у фіатні гроші для легальної економіки. Тут абсолютно домінують великі централізовані біржі (CEX) та професійні позабіржові (OTC) брокери (звіт ідентифікує 14 ключових платформ-гравців з підтвердженим кримінальним відтоком у 22 млрд доларів). Інституційна імпотенція державних правоохоронних органів на цьому ключовому етапі є разючою: через правозастосовні дії проти сервісів виходу було конфісковано менше 500 млн доларів (2% від незаконного обсягу на цьому етапі), що вказує на системний провал AML-комплаєнсу на рівні ліцензованих світових криптобірж, які часто закривають очі на джерело походження коштів заради збереження ліквідності.

Етап відмивання (за методологією HJS)	Обсяг незаконних коштів	Ключові інструменти та механізми	Частка конфіскованих активів
On-Ramps (Розміщення/Вхід)	$127 млрд ($307 млрд у поточних цінах)	Даркнет-маркетплейси (Xinbi, Haowang), Хаки (Mt.Gox, ByBit), Ransomware, Схеми Понці.	29% ($90.2 млрд) — завдяки арештам серверів та гаманців у момент атаки.
Layering (Розшарування)	N/A (Транзитна ліквідність)	Міксери (ChipMixer), Cross-chain мости, DeFi-протоколи, **Стейблкоїни (домінують - 63%)**.	N/A (Етап приховування слідів, прямі конфіскації технологічно ускладнені).
Off-Ramps (Інтеграція/Вихід)	$22 млрд (Ідентифіковані кримінальні відтоки)	Централізовані біржі (CEX), Позабіржові брокери (OTC), Нелегальні P2P	**Менше 2%** (< $500 млн) — свідчить про неефективність традиційного

Етап відмивання (за методологією HJS)	Обсяг незаконних коштів	Ключові інструменти та механізми	Частка конфіскованих активів
		платформи та платіжні шлюзи.	банківського та біржового комплаєнсу.

Найбільш тривожним висновком звіту Александра Браудера є констатація факту остаточної трансформації криптовалют з нішевого інструменту для фінансового криміналу на повноцінну стратегічну зброю геополітичного протистояння та системного ухилення від санкцій. Криптовалютні ринки перетворилися на рятівне коло для країн-ізгоїв. Тоталітарна Північна Корея (КНДР) генерує та акумулює близько однієї третини (1/3) всіх державних доходів свого уряду виключно через масовані, спонсоровані державою кібератаки (наприклад, діяльність угруповання Lazarus) на глобальні криптоплатформи. Ці викрадені цифрові мільярди направляються режимом Пхеньяна безпосередньо на фінансування та розвиток програм розробки зброї масового знищення та балістичних ракет, уникаючи глобального банківського ембарго. російська федерація, у свою чергу, перетворилася на найбільший глобальний інфраструктурний хаб криптозлочинності: половина всіх незаконних CEX та OTC-брокерів, ідентифікованих у базі даних, а також чотири з п'яти найбільших світових синдикатів програм-вимагачів фізично або операційно базуються на її території. Показовим прикладом є діяльність російської біржі Garantex (з обсягом транзакцій понад $100 млрд), яка стала фундаментальним

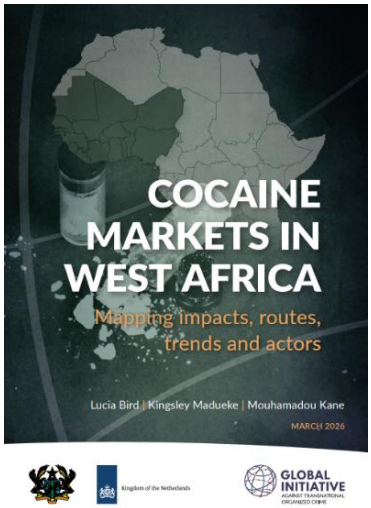
Висновки:

- **Домінування стейблкоїнів (на які припадає 63% незаконних операцій) вимагає від комплаєнс-підрозділів VASP та традиційних банків-кореспондентів впровадження алгоритмів EDD спеціально для транзакцій зі стейблкоїнами.** Особлива увага має приділятися токенам, що емітовані або активно обертаються в юрисдикціях зі слабким регуляторним наглядом (наприклад, рублеві стейблкоїни типу A7A5), оскільки вони використовуються не лише для криміналу, але й для системного обходу санкцій державами-ізгоями.
- **Вразливість етапу Off-ramps (де правоохоронцями вилучено менше 2% від усіх незаконних коштів) свідчить про неефективність поточних AML-процедур на криптобіржах**. Це вимагає на законодавчому рівні впровадження стандартизованих протоколів "fast-freeze" (швидкого заморожування), які б дозволяли органам фінансової розвідки автоматично та миттєво блокувати кошти на гаманцях CEX при спрацьовуванні AI-індикаторів, унеможливлюючи їх виведення у фіат до завершення розслідування.
- **Злиття масової кіберзлочинності з державними військовими інтересами (як у випадку фінансування ВПК Північної Кореї чи діяльності російського ГРУ через міксери) вимагає від СПФМ об'єднання процедур стандартного AML-скринінгу з жорсткими механізмами контролю за санкціями та фінансуванням розповсюдження ЗМЗ**. Будь-який, навіть транзитний зв'язок активів з російськими, іранськими або північнокорейськими OTC-брокерами чи гарантійними ринками має автоматично класифікуватися як ризик найвищого рівня.
- **Еволюція технологій відмивання доводить, що традиційного блокчейн-аналізу (виключно on-chain моніторингу потоків між гаманцями) недостатньо для превентивної боротьби.** Провайдерам фінансових послуг та регуляторам необхідно інвестувати в AI-інструменти для безперервного аналізу даних поза блокчейном (off-chain), включаючи семантичний моніторинг тіньових Telegram-каналів, повідомлень у Darknet, форумів хакерів та публічних реєстрів санкцій для раннього предикативного виявлення шахрайських мереж та схем pig butchering ще на стадії їхнього формування.

інституційним інструментом обходу санкцій для російського ВПК, а після потрапляння під санкції США успішно переродилася у вигляді нових платформ, створених тими ж бенефіціарами. Більше того, звіт ідентифікує створення державами спеціалізованих, санкційно-стійких платіжних інструментів, таких як забезпечений російським рублем стейблкоїн A7A5, створений у Киргизстані у тісному партнерстві з підсанкційним російським «Промсвязьбанком», що дозволяє корпораціям рф щомісяця проводити тіньові розрахунки на мільярди доларів абсолютно поза контролем та видимістю західної фінансової системи.

Паралельно з геополітичними загрозами, звіт фіксує катастрофічне зростання впливу криптозлочинності на звичайних роздрібних інвесторів через масове розгортання індустріалізованих психологічних схем, таких як pig butchering, де використовуються соціальна інженерія та фейкові інвестиційні платформи. Ще більш серйозною є зафіксована епідемія застосування прямого фізичного насильства (викрадення, тортури, збройні напади на власників криптоактивів) з метою примусового заволодіння їхніми приватними ключами (private keys). Для протидії цій розростаючій «Гідрі» звіт HJS пропонує серію радикальних регуляторних та технологічних заходів. Зокрема, ініціюється вимога до регуляторів зобов'язати постачальників послуг віртуальних активів (VASP) впровадити протоколи екстреного заморожування (fast-freeze mechanisms) або «kill switches», які б дозволяли правоохоронцям миттєво блокувати рух викрадених коштів на смарт-контрактах до їх конвертації. Крім того, наголошується на критичній необхідності розгортання моделей обробки природної мови (Natural Language Processing, NLP) та алгоритмів штучного інтелекту для глибокого контекстуального аналізу off-chain сигналів ризику — моніторингу відкритих даних, форумів, соціальних мереж та баз даних витоків, що дозволить комплаєнс-системам бірж предикативно блокувати підозрілі транзакції на етапі Off-ramps ще до того, як вони будуть легалізовані та інтегровані у традиційну фінансову систему.10

Нова географія зла: Як Західна Африка стала кокаїновим хабом планети [10]



Масштабне дослідження GI-TOC фіксує тектонічний зсув у структурі світової наркоторгівлі та його руйнівний вплив на цілий регіон. Автори зібрали, проаналізували та систематизували величезний масив даних, щоб показати, як Західна Африка з периферійної транзитної зони перетворилася на центральний логістичний вузол, величезний склад і стратегічний операційний плацдарм для найпотужніших злочинних синдикатів світу, з усіма трагічними наслідками, що з цього випливають. Це історія про те, як глобальний попит і пропозиція, взаємодіючи з локальними вразливостями, створюють ідеальний шторм, який загрожує підірвати основи державності, безпеки та громадського здоров'я в регіоні, де й без того вистачає викликів.

Дослідження починається з констатації очевидного, але від того не менш тривожного факту: ринок кокаїну в Західній Африці сьогодні більший, ніж будь-коли раніше. Це не просто відновлення після 2013-2018 років, коли кількість вилучень тимчасово впала. Це якісно новий рівень, зумовлений одразу кількома глобальними факторами. Рекордне виробництво кокаїну в Латинській Америці, яке невпинно зростало з 2017 року, досягнувши історичних максимумів, наклалося на таке ж рекордне зростання попиту в Європі. Європейське агентство з наркотиків (EUDA) фіксує, що присутність залишків кокаїну в стічних водах

[10] https://globalinitiative.net/wp-content/uploads/2026/03/Lucia-Bird-et-al-Cocaine-markets-in-West-Africa-Mapping-impacts-routes-trends-and-actors-GI-TOC-March-2026.pdf

європейських міст зросла майже на 150 відсотків за останнє десятиліття. Це створило колосальний тиск на ланцюги постачання.

У відповідь на це європейські правоохоронці посилили тиск на прямі маршрути з Латинської Америки, що призвело до безпрецедентних вилучень, які зросли більш ніж на 400 відсотків між 2010 та 2020 роками. Здавалося б, успіх. Але цей успіх мав зворотний бік: він зробив прямі шляхи надто ризикованими для наркоторговців, змусивши їх шукати обхідні, менш контрольовані маршрути. Ідеальним притулком стала Західна Африка. Сьогодні, за оцінками міжнародних аналітиків, до 30 відсотків усього кокаїну, що потрапляє на європейський ринок, проходить через цей регіон.

Чому ж Західна Африка стала настільки привабливою? По-перше, це географія. Регіон розташований на перехресті шляхів між виробниками в Латинській Америці та споживачами в Європі, а також на зростаючих ринках Близького Сходу та Азії.

По-друге, і це, мабуть, найважливіше, це прогалини в управлінні та тотальна корупція. Кокаїнові гроші, обсяги яких сягають десятків мільярдів доларів, є найпотужнішим корупційним чинником у світі. У Західній Африці вони купують захист на всіх рівнях — від поліцейського на вулиці до високопосадовця в міністерстві. Як зазначають автори, хоча маршрут через Африку довший, він може бути безпечнішим, оскільки ризик вилучення знижується завдяки купленому "даху".

По-третє, регіон стрімко інтегрується у світову торгівлю. Інвестиції в портову інфраструктуру, зокрема в Сенегалі, Гамбії, Кот-д'Івуарі, Гані та Того, призвели до безпрецедентного зростання контейнерних перевезень. Між 2010 і 2022 роками контейнерний трафік в Африці зріс на 57 відсотків, причому найшвидше це зростання відбувалося саме в Західній Африці. Це створило ідеальне середовище для приховування нелегальних вантажів серед легальних.

І нарешті, стрімке зростання інтернету та розвиток фінансових технологій, зокрема криптовалют, створили нові можливості для відмивання грошей. Нігерія, наприклад, посідає друге місце у світі за рівнем впровадження криптовалют, що, за словами місцевих правоохоронців, додає абсолютно новий рівень складності в боротьбі з незаконними фінансовими потоками.

Основним каналом надходження кокаїну залишається море, яке забезпечує левову частку обсягів. Дослідження детально описує дві основні морські моделі: контейнерну та неконтейнерну. Контейнерні перевезення, які домінували на початку 2000-х, і сьогодні відіграють значну роль. Більшість вилучених у західноафриканських портах контейнерів з кокаїном походять з Бразилії, особливо з порту Сантус, який став ключовим хабом для експорту завдяки активній діяльності бразильського угруповання PCC (Primeiro Comando da Capital).

Однак, як зазначають автори, статистика вилучень може бути оманливою. Відсутність великих вилучень на вихідних потоках з Африки до Європи не обов'язково означає, що таких потоків немає. Швидше, це свідчить про прогалини в розвідданих і застарілі профілі ризику в європейських портах, які не розглядають Західну Африку як пріоритетне джерело загрози. Лише 15 тонн кокаїну було офіційно зареєстровано як вилучені на маршрутах із Західної Африки між 2019 і 2024 роками, що, найімовірніше, є лише верхівкою айсберга. Вилучення 4,5 тонни в порту Амстердама в червні 2025 року є красномовним свідченням того, що цей канал активно використовується.

Ще більш тривожною є тенденція до зростання неконтейнерних перевезень. Цей метод передбачає використання рибальських човнів, буксирів, вітрильників та швидкісних катерів для транспортування багатотонних партій кокаїну. Типова схема виглядає так: велике судно-донор доправляє вантаж з Латинської Америки (особливо з Бразилії, Гаяни та Суринаму) у міжнародні води біля узбережжя Західної Африки, наприклад, у Гвінейській затоці. Там вантаж або перевантажують на менші судна, або скидають за борт із GPS-трекерами, щоб пізніше його

забрали «дочірні» човни. Березень 2024 року став знаковим, коли французька влада вилучила понад 10 тонн кокаїну з рибальського судна в Гвінейській затоці. Цей метод дозволяє обходити портовий контроль, висаджуючи тонни наркотику на сотнях кілометрів погано контрольованого узбережжя, від Сенегалу до Сьєрра-Леоне. Місцеві рибалки все частіше розповідають про пропозиції транспортувати партії вагою понад 100 кілограмів між країнами, що вказує на глибоке проникнення злочинних мереж у прибережні громади.

Повітряна контрабанда, хоч і поступається морській за обсягами, забезпечує стабільний потік менших партій, що в сумі можуть сягати кількох тонн на рік. Це як традиційні «мули» на комерційних рейсах, які ковтають до кілограма кокаїну, так і перевезення у багажі (10-15 кілограмів) або вантажних відправленнях (до 90 кілограмів). Особливе занепокоєння викликає використання приватної авіації. Вилучення 2,63 тонни кокаїну з приватного літака, який приземлився в аеропорту Бісау у вересні 2024 року, є лише найяскравішим прикладом. Літак, що вилетів з Венесуели, прямував до Малі, яке ще з початку 2000-х років є відомим пунктом призначення для наркорейсів. Слідчі дані вказують на те, що багато приватних літаків літають із вимкненими транспондерами, що робить їх практично невидимими. Мережі з Західних Балкан, як випливає з розшифровок повідомлень EncroChat, активно вивчали можливість використання приватних літаків для транспортування кокаїну не лише до Європи, а й між країнами Африки, наприклад, із Сьєрра-Леоне до Південної Африки.

Внутрішньоконтинентальні сухопутні маршрути через Сахель демонструють найтісніше переплетення наркоторгівлі з політикою та конфліктом. Чотири основні коридори з'єднують порти узбережжя з Лівією, Марокко та Мавританією. До 2023 року спостерігалося зростання трафіку через центральний Сахель, але відновлення активних бойових дій на півночі Малі, де малійська армія та її союзники з ПВК «Вагнер» розпочали наступ, а також переворот у Нігері, кардинально змінили ситуацію. Традиційна система захисту конвоїв, яку забезпечували повстанські групи, такі як CSP-DPA, була зруйнована.

Втрата контролю над ключовими транспортними вузлами, такими як Кідаль, та посилення ризику атак з безпілотників змусили торговців шукати нові, безпечніші маршрути. Це призвело до часткового переміщення потоків на користь Мавританії та, що більш тривожно, посилення ролі джихадистських угруповань. JNIM (Jama'at Nasr al-Islam wal Muslimin) та «Ісламська держава в Сахелі» (IS Sahel) не обов'язково самі організовують перевезення, але вони активно «оподатковують» конвої, що проходять через підконтрольні їм території. У документі наводиться приклад тісних зв'язків між кланом Тілемсі та IS Sahel, що дозволяє припустити, що доходи від кокаїну стають дедалі важливішим джерелом фінансування для терористів.

Але найтрагічніші наслідки кокаїнового буму для простих людей — це стрімке зростання споживання, особливо креку. Це явище відоме як "spillover" або ефект переливу. Великі партії кокаїну, які проходять через регіон, неминуче потрапляють на місцеві ринки. Дрібних дилерів часто оплачують товаром, і вони змушені збувати його на місці. Великі торговці, яким терміново потрібні кошти, іноді скидають надлишки товару на місцевий ринок, що призводить до різкого падіння цін. У липні 2025 року в Гвінеї-Бісау оптова ціна на кокаїн впала з 10-16 тисяч євро до 7 тисяч за кілограм саме через спробу великого торговця терміново продати значний обсяг.

Споживання креку, який варять з бензолом або бікарбонатом натрію, зростає по всьому регіону. В Аккрі та Конакрі він став другим за популярністю наркотиком після канабісу. У Того ринок креку найдинамічніше розвивається на півночі країни, а в Агадезі (Нігер) споживання зростає серед мігрантів, які прямують через місто. Найбільш вразливі верстви населення, які вживають крек, стають ще більш маргіналізованими. Жінки, для яких соціальна стигма є особливо високою, починають вживати крек дедалі частіше, хоча реальні масштаби, ймовірно, занижені через страх осуду. Спроби диджиталізації ринку через закриті групи в WhatsApp та Telegram, які

активізувалися під час пандемії COVID-19, не змінюють загальної картини: основний обсяг роздрібних продажів, як і раніше, відбувається віч-на-віч.

Найбільша ж небезпека полягає в тому, що кокаїнові гроші системно руйнують державні інститути. Корупція є не просто побічним ефектом, а фундаментальною умовою існування цього ринку. Дослідження описує складну екосистему, в якій тісно переплітаються три категорії акторів: регіональні посередники, іноземні злочинці та представники держави.

Саме третій елемент є критичним. За оцінками, близько 50 відсотків платежів за захист ідуть на підтримку патронажних мереж. Це означає, що кокаїнові гроші не просто збагачують окремих корупціонерів, а вбудовуються в саму тканину політичної системи, стаючи інструментом утримання влади. Вони фінансують виборчі кампанії, купують лояльність військових та чиновників, створюючи замкнене коло, де держава стає залежною від злочинних доходів. Така ситуація не лише підриває довіру до держави, а й робить її заручницею злочинців, які прагнуть убезпечити свій бізнес, фінансуючи одразу кілька політичних сил.

Кримінальний ландшафт регіону надзвичайно різноманітний. Місцеві мережі, часто очолювані бізнесменами з подвійним громадянством, забезпечують зв'язок із місцевою владою та контролюють логістику. Іноземні гравці, такі як латиноамериканські картелі (Clan del Golfo, Sinaloa), приносять капітал і зв'язки з виробниками. Однак найпомітнішою тенденцією останніх років є активізація європейських злочинних угруповань. Італійська 'Ндрангета, іспанські галісійські мережі та, особливо, організовані групи із Західних Балкан не просто купують товар, а фізично присутні в регіоні. Вони відправляють туди своїх брокерів, які на місці організовують перевезення, зберігання, перепакування в контейнери та підкуп посадовців. Такі постаті, як боснієць Маріо Крезич, що координував операції в Сьєрра-Леоне для сербської мережі, чи італієць Бартоло Бруццаніті, який понад п'ять років жив у Кот-д'Івуарі та хвалився, що знає, «які важелі натискати в Африці», стають ключовими, незамінними вузлами в цій злочинній екосистемі.

Нігерійські культистські угруповання, такі як Black Axe, є прикладом полікримінальних структур глобального масштабу, які використовують свої діаспоральні зв'язки для торгівлі кокаїном між Бразилією, Африкою та Європою, а отримані прибутки спрямовують назад до Нігерії для фінансування внутрішніх конфліктів та політичних кампаній.

Попри всю глибину та масштаб проблеми, реакція на неї залишається фрагментарною і ґрунтується на неповних даних. Автори дослідження наголошують на критичних прогалинах у знаннях. Ми майже нічого не знаємо про реальні обсяги контейнерних перевезень з Африки до Європи, оскільки вилучення поодинокі. Інформація про використання напівсубмарин або про можливе будівництво таких апаратів у регіоні залишається уривчастою. Немає чіткого розуміння того, чи використовується в Західній Африці метод зрідження кокаїну для маскування. Дані про споживання, які збирає WENDU (West African Epidemiology Network on Drug Use), базуються на статистиці лікування, яка є вкрай неповною через брак самих лікувальних програм. Без емпіричних досліджень поширеності вживання наркотиків ми можемо лише здогадуватися про реальні масштаби.

Заглядаючи в майбутнє, автори окреслюють кілька тривожних тенденцій. По-перше, очікується подальше зростання споживання креку, що створить непосильне навантаження на і без того слабкі системи охорони здоров'я. По-друге, Західна Африка стає дедалі важливішим логістичним вузлом для зростаючих ринків Азії та Близького Сходу, про що свідчить поява турецьких та китайських громадян у кримінальних справах. По-третє, посилюється тенденція до «розміщення поблизу» (near-shoring) великих запасів кокаїну безпосередньо в Західній Африці для швидкого постачання європейським покупцям, що неминуче призведе до подальшого просочування наркотику на місцеві ринки. І нарешті, зростає ризик бартерних схем, коли кокаїн

обмінюватимуть на синтетичні наркотики з Європи, що ще більше переплітає різні нелегальні ринки.

Підсумовуючи, дослідження GI-TOC малює картину регіону, який опинився в пастці власної вразливості. Кокаїновий транзит приносить величезні прибутки, але ці прибутки не залишаються в регіоні, а вимиваються в офшори, залишаючи після себе лише отруєних людей, зруйновані інститути та війну.

Висновки:

- **Західна Африка — новий глобальний логістичний хаб.** Сьогодні це ключовий вузол, де складуються, перепаковуються та звідки переправляються до Європи багатотонні партії кокаїну. Обсяги цього ринку є безпрецедентними, що робить регіон невід'ємною частиною глобальної індустрії.
- **Корупція як бізнес-модель.** На відміну від латиноамериканського сценарію, де ключову роль відіграє насильство, у Західній Африці основою успіху наркоторгівлі є тотальна корупція. Це робить державу не борцем, а співучасником і гарантом безпеки злочинного бізнесу.
- **Ескалація споживання та руйнація здоров'я населення.** Через "ефект переливу" (коли великі партії наркотику осідають на місцевих ринках) у регіоні стрімко зростає споживання, особливо дешевого та небезпечного креку.
- **Глобальний характер загрози.** У регіоні діють найпотужніші злочинні синдикати світу — від латиноамериканських картелів до італійської 'Ндрангети та балканських угруповань.

Відповідь на цей виклик, на думку авторів, має бути комплексною та рішучою. Вона не може зводитися лише до посилення правоохоронних органів. Потрібна політична воля, щоб розірвати зв'язки між наркоторгівлею та політикою, реформувати фінансування виборчих кампаній, посилити міжнародну співпрацю для відстеження та арешту активів, а головне — змінити підхід до наркоспоживачів, розглядаючи їх не як злочинців, а як жертв, які потребують лікування та реабілітації.

Час для ілюзій минув. Західна Африка стоїть на роздоріжжі, і від рішень, ухвалених сьогодні, залежить, чи зможе вона вирватися з лещат кокаїнової залежності, чи назавжди залишиться заручницею цього кривавого бізнесу.

Епоха гібридних загроз: Як технології, геополітика та інновації змінюють ландшафт фінансової безпеки [11]

Світ вступив у фазу перманентної нестабільності, де старі парадигми захисту втрачають силу швидше, ніж регулятори встигають написати нові правила. Звіт ACAMS, підготовлений на основі опитування майже 1400 професіоналів з понад 200 країн, є щорічним зрізом думок експертної спільноти.

Ландшафт загроз змінюється настільки радикально, що звичні системи захисту, побудовані на реактивних підходах, статичних правилах і закритих базах даних, стрімко втрачають будь-яку ефективність. Вони перетворюються на музейні експонати в той час, як кримінальний світ опановує технології майбутнього. Єдиною альтернативою стає перехід до адаптивних, інтелектуально-керованих моделей, здатних функціонувати в умовах, де швидкість інновацій злочинців випереджає спроможність регуляторів, а фундаментальне поняття довіри до фінансової системи опиняється під безпрецедентною загрозою.

Абсолютним домінантом порядку денного 2026 року стає штучний інтелект, який звіт називає не просто інструментом у руках зловмисників, а справжнім «мультиплікатором сили» для

[11] https://www.acams.org/sites/default/files/2026-01/ACAMS%20Global%20AFC%20Threats%20Report%202026.pdf

транснаціональних злочинних угруповань. Якщо в попередні роки експертна спільнота з обережним оптимізмом говорила про потенційні ризики ШІ, то тепер мова йде про їхню тотальну матеріалізацію в щоденній практиці.

Генеративний штучний інтелект та великі мовні моделі радикально демократизували доступ до складних шахрайських схем, які раніше були прерогативою вузького кола висококваліфікованих хакерів. Концепція «fraud-as-a-service», або шахрайство як послуга, остаточно сформувала цілий чорний ринок, де за відносно невелику плату можна орендувати інструменти для створення діпфейків, замовити кампанію з персоналізованого фішингу або придбати бази даних, зібрані ШІ-ботами. Це явище знизило поріг входження до кримінального світу до мінімуму, дозволяючи навіть технічно непідготовленим зловмисникам запускати масштабні кампанії, що вражають сотні тисяч жертв.

Соціальні мережі та месенджери остаточно перетворилися на головні поля бою, де базові людські емоції — страх, жадібність, співчуття, відчуття терміновості — обробляються складними алгоритмами для маніпуляції поведінкою в масштабах, абсолютно недосяжних для традиційних шахраїв минулого. Повідомлення, створені ШІ, імітують стиль спілкування близьких людей, керівників або представників офіційних установ з такою точністю, що навіть досвідчені користувачі не завжди здатні розпізнати підробку.

Руйнівний вплив цієї технологічної інфільтрації найбільш гостро відчувається у сфері ідентифікації особи. Як із гіркотою констатує один із провідних експертів, цитованих у звіті, документальна ідентифікація стає «по суті марною». Це не перебільшення, а констатація нового факту реальності: сучасні інструменти на основі ШІ здатні з ідеальною, майже голографічною точністю відтворювати складні елементи захисту документів, такі як голограми, мікродрук, ультрафіолетові зображення і навіть машинозчитувані штрих-коди.

Ще більш загрозливою є вразливість біометричних систем. Системи розпізнавання обличчя, голосу та навіть відеоідентифікації дедалі частіше обходяться за допомогою діпфейків, реалістичність яких стрімко наближається до абсолюту, не кажучи вже про численні детальні посібники з обходу систем захисту, які вільно циркулюють у даркнеті. Злочинці більше не обмежуються викраденням окремих особистостей; вони переходять до створення цілих синтетичних екосистем.

Уявіть собі неіснуючу компанію з переконливим вебсайтом, позитивними відгуками на галузевих порталах, активними профілями в соціальних мережах і навіть підробленою історією комерційної діяльності, причому всю цю інфраструктуру підтримують та оновлюють автономні агенти на основі штучного інтелекту, що потребують мінімального втручання людини.

Для професіоналів з протидії фінансовим злочинам обсяг і швидкість таких атак створюють ситуацію, коли наявні захисні механізми працюють на межі колапсу, і більшість експертів прогнозують, що крива загроз буде лише зростати в міру подальших інновацій злочинців. Протидія цьому явищу вимагає фундаментального зрушення парадигми: від статичної верифікації установи змушені переходити до багаторівневих стратегій, що поєднують авторитетні джерела даних для перехресного підтвердження, розширену біометрію, аналітику поведінкових патернів, геолокацію та аналіз цифрового відбитку пристрою.

Однак криза ідентифікації — лише один із фронтів складної війни. Звіт 2026 року чітко окреслює контури нового геополітичного ландшафту, який аналітики ACAMS характеризують як

«багатополярний, конкурентний і волатильний». Фрагментація світового порядку, що поглиблюється, призводить до безпрецедентної регуляторної дивергенції, яка стає головним болем для глобальних фінансових інституцій.

Країни дедалі частіше розглядають санкції, експортний контроль та технологічні обмеження не як виняткові заходи у відповідь на конкретні порушення, а як постійні, тонко налаштовані інструменти державної політики та економічної конкуренції. Розрив між підходами США, Великої Британії та Європейського Союзу не просто зберігається, а в деяких аспектах поглиблюється, створюючи операційні проблеми для будь-якої організації, що працює на кількох континентах. Фінансові установи опиняються в пастці регуляторного лабіринту, де сумлінне дотримання норм в одній юрисдикції може автоматично призводити до порушень в іншій, що загрожує не лише фінансовими санкціями, а й репутаційними втратами та навіть кримінальною відповідальністю для посадових осіб.

Ситуація ускладнюється настільки, що деякі установи вже розглядають можливість створення «юрисдикційно-специфічних» комплаєнс-програм або навіть згортання окремих напрямків бізнесу в цілих регіонах, що є безпрецедентним кроком, який яскраво підкреслює глибину системного ризику.

Паралельно з цими процесами відбувається глибинна трансформація тіньових фінансових потоків. Традиційні неформальні системи переказу коштів, такі як хавала, що століттями базувалися на усній довірі та паперовому обліку, переживають стрімку цифрову еволюцію. Сучасні оператори хавали дедалі активніше інтегрують зашифровані месенджери для координації, створюють власні мобільні додатки для зручності клієнтів і, що найважливіше, використовують криптовалютні розрахунки для клірингу позицій між різними хавала-центрами. Це робить їх не просто швидшими, а й практично невидимими для традиційних систем фінансового моніторингу, оскільки гроші фізично не перетинають кордони, а зобов'язання погашаються через децентралізовані платформи.

Китайські мережі з відмивання грошей, завдяки своїй децентралізованій структурі та високій цифровій координації, залишаються одними з найвпливовіших гравців у цьому просторі, обслуговуючи не лише організовану злочинність, а й приватних осіб, які прагнуть обійти жорсткий контроль за рухом капіталу, створюючи таким чином величезний паралельний ринок.

Ці кримінальні мережі демонструють вражаючу адаптивність, масово застосовуючи стратегію, яку ACAMS називає «дефлексією» — свідоме та систематичне перенаправлення незаконної діяльності в юрисдикції зі слабкішим наглядом та правозастосуванням. Злочинці буквально картографують глобальний регуляторний ландшафт, виявляючи регіони, де комплаєнс-вимоги є недостатніми, а правоохоронні органи не мають ресурсів для ефективної роботи.

Як тільки такі фінансові хаби, як Велика Британія, Сінгапур чи Гонконг, посилюють законодавство щодо боротьби з шахрайством, запроваджуючи жорсткішу відповідальність для банків, телекомунікаційних компаній та цифрових платформ, злочинні групи миттєво переорієнтовують свої операції на менш захищені ринки, де ранні індикатори вже фіксують зростання рівня шахрайства.

У самому центрі цього складного протистояння опиняються дані. Звіт ACAMS прямо називає їх «ахіллесовою п'ятою» сучасної протидії фінансовим злочинам. Ефективність будь-яких інструментів, особливо на основі штучного інтелекту, напряму залежить від якості, доступності, цілісності та належного управління даними. Саме високоякісні, уніфіковані набори даних дозволяють зменшити кількість хибних спрацьовувань, точніше пріоритезувати ризики та спрямовувати обмежені ресурси на справді серйозні загрози. Регулятори вже чітко дають зрозуміти, що розглядають управління даними не як технічну деталь, а як стратегічний імператив, і готовність даних стає одним із визначальних показників інституційної стійкості.

Однак результати опитування демонструють тривожний розрив між вимогами часу та реальністю: застарілі IT-системи та фрагментовані архітектури даних залишаються найбільшими внутрішніми ризиками для фінансових функцій, випереджаючи навіть такі болючі проблеми, як утримання персоналу чи бюджетні обмеження. Саме фрагментація, несумісність систем та величезні обсяги неузгоджених даних, а не вартість чи регуляторна невизначеність, стають головною перешкодою на шляху впровадження ШІ. Без сучасної, інтероперабельної інфраструктури даних будь-які інвестиції в передову аналітику ризикують залишитися марними, а зусилля з протидії складним фінансовим злочинам будуть приречені відставати від загроз.

Це підводить нас до критичної дилеми, яка постала перед індустрією: чи здатний комплаєнс розвиватися з тією ж швидкістю, що й фінансові інновації? Фінансова екосистема переживає глибоку трансформацію, і бізнес-підрозділи стрімко інтегрують цифрові активи, керуючись прагненням до швидкості, ефективності та вирішення проблем ліквідності. Для керівників бізнесу імператив є гранично ясним: багато хто сьогодні вважає, що найбільшим конкурентним ризиком є недостатньо швидке зростання в криптосфері.

Однак ця гонка за інноваціями створює небезпечний і дедалі ширший розрив із реальними комплаєнс-спроможностями. Регулятори досягли певного прогресу в нарощуванні експертизи, але кадрові обмеження залишаються гострими, особливо через відтік талантів із державного в приватний сектор. Команди комплаєнсу стикаються з аналогічними викликами: стрімка еволюція цифрових активів та децентралізованих фінансів спричинила гострий дефіцит кваліфікованих кадрів.

Половина опитаних професіоналів на нещодавній ACAMS Las Vegas Assembly назвали «цифрові активи та Web3» своїм найкритичнішим пробілом у навичках. Традиційні фінансові установи, від яких дедалі частіше очікують роботи з криптоактивами, часто не мають ані досвіду, ані чіткого розуміння, як впроваджувати ризик-орієнтований AML-контроль. І поки бізнес прискорює інтеграцію криптовалют без належних запобіжників, ризик правозастосовних дій, фінансових втрат та непоправної репутаційної шкоди зростає в геометричній прогресії.

Нарешті, звіт звертає пильну увагу на людський фактор, який постає у двох іпостасях: як найвразливіший елемент системи і як об'єкт неминучої трансформації. Парадигма інсайдерських загроз кардинально змінилася. Вона вийшла далеко за межі традиційного уявлення про зраду з боку одного працівника. Сьогодні це складна, багатовимірна екосистема, що включає змову з транснаціональними злочинними угрупованнями, цілеспрямоване державне проникнення та використання вразливостей третіх сторін — підрядників і вендорів.

Висновки:

- **ШІ як головний дестабілізатор:** Штучний інтелект перетворився з інструменту на «мультиплікатор сили» для злочинців, уможлививши створення масштабованих, схем та зробивши традиційні методи верифікації особи, включно з біометрією, неефективними.
- **Геополітична фрагментація як новий ризик:** Багатополярний світ та регуляторна дивергенція створюють для бізнесу ситуацію, де дотримання правил в одній юрисдикції може призводити до порушень в іншій, змушуючи установи згортати цілі напрямки діяльності.
- **Трансформація тіньових фінансів:** Традиційні мережі на кшталт «хавали» цифровізуються, інтегруючи криптовалюти та децентралізовані платформи, що робить їх практично невидимими.
- **Криза даних та людського капіталу:** Головною внутрішньою перешкодою для боротьби з фінансовими злочинами є застарілі, фрагментовані IT-системи та погані дані, що робить неможливим їхнє ефективне використання.

Північнокорейські оперативники стали хрестоматійним прикладом складності цієї загрози: вони масово використовують синтетичні особистості, згенеровані ШІ, для працевлаштування в технологічних компаніях і отримання доступу до конфіденційних систем і даних клієнтів. Інші вдають із себе рекрутерів або менеджерів з найму, розгортаючи шкідливе програмне забезпечення під час фіктивних співбесід.

ACAMS попереджає, що більшість організацій залишаються сліпими до такого проникнення, виявляючи факти лише після втручання правоохоронних органів, що підкреслює нагальну потребу в посиленні протоколів безпеки та постійному моніторингу.

Паралельно, самі професіонали з протидії фінансовим злочинам перебувають у стані глибокої тривоги через неминучу автоматизацію: функції, які ще вчора вважалися «стабільно людськими» вже масово автоматизуються.

Поява «агентного штучного інтелекту», здатного до автономного прийняття рішень, лише прискорить цю структурну трансформацію. Єдиною адекватною відповіддю на цей виклик є адаптація через безперервне навчання та підвищення кваліфікації. Базова грамотність — глибоке розуміння того, як працюють ці системи, як ними керувати, як інтерпретувати їхні результати та інтегрувати в робочі процеси — стає не просто конкурентною перевагою, а безумовною вимогою для збереження професійної релевантності в майбутньому.

Підсумовуючи, звіт малює перед нами картину світу, який остаточно попрощався зі старими парадигмами безпеки. Швидкість, масштаб і експоненційна складність загроз, породжених симбіозом технологій, геополітичної фрагментації та кримінальної винахідливості, вимагають від усієї світової фінансової системи фундаментальної, болісної, але неминучої перебудови.

Успіх у цьому новому середовищі залежатиме не від здатності реагувати на вже скоєні злочини, а від проактивної стійкості. Ті фінансові інституції, які зможуть не лише зрозуміти, а й опанувати цю нову реальність, перетворюючи виклики на стратегічні переваги, не просто мінімізують ризики, а й візьмуть на себе провідну роль у формуванні безпечного та стійкого фінансового майбутнього.

Мережі брехні: Анатомія гібридної війни кремля проти Європи [12]

У січні 2026 року, коли міжнародна спільнота намагалася осмислити черговий масив оприлюднених документів у справі Джеффрі Епштейна, в інформаційному просторі Франції та Німеччини почала циркулювати дивна історія. Вона стверджувала, що президент Еммануель Макрон нібито мав тісні зв'язки з покійним фінансистом. На перший погляд, це могло здатися черговою теорією конспірологів. Але за цим фейком стояла складна, багаторівнева структура, коріння якої сягало самої глибини російського державного апарату.

Журналісти OCCRP разом із партнерами з Болгарії (Bird.bg) та Чехії (Investigace.cz) провели безпрецедентне розслідування, яке оголило справжню анатомію прокремлівської дезінформації в Європі. Те, що вони виявили, нагадує не просто пропагандистську кампанію, а

[12] https://www.occrp.org/en/feature/spies-lies-and-video-clicks-the-warped-world-of-pro-russian-disinformation-in-europe

повноцінну гібридну операцію, де переплелися інтереси військової розвідки (ГРУ), служби безпеки (ФСБ), ультраправих радикалів та звичайних людей, чиї імена та долі стали розмінною монетою у великій грі.

Історія починається майже як шпигунський роман. У Східній Німеччині 1970-х років, коли холодна війна сягнула свого піку, величезною популярністю користувався телесеріал "Das Unsichtbare Visier" ("Невидиме забрало"). Головним героєм був вигаданий агент Штазі на ім'я Ахім Детьєн — своєрідний комуністичний антипод Джеймса Бонда, який викривав підступні плани Заходу.

Через пів століття це ім'я несподівано спливло знову. У лютому 2026 року німецькомовний сайт Anonymous News опублікував статтю з провокаційним заголовком: "Чому Еммануель Макрон знайомий з Джеффрі Епштейном?". Автором матеріалу був зазначений... Ахім Детьєн.

Для уважного спостерігача це мало б стати червоним прапорцем. Але найцікавіше крилося в деталі: гіперпосилання з підпису вело не на профіль журналіста, а на німецькомовну версію сайту Russia Today (RT) — державного російського мовника. Виявилося, що на сайті RT справді публікувалися статті за авторством вигаданого шпигуна часів Холодної війни. Це був не просто плагіат чи випадковість — це був свідомий вибір, зрозумілий лише тим, хто знає історію німецько-радянських відносин.

Використання історичного образу мало на меті створити ефект легітимності та ностальгії за часами, коли світ був біполярним і зрозумілим. Для літньої аудиторії Східної Німеччини, яка все ще з ностальгією згадує про НДР, ім'я Детьєна було впізнаваним символом боротьби з "ворогами".

За тиждень до публікації на Anonymous News у Франції відбулася «прем'єра» цього фейку. На сайті-клоні, що маскувався під відоме видання France-Soir, з'явилася стаття, яка стверджувала, що модельний агент Жан-Люк Брюнель (пов'язаний з Епштейном) нібито писав у листі про "особливі вподобання" Макрона та організацію вечірок.

Аналіз цього матеріалу виявив класичні ознаки фейку: цитовані листи були відсутні в оприлюднених файлах Мін'юсту США, а підпис під статтею було просто вкрадено у справжнього французького журналіста. Проте технологія спрацювала: відео з цими "викриттями" миттєво підхопили анонімні акаунти в соціальній мережі X (колишній Twitter), і воно почало вірусно поширюватися.

Французька урядова служба Viginum, створена спеціально для боротьби з іноземним цифровим втручанням, спрацювала блискавично. Вона ідентифікувала цю атаку як частину діяльності структури під назвою Storm-1516. У своїй заяві Viginum прямо вказала, що ця група "публічно приписана до військової частини 29155 Головного управління розвідки (ГРУ) російської федерації".

Мета операції була очевидною: дискредитувати лідера країни, яка є ключовим союзником України. Макрон неодноразово наголошував на необхідності стратегічної поразки росії, і кремль відповів у найболючіший спосіб — вдаривши по особистій репутації президента. Viginum визначила цю кампанію як "значну загрозу для цифрового публічного простору не лише Франції, а й усієї Європи".

Якщо французька частина операції була технічно складною, то німецька виявилася набагато брутальнішою і водночас показовішою. У центрі мережі Anonymous News опинилася постать, яка могла б стати персонажем кримінальної драми — Маріо Рьонш.

Його біографія — класичний приклад того, як європейські маргінали стають ідеальними інструментами в руках іноземної держави. Рьонш починав ще у 2014 році на анти-імігрантських

мітингах "Варти за мир" у Німеччині. Саме тоді, за даними прикордонних записів, він вперше відвідав москву. Мета тієї поїздки досі невідома, але хронологія подій красномовна.

Того ж року він запустив Facebook-групу "Anonymous Kollektiv", яка поширювала конспірологічні теорії, антимігрантський та прокремлівський контент. Група налічувала близько двох мільйонів підписників, поки її не видалили у травні 2016 року. Але Рьонш не зупинився: одразу ж з'явився сайт-наступник anonymousnews.ru.

Проте інформаційна діяльність була лише вершиною айсберга. Паралельно Рьонш керував інтернет-магазином "Migrantenschreck" ("Жах мігрантів"), де продавав зброю. За даними німецьких судових документів, він реалізував понад 170 одиниць зброї майже на 100 тисяч євро німецьким покупцям. У 2018 році його заарештували в Угорщині, екстрадували до Німеччини та засудили до 2 років і 10 місяців ув'язнення за незаконну торгівлю зброєю. Відсидівши трохи більше року, у грудні 2020-го він вийшов на свободу умовно-достроково.

Вийшовши з в'язниці, Рьонш майже одразу відродив свій проєкт під новим доменом — anonymousnews.org. Журналісти з'ясували, що новий сайт використовував ту ж саму російську хостингову інфраструктуру, що й попередній. Зв'язок із росією ставав дедалі очевиднішим.

У 2023 році Рьонш переїхав до москви, а у 2024-му зареєстрував там консалтингову фірму та запустив англомовну версію свого Telegram-каналу. Його нове дітище — YouTube-канал "ANTVAuslandsStudio" — набирає мільйони переглядів. У першому ж відео, знятому на тлі кремля, Рьонш представляється як "правдоруб", переслідуваний німецькими спецслужбами, і обіцяє показувати росію "автентично, без цензури та завжди віддано правді".

Сьогодні Рьонш активно використовує зламані документи, зокрема матеріали британського МЗС та посольства Великої Британії в москві, які потім поширює і російське МЗС. Таким чином він вписує себе в єдиний інформаційний простір із державними структурами рф.

Найбільш показовим елементом цієї схеми, що демонструє справжню природу "незалежних" ЗМІ, став пошук джерел фінансування Anonymous News. Сайт позиціонує себе як "альтернативне медіа" і закликає читачів донатити, нібито для покриття редакційних витрат. Зараз на сайті вказано, що для бюджету 2026 року необхідно зібрати ще 102 тисячі євро.

Донати спрямовуються на PayPal-акаунт чеської компанії AN Media a Platební Služby s.r.o. На папері власником компанії є болгарин Івелін Борисов. Коли журналісти Bird.bg знайшли його, вони побачили 56-річного чоловіка, який живе в занедбаному будинку у віддаленому болгарському селі. Він був одягнений у простий одяг, а його обличчя виражало розгубленість.

Борисов розповів, що колись працював у Німеччині, а потім якийсь знайомий запропонував йому за 200-300 євро просто підписати "якісь папери" в Чехії. Він поняття не мав, що став власником медійної компанії. Коли йому показали статті на Anonymous News, підписані його іменем, він тільки розвів руками: "Це не я писав, це неможливо". Борисов не володіє німецькою мовою і не має жодного стосунку до журналістики.

Документи компанії також містять ім'я чешки Магдалени Прусової, яка значилася "адміністратором" з правом підпису. Вона підтвердила журналістам із чеського центру Investigace.cz, що справді супроводжувала Борисова до нотаріуса, але це була лише технічна процедура.

Прусова зізналася, що працювала в компанії, яка займалася реєстрацією фірм, і просто виконувала замовлення. За її словами, реальним бенефіціаром був німець на ім'я Маріо — безсумнівно, Маріо Рьонш. Вона також повідомила, що за перші півтора року роботи AN Media отримала донатів на суми від 10 до 200 євро: "Це були не великі суми, точно не мільйони". Проте на подальші запитання про фінансову звітність вона відповідати відмовилася.

Це відкриття малює жахливу картину: структура, яка збирає гроші європейців начебто для незалежної журналістики, насправді побудована на підставних особах, використовуючи вразливе становище бідних громадян ЄС. Чеський суд уже ліквідував компанію AN Media через фінансові порушення, але сама схема залишається викритою як типова для прокремлівських операцій впливу.

Якщо фінансовий слід привів до болгарського села, то шлях поширення контенту вивів просто до дверей російської спецслужби. Журналісти проаналізували, як саме поширюються матеріали Anonymous News, і виявили, що з англомовного Telegram-каналу видання статті найактивніше ретранслював акаунт із ніком "Corob_12".

Аналіз цього акаунту виявив його прив'язку до номера телефону, зареєстрованого на Олексія Башилова. Далі — більше. Використовуючи злиті бази даних, журналісти знайшли другий номер Башилова, який у 2018 році використовувався для замовлення доставки їжі. Адреса доставки: Велика Луб'янка, 1 — будівля, де розташована штаб-квартира ФСБ Росії.

Це не могло бути випадковістю. Онлайн-довідник Numbuster зберіг позначки, якими користувачі підписували номер Башилова у своїх телефонних книгах: "Льоша ФСБ", "UK Олексій Пашилов" (з очевидною орфографічною помилкою). Контакти в його мобільному телефоні містили "робочий" номер, закріплений за військовою частиною 43753. Це не просто абстрактна військова частина — це Центр захисту інформації та спеціального зв'язку ФСБ.

Інші контакти в телефоні Башилова включали співробітників різних підрозділів ФСБ, чиї посади були збережені поряд з іменами. Офіцер російської спецслужби особисто займався поширенням контенту німецького пропагандистського сайту.

Але це ще не все. "Corob_12" активно поширював пости з Telegram-каналу "Нотатки Воланда". Адміністратором цього каналу виявився той самий Олексій Башилов. "Нотатки Воланда" мають лише близько 5200 підписників — небагато за мірками соцмереж. Але якість аудиторії компенсує кількість.

Контент каналу регулярно передруковують такі одіозні особи, як державний пропагандист Володимир Соловйов, чиї програми на державному телебаченні дивляться мільйони. Ще один ретранслятор — депутат Держдуми Андрій Луговий, якого британське слідство називає одним із виконавців убивства Олександра Литвиненка в Лондоні у 2006 році.

Саме "Нотатки Воланда" стали одним із перших джерел, які ретранслювали фейк про Макрона та Епштейна менш ніж за годину після його публікації на фейковому сайті France-Soir. Вимальовується завершена картина: скромний Telegram-канал слугує своєрідним полігоном або первинним ретранслятором для наративів, які потім підхоплюються на державному рівні російської пропаганди.

Після того як журналісти направили запити Башилову та ФСБ, акаунт "Corob_12" було видалено, а "Нотатки Воланда" замовкли. Це мовчання красномовніше за будь-які слова.

Діяльність з впливу — не новий феномен, але технологічні розробки, такі як соціальні медіа та штучний інтелект, загострюють виклик. Простежити, хто стоїть за проросійськими кампаніями в Європі та хто їх фінансує, рідко вдається зі стовідсотковою впевненістю. Але в цьому випадку докази виявилися надзвичайно переконливими. Ланцюжок простежується чітко і недвозначно.

Такі канали поступово руйнують довіру до політики та до того, що вони називають мейнстримними медіа. Регулярне знайомство з такими наративами достатньо, щоб зрештою почати вважати пропагандою майже все.

І в цьому полягає ключ до розуміння стратегії кремля. Мета навіть не в тому, щоб змусити європейців повірити в конкретну брехню. Головна ціль — створити інформаційний хаос, де правда стає невиразною, де неможливо відрізнити реальну новину від фейку, де кожне джерело викликає підозру.

У такому середовищі демократичні суспільства втрачають здатність до колективних дій. Громадяни, які не вірять нікому, не зможуть об'єднатися навколо спільних цінностей чи підтримати спільні рішення. Суспільство атомізується, стає вразливим до маніпуляцій і, зрештою, перестає функціонувати як єдиний організм.

Висновки:

- **Державний рівень організації.** Прокремлівська дезінформація в Європі є не стихійним явищем, а системною діяльністю російських спецслужб. Розслідування підтвердило пряму участь ФСБ та ГРУ у створенні та поширенні фейків.
- **Багаторівнева структура впливу.** Мережа має складну архітектуру: від публічних облич та фінансового прикриття до безпосередніх виконавців у Москві, які керують поширенням контенту.
- **Використання вразливостей ЄС.** Кремль ефективно використовує "сірі зони" європейської демократії: бідність та відчай громадян, радикальні політичні рухи та прогалини в регулюванні соціальних мереж.
- **Справжня мета — руйнування довіри.** Кінцева ціль таких кампаній — не просто дискредитувати конкретних політиків, а тотально підірвати довіру суспільства до будь-якої інформації, зробити неможливим консолідоване ухвалення рішень у демократичних країнах.

Рекомендовані матеріали та події

Еволюція санкційного комплаєнсу та криза міжнародного арбітражу в умовах геополітичної турбулентності [13]

Глибинний аналіз фахової дискусії, представленої у відеоінтерв'ю між експертом із санкційної політики Яном Дунін-Васовичем та радником люксембурзької юридичної фірми Arendt & Medernach Пасхалісом Пасхалідісом, розкриває фундаментальну кризу в системі міжнародного комерційного та інвестиційного арбітражу, яка була безпосередньо спровокована екстериторіальним та багаторівневим застосуванням глобальних санкційних режимів. В умовах п'ятого року повномасштабної збройної агресії російської федерації проти України, а також на тлі безпрецедентної військової ескалації на Близькому Сході, санкційна доктрина Європейського Союзу проходить жорсткий інституційний стрес-тест. Як зазначається в обговоренні, ця турбулентність вимагає від

[13] https://www.youtube.com/watch?v=vPLra9T4xcc&list=PL6ybZvED_Z6HhcUsbUyPMwyDMtOP8U_yi&index=1

європейських інституцій відмови від парадигми виключного покладання на традиційний світовий порядок, заснований на правилах, та переходу до формування власної, автономної санкційної доктрини, про що публічно наголошувала Президентка Європейської Комісії Урсула фон дер Ляєн. Ця макроекономічна та правова нестабільність суттєво обтяжується внутрішніми політичними розбіжностями всередині самого Європейського Союзу, найбільш яскравим проявом яких стало тривале блокування 20-го пакету санкцій з боку Угорщини та Словаччини. Водночас, зростаюча дивергенція між санкційними політиками Сполучених Штатів Америки та Європейського Союзу, зокрема щодо регулювання обігу іранських та російських енергоносіїв, формує середовище тотальної правової невизначеності для транснаціонального бізнесу. Відповідно, приватний сектор та фінансові установи змушені переходити від парадигми статичного, формалізованого комплаєнсу до геостратегічної гнучкості, що передбачає безперервне предиктивне картування вразливостей складних ланцюжків постачань та імплементацію глибокої, ризик-орієнтованої належної обачності на всіх без винятку етапах операційної діяльності.

Центральним елементом аналітичного дискурсу в інтерв'ю є руйнівний вплив санкційних обмежень на існуючі договірні зобов'язання та архітектуру розв'язання міжнародних комерційних спорів. Абсолютна більшість сучасних арбітражних проваджень у цій сфері генерується через об'єктивну неможливість фізичного постачання товарів чи надання послуг внаслідок запровадження жорстких секторальних ембарго, а також через системне блокування платежів контрагентам, які прямо чи опосередковано підпадають під дію фінансових санкцій. Найбільшим та найнебезпечнішим викликом для підрозділів комплаєнсу стають так звані «сірі зони» застосування права, де відсутність прямого лістингу контрагента у санкційних списках вимагає від аналітиків надзвичайно складного дослідження структури корпоративної власності та неформального контролю. У таких ситуаціях компанії постійно балансують між ризиком порушення публічно-правових санкційних норм з боку регуляторів та ризиком отримання багатомільйонних позовів за безпідставне порушення приватних контрактних зобов'язань. У цьому складному правовому контексті фундаментальну роль відіграє Стаття 11 європейських санкційних регламентів (зокрема, імплементована у Регламенті 833/2014) — так зване «застереження про відсутність претензій» (no claims clause). Ця норма була сконструйована як правовий щит, що імунізує європейських економічних операторів від цивільно-правової та матеріальної відповідальності за відмову від виконання зобов'язань, якщо така відмова була продиктована імперативом дотримання європейського санкційного законодавства.

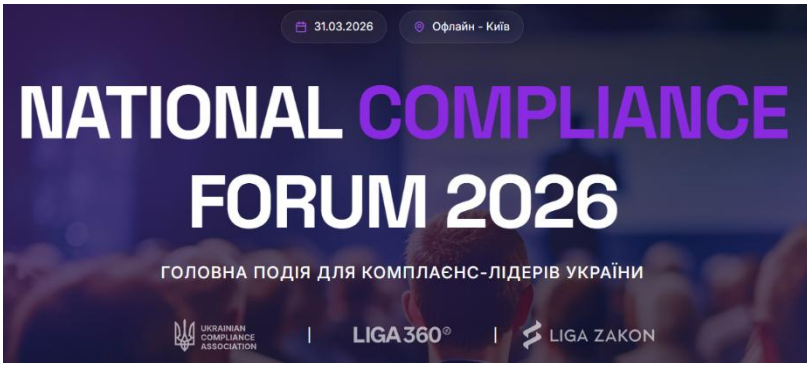
Однак практичне застосування цієї норми спровокувало глибокий концептуальний та юрисдикційний конфлікт щодо самої можливості арбітрабельності таких спорів на міжнародному рівні. Європейська Комісія активно просуває жорстку доктрину неарбітрабельності, безапеляційно стверджуючи, що питання тлумачення та застосування санкцій є виключною прерогативою національних державних судів ЄС. Логіка європейського регулятора базується на побоюванні, що закриті приватні арбітражні трибунали можуть бути використані сторонами для обходу імперативних норм публічного порядку (ordre public) Європейського Союзу. Натомість авторитетні правники та генеральні адвокати Суду Європейського Союзу (CJEU), зокрема наголошується на позиції адвоката Бонді, відстоюють значно більш прагматичний підхід. Вони розглядають Статтю 11 не як юрисдикційний бар'єр, а як фундаментальний інструмент матеріального права, що дозволяє міжнародним арбітрам зберігати свою юрисдикцію над спором, за умови обов'язкового, неухильного застосування ними захисних положень європейського законодавства як норм прямої та вищої дії при винесенні остаточного арбітражного рішення. Як зазначає експерт Пасхаліс Пасхалідіс, спроба Єврокомісії штучно визнати такі спори неарбітрабельними є контрпродуктивною, оскільки вона не гарантує перенесення слухань до судів ЄС, а натомість створює правовий вакуум, яким негайно користується протилежна сторона.

Реакція російської федерації на цю правову блокаду була стрімкою і набула форми повноцінної, асиметричної юридичної війни, яка докорінно змінює ландшафт міжнародного правосуддя. Російська влада системно модифікувала власний Арбітражний процесуальний кодекс, законодавчо закріпивши за російськими державними судами виключну юрисдикцію над будь-якими контрактами, міжнародними спорами та арбітражними застереженнями, що були ускладнені або заблоковані санкціями з боку юрисдикцій, які в рф отримали офіційний статус «недружніх». Цей агресивний законодавчий крок став потужним каталізатором масового застосування російськими судами так званих антипозовних заборон (anti-suit injunctions). Ці судові накази юридично зобов'язують західних контрагентів негайно припинити будь-які арбітражні або судові провадження за кордоном під прямою загрозою накладення колосальних фінансових штрафів на користь російських позивачів. Хоча такі заборони та багатомільярдні штрафи є апріорі юридично нікчемними та невиконуваними в юрисдикціях Європейського Союзу, Великої Британії чи Сполучених Штатів, вони створюють критичний, екзистенційний ризик екстериторіального стягнення для транснаціональних корпорацій. Як підкреслюється в аналізі, новим і найголовнішим полем юридичної битви стають нейтральні юрисдикції третіх країн — зокрема, держави БРІКС, такі як Бразилія, Індія, Китай, а також держави Близького Сходу. Саме в цих регіонах західні корпорації володіють значними ліквідними активами, заводами та інтелектуальною власністю, і саме туди російські підсанкційні суб'єкти активно звертаються з метою легалізації та примусового виконання рішень своїх «кишенькових» судів. Ця ситуація кардинально та безповоротно змінює традиційні підходи до договірного структурування в міжнародній торгівлі. Фахівці з комплаєнсу та юрисконсульти дійшли висновку, що наявність у контракті розмитого, стандартного або формального санкційного застереження може бути значно небезпечнішою за його повну відсутність. Сучасні контракти вимагають ювелірної інтеграції принципу презумпції добросовісності (benefit of the doubt) безпосередньо в текст договору для тієї сторони, яка ініціює зупинення виконання зобов'язань на підставі власного, внутрішнього комплаєнс-аналізу ризиків прихованого контролю чи власності контрагента, відокремлюючи такі специфічні механізми від стандартних, недієвих у цих умовах застережень про форс-мажор.

Паралельно з комерційними спорами, у глобальній правовій системі розгортається масштабна криза у сфері інвестиційного арбітражу, що базується на двосторонніх інвестиційних договорах (BITs), створюючи нові виклики для суверенного імунітету та захисту капіталу. З одного боку, обурені європейські інвестори масово ініціюють багатомільярдні позови проти російської федерації через прийняття нею законів про передачу корпоративних прав іноземних інвесторів під примусове «тимчасове управління» російського менеджменту, що де-факто та де-юре кваліфікується міжнародним правом як прихована, некомпенсована експропріація активів. З іншого боку, російські підсанкційні олігархи, державні банки та компанії цинічно використовують ті самі інструменти BITs для оскарження масштабного заморожування їхніх коштів та конфіскації майна на території Європейського Союзу, вимагаючи астрономічних компенсацій за нібито порушення стандартів захисту інвестицій. У відповідь на цю правову агресію, європейський законодавець пішов на безпрецедентний крок, імплементувавши у свої санкційні інструменти спеціальні запобіжні норми, які апріорі блокують будь-яку можливість визнання та виконання на території ЄС будь-арбітражних рішень, винесених інвестиційними трибуналами проти держав-членів у зв'язку з виконанням останніми своїх зобов'язань щодо дотримання санкційного законодавства. Це призводить до фактичного паралічу існуючої архітектури міжнародного інвестиційного правосуддя, перетворюючи його на інструмент політичної конфронтації. Історичні паралелі, глибоко проаналізовані в інтерв'ю, зокрема пряма згадка про 80-річне заморожування активів Російської імперії у Великій Британії, яке тривало з моменту більшовицького перевороту 1917 року аж до епохи розпаду СРСР, слугують чітким, недвозначним індикатором того, що поточний правовий та фінансовий глухий кут має надзвичайно довгостроковий характер. На очах світової спільноти відбувається глобальне та

системне «заморожування» правовідносин, за якого фундаментальна Нью-Йоркська конвенція про визнання та виконання іноземних арбітражних рішень стрімко втрачає свою універсальність. Це відбувається через радикально антагоністичне, взаємовиключне трактування самої концепції міжнародного публічного порядку різними геополітичними блоками, що вимагає від фахівців з комплаєнсу переходу до стратегій довгострокового управління ризиками ізольованих юрисдикцій.

National Compliance Forum 2026 [14]



Проведення масштабного заходу National Compliance Forum, офіційно заплановане на 31 березня 2026 року спільними зусиллями Української комплаєнс асоціації (УКА) та аналітичної компанії LIGA ZAKON. Цей спеціалізований захід акумулює глибоку експертизу понад 100 ключових стейкхолдерів та 25 провідних спікерів національного і міжнародного рівня, створюючи унікальний синергетичний простір для відкритої взаємодії корпоративного сектору, державних регуляторних органів та академічної експертної спільноти. В умовах тривалої та виснажливої військової економіки, безпрецедентно посиленого регуляторного тиску з боку державних інституцій та невідворотного, законодавчо закріпленого курсу на європейську інтеграцію, парадигма комплаєнсу в Україні остаточно і безповоротно еволюціонувала. Вона перетворилася від формального, суто «паперового» декларування корпоративних політик, яке використовувалося здебільшого для маркетингових цілей, до жорстко інтегрованої, дата-центричної системи управління виживанням, мінімізацією ризиків та операційною сталістю транснаціонального та локального бізнесу. Форум концептуально розроблений та ретельно структурований для задоволення складних професійних потреб крос-функціональної цільової аудиторії вищої управлінської ланки: сертифікованих комплаєнс-офіцерів, керівників юридичних департаментів, директорів з економічної та корпоративної безпеки, вузькопрофільних фахівців у сфері фінансового моніторингу та управління санкційними ризиками, а також CEO та членів наглядових рад, які несуть пряму фідуціарну та кримінальну відповідальність за стратегічний розвиток, операційну стійкість та репутаційний капітал своїх компаній.

До дискусійних панелей залучено спікерів найвищого рівня, таких як Ганна Горбенко (Голова УКА, директорка департаменту комплаєнсу та фінмоніторингу АТ ОТП БАНК), Тетяна Громова (керівниця з комплаєнсу АТ Укрзалізниця), Артем Хаванов (голова Антикорупційного комітету УКА) та інших.

Архітектура програми форуму концептуально охоплює шість фундаментальних тематичних напрямів, які повною мірою репрезентують найбільш гострі, екзистенційні виклики сучасного корпоративного управління. Перший блок, присвячений внутрішнім розслідуванням (Internal Investigations & Forensics), фокусується на розробці чітких, юридично бездоганних алгоритмів дій для компаній у кризових ситуаціях. Уміння правильно ініціювати, процесуально грамотно документувати, збирати цифрові докази та легітимно завершувати внутрішні розслідування складних економічних злочинів, фактів шахрайства або грубих порушень корпоративної етики є

[14] https://ligazakon.net/national-compliance-forum-2026/?utm_source=linkedin&utm_medium=post&utm_campaign=mish

базовим, невід'ємним елементом захисту активів компанії від колосальних репутаційних втрат та потенційного кримінального переслідування з боку правоохоронних органів. Наступний, стратегічно критичний напрям дискусії — інтеграція технологій штучного інтелекту в процеси комплаєнсу (AI & Compliance). На форумі штучний інтелект розглядається через призму складного технологічного дуалізму: як потужний, інноваційний інструмент для автоматизації рутинного скринінгу контрагентів, глибокої предиктивної аналітики великих даних та безперервного моніторингу транзакцій у реальному часі, і водночас як джерело новітніх, непередбачуваних загроз. Ці загрози пов'язані з критичними вразливостями захисту персональних даних клієнтів, алгоритмічною упередженістю систем прийняття рішень та здатністю зловмисників генерувати надзвичайно складні, багатоланцюгові шахрайські схеми (зокрема, з використанням deepfakes для обходу систем біометричної верифікації). Відповідно, ефективне, етичне та законодавчо обґрунтоване регулювання використання AI всередині корпорацій стає обов'язковою, стандартизованою вимогою для сучасних систем управління ризиками.

Особливе місце в порядку денному форуму посідає розширена панель з антикорупційного комплаєнсу (Compliance & Anti-Corruption), яка аналізує антикорупційні програми не як ізольований, бюрократичний документ, а як функціональне ядро комплексної архітектури корпоративного ризик-менеджменту, що безпосередньо впливає на операційну прибутковість. У тісному логічному зв'язку з цією темою знаходиться експертна панель, присвячена взаємодії з державними органами (Government Relations), де центральною, найбільш гострою темою заявлено демаркацію тонкої, часто невидимої межі між легальним цивілізованим лобізмом, інституційною адвокацією інтересів бізнесу та латентними корупційними правопорушеннями. Розробка чітких, деталізованих етичних протоколів для GR-менеджерів є абсолютною запорукою захисту компанії від звинувачень у наданні неправомірної вигоди чи торгівлі впливом. Крім того, інноваційний блок, присвячений екологічному, соціальному та корпоративному управлінню (ESG), глибоко відображає форсовану підготовку українського великого та середнього бізнесу до неминучого впровадження нових жорстких європейських стандартів нефінансової звітності (зокрема, директив CSRD та CSDDD). Інтеграція ESG-метрик у щоденні комплаєнс-процеси стрімко еволюціонує з факультативної практики в обов'язкову умову для збереження доступу компаній до міжнародного фінансування, грантових програм відновлення та глобальних ринків капіталу.

Для фахівців у сфері ПВК/ФТ найбільш вагомою, практико-орієнтованою є спеціалізована панель «AML & Sanctions», яка максимально концентрується на прикладних аспектах побудови стійких систем фінансового моніторингу та безперебійного санкційного контролю в умовах надзвичайно високої динаміки оновлення глобальних санкційних списків та перманентної геополітичної нестабільності. Професійне обговорення охоплює складні механізми інтеграції суворих регуляторних вимог без допущення критичної втрати операційної ефективності та швидкості обслуговування клієнтів бізнесу. Детально розглядається розробка адаптивних, ризик-орієнтованих сценаріїв моніторингу поведінки клієнтів та алгоритмів протидії багаторівневим, глибоко законспірованим схемам ухилення від санкцій через використання компаній-оболонок у транзитних юрисдикціях.

Національний комплаєнс-форум 2026 року виконує функцію інституційної платформи для вироблення єдиного галузевого стандарту корпоративної стійкості, що дозволить українським компаніям не лише ефективно мінімізувати потенційні багатомільйонні регуляторні штрафи, але й успішно вибудувати довірчі, прозорі відносини з міжнародними інвесторами та кредиторами в процесі стратегічної повоєнної відбудови національної економіки.

Інші новини

Фрагментований світ: Як Іран використовує геополітику та технології для обходу санкцій [15]

Світовий порядок, що склався після холодної війни з його ілюзією однополярної стабільності, остаточно відійшов у минуле, поступившись місцем епосі турбулентності, яка характеризується двома фундаментальними силами: поглибленням геополітичної фрагментації та стрімким, часто неконтрольованим технологічним розвитком.

Для професіоналів у сфері протидії фінансовим злочинам це поєднання створює безпрецедентний рівень складності та екзистенційний виклик. Традиційні межі контролю, які десятиліттями вибудовувалися через гармонізацію законодавств та обмін фінансовою розвідкою, стрімко розмиваються, а новітні технологічні інструменти стають однаково доступними як для доброчесних користувачів, так і для гравців, які прагнуть обійти міжнародні норми та фінансувати дестабілізацію.

Найбільш промовистим, складним та небезпечним прикладом цього явища сьогодні є Ісламська Республіка Іран, яка майстерно використовує як прогалини в роз'єднаному світі, так і інноваційні фінансові технології для фінансування своїх проксі-сил, підриву регіональної та глобальної стабільності, що безпосередньо вплинуло на ескалацію поточних конфліктів на Близькому Сході та поставило під загрозу безпеку міжнародного судноплавства.

Іранська стратегія впливу вже давно будується не на прямому військовому вторгненні, а навколо розгалуженої, добре законспірованої мережі підтримуваних угруповань, таких як "Хезболла" в Лівані та Сирії, хусити в Ємені, ХАМАС та "Ісламський джихад" у Палестині, а також численних шиїтських угруповувань в Іраку та Сирії. Ці проксі-сили діють як "гібридні" суб’єкти, поєднуючи партизанську тактику, політичну діяльність та терористичні методи, що дозволяє Ірану проєктувати свою міць на відстань, уникаючи прямої відповідальності та повномасштабної війни.

Основним інструментом для цього є "Аль-Кудс" — елітний підрозділ Корпусу вартових ісламської революції, який діє як паралельна структура до регулярної армії, відповідаючи виключно за зовнішні операції, навчання союзних сил, перекидання зброї та, що найважливіше, — фінансування цих угруповань. Головним і практично єдиним джерелом доходу для цієї діяльності залишається експорт нафти та нафтопродуктів, найбільшим покупцем яких виступає Китай, який продовжує нарощувати імпорт, незважаючи на тиск із боку Заходу.

Однак, через жорсткі та багатосторонні санкції, впроваджені Сполученими Штатами, Європейським Союзом, Великою Британією та іншими країнами, Іран не може продавати свою нафту відкрито на світових ринках, використовуючи традиційні банківські канали. Це призвело до створення складної, багаторівневої та адаптивної системи приховування, що включає два ключові компоненти.

По-перше, це "тіньовий флот" із старих, часто технічно несправних танкерів із вимкненими транспондерами, які здійснюють перевантаження нафти з судна на судно у відкритому морі, щоб заплутати ланцюжки постачання.

[15] https://www.acams.org/en/opinion/fragmented-world-irans-exploitation-geopolitical-and-technological-gaps-illicit-activity

По-друге, і це ще важливіше, Іран створив паралельну "тіньову банківську систему" — розгалужену інфраструктуру фінансових посередників, яка не залежить від глобальної мережі SWIFT та західних кореспондентських рахунків. Ця мережа складається з тисяч підставних компаній, торговельних домів, обмінних пунктів та криптотрейдерів, які діють у юрисдикціях зі слабким регулюванням і забезпечують безперебійний рух коштів від кінцевого покупця іранської нафти до бойовиків, що атакують цивільне судноплавство в Червоному морі балістичними ракетами чи завдають ударів безпілотниками по військових базах США в Сирії та Йорданії.

Ключовим фактором, що уможливлює існування та процвітання цієї схеми, є глобальна фрагментація. Відсутність єдності та консенсусу серед міжнародної спільноти щодо санкційної політики створює для Ірану широкий простір для фінансового маневру. Якщо США та Європа постійно посилюють обмеження та розширюють санкційні списки, то такі країни, як Китай, відверто ігнорують їх, продовжуючи та навіть нарощуючи торговельні відносини з Тегераном. Більше того, існує цілий спектр держав — від Об'єднаних Арабських Еміратів та Туреччини до країн Південно-Східної Азії та Кавказу — які або свідомо підтримують певні аспекти діяльності режиму в обмін на економічні вигоди, або просто заплющують очі на сумнівні фінансові потоки, що проходять через їхню територію та фінансові установи через брак ресурсів, політичної волі чи належного нагляду.

Іран активно використовує регуляторну асиметрію, реєструючи компанії в державах зі спрощеними процедурами та мінімальним наглядом за бенефіціарними власниками. Ці компанії відкривають банківські та криптовалютні рахунки, зокрема й у фінансових установах країн зі слабким законодавством у сфері протидії відмиванню грошей та фінансуванню тероризму. Транзакції навмисно проводяться через численні країни з різними правовими системами, що ефективно використовує затримки, бюрократичні перепони та обмежені можливості оперативного транскордонного обміну інформацією між правоохоронними органами, підрозділами фінансової розвідки та приватними фінансовими установами, які відповідають за виявлення підозрілих потоків.

Найбільш яскравим, майже хрестоматійним прикладом такої операції з відмивання коштів та обходу санкцій є кейс Саїда аль-Джамаля, відомого фінансиста єменських хуситів, який зміг генерувати десятки мільйонів доларів від продажу іранської нафти, незважаючи на численні раунди персональних санкцій. Його схема ілюструє справжню глобалізацію підпільної діяльності та досконале розуміння прогалин у міжнародному контролі.

Ліберійська компанія, зареєстрована в офшорній зоні, володіла танкером під прапором Панами для транспортування нафти з Ірану до Китаю. Індійська фірма спеціалізувалася на фабрикації суднових документів та сертифікатів походження, щоб приховати іранське походження вантажу. Логістикою всього ланцюжка постачання керував експерт-індус, який знаходився в ОАЕ. А бухгалтер-єменець, що фізично перебував у Туреччині, керував складною мережею підставних компаній (shell companies) та банківських рахунків у різних країнах. Саме через цю мережу кошти, перш ніж потрапити до керівництва хуситів, проходили через турецьку торговельну компанію, зареєстровану в ОАЕ, та інші заплутані структури, які унеможливлювали швидке відстеження кінцевих бенефіціарів та джерел фінансування терористичної діяльності.

На цей складний ландшафт геополітичних розломів та регуляторних невідповідностей накладається стрімка технологічна революція, зокрема поява та масове поширення криптовалют, блокчейну та технологій децентралізованих фінансів, що кардинально змінює глобальну платіжну інфраструктуру. Іранський режим, і особливо КВІР, продемонстрував надзвичайну адаптивність, дедалі активніше інтегруючи цифрові активи у свою стратегію фінансування проксі-сил та обходу санкцій.

Цей стратегічний перехід зумовлений кількома вагомими факторами: по-перше, криптовалюти сприймаються як значно менш ризикований інструмент порівняно з великими обсягами готівки, яку небезпечно перевозити через кордони, або з традиційними банківськими переказами, які легко відстежити та заблокувати.

По-друге, вони забезпечують майже миттєві та відносно дешеві міжнародні транзакції, непідвладні графікам роботи банків та географічним обмеженням.

По-третє, регулювання цього ринку в багатьох юрисдикціях залишається фрагментарним, слабким або взагалі відсутнім, а рівень контролю з боку фінансових розвідок та правоохоронних органів є недостатнім.

І нарешті, анонімність, яку за певних умов можуть забезпечити криптовалюти, особливо з використанням міксерів та подібних сервісів, робить відстеження кінцевих отримувачів коштів надзвичайно складним завданням, що потребує високої експертизи та міжвідомчої координації.

Масштаби цього явища вражають навіть за різними оцінками: аналітики провідних блокчейн-компаній припускають, що загальний обсяг іранської криптоекосистеми у 2025 році сягав від 8 до 11 мільярдів доларів США. Ще більш тривожним є те, що, за даними аналітичної фірми Chainalysis, до половини цієї суми може бути прямо чи опосередковано пов'язано з діяльністю КВІР.

Останні кілька років дають численні документальні підтвердження цієї тривожної тенденції. Так, у квітні 2023 року Ізраїль за сприяння Мінфіну США заблокував майже 189 криптогаманців, прив'язаних до бірж у секторі Гази та Туреччині, через які здійснювалося систематичне переведення десятків мільйонів доларів від КВІР до бойового крила ХАМАСу. Підрозділ фінансової розвідки США (FinCEN) зафіксував близько 165 мільйонів доларів підозрілої активності, безпосередньо пов'язаної з ХАМАСом та криптовалютою, за період із січня 2020 по жовтень 2023 року, яка охопила понад 200 гаманців. У березні 2024 року під міжнародні санкції потрапив сирійський фінансист, який діяв із Лівану та постачав "Хезболлі" цифрові гаманці, наповнені коштами, отриманими від продажу товарів через структури КВІР, а також організовував криптовалютні перекази для офіційних осіб угруповання. Були також викриті випадки, коли двоє громадян Ірану придбали криптовалюти на суму понад 100 мільйонів доларів для проведення розрахунків за нафтові контракти безпосередньо від імені уряду, діючи як офіційні агенти.

Кульмінацією цього тренду та сигналом для всієї індустрії стали санкції, запроваджені Міністерством фінансів США у січні 2026 року. Вперше в історії обмеження було накладено на дві криптовалютні біржі, офіційно зареєстровані у Великій Британії, за їхню системну роль в обробці значних обсягів коштів, пов'язаних із структурами, підконтрольними КВІР. За даними авторитетної аналітичної компанії TRM Labs, одна з цих бірж провела транзакції на суму, що перевищує один мільярд доларів США для підконтрольних Ірану структур, використовуючи переважно стейблкоїн USDT у мережі Tron, яка відома низькими комісіями та високою швидкістю транзакцій, що робить її особливо привабливою для таких обсягів.

Іранська модель використання геополітичних та технологічних прогалин є не просто окремим випадком, а радше передвісником та каталізатором нової реальності, з якою зіткнеться весь світ у найближчі роки. У світі, де технології розвиваються експоненційно, випереджаючи здатність національних регуляторів та міжнародних органів до координації та вироблення спільних правил, традиційні, засновані на повільному обміні паперовими запитами підходи до протидії фінансовим злочинам стрімко втрачають свою ефективність.

Успіх тепер визначають не просто глибокі знання нормативної бази та вміння заповнювати звіти, а інтелектуальна гнучкість, здатність до прогнозування, оперативність отримання та

аналізу розвідувальних даних у режимі реального часу, а також безпрецедентний рівень співпраці та довіри між державним і приватним секторами, між фінансовими установами різних країн та технологічними компаніями. Здатність адаптуватися до цієї нової динаміки, вчитися на прикладі Ірану та будувати стійкі до таких викликів системи стане ключовим фактором національної безпеки для урядів та фінансової стабільності для бізнесу в найближчі роки. Ігнорування цих змін загрожує не просто фінансовими втратами, а фундаментальним підривом глобальної безпеки та верховенства права.

Ваша думка важлива!

1. Звіт Global Terrorism Index 2026 фіксує шокуючий факт: 93% фатальних терактів у західних країнах здійснюються терористами-одинаками, а процес радикалізації молоді через соцмережі скоротився до лічених тижнів. Оскільки такі особи зазвичай не мають складних фінансових мереж, як СПФМ необхідно перекалібрувати свої AML/CFT системи, щоб ефективно виявляти мікрокраудфандинг та нетипові транзакції, що передують цим автономним і швидким атакам?
2. На сьогодні, 63% незаконних криптотранзакцій здійснюються через стейблкоїни, проте частка конфіскацій на етапі виведення активів у фіат (off-ramps) на CEX становить мізерні 2%. Які регуляторні зміни необхідні для того, щоб перекрити цю "вузьку горловину" і змусити VASPs нести реальну відповідальність за джерело походження коштів?
3. Які регуляторні та технологічні інструменти повинні бути запроваджені для протидії використанню штучного інтелекту, технологій з використанням діпфейків та автоматизованих шахрайських платформ, і чи готові українські фінансові установи та державні органи до протидії таким новим формам цифрового шахрайства?
4. Враховуючи активне використання Іраном криптовалют для обходу санкцій, наскільки вразливою є українська крипто екосистема до використання її елементів для транзиту коштів, призначених для підривної діяльності проти України? Наскільки регулятори та правоохоронні органи мають змогу відстежувати такі транзакції?
5. В Україні функціонує великий сектор соціального житла та програм підтримки ВПО, через який проходять значні бюджетні кошти та благодійні внески. Наскільки існує ризик використання соціального житла та програм допомоги для відмивання коштів? Які механізми контролю за діяльністю ОСББ, благодійних фондів та місцевих органів влади у цій сфері є найбільш вразливими, та як посилити фінансову дисципліну без створення надмірного бюрократичного тиску?
6. Російські спецслужби часто шукають соціально вразливих осіб та використовують їхні персональні дані для реєстрації компаній, рахунків, медійних активів тощо. Як держава може захистити вразливих українців у Європі від втягнення в прокремлівські схеми?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-12

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.

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