Методологічний бюлетень

Серійний номер: МінФін-AML-2025-45

Листопад 2025

“Перемога починається з першого кроку”

Роберт Шуллер

Мета

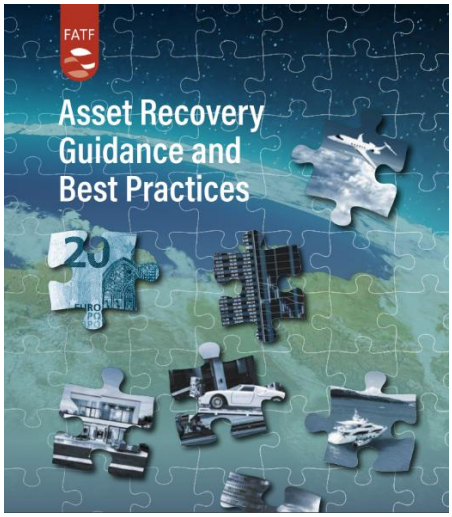
Методологічний Бюлетень видається Міністерством Фінансів України на регулярній основі з січня 2025 р. та містить інформацію щодо національних та світових тенденцій у сфері протидії відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ПВК/ФТ/ФР). Розроблено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

Керівництво та найкращі практики щодо повернення активів [1]



Представлений документ є Керівництвом та найкращими практиками, розробленим FATF/OECD, що відображає трансформацію підходу до конфіскації та міжнародного співробітництва, спричинену значними змінами у Рекомендаціях FATF у жовтні 2023 року та відповідними змінами до Методології оцінювання FATF у червні 2024 року. Ці оновлення є першими суттєвими поправками, пов'язаними з конфіскацією, за понад три десятиліття, і спрямовані на надання юрисдикціям більш надійного інструментарію для підвищення ефективності заходів конфіскації. Керівництво не призначене для однієї аудиторії, а є модульним продуктом для політиків, різних національних органів, що займаються поверненням активів (ПА),

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Asset-Recovery-Guidance-Best-Practices.pdf.coredownload.pdf

постачальників технічної допомоги та широкої громадськості.

Основою для успішного повернення активів є фінансові розслідування, які мають бути інтегровані в усі розслідування, пов'язані з відмиванням коштів (ВК), предикатними злочинами та фінансуванням тероризму (ФТ). Компетентні органи, включаючи правоохоронні органи (ПО), прокурорів та підрозділи фінансової розвідки (ПФР), повинні мати своєчасний доступ до широкого спектру інформації, необхідної для ідентифікації та відстеження злочинного майна та майна відповідної вартості. Це включає інформацію про кінцевих бенефіціарних власників (КБВ), податкову інформацію, а також дані з реєстрів активів (землі, нерухомості, транспортних засобів, акцій). Суттєва увага приділяється відстеженню активів, які можуть бути номінально оформлені на третіх осіб (наприклад, членів сім'ї, ділових партнерів, підставні компанії). Керівництво детально описує поняття "злочинне майно", яке охоплює прямі та непрямі доходи, засоби (інструменти), використані або призначені для використання у злочині, та майно, щодо якого вчинено ВК, а також майно відповідної вартості. При цьому конфіскація не повинна порушувати прав добросовісних третіх сторін (bona fide third parties).

Ключовим аспектом, що забезпечує ефективність ПА, є запобіжні заходи для швидкого забезпечення активів. Інструментарій заходів варіюється від найкоротших і найменш інвазивних відстрочок до більш тривалих попередніх судових рішень. Новою вимогою є повноваження щодо призупинення транзакцій або відмови у наданні згоди на них, якщо є обґрунтована підозра щодо їхньої причетності до ВК, предикатних злочинів чи ФТ. Це короткочасний захід, який дає владі час для аналізу та ініціювання більш тривалого арешту. Призупинення може бути прямим (ПФР або ПО діють без початкового судового втручання) або непрямим (діяльність розпочата суб'єктами за вказівкою компетентного органу, наприклад, через судовий наказ або розпорядження ПФР до фінансової установи (ФУ), постачальника послуг віртуальних активів (VASP) або визначених нефінансових установ та професій (ВНУП)). Ухвалення рішення про призупинення повинно бути швидким, тимчасовим, та вимагає заходів щодо запобігання розкриття (tipping-off), яке може підірвати розслідування.

Керівництво наголошує на необхідності комплексного набору заходів конфіскації. FATF вимагає наявність:

1. Конфіскації на підставі вироку (CBC), яка прив'язана до кримінального переслідування та обвинувального вироку, і може бути заснована на об'єкті (потребує доведеного зв'язку між майном та злочином) або на вартості (вимагає розрахунку злочинного прибутку).
2. Розширеної конфіскації (Extended Confiscation), яка є формою CBC, що виходить за межі конфіскації активів, пов'язаних із конкретним злочином, за який особу засуджено, і може бути особливо корисною для боротьби з організованою злочинністю або проти осіб, які накопичують незаконне багатство, ґрунтуючись на підозрі, що майно походить від злочинної діяльності.
3. Конфіскації без вироку (NCBC), яка тепер є обов'язковою згідно зі стандартами FATF. NCBC дозволяє конфіскацію через судові процедури без необхідності кримінального вироку, націлюючись на майно, задіяне у злочинах або отримане від них, у випадках, коли кримінальне переслідування неможливе або недоцільне (наприклад, смерть, втеча, невідомий злочинець). Зв'язок між майном і злочином має бути продемонстрований відповідно до стандарту доведення, встановленого внутрішнім законодавством (який зазвичай є нижчим, ніж "поза розумним сумнівом", наприклад, "баланс імовірностей").

Усі ці заходи повинні бути реалізовані з урахуванням фундаментальних принципів внутрішнього законодавства (FPDL), таких як ті, що закріплені в конституціях або рішеннях вищих судів, які можуть впливати на впровадження деяких заходів конфіскації. Країнам рекомендується шукати

шляхи адаптації заходів до FPDL, а не використовувати їх як абсолютну заборону для впровадження вимог FATF.

Міжнародне співробітництво є критично важливим, оскільки злочинна діяльність часто має транскордонний характер. Новий підхід FATF до співробітництва з питань ПА ґрунтується на чотирьох практичних міркуваннях: взаємність (країни повинні робити для інших стільки ж, скільки у своїх внутрішніх справах), проактивність (спонтанний обмін інформацією), доцільність (вибір найефективніших засобів, використання експертів) та неформальність (використання неформальних каналів зв'язку перед офіційними запитами, такими як MLA). Співробітництво має охоплювати як формальну правову допомогу (MLA), так і неформальні мережі (наприклад, ARINs — міжвідомчі мережі з повернення активів), які можуть допомогти в ідентифікації та відстеженні активів на ранніх стадіях. Країни повинні бути здатні забезпечувати виконання як попередніх, так і остаточних рішень про конфіскацію, включаючи рішення, засновані на NCBC, навіть якщо вони не мають прямої відповідності у внутрішньому законодавстві. Процес

Висновки:

- **Необхідно негайно впровадити або посилити повноваження щодо NCBC/розширеної конфіскації та забезпечити їхнє подвійне використання (Dual Track):** Юрисдикції повинні мати повноваження NCBC, що охоплюють усі серйозні злочини (ВК, ФТ, предикатні злочини), і особливо активно використовувати їх у справах, пов'язаних з організованою злочинністю, корупцією або віртуальними активами, де отримання кримінального вироку є складним або неможливим (наприклад, у випадках втечі, смерті чи невідомого злочинця). Практична дія: Забезпечити, щоб фінансові розслідування завжди розглядали можливість паралельного (подвійного) застосування як CBC, так і NCBC, щоб максимізувати повернення активів.
- **Інституціоналізувати повноваження щодо призупинення транзакцій та інтегрувати планування АМ:** Компетентні органи (ПФР або ПО) повинні мати чіткі законні повноваження прямо чи опосередковано призупиняти транзакції (включаючи операції з віртуальними активами та нерухомістю) на короткий, визначений період (на основі підозри), щоб швидко запобігти розсіюванню коштів, перш ніж буде отримано більш тривалий судовий наказ про арешт/вилучення. Практична дія: Розробити та застосовувати обов'язкове планування управління активами (pre-seizure planning) для кожного значного арешту, щоб оцінити вартість, ризики та стратегії збереження активів, включаючи залучення спеціалізованих експертів для складних активів (наприклад, віртуальних активів, бізнесу).
- **Пріоритезувати неформальне міжнародне співробітництво та спеціалізацію ПА:** Активно використовувати неформальні канали співробітництва (наприклад, ARINs, прямий зв'язок між ПО/прокурорами) на ранніх стадіях розслідування для проактивного обміну інформацією щодо ідентифікації та відстеження активів. Практична дія: Центральним органам влади слід налагоджувати зв'язки між запитуючими прокурорами та виконавцями запитів у запитуваній державі, щоб консультуватися щодо вимог законодавства та обговорювати проєкти наказів, які мають бути виконані, до подання офіційного запиту MLA, уникаючи затримок через технічні дефекти.
- **Забезпечити прозорість і підзвітність використання активів з акцентом на жертвах:** Забезпечити чіткі механізми повернення конфіскованого майна його законним власникам або компенсації жертвам, що є пріоритетною метою. Практична дія: Встановити фонди повернення активів (Asset Recovery Funds) для управління конфіскованими коштами, забезпечуючи їхнє прозоре використання для компенсації жертвам, реінвестування у правоохоронну діяльність та громадські проекти, а також запровадити незалежний нагляд та аудит рішень щодо використання цих коштів.

виконання іноземних рішень має бути спрощеним, усуваючи необхідність проведення дублюючих внутрішніх розслідувань.

Управління активами (АМ) є необхідним для збереження вартості арештованого майна. Це включає ретельне планування перед арештом (pre-seizure planning), оцінку активів та управління ризиками. Продаж активів до конфіскації (interlocutory sales) може бути дозволений для майна або активів, які можуть швидко зіпсуватися, витрати на утримання яких непропорційні їхній вартості, забезпечуючи при цьому належну судову санкцію та прозорість. Кінцеве використання конфіскованих активів включає повернення законним власникам або компенсацію жертвам злочинів, а також реінвестування у правоохоронні органи, громадські програми або використання для поповнення державного бюджету.

При впровадженні нових інструментів ПА, особливо NCBC та розширеної конфіскації, необхідно забезпечити захист прав постраждалих осіб. Це передбачає забезпечення належної правової процедури (повідомлення та право оскаржити дії держави) та дотримання принципу пропорційності, щоб уникнути надмірного або невиправданого позбавлення майна. Репутація системи ПА в цілому залежить від професіоналізму та доброчесності, з якими ці значні повноваження застосовуються.

Повідомлення щодо політики розширення ЄС за 2025 рік [2]

Даний документ є щорічним стратегічним документом Європейської Комісії, який визначає загальний стан, динаміку та пріоритети політики розширення Європейського Союзу. У ньому оцінюється прогрес країн-кандидатів та потенційних кандидатів на вступ, зокрема України, Молдови, країн Західних Балкан, Туреччини та Грузії. Документ має геополітичний характер і розглядає розширення як інструмент посилення європейської безпеки, стабільності та демократичних цінностей, наголошуючи на тому, що процес приєднання залишається суворо заснованим на принципі «merit-based» — тобто залежить від реального виконання реформ і наближення до стандартів ЄС у сферах верховенства права, прав людини, економічного управління та спільної зовнішньої політики.

У Повідомленні Європейська Комісія приділяє Україні особливу увагу, визнаючи її як одного з головних кандидатів на вступ до ЄС, який демонструє послідовність реформ навіть в умовах триваючої війни. Документ зазначає, що Україна завершила технічний процес по чотирьох кластерах acquis — «фундаментальні принципи», «внутрішній ринок», «конкурентоспроможність і інклюзивне зростання» та «зовнішні відносини». Комісія оцінила, що ці кластери готові до відкриття переговорів. У травні 2025 року Україна ухвалила дорожні карти реформ у сферах верховенства права, державного управління, функціонування демократичних інститутів та план дій щодо національних меншин — у відповідності з рекомендаціями Єврокомісії.

Підкреслюється, що, попри наслідки російської агресії, Україна демонструє високу політичну волю та стабільне виконання реформ, особливо в антикорупційній сфері, де ЄС позитивно оцінив відновлення незалежності антикорупційних інституцій після спроб їхнього ослаблення. Водночас Комісія наголошує на потребі «сталого і поступового прогресу» у боротьбі з корупцією

[2] https://enlargement.ec.europa.eu/document/download/eb69a890-40d6-4696-801e-612d51709fdd_en?filename=2025%20Communication%20on%20EU%20Enlargement%20Policy.pdf

на високому рівні та у забезпеченні невідворотності реформ. «Ukraine Plan» у межах Ukraine Facility визначається як центральний елемент, який координує процес відновлення, структурних реформ і поступової інтеграції до внутрішнього ринку ЄС.

Єврокомісія вказує, що антикорупційні заходи, реформа публічної адміністрації та модернізація судової системи є фундаментом для стійкого розвитку та залучення приватного сектору до відбудови. Значним проривом визнано поступ у поступовій інтеграції України до внутрішнього ринку ЄС. Зокрема, з 1 січня 2026 року набуде чинності рішення про режим «Roam like at home», що фактично включить Україну до спільного простору телекомунікацій. Україна також готує приєднання до системи SEPA, що забезпечить повну інтеграцію у єдину зону єврових платежів, зниження транзакційних витрат і зміцнення прозорості фінансової системи.

У розділі щодо верховенства права відзначається, що Україна продовжує реалізацію секторальних реформ, включно з прозорим відбором суддів і підвищенням відповідальності судових органів. Комісія позитивно оцінює зміцнення незалежності судової влади та створення передумов для ефективної протидії корупції. Водночас підкреслено необхідність послідовного застосування антикорупційного законодавства і подальшого зміцнення спроможності правоохоронних органів.

В економічному контексті ЄС визнає стійкість української економіки, яка у 2024 році зросла на 2,9%, незважаючи на воєнні дії. Однак від середини 2025 року зростання сповільнилося через посилення російських атак на критичну інфраструктуру. У межах Ukraine Facility ЄС мобілізував €31,3 млрд, з яких €22,7 млрд спрямовано безпосередньо до бюджету України як підтримку реформ. Станом на жовтень 2025 року Україна виконала 44 реформаційні кроки, зокрема посилення корпоративного управління, боротьбу з ухиленням від податків, прийняття Національного енергетичного і кліматичного плану, а також кліматичного закону.

Висновки:

- **Реформи та інтеграція:** Україна виконала значну частину дорожньої карти реформ (44 кроки) і готова до відкриття переговорів за чотирма кластерами acquis, особливо у сферах верховенства права, антикорупційної політики та державного управління.
- **Економічна підтримка:** ЄС надав Україні €31,3 млрд у межах Ukraine Facility, що забезпечує фінансування реформ, відбудову та макрофінансову стабільність.
- **Поступова інтеграція:** З 2026 року Україна приєднається до режиму «Roam like at home» та готується до входження у SEPA, що є ключовими кроками до повної інтеграції у внутрішній ринок ЄС.
- **Пріоритети подальших дій:** ЄС очікує на посилення боротьби з корупцією на високому рівні, подальше зміцнення незалежності судової системи, розширення антикорупційного треку та підвищення прозорості фінансових операцій, зокрема у сфері відмивання коштів і криптовалют.

Україна активно бере участь у регіональному співробітництві, включно з ініціативами Чорноморського регіону, Східного партнерства, Організації Чорноморського економічного співробітництва тощо. ЄС наголошує на стратегічній ролі України в забезпеченні стабільності в регіоні та інтеграції енергетичних ринків. Заплановано повну інтеграцію енергетичного ринку України з ринком ЄС до 2027 року, що розглядається як ключовий елемент економічного зближення.

Комісія також визнає поступ України у контролі за стрілецькою зброєю (SALW) та у боротьбі з організованою злочинністю, наголошуючи на важливості подальшого зміцнення потенціалу фінансових розслідувань, запобігання відмиванню коштів та фінансуванню тероризму. Україна, як зазначено, продемонструвала прогрес у систематичному запуску фінансових

розслідувань, але потребує подальшого розвитку інституційних механізмів для ефективного вилучення активів, зокрема у криптосфері.

У сфері прав людини відзначено ухвалення законів, що зміцнюють права меншин та дітей, а також підтримку інститутів громадянського суспільства. Разом з тим, Україна має продовжувати роботу над забезпеченням належних умов у місцях позбавлення волі, запобіганням катувань, розширенням участі жінок і меншин у суспільному житті.

Санкційні ризики для окремих банківських послуг [3]

Даний документ є консультативною запискою Австралійського офісу із питань санкцій (ASO). Цей документ інформує піднаглядну спільноту про нові виклики та значні санкційні ризики, пов'язані з використанням певних банківських послуг, підкреслюючи, що хоча він містить резюме відповідних законів, він не є заміною незалежній юридичній консультації, а забезпечення відповідності австралійському санкційному законодавству залишається відповідальністю користувачів. У записці детально розглянуто чотири ключові механізми, які можуть бути використані для обходу санкцій, приділяючи особливу увагу ознакам, що підвищують ризик.

Першим із розглянутих напрямків є торговельне фінансування, яке є критично важливим для міжнародної та внутрішньої торгівлі, оскільки допомагає зменшити ризики для імпортерів та експортерів. Однак цей інструмент часто зловживається шляхом надання неправдивої, зміненої або неповної документації (наприклад, для акредитивів, документарних інкасо, торгових позик чи розрахункових послуг). Санкційні ризики значно зростають, якщо клієнт раніше мав торговельні відносини із суб'єктами або юрисдикціями, які тепер підпадають під санкції, або якщо він веде торгівлю з юрисдикціями, які мають вищий ризик обходу санкцій (зазвичай це країни, що не визнають чи не дотримуються автономних санкцій). Додаткові індикатори ризику включають торгівлю товарами, що підпадають під санкції, надання неповної або суперечливої документації для підтримки транзакції, а також використання для перевезення фізичних товарів суден високого ризику, включно із суднами, ідентифікованими як частина так званого «Тіньового флоту», або незвичних та непрямих маршрутів доставки. ASO спеціально опублікував додаткові рекомендації щодо ідентифікації російських методів ухилення.

Наступним механізмом, який несе підвищений санкційний ризик, є бук-трансфери (book transfers, або внутрішні перекази), що являють собою переміщення активів чи коштів у межах однієї облікової системи без фізичного руху грошей. Цей механізм ідентифіковано як спосіб обходу санкцій в інших юрисдикціях, особливо коли транзакції відбуваються між рахунками, що належать різним особам чи підприємствам. Ризики бук-трансферів посилюються при використанні складних структур бенефіціарної власності, що дозволяє прямо чи опосередковано здійснювати платежі підсанкційним особам, наприклад, для виплати дивідендів чи прибутків компаніям. Головна проблема полягає в тому, що бук-трансфери знижують прозорість, ускладнюючи ідентифікацію базових транзакцій, які можуть порушувати санкційне законодавство, тим самим ускладнюючи процеси комплаєнсу, належної перевірки та аудиту.

[3] https://www.dfat.gov.au/international-relations/security/sanctions/guidance/sanctions-risks-specific-banking-services

Також у документі акцентовано увагу на рахунках «Ностро» та «Востро», які використовуються для міжнародних транзакцій та розрахунків між банками-кореспондентами. Ці рахунки є вразливими для експлуатації підсанкційними суб'єктами чи особами, оскільки банк-ініціатор не завжди має повну видимість щодо кінцевих бенефіціарних власників або мети транзакцій. Банки повинні гарантувати, що їхні кореспондентські відносини не залучають підсанкційних осіб і не сприяють наданню активів. Ризик значно посилюється при використанні «вкладених кореспондентських банківських відносин» (nested correspondent banking), де існує кілька рівнів кореспондентських зв'язків, що ще більше ускладнює належну перевірку. Крім того, ці рахунки часто використовуються заможними особами, такими як російські олігархи, які мають доступ до складних фінансових механізмів.

Четвертим важливим питанням, що розглядається, є неттінг (залік взаємних зобов'язань), який є договірною або операційною домовленістю між сторонами про взаємозалік, що призводить до єдиного чистого платежу. Хоча неттінг підвищує операційну ефективність, він створює значні санкційні ризики, якщо ним не керувати обережно. Основні ризики неттінгу включають непряму участь підсанкційних сторін, оскільки санкції забороняють непряму вигоду, а базові зобов'язання, що підлягають заліку, можуть бути пов'язані з підсанкційним суб'єктом. Виникає ризик сприяння (facilitation), якщо неттінг приносить користь або очищає зобов'язання підсанкційної особи, навіть опосередковано. Існує також концепція «конструктивного отримання» (constructive receipt), коли неттінг дозволяє підсанкційній стороні отримати вигоду від зменшення зобов'язань без фактичного переказу коштів. Як і у випадку бук-трансферів, неттінг знижує прозорість, ускладнюючи ідентифікацію порушень санкційного законодавства.

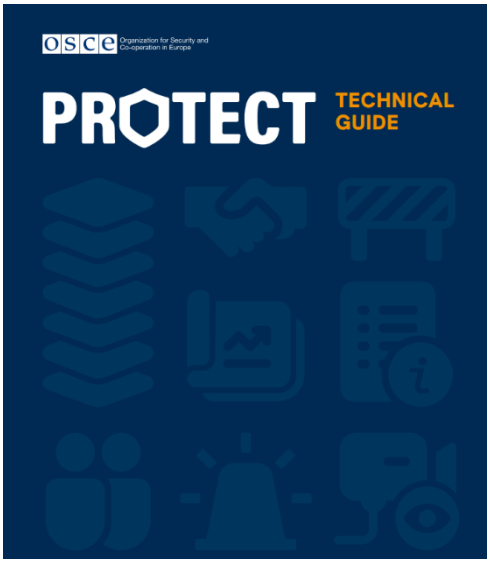
Загальні індикатори підозрілої діяльності (хоча і не вичерпні) включають ситуації, коли експортери відвантажують продукцію без відповідних чи достатніх міжнародних платежів, імпортери купують товари, маючи мало доказів платежів, або коли існують розбіжності між країнами призначення товарів та юрисдикціями, з яких надходять платежі. На завершення, документ підкреслює, що дотримання санкцій є постійним зобов'язанням, яке потребує безперервного моніторингу та переоцінки стратегій комплаєнсу, оскільки санкційні

Висновки:

- **Посилення перевірки торгівлі та логістики:** Необхідно впровадити обов'язкову поглиблену перевірку документації та логістичних ланцюгів у торговельному фінансуванні, звертаючи особливу увагу на відповідність даних, КБВ та використання високоризикових суден, які належать до тіньового флоту, або непрямих маршрутів, оскільки ці фактори прямо вказують на спроби обходу санкцій.
- **Забезпечення прозорості внутрішніх механізмів:** Банки повинні розробити спеціальні внутрішні політики моніторингу та аудиту для бук-трансферів та операцій неттінгу, щоб запобігти використанню складної структури власності для прихованої виплати дивідендів або взаємозаліку зобов'язань підсанкційних осіб, оскільки ці механізми критично знижують прозорість.
- **Мінімізація ризику кореспондентських відносин:** Слід встановити суворіші стандарти належної перевірки для рахунків «Ностро»/«Востро», активно виявляючи та керуючи ризиками «вкладених кореспондентських банківських відносин» та контролюючи операції, що залучають заможних осіб, забезпечуючи повну видимість КБВ та мети операції.
- **Встановлення циклічності комплаєнсу:** Підзвітні суб'єкти повинні сприймати дотримання санкцій не як одноразову оцінку, а як безперервний процес, що вимагає постійного моніторингу, регулярної переоцінки стратегій комплаєнсу та використання спеціалізованих інструментів (наприклад, Sanctions Risk Assessment Tool) для адаптації до мінливого санкційного середовища.

заходи та ризики постійно розвиваються. Регульованим суб'єктам настійно рекомендується звертатися за незалежною юридичною консультацією та використовувати додаткові ресурси ASO, такі як Інструментарій з комплаєнсу та Керівництво щодо російських методів ухилення.

Міркування щодо фізичної безпеки для захисту критичної інфраструктури від терористичних атак [4]



Документ є спеціалізованим технічним посібником, розробленим у межах проєкту OSCE Project PROTECT. Його підготовлено під егідою Підрозділу з протидії тероризму (ATU) Департаменту транснаціональних загроз ОБСЄ. Посібник має на меті надати державам-учасницям ОБСЄ, політикам, власникам критичної інфраструктури (КІ), операторам та приватним охоронним структурам структуровані орієнтири щодо зміцнення фізичної безпеки об'єктів КІ для запобігання, підготовки та пом'якшення наслідків терористичних атак. Документ поєднує політичні, стратегічні, правові, технічні, а також правозахисні аспекти, створюючи всеохопну рамку, що базується на досвіді держав-учасниць ОБСЄ, рекомендаціях ООН та кращих міжнародних практиках.

Посібник підкреслює, що критична інфраструктура (КІ) — це основа сучасного суспільства, адже її системи забезпечують енергію, транспорт, воду, зв'язок і цифрові сервіси, від яких залежить безперервність економіки та добробут населення. Саме тому КІ є привабливою ціллю для терористичних і екстремістських угруповань. Через взаємозалежність таких систем навіть одинична атака може призвести до каскадних ефектів, порушивши роботу інших секторів (наприклад, енергетика → транспорт → медичні заклади). ОСБЄ наголошує, що мета посібника — допомогти державам формувати цілісну політику захисту, яка включає як фізичну безпеку, так і кіберзахист, правові рамки та людський фактор.

Документ деталізує мандат ОБСЄ у сфері захисту критичної інфраструктури, починаючи з Рішень Міністерської ради №5/07 та №6/07 (2007 р.) і Рамкової програми боротьби з тероризмом (2012 р.), що визначили пріоритетом підвищення безпеки міжнародного транспорту та інших об'єктів КІ. Також наведено зв'язок із резолюцією РБ ООН №2341 (2017), яка зобов'язує держави-учасниці створювати національні стратегії протидії атакам на КІ, розвивати партнерства державного і приватного секторів та зміцнювати міждержавне співробітництво.

Окремо описано проєкт OSCE PROTECT, запущений у 2023 році, який складається з трьох напрямів: (1) консолідація практик та підготовка технічних керівництв (цей посібник є одним із результатів); (2) підвищення національного потенціалу через навчання і тренінги; (3) розвиток регіональної співпраці, включно з участю приватного сектору та громадянського суспільства.

У теоретичній частині посібник пояснює відмінності між "захистом критичної інфраструктури (CIP)" та "стійкістю критичної інфраструктури (CI resilience)". Якщо перше зосереджується на запобіганні та фізичному захисті активів, то друге спрямоване на забезпечення неперервності послуг навіть у разі нападу. Як приклад наведено Директиву ЄС 2022/2557 (CER Directive), яка змінила попередній підхід до охорони КІ, зосередивши увагу на здатності держав і операторів КІ запобігати, протидіяти, адаптуватися та відновлюватися після інцидентів. Водночас

[4] https://www.osce.org/files/f/documents/e/6/597756_0.pdf

підкреслено взаємозв'язок з NIS2 Directive (2022/2555), що визначає високий рівень кібербезпеки, наголошуючи на "cyber-physical convergence" — єдності фізичного й кіберзахисту.

Посібник має багаторівневу структуру:

1. Стратегічно-правові засади

Цей рівень формує нормативно-інституційне підґрунтя для розбудови системи безпеки критичної інфраструктури. Документ наголошує, що ефективний захист КІ можливий лише тоді, коли національне законодавство чітко визначає компетенції органів державної влади, механізми координації, стандарти безпеки та процедури взаємодії з приватним сектором. У межах ОБСЄ існують значні розбіжності між державами-учасницями щодо рівня розвиненості цих механізмів — від централізованих моделей (як у Франції чи Польщі), до гібридних або регіонально диференційованих (як у США чи Німеччині). Посібник підкреслює важливість гармонізації з положеннями Директиви ЄС 2022/2557 (CER Directive), яка вводить нову концепцію «критично важливих суб'єктів» (essential entities) і зобов'язує держави створювати національні стратегії стійкості КІ. У статті 13 цієї директиви визначено мінімальні вимоги до фізичної безпеки, зокрема обов'язковість оцінки ризиків, планів безперервності діяльності та внутрішнього контролю доступу. Також посібник підкреслює роль міжурядових рамок, як-от Резолюція РБ ООН №2341 (2017), яка покладає на держави обов'язок запровадити комплексний захист об'єктів КІ від тероризму.

2. Права людини та принципи правомірності заходів безпеки

Фізична безпека не може розглядатися ізольовано від правових гарантій і міжнародних зобов'язань держав. Посібник особливо наголошує, що заходи із запобігання терористичним атакам повинні відповідати Міжнародному пакту про громадянські та політичні права, а також Кодексу поведінки приватних охоронних компаній (ICoC). Особливу увагу приділено недопущенню надмірного втручання у приватне життя, дискримінаційних перевірок та неправомірного використання біометричних даних. Залучення приватних охоронних структур до охорони КІ має супроводжуватись суворим контролем, чіткими контрактними зобов'язаннями, стандартами застосування сили та процедурами звітування. Посібник акцентує на важливості прозорості, підзвітності та дотримання прав людини у будь-яких заходах, що здійснюються в рамках антитерористичного захисту.

3. Партнерства держави й бізнесу (Public–Private Partnerships, PPP)

Близько 80% об'єктів КІ у державах ОБСЄ належать або управляються приватними суб'єктами, тому посібник визначає партнерство між державними органами та бізнесом як наріжний камінь ефективної системи захисту. У цьому контексті держави мають створювати координаційні платформи для обміну інформацією про загрози, інциденти та вразливості. Рекомендовано впровадження Information Sharing and Analysis Centres (ISACs) — центрів аналітики, що збирають і поширюють інформацію між операторами КІ та органами безпеки. ОБСЄ наголошує на необхідності єдиних стандартів комунікації, конфіденційності та класифікації ризиків, щоб забезпечити своєчасне попередження про потенційні атаки. PPP також мають сприяти спільним навчанням, сертифікації систем безпеки та координації дій у кризових ситуаціях.

4. Технічні заходи фізичної безпеки

Цей рівень охоплює конкретні інженерні та технологічні рішення, спрямовані на запобігання несанкціонованому доступу, виявлення та стримування атак. Посібник рекомендує підхід «defence-in-depth» — багаторівневу систему захисту, де кожен елемент є частиною єдиного ланцюга безпеки. До таких заходів належать: укріплені периметри (огорожі, бар'єри, боларди), контроль доступу з використанням багатофакторної ідентифікації, відеоспостереження з аналітикою поведінки, системи виявлення вибухівки або хімічних агентів, технології скринінгу транспортних засобів і персоналу. Особливо підкреслюється необхідність інтеграції фізичних

систем безпеки з кіберінфраструктурою моніторингу, що дозволяє відстежувати події в режимі реального часу та координувати дії між диспетчерами, службами охорони і поліцією.

5. Оцінка загроз і ризиків

Посібник орієнтований на впровадження ризик-орієнтованої методології (Risk-Based Performance Standards, RBPS). Це означає, що рівень захисту має відповідати оціненому рівню ризику, а не бути універсальним для всіх об'єктів. Рекомендовано проводити систематичну оцінку загроз із врахуванням усіх потенційних сценаріїв: вибухові пристрої, атаки з використанням транспортних засобів, диверсії на енергетичних об'єктах, CBRN-загрози, кібератаки, а також інсайдерські ризики. Методологія має включати три етапи: ідентифікацію активів, аналіз вразливостей і визначення потенційних наслідків. Для зменшення суб'єктивності рекомендується використання кількісних показників ризику та регулярне оновлення бази даних загроз.

6. Планування безпеки та реагування

Цей рівень охоплює комплекс заходів, спрямованих на підготовку до інцидентів, їх локалізацію та мінімізацію наслідків. Документ детально описує процедури планування безпеки для різних сценаріїв атак — від фізичного вторгнення до застосування хімічних чи біологічних агентів. Особлива увага приділяється створенню Emergency Response Plans (ERP) та Business Continuity Plans (BCP), що визначають відповідальних осіб, алгоритми дій, евакуаційні маршрути, резервні джерела енергії та комунікації. Крім того, наголошується на важливості кризових комунікацій — прозорого й оперативного інформування громадськості, щоб запобігти паніці та дезінформації.

7. Управління інсайдерськими загрозами

Інсайдерські загрози визнаються одним із найскладніших викликів у сфері захисту КІ. Посібник радить впроваджувати системи перевірки персоналу, моніторинг поведінкових аномалій, програми довіри, а також політику нульової толерантності до порушень внутрішньої безпеки. До ключових індикаторів належать нетипові робочі дії, спроби несанкціонованого доступу, незвичні комунікації або прояви радикалізації. ОБСЄ рекомендує створювати внутрішні канали анонімного повідомлення, проводити періодичні оцінки доброчесності персоналу та застосовувати принцип розподілу обов'язків.

Висновки:

- **Інституційна інтеграція:** Державам необхідно створювати міжвідомчі механізми координації для поєднання фізичної, кібер- та правової складових у системах безпеки КІ відповідно до стандартів CER і NIS2.
- **Ризик-орієнтований підхід:** Впровадження систем оцінки ризиків, які враховують усі типи загроз (вибухи, CBRN, кібератаки, інсайдери), має стати обов'язковою практикою для операторів КІ.
- **Партнерства та навчання:** Ефективний захист КІ можливий лише за умов постійного діалогу між державними структурами, приватними операторами та правоохоронними органами, з акцентом на регулярне навчання персоналу.
- **Фокус на стійкість, а не лише захист:** Підхід до безпеки КІ має еволюціонувати від реактивного ("захист об'єкта") до проактивного — забезпечення безперервності критичних послуг навіть під час атак чи криз.

8. Підготовка та тренування персоналу

Фінальний рівень системи — розвиток людського потенціалу. Посібник підкреслює, що навіть найдосконаліші технічні рішення втрачають ефективність без належно підготовленого персоналу. Рекомендується проводити регулярні навчання, тренінги, кризові симуляції, а також спільні навчання з поліцією, пожежними, медичними службами і військовими структурами. Участь

приватного сектору є ключовою, оскільки саме оператори КІ мають забезпечувати оперативне реагування на загрози. Посібник радить впровадити систему сертифікації охоронного персоналу, навчальні програми з управління ризиками, кризового лідерства та психологічної стійкості.

Посібник послідовно підкреслює, що жодна система фізичної безпеки не може бути ефективною без системного управління ризиками, міжвідомчої координації та дотримання прав людини. Високий рівень приватного сектору у володінні об'єктами КІ вимагає формування сталих публічно-приватних партнерств, а також впровадження принципів "defence-in-depth" — багаторівневого захисту об'єктів, де кожен елемент (від огорожі до кіберзахисту) є складовою єдиної системи.

Кохання як зброя: як банки мають протидіяти романтичному шахрайству[5]

У новому звіті Financial Conduct Authority (FCA) розкрито одну з найскладніших і водночас найбільш емоційно руйнівних форм фінансових злочинів сучасності — romance fraud, романтичне шахрайство або шахрайство "на довірі". Цей вид злочину базується на маніпуляції людськими почуттями, коли злочинці, видаючи себе за потенційних партнерів, вибудовують довготривалі "стосунки" онлайн, а потім переконують жертву надсилати їм гроші, дарунки чи навіть брати кредити.

Згідно з даними FCA, лише за фінансовий рік 2024–2025 жертви втратили понад £106 мільйонів, а середній збиток на одну особу склав £11 222 — і це лише офіційно зафіксовані випадки. Реальні масштаби можуть бути в рази більшими, адже багато людей не звертаються до поліції через сором і страх бути осміяними.

FCA провела міжгалузевий аналіз шести банків і платіжних компаній у Великій Британії, щоб оцінити ефективність їхніх систем виявлення, попередження та підтримки жертв романтичного шахрайства. Розслідування охопило 60 підтверджених випадків, у яких збитки варіювались від £100 до £428 249. Регулятор дійшов висновку, що, попри наявність передових технологій моніторингу, людський фактор залишається вирішальним — саме дії або бездіяльність працівників банків часто визначають, чи буде шахрайство зупинене, чи жертва продовжить втрачати кошти.

Вражаючим є той факт, що 85% випадків починаються з онлайн-платформ — сайтів знайомств або соціальних мереж. Шахраї діють за однаковим сценарієм: створюють вигаданий образ (часто військовий, лікар, інженер або підприємець), поступово здобувають довіру жертви, а потім переходять до фінансових прохань. Спершу це можуть бути дрібні платежі — "на ліки", "на квиток", "на подарунок" — щоб не викликати підозри. Ці суми виглядають як звичайні транзакції, тому навіть автоматичні системи банків не помічають небезпеки. Коли ж довіра встановлена, починається фаза ескалації, і суми переказів зростають у десятки разів.

Банки, своєю чергою, стикаються з дилемою: втручання у "особисті стосунки" клієнта може викликати скарги або навіть звинувачення у дискримінації. Проте FCA наголошує: відсутність реакції означає потурання злочину. Деякі фінансові установи продемонстрували зразкову роботу — блокували перекази, коли виявляли підозрілі моделі платежів, створювали "перепони" у процесі оплати (наприклад, вимагали підтвердження через дзвінок менеджера) і

[5] https://www.fca.org.uk/publications/multi-firm-reviews/combating-romance-fraud-prevention-detection-and-supporting-victims

навіть навчали клієнтів розпізнавати шахрайські маніпуляції. В окремих випадках саме завдяки такому підходу вдалося врятувати десятки тисяч фунтів, які інакше пішли б на криптогаманці злочинців.

Водночас огляд FCA показав і серйозні прогалини: у 25% випадків жертви брали кредити або продавали власне майно, щоб профінансувати "кохану людину", а банки не реагували на аномальну активність. У деяких випадках люди здійснювали сотні дрібних переказів протягом року — один клієнт зробив 403 транзакції на суму понад £72 000, і жодна не була зупинена. Це свідчить про брак аналітики поведінкових шаблонів та надмірну залежність від стандартних алгоритмів, що не враховують емоційного контексту злочину.

Ще одна важлива проблема — низький рівень кваліфікації персоналу. У частині установ працівники не розпізнавали ознак обману або приймали пояснення жертв за чисту монету. Наприклад, один клієнт намагався переказати £190 000 "на купівлю нерухомості для нареченої за кордоном", інший — відправити криптовалюту до Іраку "військовому партнеру", і обидва платежі були схвалені без перевірки. FCA прямо зазначає: співробітники повинні бути підготовлені не лише технічно, але й психологічно, щоб уміти спілкуватися з жертвами маніпуляцій, які часто відмовляються визнавати себе ошуканими.

Важливим елементом нової політики є виявлення вразливих клієнтів і повторного шахрайства. 15% жертв раніше вже ставали жертвами інших схем, проте не отримали належного моніторингу. FCA рекомендує банкам запровадити "вразливі маркери" у клієнтських профілях, які активують підвищений рівень перевірки під час великих переказів або незвичних транзакцій. Такі системи вже працюють у деяких британських банках, де кожен випадок шахрайства супроводжується індивідуальним наглядом і періодичними дзвінками клієнтові, щоб запобігти повторним злочинам.

У межах аналізу FCA також відзначила практику "психологічного реагування": у найкращих установах працівники не лише блокували транзакції, а й супроводжували жертву психологічно — проводили кілька дзвінків протягом кількох тижнів, спрямовували до благодійних організацій і пояснювали, що шахрайство не є "виною клієнта". В одному випадку банк провів 11 контактів протягом шести тижнів, допомігши клієнтці вийти з-під контролю шахрая і повернути частину коштів.

Попри ці успіхи, FCA вказує на відсутність єдиного стандарту реагування в галузі. Одні банки впроваджують прогресивні політики, інші — продовжують покладатися на шаблонні повідомлення або "автоматизовані скрипти", які не враховують людський фактор.

Регулятор вимагає створення галузевого стандарту боротьби, який об'єднає державу, фінансові інституції та онлайн-платформи в спільну екосистему обміну інформацією. Особливо важливим визнано взаємодію з соціальними

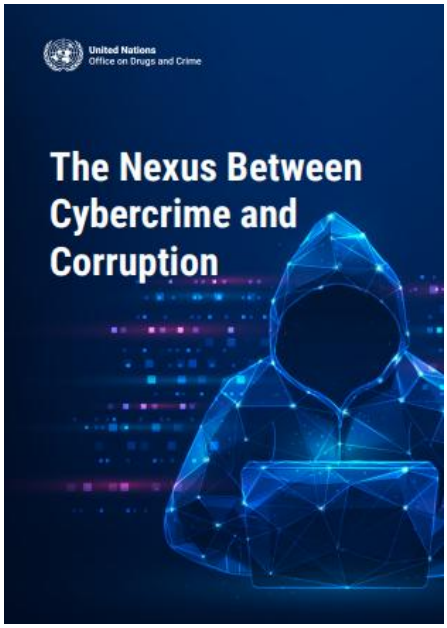
Висновки:

- **Фінансовим установам необхідно запровадити спеціальні протоколи** для виявлення «емоційно зумовлених» транзакцій — коли поведінка клієнта різко змінюється, а платежі мають нетиповий характер, навіть без технічних ознак шахрайства.
- **Банки мають створити програми "людської взаємодії" —** персональні дзвінки, верифікаційні розмови та консультації для клієнтів, які можуть бути під психологічним впливом шахраїв.
- **Потрібно інтегрувати фінансову безпеку в інформаційні кампанії** про цифрову грамотність, поєднуючи психологічну освіту, кіберзахист і правові поради для потенційно вразливих груп населення.
- **Регулятори мають встановити обов'язковий стандарт** для всіх банків щодо реагування — включно з процедурами підтримки жертв, обміну даними та компенсаційних механізмів.

мережами, адже саме вони є первинним джерелом більшості випадків.

У підсумку FCA дійшла до чіткої тези: боротьба з романтичним шахрайством — це не лише фінансова, а й соціальна відповідальність. Це новий тип кіберзлочину, де фінансова грамотність, психологічна підтримка та міжгалузева співпраця є так само важливими, як і технічні інструменти моніторингу. Злочинці використовують емоції як зброю, і лише системна, гуманна реакція здатна зупинити їхній вплив. Банки мають перестати бути пасивними спостерігачами і стати активними учасниками у захисті громадян від маніпуляцій, що руйнують життя. У час, коли технології стають інструментом зла, саме емпатія, критичне мислення та міжсекторальна співпраця залишаються найефективнішою лінією оборони

Кібер-корупція як нова архітектура злочинності: як цифрова доба змінила природу влади, грошей і безкарності [6]



Системне дослідження UNODC демонструє, що в XXI столітті корупція перестала бути виключно політичним або адміністративним явищем і перетворилася на структурний елемент глобальної кіберзлочинності. Документ побудований на міжрегіональних кейсах з Африки, Південно-Східної Азії, Латинської Америки та пострадянського простору, і робить переконливий висновок: у цифрову добу хабарництво стало інфраструктурою кіберзлочинного світу, а не лише його наслідком. Кіберзлочинність і корупція зливаються в єдиний симбіоз — мережу, де державні посадовці, фінансові структури, технологічні компанії та організовані злочинні групи взаємно підживлюють одна одну.

UNODC підкреслює, що сучасна корупція вже не обмежується “традиційними” хабарями чи зловживаннями. Вона еволюціонувала у цифрову форму співучасті, де посадовці не просто покривають злочини, а беруть участь у створенні цифрових інструментів, що забезпечують їх безкарність. Саме завдяки таким практикам у багатьох країнах з’явилися цілі “корумповані цифрові екосистеми”, які дозволяють кіберзлочинним угрупованням діяти майже легально. Наприклад, державні реєстри, платіжні шлюзи або платформи електронних тендерів часто використовуються для “підчищення” цифрових слідів, маніпуляцій із закупівлями чи створення фіктивних компаній для переказу хабарів у криптовалюті.

Автори звіту наводять десятки кейсів, які демонструють цю взаємозалежність. У Східній Азії “scam factories” — величезні комплекси, де тисячі працівників здійснюють шахрайські дії в Інтернеті — функціонують лише тому, що їх прикривають місцеві чиновники, поліція й навіть окремі дипломати. В Африці злочинні структури на кшталт Black Axe діють під покровом політичної верхівки, перетворюючи отримані через шахрайство криптовалюти в “політичні інвестиції”, тобто хабарі. У Латинській Америці корупційні угоди часто укладаються не готівкою, а через цифрові токени, “віртуальні ваучери” або NFT, що дозволяють приховати хабар як нібито інвестиційну транзакцію.

UNODC називає цю модель “цифровим циклом безкарності”:

6 https://www.unodc.org/roseap/uploads/documents/Publications/2025/2025.10.21_The_Nexus_Between_Cybercrime_and_Corruption.pdf

- корупція відкриває доступ до інфраструктури або інформації;
- кіберзлочинність генерує прибуток;
- прибуток "відмивається" через цифрові активи;
- частина цих коштів повертається у вигляді хабарів — і коло замикається.

Таким чином, цифрова економіка стає середовищем взаємного симбіозу між незаконними доходами й владою. У деяких країнах це вже не просто тіньова діяльність — це "цифрова державність злочину", у якій кіберкорупційні зв'язки фактично визначають політику.

Звіт приділяє особливу увагу новим технологічним драйверам цього процесу. З одного боку, криптовалюти, блокчейн і штучний інтелект відкрили можливості для створення прозорих і безпечних систем. Але, з іншого — вони стали знаряддям прихованих транзакцій, шахрайських ICO, "смарт-контрактів" для хабарів і автоматизації відмивання коштів. У 2024–2025 роках кількість хабарів, здійснених у криптовалюті, зросла більш ніж утричі — не лише через анонімність, а й тому, що такі платежі неможливо скасувати чи відстежити у традиційній банківській системі.

Особливе місце у звіті займає аналіз ролі "внутрішніх агентів" — співробітників банків, IT-компаній, телекомів чи держустанов, які за винагороду надають доступ до баз даних, кодів верифікації або адміністрування систем. Це так званий "корупційний фундамент" кіберзлочинності, без якого будь-яка масштабна кібератака чи шахрайство неможливі. У ряді випадків такі працівники не лише "закривають очі", а й беруть участь у створенні шкідливого ПЗ або продажу даних користувачів.

UNODC також наголошує, що цифрова корупція дедалі частіше використовується для політичного контролю. У низці країн авторитарні уряди фінансують власні "кібергрупи", які одночасно атакують політичних опонентів і допомагають кримінальним структурам зберігати анонімність. У результаті з'являється нове явище — "гібридна корупційна держава", у якій корупція та кіберзлочинність зливаються з державною владою, створюючи цифрову олігархію.

Висновки:

- **Корупція є не лише наслідком, а фундаментом кіберзлочинності,** тому держави повинні створювати спільні антикорупційно-кіберпідрозділи, що розслідують злочини одночасно у фінансовому та цифровому вимірах.
- **Використання штучного інтелекту в аналітиці транзакцій і держзакупівель** може стати найефективнішим інструментом виявлення цифрових корупційних схем, якщо його застосовувати незалежно від політичного впливу.
- **Боротьба з кіберкорупцією вимагає єдиного глобального стандарту,** який поєднує норми UNCAC, UNTOC і нової Конвенції ООН проти кіберзлочинності, щоб уникнути «сірого простору безкарності» між юрисдикціями.
- **Приватний сектор, зокрема IT-компанії, криптоплатформи та фінансові посередники, повинен нести відповідальність** за моніторинг і попередження зловживань своїми технологіями, запроваджуючи етичні стандарти "цифрової доброчесності".

Однак у доповіді звучить і стриманий оптимізм. UNODC пропонує низку практичних рекомендацій для урядів і приватного сектору. Передусім — створення спільних підрозділів, що мають розслідувати злочини одночасно за двома лініями — цифровою та фінансовою. Розробка інтегрованих систем обміну даними між підрозділами фінансової розвідки (ПФР) і центрами реагування на кіберінциденти (CSIRT) дозволила б оперативно виявляти зв'язки між електронними транзакціями та корупційними схемами.

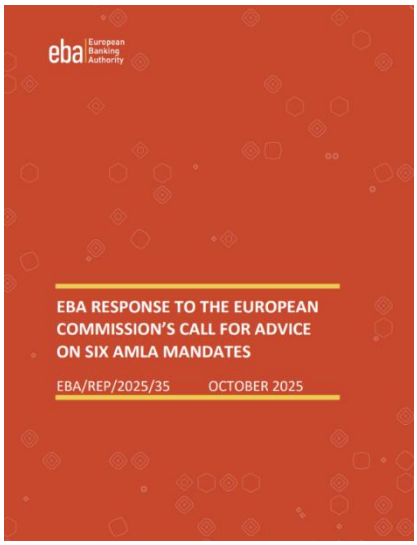
Ключовим елементом є впровадження аналітики на основі штучного інтелекту у сфері антикорупційного нагляду. Алгоритми можуть виявляти

“аномальні” транзакції — повторювані схеми платежів на пов’язані гаманці, сплески активності після тендерів чи політичних рішень, нетипову поведінку в цифрових системах держслужбовців. UNODC підкреслює, що такі системи повинні діяти незалежно від політичного впливу, щоб не перетворитися на інструмент переслідування.

Водночас автори наголошують: жодна технологія не здатна подолати корупцію без політичної волі. Без реальної незалежності судів, відкритості державних закупівель і захисту журналістів цифрові інструменти можуть лише створити ілюзію контролю.

Саме тому UNODC закликає до інтегрованої імплементації трьох ключових міжнародних інструментів — Конвенції ООН проти корупції (UNCAC), Конвенції ООН проти транснаціональної організованої злочинності (UNTOC) та нової Конвенції ООН проти кіберзлочинності (UNCC), що формує “трикутник відповідальності” сучасного світу.

Європейський банківський орган формує основу діяльності AMLA: нова архітектура єдиного нагляду та гармонізованих стандартів ПВК/ФТ у ЄС [7]



Документ є ключовою аналітичною та нормативною відповіддю Європейського банківського органу (EBA) на офіційний запит Європейської Комісії щодо розроблення технічних стандартів (RTS) і консультаційних пропозицій, покликаних сформувати операційну, методологічну та правову основу для новоствореного Європейського органу з протидії відмиванню коштів і фінансуванню тероризму (AMLA). Цей звіт є частиною реалізації нового пакета законодавства ЄС у сфері ПВК/ФТ, який охоплює 6 Директиву щодо боротьби з відмиванням грошей (AMLD6, Директива (ЄС) 2024/1640), Регламент про боротьбу з відмиванням коштів (AMLR, Регламент (ЄС) 2024/1624) та Регламент про створення AMLA (AMLAR, Регламент (ЄС) 2024/1620). У сукупності ці документи формують єдину систему нагляду за виконанням вимог ПВК/ФТ у межах Європейського Союзу, спрямовану на посилення узгодженості, пропорційності та ефективності протидії фінансовим злочинам.

EBA у своєму звіті розробила та подала шість масштабних блоків технічних рекомендацій, кожен з яких відображає стратегічну функцію AMLA в новій архітектурі фінансового моніторингу. Основна мета полягає у забезпеченні гармонізованого підходу до оцінювання ризиків, контролю, санкцій і групової політики у всіх державах-членах ЄС. Робота органу ґрунтувалася на п’яти керівних принципах: пропорційності, ефективності, технологічній нейтральності, максимальній гармонізації наглядових практик і мінімізації витрат для суб’єктів. В основу звіту покладено значний масив емпіричних даних, отриманих у результаті оглядів виконання ПВК/ФТ, аналізу інформації з бази EuReCA (Європейська система звітності про суттєві недоліки ПВК/ФТ), результатів національних оцінок ризиків, консультацій з понад 60 компетентними органами держав-членів, Європейським центральним банком, Європейськими наглядовими органами (ESMA, EIOPA), платформою ПФР, а також представниками приватного сектору і наукової спільноти. Такий інклюзивний процес підготовки забезпечив практичну спрямованість і узгодження рекомендацій із реальною регуляторною практикою.

[7] https://www.eba.europa.eu/sites/default/files/2025-10/b5a9a9aa-ce4f-4130-89a7-a19f2e791750/EBA%20response%20to%20EC%20CfA%20on%20six%20AMLA%20mandates%202025%2010%2030.pdf

Зміст документа охоплює низку концептуальних і технічних рішень, що безпосередньо формують майбутні операційні стандарти AMLA. Першим фундаментальним елементом є створення уніфікованої методології оцінювання властивого та залишкового ризику суб'єктів, на яких поширюються вимоги AMLD6. Ця методологія передбачає трирівневий процес: оцінку вихідного рівня ризику, визначення якості системи контролів і формування залишкового ризику з використанням стандартизованої шкали оцінювання та матричного підходу. Вперше пропонується встановити єдині показники (data points), що застосовуватимуться всіма наглядовими органами, а також розробити єдину інтерпретаційну нотатку, яка забезпечуватиме уніфіковане розуміння кожного показника в усіх державах ЄС. Цей підхід ліквідує фрагментарність національних практик, спрощує транскордонний нагляд і зменшує витрати на звітність для установ, які працюють у кількох юрисдикціях. Особливий акцент зроблено на тому, що контроль і перегляд профілів ризику мають здійснюватися щороку, а для малих або низькоризикових установ — не рідше ніж раз на три роки. Для нефінансового сектору (ВНУП) передбачено розроблення адаптованих RTS, що враховують відмінність бізнес-моделей і ризиків цих суб'єктів.

Другий важливий напрям — розроблення єдиної системи критеріїв для відбору кредитних та фінансових установ, які підлягатимуть прямому нагляду AMLA відповідно до статті 12 AMLAR. EBA пропонує застосування кількісних порогів для визначення «матеріальної присутності» установ у державах-членах, таких як мінімум 20 000 клієнтів-резидентів або обсяг транзакцій понад 50 мільйонів євро на території конкретної країни. Методологія оцінювання ризику для такого відбору базується на тій самій системі, що й загальна методика оцінювання ризиків за AMLD6, що гарантує порівнянність результатів і рівні умови для всіх суб'єктів. З метою уникнення регуляторних розбіжностей EBA обмежує можливості для національних коригувань та встановлює єдині стандарти для оцінювання як на рівні окремих установ, так і груп. Передбачено також плавний перехід до нової системи, оскільки перший цикл відбору для прямого нагляду AMLA розпочнеться у 2027 році.

Третій розділ присвячено гармонізації підходів до ідентифікації та перевірки клієнтів (CDD, SDD, EDD) відповідно до статті 28 AMLR. У документі наголошено, що новий Регламент скасовує національні відмінності у трактуванні вимог до клієнтської перевірки, усуваючи ризики регуляторних розбіжностей. EBA пропонує перейти від суто формалізованого до принципово-орієнтованого ризико-орієнтованого підходу, який дозволить установам обирати адекватні джерела перевірки особи залежно від контексту операції, типу клієнта та рівня ризику. Водночас встановлюється п'ятирічний перехідний період для оновлення даних по існуючих клієнтах, із пріоритетним охопленням високоризикових бізнес-відносин. Також звіт визнає значення електронних засобів ідентифікації (eIDAS) та кваліфікованих довірчих сервісів як інструментів для дистанційної перевірки клієнтів.

Особливо значущим є блок, присвячений санкціям, адміністративним заходам та періодичним штрафам (PePPs). EBA пропонує єдиний підхід до класифікації серйозності порушень на чотири рівні з чіткими індикаторами, що дозволить забезпечити однакове трактування подібних випадків у різних країнах. Запроваджується нова логіка визначення пропорційності та ефективності санкцій, у тому числі щодо фізичних осіб — членів керівних органів, чия відповідальність розглядається як ключовий елемент стримування порушень. Запропоновано створити у межах AMLA або під її координацією мережу практиків з питань правозастосування для обміну досвідом і забезпечення уніфікації підходів у застосуванні санкцій. Для забезпечення плавного переходу до нового режиму пропонується дата повного набрання чинності спільних правил — 10 липня 2027 року, що збігається з терміном імплементації AMLD6 у національні законодавства.

У частині, що стосується визначення базових сум штрафів (стаття 53(11) AMLD6), EBA пропонує AMLA розробити керівні принципи, які встановлюватимуть єдині правила для розрахунку

базових сум з урахуванням обороту, типу порушення та категорії суб'єкта. Передбачається чітке тлумачення ключових термінів («базова сума», «тип порушення», «категорія суб'єкта», «оборот») і поширення цих правил як на фінансові установи, так і на суб'єктів нефінансового сектору, з урахуванням принципу пропорційності.

Завершальний розділ присвячений розробленню технічних параметрів групових політик і процедур щодо обміну інформацією всередині корпоративних груп (стаття 16(4) AMLR). EBA наголошує, що ефективний внутрішньогруповий обмін інформацією є критично важливим для формування консолідованої оцінки ризиків, у тому числі щодо підозрілих операцій, клієнтів із високим ризиком або загальних типологій фінансових злочинів. Водночас такий обмін повинен суворо відповідати принципам захисту персональних даних. Рекомендується надати доступ установам усередині групи до повного спектру релевантної інформації, за умови належного дотримання принципів конфіденційності та недискримінації. Окремо підкреслюється необхідність уникати необґрунтованого «дерискінгу», коли клієнти або операції блокуються лише через те, що інша філія або дочірня компанія класифікувала їх як ризикові.

У цілому, документ EBA є комплексною програмою технічного і регуляторного переходу Європейського Союзу до єдиної системи нагляду за ПВК/ФТ, де AMLA виступатиме центральним координатором і стандартотворцем. Звіт забезпечує концептуальний баланс між централізацією нагляду та дотриманням принципу субсидіарності, між уніфікацією правил і врахуванням секторних особливостей. Його впровадження спрямоване на досягнення ключових стратегічних цілей — створення єдиного AML Rulebook, підвищення прозорості, консолідацію практик нагляду, скорочення регуляторних витрат і підвищення стійкості фінансової системи ЄС до відмивання коштів і фінансування тероризму.

Висновки:

- **Єдиний ризик-орієнтований підхід у межах ЄС.** EBA заклала основу для гармонізованої методології оцінки ризиків і нагляду, що підвищує прозорість, забезпечує єдині правила для всіх суб'єктів та усуває регуляторні розбіжності між державами-членами ЄС.
- **Пропорційність і технологічна нейтральність.** Пропозиції забезпечують можливість адаптації вимог до масштабу діяльності установ та сприяють цифровій ідентифікації клієнтів і автоматизованому аналізу ризиків.
- **Уніфіковані санкційні стандарти.** Вперше закладається єдина європейська методика визначення серйозності порушень і розрахунку штрафів, що зміцнить довіру до AMLA як наднаціонального наглядового органу.
- **Поступовий перехід і інституційна узгодженість.** Всі RTS узгоджені у часі із запуском AMLA (2027 рік) і містять перехідні положення, що зменшують адміністративне навантаження для піднаглядних установ.

Аналітична держава: роль статистичних процесів у зміцненні національної системи фінансового моніторингу [8]

Посібник GAFILAT, підготовлений за підтримки ЄС через EU Global Facility, є комплексним методологічним документом, спрямованим на підвищення спроможності держав-членів Латиноамериканської групи з протидії відмиванню коштів (GAFILAT) у сфері збирання, аналізу та використання статистичних даних для демонстрації ефективності національних режимів

[8] https://www.global-amlcft.eu/wp-content/uploads/2025/10/ENG-GAFILAT-Global-Facility-Handbook-for-strengthening-statistical-processes-and-tools_compressed-1.pdf

ПВК/ФТ. Його ключова ідея полягає в тому, що систематичне та методологічно обґрунтоване використання статистики є не лише технічним елементом відповідності Рекомендаціям FATF, а стратегічним інструментом забезпечення об'єктивності, узгодженості та доказовості у процесах взаємної оцінки. Автори підкреслюють, що хоча формально Рекомендація 33 FATF зобов'язує країни лише підтримувати наявність статистики щодо фінансової розвідки, розслідувань, конфіскацій і міжнародної співпраці, її реальна цінність проявляється тоді, коли дані перетворюються на основу аналітичних висновків, що дозволяють оцінити рівень ризиків, результативність заходів, а також спрямувати ресурси відповідно до принципів ризик-орієнтованого підходу.

Посібник докладно розкриває взаємозв'язок між статистикою та вимірюванням ефективності у системі FATF, пояснюючи, що достовірні та розподілені дані є опорою для формування висновків про досягнення одинадцяти результатів (Immediate Outcomes). У ньому наголошується, що статистика не може обмежуватись механічним підрахунком підозрілих операцій чи кримінальних справ — вона повинна забезпечувати контекстуалізоване уявлення про загрози, вразливості, якість реагування та фактичний вплив політик. Документ окреслює основні напрями аналітичної роботи зі статистикою: описовий аналіз для узагальнення даних, трендовий аналіз для виявлення динаміки системи у часі, регіональні порівняння для визначення диспропорцій, побудову індикаторів ефективності (рівень розслідувань, санкцій, вилучених активів), кореляційний аналіз для визначення чинників, що впливають на успіх політик, а також оцінювання чутливості систем виявлення ризиків. Окремий акцент зроблено на тому, що відсутність достовірних статистичних даних породжує цілу низку проблем — від суб'єктивності у висновках оцінювачів і труднощів у вимірюванні ефективності до втрати довіри з боку міжнародної спільноти та спотворення реальної картини виконання Рекомендацій FATF.

Важливою частиною посібника є опис системи організації збору та координації статистичних процесів. Рекомендовано визначати єдиний провідний орган — зазвичай це національна координаційна установа з ПВК/ФТ або фінансова розвідка — та формувати міжвідомчу групу з чітко окресленими повноваженнями, контактними особами й каналами обміну інформацією. Документ наголошує на потребі розроблення формалізованої методології збору даних, яка охоплює визначення статистичних одиниць і змінних, стандартизацію періодів звітності, валютних конверсій, одиниць вимірювання та критеріїв підрахунку, а також чітке розмежування понять «нульові дані» і «відсутність даних». Посібник містить опис типових помилок: дублювання звітності між органами, розбіжності у визначеннях показників, змішування часових рамок, а також подання часткових чи застарілих відомостей. Пропонується послідовний підхід до планування процесу — від складання календарного графіка і розподілу ролей до верифікації результатів і міжінституційного погодження кінцевих даних.

Значну увагу приділено етапам обробки та аналізу даних. Рекомендується починати з очищення масивів — виявлення пропусків, дублів і помилок — із подальшою нормалізацією, групуванням, трансформацією та моделюванням. Для цього пропонуються інструменти — від базових (Excel, Google Sheets) до аналітичних платформ (Python, R, Power BI, Tableau), а також зазначається перспектива застосування штучного інтелекту й технологій інтелектуального аналізу даних для виявлення нових закономірностей і прогнозування тенденцій у злочинності. Особливе місце займає розділ про інтерпретацію даних: статистика повинна тлумачитися у зв'язку з

національним ризиковим профілем, законодавчим контекстом і поточною операційною ситуацією. Помилки тлумачення — такі як ототожнення кількості звітів з ефективністю, використання несвоєчасних або неверифікованих даних, ігнорування якісних пояснень — знижують цінність аналітики та підривають довіру до результатів оцінки.

Окремо підкреслено принцип «каскадного впливу» статистики, коли одне джерело даних може підтверджувати ефективність за кількома результатами одночасно. Наприклад, показник «кількість підозрілих операцій, що призвели до розслідувань» демонструє взаємозв'язок між використанням фінансової розвідки (IO6), розслідуваннями та переслідуванням (IO7), конфіскаціями активів (IO8) і міжнародною співпрацею (IO2). Такий підхід сприяє побудові цілісної логічної картини результативності системи. Автори радять створювати національні матриці відповідності між статистичними показниками та Immediate Outcomes, що підвищує послідовність аргументації та зменшує дублювання зусиль.

Висновки:

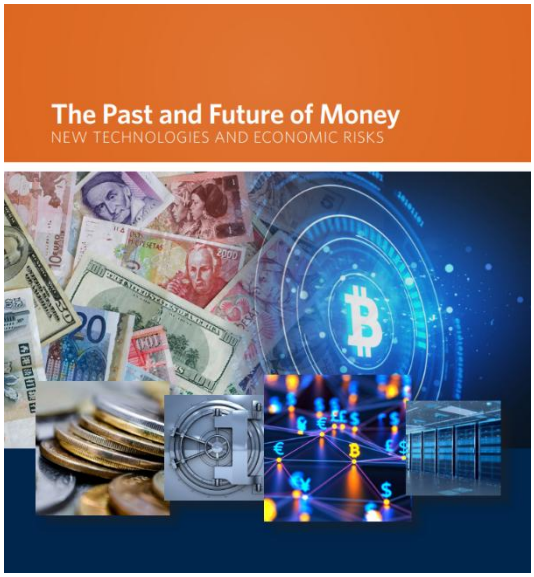
- **Необхідно створити централізовану міжвідомчу систему збору статистики у сфері ПВК/ФТ.** Ключовий орган (ПФР або національний координатор) має очолювати роботу, забезпечуючи уніфіковані визначення, періодичність і структуру даних.
- **Впровадити стандартизовану методологію та цифрову платформу.** Створення єдиної електронної бази дозволить усунути дублювання, підвищити точність, забезпечити автоматизацію обробки та можливість візуалізації трендів.
- **Забезпечити аналітичне використання даних у взаємних оцінках.** Країни повинні не лише подавати дані, а демонструвати їхню аналітичну цінність — як статистика підтверджує досягнення Immediate Outcomes і ефективність системи.
- **Розвивати спроможність кадрів та впроваджувати інноваційні технології.** Необхідне навчання аналітиків і статистиків у сфері інтелектуального аналізу даних, Python/R, AI-інструментів, що дозволить перейти від механічного збору даних до інтелектуального аналізу ризиків.

У завершальних розділах надано рекомендації щодо представлення даних групам оцінювачів FATF. Підкреслюється, що статистика не є самоціллю, а лише елементом ширшого доказового пакету, який має поєднувати кількісні та якісні докази. Відповідно до методології FATF, дані повинні бути контекстуалізовані — пояснювати, як країна реагує на власні ризики, а не просто демонструвати кількість показників. Автори радять розробити єдину структуру звіту, що міститиме опис контексту ризиків, аналітичні таблиці, графіки, діаграми та виноски із зазначенням джерел. Особливо наголошено на питаннях безпеки — перед оприлюдненням інформації необхідно проводити оцінку потенційних ризиків для розслідувань, фінансових установ і стратегічних інституцій.

Таким чином, посібник GAFILAT формує концептуальну основу для переходу від формального звітування до культури управління даними у сфері ПВК/ФТ. Він визначає статистику як ключовий інструмент стратегічного управління ризиками та підтвердження ефективності, а не як адміністративний обов'язок. Запровадження викладених підходів дозволяє країнам підвищити об'єктивність самооцінок, обґрунтованість взаємних оцінок FATF, а також забезпечити прозорість, довіру та сталість національної системи протидії відмиванню коштів і фінансуванню тероризму.

Звіти окремих інституцій та експертів

Минуле та майбутнє грошей: нові технології та економічні ризики [9]



Цей документ є фундаментальною доповіддю Групи Тридцяти (G30), яка розглядає поточну трансформацію грошово-кредитної системи як критичний "переломний момент". Документ стверджує, що хоча нові технології, такі як криптовалюти, стейблкоїни та цифрові валюти центральних банків (CBDC), пропонують значні переваги (наприклад, швидші та дешевші платежі), вони також несуть величезні ризики, що можуть повернути нас до епохи фінансового хаосу. Головна теза звіту полягає в тому, що стабільність сучасної "дворівневої" монетарної системи є ключовим суспільним благом, яке необхідно захищати . Ця система, що складається з грошей центрального банку (як якоря) та грошей комерційних банків (депозитів), забезпечує так звану "єдність" грошей. Це фундаментальний принцип, завдяки якому долар у вашій кишені, долар на вашому банківському рахунку та долар на рахунку іншого банку є взаємозамінними за номіналом . Автори наголошують, що ця єдність не є даністю — вона є продуктом століть еволюції та підтримується складною архітектурою регулювання, нагляду, страхування вкладів (наприклад, FDIC) та роллю ЦБ як кредитора останньої інстанції.

Історичний аналіз у звіті є ключовим для розуміння поточних ризиків. G30 проводить пряму і тривожну паралель між поточною "крипто-лихоманкою" та "ерою вільного банкінгу" (free banking era) в США (приблизно 1837-1863 рр.). У той період сотні приватних, слабко регульованих банків випускали власні паперові банкноти, які нібито були конвертовані у золото чи срібло. На практиці ж ці банкноти циркулювали з постійно мінливими дисконтами залежно від репутації банку-емітента, географічної відстані та чуток. Це створювало величезні транзакційні витрати (люди потребували спеціальних "детекторів банкнот", щоб оцінити вартість грошей), сприяло шахрайству (так звані "дикі банки") та підривало довіру до всієї системи. Автори попереджають, що неконтрольована проліферація приватних стейблкоїнів (наприклад, "Amazoncoin", "Walmartcoin" тощо) може повернути нас у цей світ фрагментованих грошей, де "єдність" буде втрачено.

Звіт чітко розмежовує непідкріплені криптовалюти та стейблкоїни. Автори стверджують, що Bitcoin категорично відкидається як гроші. «Він не виконує жодної з трьох функцій: він є жахливим засобом збереження вартості через екстремальну волатильність, поганим засобом обміну через низьку швидкість та високі комісії і не використовується як одиниця розрахунку.». Натомість стейблкоїни, через їхню прив’язку до фіатних валют, є "набагато складнішим випадком". Вони пропонують реальні інновації у платежах, особливо транскордонних, та програмованість. Однак, як і банкноти "ери вільного банкінгу", вони є "внутрішньо крихкими" (inherently fragile), а їхня стабільність залежить від непрозорих та потенційно ризикованих резервів емітента . Звіт наводить приклад "депеггінгу" (втрати прив'язки) USDC у березні 2023 року як доказ цієї вразливості.

З точки зору ПВК/ФТ/ФР, звіт б'є на сполох. Автори стверджують, що нові технології не повинні ставати "санкціонованим засобом для широкомасштабного ухилення від регулювання". Стейблкоїни, завдяки їхній псевдонімності на блокчейні, вже є улюбленим інструментом

[9] https://group30.org/images/uploads/publications/G30_Future-of-Money_RPT_E.pdf

злочинців. У звіті цитуються дані, що стейблкоїни становлять 63% усього обсягу незаконних транзакцій на блокчейні, а USDT (Tether) активно використовується наркокартелями та терористичними групами. Особливу критику викликає (гіпотетичний на момент написання звіту) закон США "GENIUS Act". G30 вважає, що цей закон має серйозні недоліки , оскільки його вимоги з ПВК/ФТ не вирішують проблему псевдонімності транзакцій "в ланцюжку" (on-chain) . Крім того, закон має слабку заборону на виплату відсотків (дозволяючи робити це афілійованим особам), що перетворює стейблкоїни на ризиковий інвестиційний продукт, а не платіжний інструмент.

У відповідь на ці виклики, G30 пропонує трьохкомпонентну стратегію. По-перше, прискорити роботу над CBDC, особливо над оптовими wCBDC. wCBDC необхідні для забезпечення розрахунків у безпечних грошах центрального банку в майбутній токенізованій фінансовій системі. Роздрібні CBDC (rCBDC) вважаються більш складними через ризики фінансової стабільності (відтік депозитів з банків) та проблеми конфіденційності. По-друге, заохочувати інновації всередині дворівневої системи, а саме токенізовані депозити (tokenized deposits). Це дозволяє комерційним банкам пропонувати переваги токенізації (наприклад, програмованість), але зберігає операції, управління ризиками та, що найважливіше, процедури комплаєнсу ПВК/ФТ в межах існуючого, надійного банківського регуляторного периметра . По-третє, якщо стейблкоїни і мають існувати, вони повинні підлягати жорсткому регулюванню за принципом "однакова діяльність, однаковий ризик, однаковий регуляторний результат".

Геополітика зерна: як сирійські судна допомагають красти українські ресурси [10]

Розслідування OCCRP та сирійської мережі журналістів SIRAJ розкриває масштабну, ретельно сплановану злочинну операцію з легалізації вкраденого українського зерна, у якій переплітаються інтереси російського військово-олігархічного апарату, режиму Башара Асада та транснаціональних мереж контрабанди, що функціонують через офшори та псевдокомпанії. У центрі цієї схеми — три судна під сирійським прапором — Finikia, Souria та Laodicea, які з 2022 року стали частиною “тіньового флоту” росії, використовуючись для транспортування зерна, награбованого в окупованих українських регіонах — Запорізькій, Херсонській та Донецькій областях.

Розслідувачі встановили, що всі три судна колись належали державному флоту Сирії і перебували під контролем міністерства транспорту країни, але у 2023 році вони були “продані” за символічну суму — всього по одному долару кожне — компанії AlHouda Holding, зареєстрованій у Сейшельських офшорах. Формально угода виглядала законною, проте документи, отримані OCCRP, доводять, що продаж був фіктивним, а справжні власники залишилися ті ж самі — особи з близького кола Башара Асада, зокрема бізнесмен Алі Мохамед Діб, який у минулому керував низкою підприємств, безпосередньо пов’язаних із сирійською владою. Таким чином, це була класична схема “номінального відчуження”, що дозволила вивести активи з-під міжнародних санкцій, накладених на сирійський уряд і держпідприємства ще у 2011 році.

[10] https://www.occrp.org/en/investigation/ships-accused-of-stealing-ukrainian-grain-linked-to-assad-regime-front

Після “зміни власності” судна почали зникати з міжнародних суднових реєстрів, міняти прапори та назви, щоб ускладнити їхнє відстеження. Finikia стала Monte Bianco, Souria — Samira, а Laodicea — Okeanos. Вони три або більше разів змінювали країну прапора, зокрема на Гамбію, Есватіні (колишній Свазіленд) та навіть Коморські острови, що дозволяло уникати контролю Міжнародної морської організації. Коли влада Есватіні виявила, що її прапор використовується у злочинних схемах, вона відкликала реєстрацію, але судна продовжили плавати, видаючи себе за “нейтральні” торгові кораблі.

Згідно з супутниковими даними Planet Labs і MarineTraffic, з 2022 по 2024 рік ці судна неодноразово заходили до кримських портів — Севастополя, Керчі, Феодосії, а також до окупованого Бердянська. Вони відключали транспондери AIS, щоб приховати маршрут, і знову вмикали їх лише після виходу з Чорного моря. На знімках чітко видно завантаження зерна з терміналів, які раніше належали українським компаніям Нібулон і Kernel, а нині контролюються російськими військовими адміністраціями.

Подальший маршрут веде через Босфор до портів Латакії (Сирія), Олександрії (Єгипет), Тартуса і навіть Тріполі (Ліван). Там зерно “перевантажується” на склади під виглядом “сирійського” або “російського” походження і експортується далі через компанії-посередники, пов’язані з російською United Grain Company. Таким чином, зерно, викрадене в Україні, стає легальним товаром на світових ринках, а прибуток осідає у кишенях сирійських і російських бізнес-груп, які підтримують воєнну економіку двох режимів.

Центральною ланкою цієї схеми є AlHouda Holding, компанія без фізичного офісу, але з філіями в Дамаску, Бейруті та Дубаї. Власник — уже згаданий Алі Мохамед Діб, підставна особа з глибокими зв’язками з сім’єю Асада. OCCRP встановило, що він одночасно є співвласником Iloma Investment JSC, яка у 2024 році придбала контрольний пакет акцій державної Syrian Airlines, фактично узурпувавши частину транспортної інфраструктури країни. Через цей бізнес Діб і його партнери — колишні офіцери спецслужб — створили логістичну мережу, що об’єднує перевезення зерна, нафти, зброї та наркотиків (зокрема амфетаміну каптагону), який став головним джерелом нелегальних доходів сирійського уряду.

Ще один ключовий фігурант — Тахер Каялі, сирійський наркобарон, який контролює Levant Fleet Ltd. і Orient Fleet Maritime LLC, обидві зареєстровані у Великій Британії та ОАЕ. Саме ці структури офіційно “керують” суднами Finikia, Souria та Laodicea, хоча за документами не мають жодних активів чи співробітників. За даними OCCRP, Каялі перебуває під санкціями США, Канади та ЄС за участь у виробництві й контрабанді каптагону. Його морська логістика стала ключовим “сервісом” для російських і сирійських угод, які в обхід санкцій перевозять зерно, нафту та навіть озброєння.

Фінансова інфраструктура операції також вражає масштабом. Платежі за транспортування зерна проходять через мережу компаній-оболонок у Дубаї, Стамбулі та Нікосії, зокрема Mar Group FZE та Cedar Trading Ltd, які “очищують” платежі за допомогою криптовалютних переказів і рахунків у банках Лівану. Водночас страхування суден здійснюється через підставні структури, зареєстровані у Великій Британії, що дозволяє їм легально отримувати сертифікати Lloyd’s навіть попри санкції.

У січні 2025 року Європейський Союз запровадив санкції проти трьох суден і компаній, які володіють ними, проте майже одразу судна були перереєстровані на нові компанії у Маршалових островах — Bayaze Shipping Ltd. та Polar Line Inc. — і продовжили курсувати. Це показує, що навіть санкції найвищого рівня не мають реального впливу, якщо не супроводжуються системою міжнародного моніторингу судновласності та контролю за зміною реєстрацій.

Окрім очевидного аспекту воєнної економіки, ця історія має глибше значення — вона демонструє, як режим Асада перетворився на ключового союзника кремля у глобальній тіньовій логістиці, надаючи не лише територію, але й юридичну, корпоративну й морську інфраструктуру для обходу санкцій. Сирія фактично стала "офшорною зоною кремля", де відмиваються гроші з незаконних продажів українських ресурсів.

За підрахунками аналітиків OCCRP, тільки у 2023–2024 роках через цю схему росія нелегально вивезла щонайменше 1,8 млн тонн зерна на суму понад $520 млн, що еквівалентно річним доходам України від експорту до країн Близького Сходу. Ці кошти стали частиною "воєнного резерву" Кремля, яким фінансується закупівля дронів, артилерійських систем і боєприпасів.

Таким чином, історія сирійських кораблів Finikia, Souria та Laodicea — це не просто кейс про контрабанду зерна. Це зразок нового типу міжнародного злочину, де держави, перебуваючи під санкціями, утворюють симбіоз і використовують корупційні структури для взаємного збагачення. У глобальному контексті це показує межі ефективності санкційного режиму — доки немає єдиної міжнародної бази судновласників, реального контролю за фрахтом і кримінальної відповідальності для портових адміністрацій, такі схеми продовжуватимуть процвітати.

Для України цей кейс має не лише економічне, а й політичне значення. Він демонструє, що війна ведеться не лише на полі бою, а й у сферах логістики, морського права, міжнародної торгівлі й фінансової прозорості. І поки російсько-сирійська "зернова мафія" збагачується, міжнародні партнери України мають вирішити — чи готові вони реально боротися з "тіньовими флотами", чи й надалі закриватимуть очі на те, що вкрадене українське зерно продовжує годувати диктаторів Близького Сходу та фінансувати війну в Європі.

Висновки:

- **Міжнародна спільнота має створити централізований реєстр судновласності** та відстеження морських маршрутів, щоб унеможливити зміну прапорів і використання офшорних компаній для легалізації крадених ресурсів.
- **Україні необхідно ініціювати в межах** ООН та Міжнародної морської організації (IMO) резолюцію щодо моніторингу суден, підозрюваних у транспортуванні викраденого зерна, із санкційним списком суден-фантомів.
- **Європейським банкам і страхувальникам варто запровадити обов'язкову перевірку** судновласників та експедиторів, щоб перекрити фінансові канали "чорного зернового експорту".
- **Україна має розвивати аналітичну співпрацю між ПФР, митницею та міжнародними партнерами** для автоматичного виявлення товарних партій із сумнівним походженням у глобальних трейдингових системах.

Балканський синдром: як албанські кримінальні мережі з периферії перетворилися на серце європейського ринку кокаїну [11]

Еволюція албанських наркокартелів — це історія про те, як держава з невеликою економікою, слабкими інституціями й масштабною еміграцією змогла вибудувати один із найпотужніших кримінальних хабів Європи. За два десятиліття Албанія, колись відома переважно як транзитна країна для героїну, стала мозковим центром кокаїнових потоків, що з'єднують Латинську Америку з європейськими мегаполісами.

У центрі цієї трансформації — кримінальні бізнес-моделі нового покоління, що поєднують дисципліну мафії з гнучкістю стартапів. На відміну від колумбійських або мексиканських

[11] https://globalinitiative.net/analysis/how-have-albanian-networks-come-to-dominate-cocaine-trafficking-to-europe/

картелів, албанські мережі не прагнуть монополії на насильство — вони контролюють інфраструктуру і логістику, залишаючись невидимими. Їхня сила полягає у транснаціональній координації: у Парагваї вони мають брокерів, які домовляються з місцевими фермерськими кооперативами, у Бразилії — "прикриття" серед експортерів фруктів і цементу, в Бельгії та Нідерландах — своїх "інспекторів", які корумпують портових чиновників.

Система працює як мережа, а не як піраміда. Якщо одну гілку ліквідують, інша перебирає її функції без втрати ефективності. Саме ця децентралізована структура, за словами аналітиків Global Initiative, і є головною причиною того, що албанські угруповання витіснили італійську мафію 'Ndrangheta з ряду європейських ринків.

Успіх пояснюється не лише організованістю, а й інституційною корупцією. Албанські кокаїнові кластери користуються системною лояльністю у власній країні — серед митників, чиновників, політиків. Багато "бізнесменів" з наркотрафіку мають офіційний статус інвесторів, володіють готелями на узбережжі, фінансують футбольні клуби або навіть партії. У такий спосіб кримінальний капітал вбудовується в національну економіку, перетворюючи Албанію на "сіру офшорну платформу" для чорних грошей Європи.

Водночас албанські картелі не обмежуються лише наркотиками. Вони створюють повноцінні корпоративні екосистеми — від логістичних компаній до експедиторських і охоронних фірм, які надають послуги легальним клієнтам і водночас обслуговують контрабанду. Через офіційні рахунки ці компанії здійснюють міжнародні перекази, легалізуючи прибутки. Однією з таких схем стала "капіталізація на логістиці": угруповання вкладають гроші в будівництво складів у портах, портових кранів, трейдингових компаній і навіть у транспортні стартапи.

Ще одна причина їхньої стійкості — стратегічне використання криптовалют. Замість готівки все частіше застосовуються токенізовані "гарантії", що замінюють транзакції. Таким чином, навіть якщо одну партію перехоплено, постачальники в Латинській Америці не зазнають фінансових втрат — токен просто "заморожується". Це створює аналог банківської системи у тіньовому секторі, де кожен учасник має власну "кредитну історію" у межах кримінальної довіри.

Зв'язки з Латинською Америкою стали вирішальним чинником. Після 2015 року албанці почали укладати прямі угоди з картелями Колумбії, Болівії та Перу, усуваючи посередників. Це дало змогу суттєво знизити витрати, збільшити маржу та закріпити свою роль у якості "глобальних брокерів". До 2024 року близько 40% кокаїну, який надходить до Європи, має албанський слід.

Їхня економічна сила конвертується у вплив на місцях. У портах Антверпена, Роттердама та Гамбурга албанські клани не лише контролюють докери та охоронців — вони мають власних юристів, банкірів, фінансистів, що обслуговують їхні операції у "білому секторі". Це перетворює їх із злочинних груп на гібридних економічно-кримінальних суб'єктів, що впливають на реальні ринкові процеси.

У 2023–2025 роках спільні операції правоохоронних органів ЄС, Албанії, Італії та ОАЕ частково розкрили масштаби цього явища. Але навіть після арештів поставки не зменшилися. Навпаки, на авансцену вийшло нове покоління лідерів, які поєднують досвід наркотрафіку з цифровими технологіями — використовують зашифровані месенджери, дрони для морського контролю та аналітичні інструменти для моделювання ризиків.

Це свідчить, що албанські мережі стали "кримінальними корпораціями 2.0", які не залежать від конкретних осіб чи державних кордонів. Їхня бізнес-модель ближча до венчурних екосистем: диверсифікація ризиків, аутсорсинг логістики, криптоінвестиції, гнучке управління ланцюгами постачань. Саме тому вони витримують навіть наймасштабніші антинаркотичні кампанії ЄС.

Звіт Global Initiative підсумовує: албанські кокаїнові мережі стали не лише наркобізнесом, а й соціальним феноменом — символом того, як криміналізація економіки може перетворити бідну країну на стратегічного гравця. Їхній вплив вийшов далеко за межі злочинності: він формує політику, змінює інвестиційний клімат, корумпує фінансові інституції та навіть впливає на дипломатію.

Для Європи це означає, що боротьба з наркотрафіком має стати системною — не лише силовою, а й економічною. Без реформ контролю портів, фінансової прозорості й міжнародного обміну даними жодна операція не зупинить нових "кокаїнових баронів". Албанські мережі — це дзеркало глобальної слабкості: там, де відсутній ефективний фінансовий нагляд, кримінал заповнює вакуум.

І сьогодні, коли ЄС намагається створити єдину стратегію протидії наркоторгівлі, історія албанців звучить як попередження — якщо не реформувати інституції, злочинність завжди знайде нову схему, аби продовжити злочинну діяльність під виглядом легального бізнесу.

Висновки:

- **Європейським правоохоронним органам необхідно перейти від операційного реагування до фінансово-аналітичного підходу** — системного відстеження потоків коштів, логістичних активів і криптотранзакцій, що живлять албанські кокаїнові мережі.
- **Необхідно створити єдину європейську базу ризикових портових операторів**, транспортних компаній та трейдерів, які мають зв'язки з балканськими угрупованнями, з обов'язковим моніторингом їхніх митних і страхових операцій.
- **Країнам ЄС та Балканського регіону слід розробити спільну програму** — антикорупційну ініціативу з незалежним аудитом портів.
- **Україні, яка потенційно може стати транзитною ланкою** після війни, потрібно вже зараз інтегрувати стандарти FATF і ЄС щодо моніторингу ризикових логістичних операцій і фінансових потоків у морському секторі.

Психологія обману: як поведінкова економіка стає новою зброєю у боротьбі з шахрайством [12]

Звіт Axiom Economics, підготовлений для Payment Systems Regulator (PSR) у Великій Британії, є одним із найглибших досліджень у світі, яке пояснює природу Authorised Push Payment (APP) fraud — шахрайства, коли користувач самостійно авторизує платіж, переконаний, що діє правильно. Ця форма злочину, яка у 2024 році коштувала британцям понад півмільярда фунтів, унікальна тим, що вона не порушує системи безпеки — вона використовує слабкості людського мислення. Саме тут поведінкова економіка — наука, що вивчає, як люди приймають рішення під впливом емоцій, когнітивних упереджень і соціальних факторів, — дає ключ до розуміння, чому навіть розумні, освічені та обережні люди стають жертвами.

Axiom Economics

APP-шахрайство — це дзеркало людської природи. Його механізм ґрунтується на експлуатації типових когнітивних упереджень, описаних ще Деніелом Канеманом у його теорії двох систем

[12] https://www.psr.org.uk/media/efpdiwpk/using-behavioural-economics-to-understand-and-prevent-app-fraud.pdf

мислення. “Система 1” — швидке, інтуїтивне, емоційне мислення — домінує у станах стресу, страху чи довіри, коли час обмежений, а рішення здаються очевидними. “Система 2” — повільне, логічне, аналітичне мислення — вмикається лише тоді, коли людина має змогу подумати, порівняти, перевірити. Шахраї майстерно змушують людину залишатися в межах Системи 1. Вони створюють відчуття терміновості (“дійте зараз, інакше втратите гроші”), формують хибне почуття довіри (“це ваш банківський менеджер”), або грають на соціальній репрезентативності (“усі наші клієнти вже інвестували”). Людина починає реагувати автоматично — і саме в цей момент натискає “підтвердити платіж”.

Axiom Economics наводить шокуючу статистику: понад 70% жертв APP-шахрайства вважають, що діяли свідомо і логічно, навіть після того, як втратили кошти. Це означає, що механізм обману відбувається всередині свідомості, а не лише зовні. Шахраї не просто переконують — вони змінюють когнітивний контекст рішення. Вони застосовують “емоційне обрамлення”: замість раціональних аргументів — терміновість, страх, любов, авторитет або жалість. Поведінкова економіка пояснює, що в стані стресу рівень дофаміну і кортизолу змінює здатність мозку до об’єктивного аналізу — і тому людина “бачить” іншу реальність, де шахрай здається рятівником.

У звіті зазначено, що найчастіше APP-шахрайство має три сценарії: інвестиційне шахрайство, “банківський представник” та романтичні афери. У першому випадку жертву заманюють обіцянками високих прибутків — класичний “ефект втраченої вигоди” (loss aversion): люди сильніше бояться втратити можливість, ніж реально втратити гроші. У “банківському” сценарії спрацьовує ефект авторитету: шахрай видає себе за офіційного співробітника банку, що діє “для безпеки клієнта”. У романтичних схемах домінує соціальне довір’я — емоційна прив’язаність повністю блокує критичне мислення.

Поведінкова економіка не лише пояснює, але й пропонує рішення. Вона доводить: люди не завжди потребують “заборон”, вони потребують “когнітивного уповільнення”. Якщо перед натисканням “Підтвердити” людина отримує просту підказку — “цей платіж не схожий на ваші попередні”, або “у нас є інформація, що це може бути шахрайство” — активується Система 2. Достатньо кількох секунд паузи, щоб критичне мислення “прокинулося”. Дослідження показують, що навіть 10-секундна затримка у процесі авторизації може зменшити рівень успішних шахрайств на 35–50%. Це доводить, що поведінкові інтервенції можуть бути ефективнішими за дорогі технічні рішення.

Однак автори наголошують: “підказки” не повинні бути нав’язливими. Якщо банки надто часто надсилають попередження, виникає “ефект імунітету” — користувач перестає реагувати, вважаючи повідомлення частиною рутини. Тому підходи мають бути персоналізованими і ризик-орієнтованими. Наприклад, якщо система помічає, що клієнт переводить гроші вперше на міжнародний рахунок або робить це вночі, коли зазвичай не активний — попередження варто зробити більш емоційно чутливим і контекстуальним (“Ви впевнені, що знаєте цю людину особисто?”).

Звіт також підкреслює роль дизайну інтерфейсу. Банківські застосунки можуть допомогти “уповільнити мислення” користувача через структуру UX. Зміна кольору кнопки підтвердження на червоний, поява додаткового етапу перевірки, чи навіть мікроанімації — все це збільшує когнітивну залученість користувача і знижує ризик імпульсивного натискання. У контексті поведінкових наук це називається “архітектура вибору” (choice architecture) — спосіб спроєктувати процес ухвалення рішень так, щоб користувач обирав безпечніший варіант, навіть не усвідомлюючи цього.

Іншим новаторським напрямом є емоційно-орієнтоване навчання. Люди не запам’ятовують попередження, але запам’ятовують історії. Банки, які створюють короткі анімовані кейси, відео з реальними жертвами або симуляції шахрайства у своїх застосунках, знижують ризик обману в

середньому на 20%. Це пояснюється наступним ефектом: коли людина бачить приклад із реального життя, подібна ситуація здається більш можливою, і вона діє обережніше.

Ще один важливий аспект — соціальні норми. Шахраї часто грають на них ("всі мої друзі інвестували", "цей банк надійний, подивіться відгуки"). Поведінкові дослідження пропонують боротися симетрично: створювати контр-наративи ("95% клієнтів перевіряють переказ двічі перед оплатою"). Такі меседжі активують соціальне бажання діяти "як більшість", але у безпечному напрямі.

Висновки:

- **Фінансові установи повинні використовувати поведінкові інструменти —** тайм-аути, попередження й "архітектуру вибору" — щоб штучно уповільнювати емоційні рішення користувачів і активувати раціональне мислення перед переказом коштів.
- **Банки мають розробити персоналізовані алгоритми ризику,** які враховують психологічні профілі клієнтів, щоб попередження не були надмірними та не викликали "втоми від безпеки".
- **Інтерфейси банківських застосунків повинні проєктуватися за принципами поведінкової науки** — через візуальні сигнали, кольори, анімації й історичні приклади, що стимулюють критичне мислення користувачів.
- **У сфері кіберзахисту необхідно створити міжсекторальну платформу співпраці** між банками, регуляторами та соціальними мережами, щоб попереджати користувачів ще на етапі контакту з потенційним шахраєм.

Однак звіт наголошує, що жодна поведінкова стратегія не працюватиме без системної співпраці. Банки, платіжні провайдери, регулятори і соціальні платформи мають спільно формувати "ланцюг поведінкової безпеки": соціальні мережі зупиняють фальшиві реклами, банки — підказують у момент платежу, а регулятори — координують стандарти. У Британії та Сінгапурі вже тестуються спільні платформи аналізу поведінкових ризиків, де об'єднуються дані про шаблони шахрайства, контекст транзакцій і психологічні індикатори.

Від ручної перевірки до автономного контролю: еволюція KYC під впливом штучного інтелекту [13]

Документ досліджує глибоку трансформацію процесів і підходів до «Знай свого клієнта» (KYC) у банківському секторі під впливом новітніх технологій штучного інтелекту. Автори розглядають, як поєднання предиктивного, генеративного та агентного штучного інтелекту, що створює передумови для якісно нового етапу у сфері протидії фінансовим злочинам, у якому ефективність, швидкість, точність і стійкість KYC-процесів стають взаємопов'язаними елементами єдиної екосистеми управління ризиками.

BCG зазначає, що фінансові установи протягом останнього десятиліття спрямовували величезні ресурси на дотримання регуляторних вимог у сфері KYC, моніторингу транзакцій і скринінгу клієнтів, проте навіть у провідних банках майже половина перевірок клієнтів усе ще виконується вручну. Це створює дисбаланс між витратами та результатом: операційні процеси залишаються громіздкими, а витрати на управління фінансовими злочинами можуть становити до п'яти відсотків усіх витрат банку. На цьому тлі галузь поступово переходить від «регуляторного підходу за необхідністю» до нової парадигми — збалансованої ефективності, де контроль,

[13] https://web-assets.bcg.com/3c/5b/aa3ddb034bf3bc489e9c8a4c3444/the-know-your-customer-agentic-ai-revolution.pdf

стійкість і продуктивність є взаємодоповнюючими компонентами. Показники BCG свідчать, що трансформаційні програми, засновані на впровадженні AI, можуть зменшити витрати на 40–50%, водночас підвищивши якість перевірок, швидкість ухвалення рішень і ступінь автоматизації.

Автори визначають три ключові рівні еволюції штучного інтелекту у сфері KYC. Предикативний AI використовує аналітичні моделі для виявлення закономірностей і прогнозування ризиків на основі великих масивів даних. Генеративний AI здатен обробляти як структуровану, так і неструктуровану інформацію, створювати аналітичні звіти та синтезувати комплексні висновки для фахівців. Генеративний AI, найновіша технологічна хвиля, забезпечує автономне прийняття рішень і оркестрацію між різними процесами та системами, перетворюючи KYC з набору роз'єднаних операцій у безперервний, самонавчальний цикл. Успіх цієї трансформації, підкреслює BCG, залежить не лише від технологій, а насамперед від дисциплінованого впровадження, коли інтелектуальні інструменти інтегруються в операційну тканину організації. Лідируючі банки демонструють чотири основні напрями успіху: переосмислення процесів на основі дизайну, спроєктованого під штучний інтелект, чітке ранжування кейсів за впливом і складністю, побудову масштабованої архітектури даних і модулів, а також вбудовану систему довіри, пояснюваності й кіберзахисту.

Документ наголошує, що нова епоха KYC — це не епоха витіснення людини, а становлення «гібридної інтелектуальної організації», у якій людський досвід і судження підсилюються AI. Замість громіздких ієрархічних структур виникають компактні команди експертів, які взаємодіють із цифровими агентами. Людина з виконавця перетворюється на стратегічного партнера системи, який спрямовує її роботу, оцінює контекст і втручається у виняткові або високоризикові ситуації. Водночас AI поступово бере на себе масштабні завдання збору, перевірки, інтеграції й аналізу даних, виявляючи закономірності, що виходять за межі людського сприйняття. Такий симбіоз дозволяє організації навчатися разом із машиною, постійно вдосконалювати свої алгоритми, оновлювати правила поведінки та адаптуватися до нових ризиків і тенденцій у середовищі фінансових злочинів.

Звіт наводить приклади практичного впровадження AI у KYC-процеси в різних глобальних банках. Один із G-SIB банків запровадив систему автоматичного збору та перевірки даних із внутрішніх баз і зовнішніх реєстрів, що знизила обсяг ручної роботи й підвищила якість даних завдяки автоматичному визначенню «золотого джерела». Інший великий європейський банк реалізував машинне навчання для сегментації клієнтів і виявлення аномалій, що дозволило відокремити «безпечні» сценарії від ризикових і сфокусувати ресурси на останніх. Агентний AI також застосовується для динамічної взаємодії з клієнтами — автономна система надсилає запити на відсутню інформацію, проводить двосторонній діалог, зменшуючи навантаження на аналітиків і покращуючи клієнтський досвід. Інноваційні рішення включають GenAI-асистента для KYC-файлів, який автоматично формує повні клієнтські досьє та підготовлює рекомендації щодо ризик-профілю. Також банки впроваджують AI-контроль якості першої та другої ліній, де алгоритми виявляють помилки, аналізують їх причини та пропонують корекційні дії, знижуючи людські витрати на понад 50%.

BCG демонструє концепцію «North Star» — ідеальної моделі KYC, у якій кожен етап — від подачі заявки до моніторингу — координується AI. Процес починається з попередньо заповненої заявки, у якій AI автоматично перевіряє інформацію клієнта з відкритих джерел, аналізує ризики, визначає перелік необхідних документів і допомагає клієнту в процесі завантаження.

Далі AI здійснює скринінг на санкції, ризики ПВК/ФТ, компілює KYC-файл, створює обліковий запис та ініціює постійний моніторинг. Уся система працює в режимі реального часу, а високоризикові кейси автоматично передаються на розгляд людині. Результатом стає процес, де відкриття рахунку займає хвилини, а не дні, а постійний моніторинг здійснюється безперервно й адаптивно, із динамічним оновленням ризик-профілів.

Наприкінці звіт підкреслює, що трансформація KYC через AI — це не одномоментний стрибок, а довгостроковий процес, який вимагає поетапного впровадження, стабільної архітектури даних і стійкого управління. Успішні інституції починають із проєктів, що мають високу віддачу й низьку складність, здобуваючи швидкі результати та зміцнюючи довіру всередині організації. Потім поступово розширюють сферу застосування до більш комплексних рішень на основі генеративного та агентного AI, інтегруючи їх у повний життєвий цикл KYC. Такий підхід дозволяє знизити ризики, створити культуру постійного вдосконалення та забезпечити гнучкість системи до майбутніх регуляторних і технологічних змін.

У підсумку документ BCG окреслює цілісне бачення епохи «інтелектуального KYC», у якій технології та люди об'єднані у єдину систему взаємного підсилення. AI перестає бути допоміжним інструментом і стає ядром усієї моделі управління фінансовими ризиками, забезпечуючи не лише швидкість і економічність, а й якісно новий рівень контролю, пояснюваності та стійкості. Таким чином, майбутнє KYC постає як адаптивна, прозора й автономна екосистема, у центрі якої — довіра, інтелект і відповідальність.

Висновки:

- **AI стає новим ядром KYC-процесів:** агентний, предикативний та генеративний AI формують повноцінну екосистему для управління ризиками, знижуючи витрати до 50% без втрати якості контролю.
- **Людина залишається центром довіри:** роль аналітика еволюціонує від надавача послуг до стратегічного партнера AI — із фокусом на винятках, ризиках і тлумаченні рішень.
- **Практичні результати доводять ефективність:** скорочення часу обробки даних до 60%, автоматичне формування KYC-файлів, покращення якості контролю та зменшення людських помилок.
- **Стратегічний підхід до масштабування — ключ до успіху:** інституції повинні будувати AI-спроможності поступово, з акцентом на управлінні даними, міжбізнесовій інтеграції та сталому навчанні систем.

Межа між грою і злочином: глобальні підходи до протидії корупції у спортивних організаціях [14]

Документ, підготовлений Міжнародною антикорупційною академією (IACA), є одним із найґрунтовніших досліджень, присвячених питанням доброчесності, запобігання корупції та впровадження комплаєнс-систем у спортивних організаціях. У роботі розкривається масштаб проблеми корупції у спорті — від фінансових зловживань до маніпуляцій результатами матчів і системних порушень етичних стандартів — та визначається роль міжнародних інституцій, національних органів і спортивних федерацій у формуванні системного підходу до протидії таким явищам. Дослідження має міждисциплінарний характер і поєднує аналіз міжнародного права, національного законодавства, етичних кодексів і практичних кейсів. Його метою є створення універсальної моделі антикорупційного комплаєнсу, адаптованої до специфіки спортивного середовища.

[14] https://www.iaca.int/media/attachments/2025/10/09/iaca_intergrity-and-anti-corruption-compliance-in-sports-organizations_research-paper_final.pdf

На початку документа наголошується, що збереження доброчесності спорту стало пріоритетом у міжнародному антикорупційному порядку денному, зокрема у політичній декларації ООН UNGASS, у діяльності G20 та в межах ініціатив UNODC і Interpol. У цьому контексті IACA започаткувала дослідницький проєкт, спрямований на виявлення основних типів корупційних ризиків, визначення їхніх мотиваційних факторів і створення порівняльного аналізу найкращих практик запобігання корупції у спортивних організаціях. Автори висувають ключові гіпотези: корупційні практики спорту подібні до бізнес-сфери, але мають специфічні форми (договірні матчі, незаконні ставки, маніпуляції з трансферами), а також те, що ефективні системи комплаєнсу у спорті мають поєднувати бізнес-досвід і спортивну специфіку.

Перший розділ присвячений міжнародно-правовим рамкам і організаційним механізмам протидії корупції у спорті. Аналізуються універсальні міжнародні договори — Конвенція ООН проти корупції (2003) та Конвенція ОЕСР про боротьбу з підкупом (1997), а також галузеві акти: Конвенція ЮНЕСКО проти допінгу (2005), Антидопінгова конвенція Ради Європи (1989) і Маколінська конвенція про маніпуляції спортивними змаганнями (2014). Ці документи визначають правову основу міжнародного співробітництва, контроль за обігом заборонених речовин, розслідування договірних матчів і механізми захисту викривачів. Особлива увага приділяється зв’язку між допінгом, корупцією і системними порушеннями доброчесності — адже корупційні схеми часто забезпечують приховування антидопінгових порушень або фальсифікацію результатів.

Другий розділ охоплює феноменологію та типологію корупційних ризиків у спорті на міжнародному та національному рівнях. У документі наведено понад два десятки реальних кейсів, що охоплюють різні види спорту і показують, як порушення управлінських процедур, фінансового контролю або конфліктів інтересів призводять до масштабних зловживань. Серед найпоказовіших — справа колишнього президента Міжнародного союзу біатлоністів Андерса Бессеберга, який отримував дорогі подарунки та привілеї; справа Bank Hapoalim у контексті фінансування FIFA; гучні розслідування проти Джека Ворнера, Чака Блейзера та інших високопосадовців FIFA; а також низка прикладів національного рівня, включно з розкраданням державних коштів, маніпуляціями при виборі міст-господарів і корупцією у процесах призначення спортивних офіційних осіб. Ці кейси демонструють універсальність ризиків, спільних із бізнесом і політикою: підкуп, відмивання коштів, порушення тендерних процедур, нецільове використання державних фондів, а також дискримінацію та переслідування викривачів.

Окремо досліджено мотиваційні чинники, які впливають на залучення до корупції або протидію їй. Автори зазначають, що рушійними силами порушень є прагнення до прибутку, тиск середовища, відсутність ефективного контролю і культурна толерантність до неетичної поведінки. Натомість запобіжниками виступають етичне лідерство, репутаційні ризики, внутрішня комплаєнс-культура і страх санкцій.

Центральне місце у звіті займає аналіз систем доброчесності та комплаєнсу у ключових міжнародних федераціях — FIBA, FIVB, FIFA, IBU, IIHF, ITF. Для кожної з них оцінюються правові рамки, політика щодо конфлікту інтересів, процедури призначення, дисциплінарні механізми, внутрішні розслідування, політика щодо подарунків і гостинності, а також наявність навчальних програм. Порівняльний аналіз показує значні розбіжності у ступені прозорості та

відповідальності: тоді як FIFA та ITF розробили окремі антикорупційні кодекси і незалежні етичні комісії, інші федерації лише частково інтегрували ці елементи в корпоративну структуру.

У заключній частині автори формулюють системні рекомендації, що охоплюють 13 напрямів: правові основи, процедури виборів і призначень, відбір господарів змагань, перевірку третіх сторін, політики подарунків, конфлікту інтересів і доброчесності, захист учасників від зловживань і домагань, контроль ставок і маніпуляцій, міжнародні трансфери спортсменів, антидопінгову політику, механізми повідомлень і внутрішніх розслідувань, а також обов'язкове навчання й підготовку персоналу. Усі ці елементи мають бути інтегровані в єдину систему управління доброчесністю на базі ризик-орієнтованого підходу.

Висновки:

- **Стандарти корпоративного комплаєнсу слід повністю інтегрувати у спорт.** Спортивні федерації мають адаптувати корпоративні інструменти контролю — перевірка клієнтів на основі ризик-орієнтованого підходу, аудит третіх сторін, політики подарунків і конфлікту інтересів — до спортивного контексту.
- **Механізми викриття та внутрішнього розслідування є критично важливими.** Необхідно створювати незалежні канали для повідомлення про порушення та забезпечувати захист викривачів, оскільки більшість кейсів у дослідженні ставали відомими завдяки «внутрішньому каналу повідомлень.
- **Транспарентність при виборі посадовців і організації змагань — головна превенція.** Рекомендовано впровадити відкриті процедури тендерів і публічні критерії відбору країн-господарів та медіа-партнерів, що зменшує можливість хабарництва.
- **Освітні програми та культура доброчесності є фундаментом сталих змін.** IACA наголошує, що постійне навчання, етичне лідерство та обмін найкращими практиками між федераціями є необхідною умовою сталого антикорупційного прогресу у спорті.

Таким чином, дослідження IACA створює системне бачення спорту як сектора, уразливого до тих самих форм корупції, що й бізнес або політика, але з унікальними ризиками, пов'язаними з культурою змагання, фінансовими потоками та високою публічністю. Академія пропонує не просто теоретичний аналіз, а практичну дорожню карту — від міжнародних стандартів до конкретних політик і механізмів, які можуть бути запроваджені на рівні федерацій, клубів і держав. Автори підкреслюють, що боротьба з корупцією у спорті має спиратися не лише на санкції, а передусім на розвиток культури доброчесності, прозорості, колективної відповідальності та освіти. У цьому полягає головна цінність дослідження — воно поєднує юридичну, інституційну й етичну площину в єдину антикорупційну екосистему спорту, що здатна реально підвищити рівень довіри, справедливості та ефективності в усьому секторі.

Стейблкоїни у світовій економіці: між інновацією, регуляцією та геополітикою [15]

Документ є фундаментальним дослідженням, яке вперше надає повномасштабну, емпірично підтверджену картину використання стейблкоїнів у глобальній платіжній екосистемі. Звіт демонструє системну трансформацію стейблкоїнів — від допоміжного інструмента криптотрейдерів до повноцінного елемента міжнародної фінансової інфраструктури. Його унікальність полягає у застосуванні методології «знизу вгору»: автори не обмежуються макрооцінками обсягу транзакцій на блокчейнах, а базують висновки на безпосередніх даних від 33 компаній, що реально здійснюють платежі на основі стейблкоїнів у секторах B2B, B2C, P2P, карткових операцій та операцій попереднього фінансування.

[15] https://reports.artemisanalytics.com/stablecoins/artemis-stablecoin-payments-from-the-ground-up-2025.pdf

За результатами дослідження, між січнем 2023 року та серпнем 2025 року зафіксовано $136 млрд фактичних стабільних платежів, тоді як щорічний темп на серпень 2025 року становив $122 млрд. Найактивнішим сегментом стали платежі між бізнесами (B2B), на які припадає понад $76 млрд на рік, що свідчить про інтеграцію стейблкоїнів у корпоративні фінансові процеси, включно з міжнародними переказами, оплатою постачальників, казначейськими операціями та розрахунками між філіями. Наступними за обсягом є P2P-платежі (приблизно $19 млрд на рік), карткові платежі ($18 млрд), B2C-перекази ($3,3 млрд) і операції попереднього фінансування ($3,6 млрд). Окремо підкреслюється, що всі сегменти, крім P2P, демонструють динамічне зростання, тоді як ринок однорангових переказів досяг стадії зрілості.

Ключовим висновком дослідження є домінування двох стейблкоїнів — Tether (USDT) і USD Coin (USDC), які разом становлять абсолютну більшість транзакцій. Частка USDT у вибірці сягає 85%, що пояснюється його високою ліквідністю, широкою доступністю на ринках, відсутністю обмежень на використання та більшою інтегрованістю з мережею Tron, яка є головною інфраструктурною платформою для стейблкоїнів у світі. Tron забезпечує швидкість, низькі комісії та глобальну масштабованість, тому обіг стейблкоїнів у цій мережі перевищує Ethereum, Binance Smart Chain і Polygon разом узяті. Ethereum залишається другим за значенням ланцюгом завдяки своїй репутації безпечної та стандартизованої платформи, тоді як Binance Smart Chain (BSC) і Polygon обслуговують менші за обсягом, але високомасштабовані мікротранзакції, орієнтовані на фінтех-рішення.

Географічний аналіз демонструє, що стейблкоїни стали справжнім глобальним феноменом. У Латинській Америці Tron є домінуючою мережею в Колумбії, Еквадорі та Бразилії, тоді як в Аргентині та Перу Ethereum утримує сильні позиції. Саме Аргентина є єдиною країною в регіоні, де частка USDC сягає майже 50%, що відображає макроекономічну нестабільність і доларизацію економіки. В Африці USDT також є головною валютою розрахунків, що замінює дорогі міжнародні банківські перекази. Tron і Ethereum домінують у більшості країн, тоді як Binance Smart Chain відіграє допоміжну роль. Тут стейблкоїни вирішують структурну проблему відсутності валютної ліквідності та обмежень на міжнародні платежі. Компанія Yellow Card, що працює у 20 країнах, стала першим ліцензованим емітентом стейблкоїнів в Африці, і через неї пройшло понад $5 млрд у транзакціях, що фактично зробило континент одним із найактивніших майданчиків реального використання цифрових доларів.

В Північній Америці та Карибському басейні структура нагадує глобальну тенденцію: Tron перевищує Ethereum за обсягом транзакцій у більшості країн, окрім Ямайки, де їхні показники приблизно рівні. В США помітна вища частка USDC (до 25%), що пояснюється активністю компанії Circle та інтеграцією з регульованими фінансовими установами. В Європі стабільні монети майже повністю асоціюються з USDT (понад 90% усіх переказів), тоді як USDC має обмежене поширення, а інші монети — PYUSD та DAI — практично відсутні. У Азії спостерігається найрізноманітніша інфраструктура: Tron переважає у більшості країн, але Індія виділяється завдяки високій частці Polygon (мережа, створена індійськими розробниками), а також значному використанню USDC, який займає близько половини локального обсягу транзакцій.

Дослідження також деталізує особливості окремих типів платежів. B2B-перекази демонструють експоненціальне зростання: якщо на початку 2023 року щомісячний обсяг становив менше $100 млн, то до середини 2025 року перевищив $6 млрд. Середня вартість однієї транзакції сягає

понад $200 000, а найбільші потоки проходять через Tron та Ethereum. Карткові платежі, пов'язані зі стейблкоїнами, набирають популярності серед споживачів і бізнесу, досягнувши понад $1,5 млрд щомісячно, і вже порівнюються за обсягом із традиційними дебетовими та кредитними картками. P2P-сегмент, який раніше був домінантним, стабілізувався на рівні $19 млрд річного обсягу, поступившись B2B. Ці перекази мають низьку середню суму ($26–$47), що робить їх доступною альтернативою банківським або сервісним комісіям типу Western Union. B2C-перекази — наприклад, виплати заробітної плати, винагород чи повернення коштів — також зростають, особливо через сервіси Binance Pay та Orbital, що забезпечують миттєві виплати клієнтам у цифрових доларах. Нарешті, операції попереднього фінансування — це відносно новий, але швидкозростаючий напрям, який полягає у наданні короткострокової ліквідності для платежів у стейблкоїнах. Такі компанії, як Arf і Mansa, створюють фінансові мости, що дозволяють проводити платежі без затримки, а сервіси на кшталт Huma Finance запроваджують моделі «PayFi» з використанням USDC для фінансування карткових розрахунків та міжнародних переказів у режимі реального часу.

Загальний висновок дослідження полягає в тому, що стабільні монети вже перестали бути інструментом криптовалютного обміну й перетворюються на нову інфраструктуру глобальних платежів, яка доповнює або навіть частково замінює традиційні банківські механізми. Вони забезпечують миттєві транскордонні перекази, знижують транзакційні витрати, підвищують прозорість розрахунків і ліквідність бізнесу, стаючи каталізатором фінансової інклюзії у країнах із низьким рівнем банківської доступності. За прогнозами Міністерства фінансів США, обсяг емісії стейблкоїнів може досягти $2 трлн до 2028 року, а отже, їхня роль у підтримці глобальної домінації долара лише посилюватиметься. Автори звіту підкреслюють, що використання стейблкоїнів на основі долара фактично перетворює їх на цифрову форму інструменту зміцнення глобального домінування долара, де США зберігають вплив навіть через приватно емітовані цифрові активи.

Таким чином, документ фіксує історичний зсув у глобальній фінансовій архітектурі: стейблкоїни стають невід'ємною частиною платіжної екосистеми, поступово формуючи гібридну модель міжнародних фінансів, де традиційні фіатні валюти співіснують із блокчейн-забезпеченими інструментами, а фінтех-компанії та банки все частіше виступають партнерами, а не конкурентами у цій новій цифровій епосі розрахунків.

Висновки:

- **Стейблкоїни інтегруються в реальну економіку.** Вони переходять із криптоспекулятивного інструмента у повноцінний канал для B2B, B2C та транскордонних платежів, формуючи альтернативну платіжну інфраструктуру.
- **Домінування USDT і Tron як стандарту ринку.** Поєднання дешевих комісій і швидких переказів зробило Tron головною мережею для стейблкоїнів, а USDT — ключовою глобальною валютою цифрових розрахунків.
- **Регіональні драйвери зростання — валютна нестабільність і фінансова фрагментація.** Країни з високою інфляцією, обмеженим доступом до долара або повільними банківськими системами (Аргентина, Нігерія, Індія) демонструють найшвидше прийняття стейблкоїнів.
- **Формування нового платіжного континууму між банками і блокчейнами.** Інституційні учасники (BVNK, Huma Finance, Bitso Business) створюють інфраструктуру, яка інтегрує традиційні платіжні системи з on-chain мережами, відкриваючи шлях до «гібридної фінансової системи».

Ваша думка важлива!

1. Яким чином фінансові установи можуть найефективніше інтегрувати поведінковий аналіз у свої комплаєнс-процедури?
2. Які законодавчі зміни та стандарти регуляторного нагляду потрібні в Україні для впровадження AI-рішень у KYC, щоб вони відповідали принципам FATF і європейського права про захист даних (GDPR, DORA, AI Act)?
3. Які конкретні заходи контролю (governance) та технічного аудиту необхідні, щоб гарантувати доброчесність AI?
4. Які практичні кроки та інституційні зміни ви вважаєте найбільш критичними для України, щоб перебудувати систему з «формального комплаєнсу» на «демонстрацію ефективності»?
5. Як балансувати між потребою у прозорості статистичних даних у сфері ПВК/ФТ та необхідністю зберігати конфіденційність розвідувальної чи кримінально-процесуальної інформації в національних системах, зокрема в Україні?
6. З якими специфічними викликами (правовими, технічними, культурними), найімовірніше, може зіткнутися Україна при реальному впровадженні таких інструментів, як конфіскація без вироку (NCBC)?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2025-45

Бюлетень є розробкою методологічної команди Міністерства фінансів України відповідно до частини 8 статті 18 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

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