Методологічний бюлетень

Серійний номер: МінФін-AML-2026-32

Серпень 2026

“Майбутнє належить тим, хто вірить у красу своїх Мрій!”

Елеонора Рузвельт

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

Стратегія, безпека та масштабування: ключові засади впровадження генеративного AI в державних органах [1]

Документ, опублікований Державним департаментом США, є практичним посібником для державних органів, які планують розробляти, впроваджувати та масштабувати корпоративні рішення на основі генеративного штучного інтелекту. Його зміст побудований навколо досвіду створення StateChat – захищеного корпоративного чатбота, призначеного для використання працівниками Державного департаменту та дозволеного для роботи з інформацією категорії Sensitive But Unclassified, тобто службовою, але несекретною інформацією. Водночас документ виходить далеко за межі опису одного технологічного продукту. StateChat використовується як практичний приклад того, як державна установа може перейти від неформальних експериментів із загальнодоступними моделями до повноцінної корпоративної екосистеми, що охоплює захищену інфраструктуру, управління даними, тестування, правові й безпекові процедури, навчання персоналу, підтримку користувачів, оцінювання впливу та подальший розвиток спеціалізованих і агентних систем AI.

Початковим імпульсом для цієї трансформації стало поширення ChatGPT наприкінці 2022 року. Працівники дипломатичних установ почали самостійно використовувати

[1] https://www.state.gov/wp-content/uploads/2026/07/DOS-Generative-AI-Playbook_July-2026.pdf

загальнодоступні інструменти генеративного AI для підготовки промов, редагування текстів, створення документів і виконання адміністративних завдань. Таке неформальне експериментування продемонструвало значний практичний потенціал технології, але одночасно виявило потребу в безпечному, офіційно дозволеному та контрольованому корпоративному середовищі. У відповідь Державний департамент створив платформу для швидкого прототипування й розроблення корпоративних застосунків, першим з яких став StateChat. Паралельно формувалися процедури тестування, правила відповідального використання, навчальні програми, захищені програмні інтерфейси та експериментальні середовища для технічних фахівців і працівників, які не є професійними розробниками. Особливо важливо, що користувачі не розглядалися лише як кінцеві споживачі: вони брали участь у тестуванні, надавали відгуки та безпосередньо впливали на функціональність системи.

Посідник не подає запропонований підхід як універсальну або обов'язкову модель. Автори прямо зазначають, що кожна державна установа повинна адаптувати описані процеси до власного мандата, структури, категорій даних, ризиків і нормативних вимог. Перед упровадженням рекомендується залучати юридичні підрозділи, служби кібербезпеки, фахівців із захисту приватності та комплаєнсу. Таким чином, документ поєднує стратегічне бачення з конкретними організаційними й технічними діями, але залишає установам можливість визначати власну модель реалізації.

Загальна архітектура посібника відображає повний життєвий цикл корпоративного AI-рішення. Спочатку організація повинна закласти стратегічну та інституційну основу. Після цього вона переходить до альфа-фази, у межах якої перевіряється принципова технічна можливість створення безпечного продукту. Бета-фаза має довести, що продукт не лише працює, а й є корисним для реальних користувачів. Наступними етапами є контрольований запуск, масштабування, поглиблення функціональності та оцінювання фактичного впливу. Документ передбачає, що формування базових стратегій, структур та інфраструктури може тривати два-три роки, альфа- і бета-фази – по чотири-шість місяців, запуск – чотири-шість тижнів, масштабування – шість-вісім місяців, перехід до складніших можливостей – ще чотири-шість місяців, а окреме оцінювання впливу – шість-вісім тижнів.

Першим фундаментальним елементом є наявність чіткої стратегії даних і штучного інтелекту. У Державному департаменті цьому передувало ухвалення корпоративної стратегії даних у 2021 році, окремої стратегії AI у 2023 році та об'єднаної стратегії даних і AI у 2025 році. Вони визначили спільні пріоритети, принципи відповідального використання технологій і загальний напрям розвитку, одночасно залишивши окремим бюро та дипломатичним представництвам достатню гнучкість для створення рішень відповідно до їхніх функціональних потреб. Такий підхід дозволив уникнути як хаотичного впровадження несумісних інструментів, так і надмірно централізованої моделі, яка не враховувала б специфіку різних підрозділів.

Організаційною основою ініціатив став Center for Analytics, який виконував роль спеціалізованого центру компетенцій із даних, аналітики та AI. Центр застосував так звану «кампанійну модель», за якої міждисциплінарні команди одночасно працювали над технологією, політиками та практичними потребами користувачів. Розробники, аналітики, керівники, фахівці з даних і представники функціональних підрозділів спільно визначали проблеми, створювали прототипи, тестували їх і коригували правила управління. Завдяки цьому прогалини в процесах, ризики й обмеження виявлялися не після завершення проєкту, а безпосередньо під час його реалізації.

Важливу роль у підготовчій фазі відігравали невеликі пілотні проєкти, які мали довести практичну цінність технології та сформувати внутрішню довіру до неї. Одним із таких прикладів був проєкт AI for Reports Modernization. У його межах було оцифровано, перекладено та опрацьовано понад 115 тисяч документів, точність фінансових даних підвищено на 28%, забезпечено відстеження більш як 800 млн доларів орендних зобов'язань, заощаджено 76,5 тисячі робочих годин і попереджено витрати в розмірі близько 6 млн доларів.

Цей приклад демонструє, що пілот має оцінюватися не за технологічною новизною, а за здатністю розв'язати конкретну проблему, дати вимірюваний результат і створити модель, придатну для подальшого відтворення.

Одним із ключових стратегічних рішень було створення не окремого чатбота, а керованої корпоративної платформи як спільної послуги. Від самого початку система проєктувалася так, щоб підтримувати роботу з чутливими даними, аналітику, розроблення застосунків, інженерію даних і контрольоване експериментування. Вимоги безпеки, договори, правила доступу та адміністративні процедури формувалися достатньо широко, щоб на платформі можна було запускати не лише StateChat, а й інші корпоративні рішення. У результаті створена інфраструктура стала основою для більш як 120 проєктів, включно з інструментами кризового реагування на ситуації, пов'язані із загрозами життю.

Альфа-фаза StateChat мала відповісти на фундаментальне питання: чи здатен Державний департамент створити безпечний корпоративний чатбот, який працюватиме в глобальному масштабі, відповідатиме вимогам кібербезпеки, не створюватиме неприйнятних ризиків і зможе вдосконалюватися з часом. Для цього було сформовано міждисциплінарну команду, налагоджено внутрішні та зовнішні партнерства, створено мінімально життєздатний продукт і запроваджено багаторівневе тестування.

Документ наголошує, що корпоративна система генеративного AI є не лише технічним продуктом, а складною організаційною зміною. До її розроблення із самого початку залучалися фахівці з кібербезпеки, мережевої інфраструктури, доступності, користувацького досвіду, незалежного тестування, зовнішньої політики, приватності та управління офіційними документами. Зовнішні партнери – федеральні установи, університети, дослідницькі центри, технологічні компанії та консультанти – забезпечили доступ до спеціалізованої експертизи, моделей і практичного досвіду, яких бракувало всередині організації.

Початковий прототип StateChat був свідомо обмеженим. Користувач мав лише один діалог, який видалявся через 24 години, оброблення завантажених документів могло тривати кілька годин, а інтеграція з внутрішніми інформаційними системами була відсутня. Проте саме раннє надання доступу реальним користувачам дозволило визначити, які можливості є дійсно важливими. Замість тривалого проєктування на основі припущень команда отримала практичні відомості про потребу в роботі з документами, підключенні внутрішніх джерел та покращенні користувацького досвіду. Основний урок альфа-фази полягає в тому, що обмежений, але функціональний продукт доцільно запускати раніше, ніж команда вважатиме його повністю готовим, за умови, що експеримент відбувається у безпечному та контрольованому середовищі.

До альфа-тестування було залучено 150 осіб, серед яких були фахівці зі штучного інтелекту, кібербезпеки, відповідального за AI та досвідчені користувачі генеративних моделей. Вони перевіряли доступ, автентифікацію, стійкість до кіберзагроз, базову функціональність і практичну придатність системи. Тестування проводилося на трьох рівнях. Внутрішнє функціональне тестування охоплювало інфраструктуру, навантаження, засоби безпеки, доступність та регресійні перевірки. Оцінювання продуктивності AI стосувалося точності, дезінформації, кібербезпеки, користувацького інтерфейсу та стабільності платформи. Приймальне тестування користувачами мало підтвердити, що продукт відповідає реальним робочим потребам. Окремо незалежні фахівці оцінювали безпечність, стійкість, пояснюваність, приватність, справедливість, контекстуальну точність, підзвітність, прозорість, валідність і надійність відповідно до підходів NIST AI Risk Management Framework.

Вирішальним чинником практичної цінності StateChat стало отримання дозволу на експлуатацію системи рівня FISMA High. Процес авторизації тривав близько року та потребував тісної взаємодії з кібербезпековими й управлінськими підрозділами. Завдяки цьому до платформи можна було підключати дипломатичні повідомлення, внутрішні звіти, SharePoint та інші джерела службової інформації. Без такого дозволу система була б обмежена

загальнодоступними або нечутливими даними, що суттєво знизило б її корисність для повсякденної роботи працівників.

Поступово сформувалася структура зрілої команди, яка включала власника продукту, розробників і фахівців із даних, експертів із платформи та управління, незалежних тестувальників, спеціалістів із навчання, комунікацій та управління змінами, а також фахівців з інновацій і досліджень. Особливе значення мав власник продукту, який перетворював потреби установи на пріоритети розробки, забезпечував підтримку керівництва та виступав посередником між технічними можливостями й операційними завданнями.

Після підтвердження технічної можливості проєкт перейшов до бета-фази, основним завданням якої було довести практичну корисність StateChat. Протягом п’яти місяців кількість користувачів збільшилася зі 150 до 8 тисяч. Доступ розширювався поступово, щоб команда могла одночасно спостерігати за поведінкою користувачів, контролювати навантаження, розвивати підтримку та вдосконалювати функціональність. Користувачам відверто повідомляли, що система перебуває на стадії бета-тестування і має обмеження. Така прозорість допомагала управляти очікуваннями та зберігати партнерський характер відносин між розробниками й користувачами.

Бета-фаза показала, що навіть інтуїтивно зрозумілий технологічний продукт не буде широко використовуватися без продуманої системи підтримки. Значна частина персоналу не мала достатнього розуміння можливостей генеративного AI або ставилася до нього скептично. Тому команда організувала регулярні консультаційні години в різних часових поясах, навчальні заходи, інформаційні розсилки та централізований портал AI.State. На цьому ресурсі розміщувалися інструкції, приклади запитів, відеодемонстрації, навчальні модулі, практичні сценарії та анонімізована статистика. Усі матеріали будувалися за принципом урахування реальних умов роботи користувачів, їхнього рівня підготовки, функцій, мов і часових поясів.

Для систематизації великого обсягу відгуків було розроблено механізм Thunderdome. Він передбачав збирання інформації з різних каналів, визначення повторюваних тем, оцінювання технічної здійсненності та стратегічного значення запропонованих функцій, голосування користувачів і формування прозорої дорожньої карти. Під час першого застосування було опрацьовано матеріали із шести каналів, відповіді 800 учасників опитування та 22 інтерв’ю з активними користувачами. Результатом стала шестимісячна дорожня карта, яка включала десять найбільш затребуваних функцій. Це дозволило перетворити розрізнені побажання на обґрунтований план розвитку та показати користувачам, що їхні пропозиції мають реальний вплив на продукт.

Бета-тестування не розглядалося як безстроковий процес. Перехід до корпоративного запуску мав відбутися після досягнення технічної стабільності, усунення критичних помилок, підтвердження користі користувачами та готовності системи підтримки працювати у значно більшому масштабі. Водночас команда розрізняла функції, для яких була необхідна майже бездоганна надійність, і менш критичні можливості, де контрольовані недоліки могли бути прийнятними заради швидшого навчання та вдосконалення.

Корпоративний запуск StateChat був організований як тритижневий поетапний процес, а не одноразове відкриття доступу. Єдиний план охоплював технічну інфраструктуру, матеріали для користувачів, комунікації, навчання, безпеку та роботу із заінтересованими підрозділами. Проводилися щоденні оперативні наради, щотижневі міжфункціональні зустрічі, репетиції масового відкриття доступу та тестове навчання працівників одного великого бюро. Така модель дозволила поступово перевірити систему, усунути проблеми й знизити ризик перевантаження платформи та служби підтримки.

Однією з основних перешкод було те, що працівники не завжди розуміли, чи дозволено використовувати StateChat у службовій діяльності. Тому керівники високого рівня безпосередньо підтримували систему, демонстрували конкретні сценарії її застосування та підтверджували можливість роботи зі службовою інформацією. Таке схвалення усувало

організаційну невизначеність, однак його обов'язково доповнювали практичним навчанням. Після шести навчальних сесій для одного бюро, у яких взяли участь понад 700 працівників, кількість користувачів StateChat у цьому підрозділі зросла на 58%.

Масштабування StateChat у межах 80-тисячного глобального персоналу базувалося на п'яти взаємопов'язаних компонентах: стратегічних комунікаціях, цільовому онбордингу, відкритих тренінгах, асинхронних навчальних матеріалах та мережі партнерів і внутрішніх AI-чемпіонів. Комунікації були спрямовані не стільки на опис технології, скільки на пояснення практичного результату. Замість повідомлення про функцію «аналіз документів за допомогою AI» працівникам демонстрували, як вона дозволяє за кілька хвилин узагальнити десятки документів і виявити тенденції. Для оцінювання ефективності повідомлень використовувалися аналітика взаємодії та A/B-тестування заголовків і змісту електронних листів.

Цільові програми навчання проводилися окремо для бюро, регіонів і функціональних груп. Завдяки цьому приклади, мови та графіки відповідали конкретному контексту працівників. Після спеціалізованого онбордингу для одного регіонального бюро загальна кількість його користувачів зросла на 31%, а середня тижнева активність – на 367%. Відкриті тренінги та консультаційні заходи охопили понад 50 тисяч учасників, а кількість користувачів StateChat у перший квартал корпоративної експлуатації збільшилася з 12 до 23 тисяч.

Асинхронна навчальна екосистема включала бібліотеку сценаріїв використання, практичні поради, інструкції з усунення технічних проблем, самостійні навчальні модулі, понад сто шаблонів запитів та аналітичні панелі. StateChat також був налаштований так, щоб відповідати на запитання про власну функціональність на основі офіційних інструкцій. Для працівників, які часто виконують завдання поза стаціонарним робочим місцем, було створено прототип прогресивного вебзастосунку. Це відображає загальний принцип документа: інструменти та навчання необхідно адаптувати до фактичного способу роботи персоналу, а не до ідеалізованих умов.

Для розширення навчальної спроможності застосовувалася модель «навчи тренера». Підготовлені викладачі, керівники з даних і AI та підготовлені працівники, відповідальні за поширення практик використання AI у своїх підрозділах, самостійно проводили навчальні заходи та консультації для колег у своїх підрозділах і дипломатичних представництвах. Такий підхід дозволив охопити понад 48 тисяч учасників у межах більш як 430 навчальних сесій без пропорційного збільшення центральної команди. Паралельно відстежувалися кількість запитів, активність користувачів, утримання та ефективність навчання. Аналіз даних проводився з урахуванням приватності, щоб отримувати інформацію про тенденції без розкриття персональних або чутливих даних.

Після досягнення широкого охоплення Державний департамент перейшов від масштабності до глибини використання AI. StateChat почав розвиватися від універсального чатбота до екосистеми взаємопов'язаних інструментів, призначених для складних багатоступеневих процесів, зокрема аналізу політики, підготовки документів, роботи з внутрішніми джерелами та перевірки рішень. Одночасно впроваджувалися поглиблені навчальні програми, які допомагали користувачам освоювати спеціалізовані функції та створювати власні рішення.

Прикладом спеціалізованого інструменту є FAMsearch, що дозволяє ставити запитання щодо положень 30-тисячосторінкових Foreign Affairs Manual і Foreign Affairs Handbook та отримувати узагальнені відповіді з прямими посиланнями на відповідні фрагменти. Спочатку користувач мав окремо відкривати FAMsearch, однак згодом StateChat почав автоматично звертатися до нього у фоновому режимі. Це стало одним із перших кроків до агентної моделі, у якій спеціалізовані компоненти взаємодіють між собою без необхідності окремого запуску кожного інструменту користувачем.

Іншим напрямом стала можливість створення користувачами власних спеціалізованих асистентів – customGPTs. Такий підхід змінює роль працівника зі споживача централізовано

створених IT-рішень на активного розробника локального інструменту. Користувач може створити асистента для підготовки регулярних звітів, відповідей на адміністративні запитання або виконання іншого вузького завдання. Це дозволяє задовольняти потреби, які через свою специфічність не стали б пріоритетом великої IT-команди, але здатні забезпечити помітну економію часу та підвищення якості роботи.

Подальший розвиток передбачає узгоджену взаємодію кількох спеціалізованих AI-агентів, які спільно виконуватимуть складні багатоступеневі завдання. У наведеному в документі прикладі під час підготовки дипломатичного повідомлення один агент може автоматично знаходити відповідні нормативні положення, інший – перевіряти попередні документи на цю тему, а третій – пропонувати належний формат. Користувачу не потрібно окремо замовляти кожну дію, оскільки система визначає необхідні кроки відповідно до контексту. Водночас документ описує такі агентні системи переважно як майбутній напрям розвитку, а не як повністю завершену корпоративну функціональність.

Через рік після корпоративного запуску було проведено комплексне оцінювання впливу StateChat. Воно мало з'ясувати, хто використовує інструмент, для яких завдань він застосовується, який результат забезпечує і які чинники сприяють або перешкоджають його прийняттю. Із 3 700 працівників, які розпочали опитування, 2 706 надали достатні відповіді для аналізу. Серед них 2 113 були регулярними користувачами, а 593 користувалися системою рідше одного разу на місяць або взагалі її не застосовували. Автори підкреслюють, що участь була добровільною, тому результати не можуть автоматично вважатися статистично репрезентативними для всього персоналу, хоча великий обсяг відповідей дає змістовне уявлення про користувацький досвід.

Серед регулярних користувачів 90% повідомили про економію часу, а 96% зазначили, що рекомендували б StateChat колегам. Середня заявлена економія становила 1,6 години на тиждень для кожного виду завдання. Зекономлений час працівники використовували для підвищення якості роботи, опрацювання більшої кількості запитів та переходу до важливіших завдань. Найчастіше StateChat застосовувався для підготовки комунікацій, редагування та дослідження інформації. Близько 51% респондентів використовували систему для написання електронних листів та інших повідомлень, заощаджуючи в сукупності понад 1 600 годин на тиждень лише серед учасників опитування. З урахуванням більш як 19 тисяч унікальних щотижневих користувачів документ припускає, що загальна економія на підготовці комунікацій може перевищувати 10 тисяч годин щотижня.

Наведена на сторінці 32 матриця впливу показує співвідношення поширеності окремих сценаріїв і середньої економії часу. Найбільше охоплення мають підготовка електронних листів, редагування, дослідження та узагальнення документів. Водночас створення навчальних матеріалів використовує менша частина працівників, але саме цей сценарій забезпечує найбільшу середню економію – 1,82 години на тиждень, причому 36% відповідних користувачів повідомляють про заощадження понад трьох годин.

Оцінювання також виявило суттєві перешкоди. Деякі користувачі зазначали, що якість відповідей є недостатньою, а перевірка результатів іноді потребує більше часу, ніж самостійне виконання завдання. Іншими проблемами були слабка інтеграція з наявними системами, недостатнє розуміння функцій, невідповідність навчання рівню підготовки та незручності інтерфейсу. Особливу увагу звернено на накопичення невеликих бар'єрів: перенесені консультації, обіцяні, але не реалізовані функції, складність окремих процедур і недостатньо адаптовані матеріали можуть поступово призвести до втрати навіть початково активних користувачів.

На підставі отриманих результатів рекомендується розвивати сценарії використання не лише для аналітичних і політичних функцій, а й для адміністративної, кадрової, навчальної та іншої діяльності. Навчання має диференціюватися відповідно до посад, рівня знань і робочих процесів, а підготовлені працівники, відповідальні за впровадження та поширення практик використання AI у своїх підрозділах, повинні підтримувати користувачів безпосередньо у

їхніх підрозділах. Виявлені проблеми необхідно усувати швидко, не допускаючи їх накопичення. Оцінювання впливу має бути постійним процесом, що поєднує кількісні показники використання з опитуваннями, інтерв'ю та фокус-групами й безпосередньо впливає на подальшу дорожню карту продукту.

У додатку StateChat представлено як один із компонентів ширшої екосистеми AI. Northstar аналізує понад 100 тисяч глобальних медіаджерел більш ніж ста мовами та щодня отримує близько мільйона нових матеріалів. SMART AI використовується для опрацювання офіційної кореспонденції та управління знаннями. Proving Ground надає працівникам середовище для створення спеціалізованих чатботів, автоматизацій і візуалізацій без розгортання окремої інфраструктури. Funhouse призначений для аналізу даних, машинного навчання та візуалізації в захищеному середовищі, а Prompter API забезпечує попередньо схвалений доступ до комерційних моделей і дозволяє вбудовувати функції перекладу, узагальнення, підготовки документів та програмування в наявні інформаційні системи.

Загалом документ демонструє, що результативне впровадження генеративного AI у державному секторі визначається не стільки вибором конкретної моделі, скільки якістю управління всім процесом. Технологічне рішення повинно спиратися на стратегію, захищену інфраструктуру, міждисциплінарну команду, поетапне тестування, підтримку керівництва, навчання персоналу та безперервний зворотний зв'язок. Надання доступу саме по собі не забезпечує прийняття технології, а велика кількість користувачів не є достатнім доказом її ефективності. Реальний результат має оцінюватися за економією часу, підвищенням якості роботи, зменшенням помилок, поліпшенням доступу до знань і здатністю працівників спрямовувати більше ресурсів на складні завдання, для яких необхідні професійне судження, аналіз і людська взаємодія.

Висновки:

- **Упровадження генеративного AI потребує** чіткої стратегії, міждисциплінарної команди та раннього врегулювання питань безпеки, права і захисту даних.
- **Рішення доцільно впроваджувати послідовно:** спочатку провести невеликий пілотний проєкт, потім створити базову робочу версію, здійснити її тестування та лише після цього переходити до повноцінного запуску й масштабування.
- **Доступ до AI сам по собі не забезпечує його використання.** Запуск потрібно одночасно супроводжувати схваленням керівництва, рольовим навчанням, консультаціями, централізованою базою знань, підготовленими працівниками, які підтримують упровадження AI у своїх підрозділах, та прозорим механізмом урахування пропозицій користувачів.
- **Ефективність AI потрібно оцінювати за конкретними результатами: економією часу, підвищенням якості роботи, скороченням помилок і усуненням бар'єрів для користувачів.**

Кіберзлочинність в Африці у 2026 році: системні загрози, штучний інтелект і транснаціональні фінансові схеми [2]

Звіт є комплексною розвідувально-аналітичною оцінкою кіберзлочинності в Африці за період із січня по грудень 2025 року. Документ підготовлено на основі кількісних і якісних даних, отриманих від правоохоронних органів, національних кіберпідрозділів та органів правосуддя 36 африканських держав, а також телеметричної інформації й аналітичних матеріалів приватних партнерів Інтерполу. Звіт має прикладний характер і призначений насамперед для підтримки стратегічних рішень національних органів влади, регіональних організацій та міжнародних партнерів. Його основна теза полягає в тому, що кіберзлочинність в Африці більше не може розглядатися як сукупність ізольованих технічних інцидентів: вона

[2] https://www.interpol.int/Media/Documents/Publications/Cybercrime/African-Cyberthreat-Assessment-Report-2026

перетворилася на індустріалізовану, транскордонну та гнучку кримінальну екосистему, інтегровану в діяльність організованих злочинних мереж.

Стрімка цифровізація африканських держав створила одночасно значні можливості для економічного розвитку та нові системні вразливості. У 2025 році на континенті було зареєстровано понад 1,1 млрд мобільних підключень, обсяг цифрових операцій перевищив 1,1 трлн доларів США, а кількість користувачів Інтернету досягла приблизно 570 млн осіб. Фінансові послуги, мобільні платежі, державні сервіси, охорона здоров'я, освіта й телекомунікації дедалі більше залежать від цифрової інфраструктури. Водночас розвиток законодавства, кіберзахисту, цифрової криміналістики та правоохоронної спроможності не встигає за масштабами технологічного поширення. Саме цей розрив між швидкою цифровою трансформацією та недостатнім рівнем захисту створює сприятливі умови для масштабних шахрайських кампаній, атак на критичну інфраструктуру, викрадення даних і відмивання доходів, одержаних унаслідок кіберзлочинів.

Найпоширенішою категорією зареєстрованих кіберзлочинів залишаються онлайн-шахрайства, включно з фішингом. Значну частку становлять також викрадення особистості, фінансове шахрайство, цифрове сексуальне вимагання, кіберпереслідування, витоки даних, компрометація корпоративної електронної пошти та атаки з використанням програм-вимагачів. Звіт показує, що сучасний кіберзлочинець дедалі рідше покладається лише на складні технічні засоби. Натомість злочинні моделі будуються на поєднанні викрадених даних, соціальної інженерії, маніпулювання довірою, автоматизації та використання штучного інтелекту. Компрометовані облікові дані стають початковою ланкою каскадного злочинного процесу: вони дозволяють отримати доступ до банківських рахунків, мобільних гаманців, електронної пошти та державних послуг, після чого використовуються для викрадення коштів, оформлення кредитів, створення фіктивних ідентичностей або проведення нових шахрайських атак.

Фінансові наслідки кіберзлочинності протягом 2025 року різко посилилися. Задокументовані збитки зросли зі 192 млн доларів США у 2024 році до 484 млн доларів США у 2025 році, а кількість встановлених потерпілих збільшилася з 35 тис. до 87 тис. Сукупні прямі економічні збитки для континенту оцінюються щонайменше у 5 млрд доларів США. Водночас Інтерпол наголошує, що реальні показники можуть бути значно вищими, оскільки в багатьох державах відсутні обов'язкові або уніфіковані механізми повідомлення про кіберінциденти, а компанії й державні органи нерідко приховують атаки через побоювання репутаційних наслідків. Недостатній рівень повідомлення про кіберінциденти обмежує спроможність держав об'єктивно оцінювати масштаби та характер кіберризиків, визначати пріоритетні загрози й ефективно розподіляти ресурси для їх мінімізації.

Кіберзагрози в Африці мають виразну регіональну специфіку. Центральна Африка характеризується високим рівнем соціальної інженерії, романтичних шахрайств, франкомовних фішингових кампаній, незаконних кредитних застосунків і ботнет-активності. Значна частина інцидентів пов'язана з людським фактором, поведінкою працівників і недостатньою цифровою обізнаністю населення. Порівняно невелика кількість офіційно зареєстрованих атак програм-вимагачів у цьому регіоні, за оцінкою Інтерполу, пояснюється передусім недостатнім рівнем повідомлень. Злочинці часто надають перевагу прихованому тривалому доступу до інформаційних систем, збору облікових даних і викраденню інформації, а не відкритому блокуванню ресурсів із вимогою викупу.

У Східній Африці центральною загрозою стало шахрайство з мобільними грошима, заміною SIM-карток і незаконним доступом до мобільних гаманців. У Кенії у 2025 році кількість випадків шахрайської заміни SIM-карток зросла на 327%, було виявлено понад 123 тис. незаконно оформлених SIM-карток, а втрати користувачів мобільних гаманців оцінювалися приблизно у 3,8 млн доларів США. Одночасно регіон зазнав атак на телекомунікаційну й енергетичну інфраструктуру. Інцидент із системами оператора електромережі Уганди продемонстрував, що кібератаки можуть становити загрозу не лише для конфіденційності

даних, а й для безперервності функціонування критично важливих державних послуг. Однією з основних вразливостей залишаються недостатньо ефективні процедури ідентифікації клієнтів і відсутність біометричної перевірки в режимі реального часу під час реєстрації SIM-карток та відкриття мобільних фінансових рахунків.

Західна Африка виступає одним із найбільш активних центрів компрометації корпоративної електронної пошти, криптовалютного шахрайства, романтичних інвестиційних схем, шахрайства з мобільними грошима та цифрового вимагання. У регіоні діють транскордонні мережі, які використовують компанії-оболонки, мобільні платіжні платформи, криптоактиви, підставних отримувачів і фіктивні фінтех-компанії для переміщення та маскування злочинних доходів. Західна Африка одночасно виступає джерелом, транзитною територією і ціллю глобальних кіберзлочинних операцій. Компрометація державних інформаційних ресурсів, зокрема вебсайту Нігерійського бюро статистики, свідчить про стратегічне значення атак на публічні дані: такі інциденти можуть порушувати роботу державних установ, ускладнювати збір економічної інформації та використовуватися для поширення дезінформації.

Південна Африка залишається найбільш цифровізованим і водночас найбільш атакованим регіоном континенту. На Південно-Африканську Республіку припало 92% виявлених атак програм-вимагачів в Африці, а також значна частка фішингових і DDoS-атак. Висока концентрація центрів обробки даних, підводних телекомунікаційних кабелів і цифрових сервісів робить регіон привабливою ціллю для глобальних кіберзлочинних угруповань. При цьому наявність відносно розвиненого законодавства сама по собі не забезпечує належного захисту. Ключовими проблемами залишаються практична реалізація вимог, недостатньо оперативний обмін розвідувальною інформацією, несвоєчасне оновлення програмного забезпечення та слабка координація між правоохоронними органами, командами реагування на кіберінциденти і приватними компаніями.

Одним із найнебезпечніших трендів стало перетворення програм-вимагачів із засобу фінансового вимагання на інструмент системного порушення роботи держави й економічного примусу. Злочинці дедалі частіше обирають цілями енергетику, транспорт, охорону здоров’я, державне управління, телекомунікації та інші критично важливі сектори. Атака на метеорологічні системи Південно-Африканської Республіки спричинила перебої в роботі сервісів, пов’язаних з авіаційною та морською навігацією. Атака на митну службу Нігерії паралізувала оформлення вантажів у портах і призвела до значних додаткових витрат. Інцидент в Уганді поставив під загрозу системи моніторингу національної електромережі. Таким чином, предметом вимагання стають уже не лише дані, а сама здатність державних і приватних установ продовжувати виконання основних функцій.

Звіт докладно описує типовий ланцюг атаки програм-вимагачів. Спочатку злочинці вивчають потенційну ціль, ідентифікують вразливі системи та відповідальних працівників, після чого отримують первинний доступ через фішинг, викрадені паролі або технічні вразливості. Далі шкідливе програмне забезпечення інтегрується в систему, проводиться внутрішнє сканування мережі, шифрування файлів і направлення вимоги про викуп. Машинне навчання використовується для автоматичного пошуку незахищених маршрутизаторів, застарілого програмного забезпечення та неправильно налаштованих хмарних сервісів. Ботнети забезпечують масштабне розповсюдження шкідливого програмного забезпечення, дозволяючи злочинцям одночасно перевіряти та атакувати значну кількість потенційних цілей.

Компрометація корпоративної електронної пошти у звіті характеризується як фінансовий двигун транскордонної кіберзлочинності. На відміну від атак, спрямованих на технічне блокування систем, BEC-схеми (шахрайство через ділову електронну пошту) експлуатують довіру працівників. Злочинці проводять попередню розвідку, визначають осіб, відповідальних за платежі, бухгалтерський облік або закупівлі, компрометують електронні скриньки та надсилають фальшиві доручення про зміну платіжних реквізитів. Штучний інтелект дає можливість відтворювати стиль керівника, корпоративну термінологію, структуру листування

та характерні мовні особливості. У межах операції Інтерполом було припинено спробу переказу 7,9 млн доларів США з рахунку нафтової компанії, що показало одночасне використання злочинцями інфраструктури та фінансових рахунків у кількох юрисдикціях.

Важливе місце у звіті займає взаємозв'язок кіберзлочинності та відмивання коштів. Доходи від BEC, програм-вимагачів, криптовалютних шахрайств і викрадення коштів із мобільних гаманців переміщуються через підставні банківські рахунки, мережі грошових посередників, компанії-оболонки, криптовалютні біржі та мобільні платіжні системи. «Грошових мулів» нерідко залучають через фіктивні оголошення про дистанційну роботу, пропонуючи виконувати функції «фінансових агентів» або «операторів транзакцій». Частина таких осіб не усвідомлює, що бере участь у легалізації злочинних доходів, однак саме їхні рахунки використовуються для швидкого розпорошення коштів і ускладнення фінансового розслідування. Недостатньо швидкий обмін інформацією між банками, телекомунікаційними операторами, фінтех-компаніями, постачальниками послуг у сфері віртуальних активів і правоохоронними органами дозволяє злочинцям виводити кошти до моменту їх блокування.

Онлайн-шахрайство у 2025 році остаточно набуло промислового характеру. Замість окремих фішингових повідомлень діють централізовані шахрайські центри з розподіленими функціями, технологічною інфраструктурою, системами залучення жертв, каналами відмивання коштів і методами уникнення правоохоронного контролю. Частина таких центрів пов'язана з торгівлею людьми: осіб залучають обманом, утримують проти їхньої волі та змушують брати участь у шахрайських кампаніях. Мобільне фінансове шахрайство було зафіксовано у 97% держав, які взяли участь в опитуванні Інтерполу. Злочинці використовують підміну SIM-карток, незаконно зареєстровані номери, фішингові повідомлення, соціальні мережі та штучний інтелект, щоб отримати доступ до мобільних гаманців або переконати потерпілих добровільно переказати кошти.

Окремими різновидами організованого шахрайства стали незаконні мікрокредитні застосунки, псевдоінвестиційні платформи, схеми Понці та романтичне інвестиційне шахрайство. Незаконні кредитні застосунки збирають персональну інформацію користувачів, контакти та дані мобільних пристроїв, після чого використовують автоматизовані дзвінки, погрози й публічне приниження для примусового стягнення коштів. Псевдоінвестиційні платформи поширюються за допомогою діпфейкових відео політичних лідерів, підприємців і відомих осіб. Романтичні схеми поєднують емоційне маніпулювання з фіктивними інвестиціями: жертву переводять із соціальної мережі до месенджера, поступово формують довіру, а потім переконують перерахувати кошти на контрольовані злочинцями рахунки або криптовалютні адреси. Операція Serengeti 2.0 дозволила ліквідувати мережу, відповідальну за збитки на суму близько 300 млн доларів США та обман приблизно 60 тис. потерпілих.

Надзвичайно небезпечним напрямом стало цифрове сексуальне вимагання, яке дедалі частіше здійснюється за допомогою штучного інтелекту. У 2025 році було виявлено близько 600 тис. випадків або спроб такого вимагання. Сучасні інструменти дозволяють створити реалістичне компрометувальне зображення на основі однієї фотографії із соціальних мереж. Злочинці погрожують поширити сфабриковані або справжні інтимні матеріали, вимагаючи регулярних платежів у криптоактивах чи через мобільні гаманці. Особливо вразливими є неповнолітні та молоді користувачі. Водночас потерпілі часто не повідомляють про злочин через сором, страх і відсутність спеціалізованих служб підтримки. Правоохоронним органам бракує підрозділів, здатних проводити експертизу діпфейків, розслідувати онлайн-насильство сексуального характеру та забезпечувати належний захист потерпілих.

Витоки даних визначаються у звіті як основа, на якій будується майже вся сучасна кіберзлочинна екосистема. Викрадені персональні дані, банківські реквізити, документи, SIM-коди та облікові записи використовуються для викрадення особистості, створення синтетичних ідентичностей, оформлення кредитів, відкриття рахунків, компрометації корпоративної електронної пошти та проведення цільових фішингових атак. Більшість виявлених уразливостей не були новими або технологічно складними. Причинами витоків

часто ставали незахищені адміністративні панелі, застарілі маршрутизатори, неоновлені VPN-системи та неправильно налаштовані вебплатформи. Інтерпол робить висновок, що витоки даних є не лише технічною проблемою, а й проявом неналежного корпоративного управління, слабкого внутрішнього контролю та недостатньої відповідальності керівництва.

У 2025 році кількість даних африканського походження на форумах даркнету збільшилася на 62% порівняно з попереднім роком. Найчастіше продавалися документи, що посвідчують особу, PIN-коди SIM-карток, банківські реквізити та інформація про мобільні гаманці. Частина цих даних походила з попередніх витоків, фішингових кампаній і скомпрометованих мобільних застосунків. Звіт підкреслює, що захист персональних даних має розглядатися як питання національної безпеки, а не лише як технічна чи адміністративна функція. Для цього необхідні обов'язкове повідомлення про інциденти, незалежний нагляд, мінімальні стандарти безпеки, своєчасне усунення вразливостей і відповідальність за неналежний захист інформації.

Фінансове шахрайство дедалі більше спирається на синтетичні ідентичності – цифрові профілі, сформовані шляхом поєднання справжніх персональних даних із вигаданими елементами. Такі профілі використовуються для проходження формальних процедур ідентифікації, відкриття банківських рахунків, отримання мобільних кредитів і реєстрації SIM-карток. Особливу проблему становить фрагментарність національних систем цифрової ідентифікації. Злочинці можуть викрасти персональні дані в одній країні, використати їх для відкриття рахунку в іншій, а потім перемістити кошти через третю юрисдикцію. Відсутність сумісних стандартів і швидкого міжвідомчого обміну даними між банками, телекомунікаційними компаніями та правоохоронними органами створює значні прогалини у виявленні та припиненні таких схем.

Штучний інтелект у 2025 році перетворився з допоміжного інструменту на один із ключових операційних механізмів кіберзлочинності. За результатами опитування Інтерполу, у 55% кіберзлочинних справ AI використовувався в тій чи іншій формі. Він застосовується для автоматизованого збору інформації про потенційних жертв, створення персоналізованих фішингових повідомлень, підроблення голосу та відео, створення синтетичних ідентичностей, обходу традиційних процедур KYC, написання шкідливого коду й адаптації атак до конкретного середовища. Діпфейки використовуються для імітації державних посадовців, керівників компаній, членів сімей і відомих осіб, що суттєво підвищує переконливість шахрайських кампаній. Звіт також звертає увагу на появу концепцій програм-вимагачів, здатних самостійно генерувати й адаптувати шкідливий код за допомогою генеративного AI.

Правоохоронна спроможність протидіяти таким загрозам залишається нерівномірною. Лише 8% аналітиків мають поглиблену компетентність у сфері AI, а 92% опитаних органів назвали нестачу технічних знань головною перешкодою для ефективного використання відповідних інструментів. Більшість слідчих продовжує працювати вручну, тоді як злочинні операції здійснюються автоматизовано та з високою швидкістю. У звіті підкреслюється, що головною проблемою є не просто відсутність дорогого програмного забезпечення, а нестача навичок розпізнавання синтетичних голосів, відео, документів, автоматизованих фішингових шаблонів і поведінкових ознак використання AI. Тому грамотність у сфері штучного інтелекту має стати базовою професійною компетенцією слідчих, прокурорів, експертів і суддів.

Інституційні проблеми посилюються гострим дефіцитом ресурсів. Дев'яносто чотири відсотки опитаних правоохоронних органів повідомили про недостатність інструментів цифрової криміналістики, а 78% – про нестачу бюджетів, технічного обладнання та спеціалізованих працівників. Лише 17% держав мають кіберпідрозділи чисельністю понад 100 осіб, тоді як у багатьох країнах такі підрозділи складаються менш ніж із десяти працівників. Особливо бракує експертів із цифрової криміналістики, аналізу шкідливого програмного забезпечення, відстеження криптоактивів, мережевої безпеки та реагування на інциденти. Вісімдесят дев'ять відсотків респондентів назвали транскордонну співпрацю одним із головних бар'єрів

результативного розслідування, а повільний обмін даними часто призводить до втрати електронних доказів і припинення перспективних слідчих дій.

Правове середовище залишається фрагментованим. Хоча більшість держав мають спеціальне законодавство про кіберзлочинність, визначення правопорушень, правила допустимості електронних доказів, строки зберігання даних і процедури міжнародної правової допомоги суттєво відрізняються. У деяких юрисдикціях нечітко врегульовані криптоджекінг, кіберпереслідування, створення діпфейків, сексуальне насильство з використанням зображень і торгівля людьми через цифрові платформи. Такі відмінності створюють можливості для юрисдикційного арбітражу: злочинці переміщують інфраструктуру або фінансові потоки до держав, де відповідна діяльність недостатньо криміналізована чи правоохоронні органи мають обмежені повноваження. Відсутність уніфікованих термінових процедур отримання та збереження цифрових доказів особливо шкодить розслідуванню BEC, програм-вимагачів і шахрайств із діпфейками.

Недостатньо розвиненими залишаються і механізми державно-приватного партнерства. Правоохоронні органи часто не мають чітких, законних та оперативних каналів отримання інформації від соціальних платформ, телекомунікаційних операторів, банків, фінтех-компаній і операторів мобільних грошей. Дані про IP-адреси, рух коштів, заміну SIM-карток і діяльність облікових записів можуть надаватися лише після тривалих судових процедур. Навіть за наявності меморандумів про взаєморозуміння державні органи нерідко не мають технічної інфраструктури або процедур для практичного обміну даними. У результаті критично важлива інформація залишається ізольованою, надається із запізненням або взагалі втрачається до моменту початку розслідування.

Попри масштаб проблем, звіт фіксує поступове посилення національних і регіональних заходів. У 2025 році 17 держав ухвалили або оновили законодавство про кіберзлочинність, створили спеціалізовані органи, національні стратегії та платформи для повідомлення про інциденти. Розширилися програми підготовки з цифрової криміналістики, роботи з електронними доказами, мобільної криміналістики, аналізу блокчейну, відстеження криптовалютних гаманців і повернення активів. Важливою тенденцією став перехід від разових навчальних заходів до інституціоналізованих і регіонально координованих програм, спрямованих на формування постійної професійної спроможності.

Результативність міжнародної координації підтверджують операції Інтерполу Serengeti 2.0, Contender 3.0, Sentinel і Red Card 2.0. Вони призвели до понад 1 500 арештів, вилучення тисяч електронних пристроїв, ліквідації шкідливих серверів, доменів і мереж, повернення мільйонів доларів та встановлення значної кількості потерпілих. Операція Sentinel охопила 19 держав і була спрямована проти BEC, цифрового вимагання та програм-вимагачів, тоді як Red Card 2.0 зосереджувалася на інвестиційному шахрайстві, мобільних фінансових схемах і фіктивних кредитних застосунках. Ключовими факторами успіху стали використання захищеної системи Інтерполу I-24/7, оперативний обмін розвідувальною інформацією та співпраця з приватними компаніями.

У заключній частині Інтерпол наголошує, що ефективна протидія кіберзлочинності потребує не окремих реактивних заходів, а системної моделі, яка поєднує стандартизовані технічні можливості, гармонізоване законодавство, швидкий транскордонний обмін інформацією, підготовку фахівців і формалізовану співпрацю з приватним сектором. Національні кіберпідрозділи повинні мати мінімальний набір інструментів мобільної та цифрової криміналістики, аналізу оперативної пам’яті, дослідження шкідливого програмного забезпечення, відстеження криптоактивів і виявлення дипфейків. Рекомендується створити цілодобову мережу контактних осіб, уніфікувати правила збереження цифрових доказів, установити обов’язкові строки реагування на термінові запити та запровадити централізовану систему повідомлення про кіберінциденти в режимі реального часу.

Окреме значення для системи протидії відмиванню коштів мають рекомендації щодо створення спеціалізованих підрозділів із розслідування операцій із криптоактивами, зокрема

у складі підрозділів фінансової розвідки, та встановлення для постачальників послуг у сфері віртуальних активів обов'язку повідомляти про підозрілі операції. Інтерпол також пропонує інтегрувати системи банків, телекомунікаційних операторів, фінтех-компаній і мобільних платіжних платформ із національними системами виявлення шахрайства, використовувати біометричну перевірку під час реєстрації SIM-карток і встановлення ділових відносин, а також проводити регулярні кібер-аудити критичної інфраструктури. Для державних установ мають бути обов'язковими мінімальні стандарти резервного копіювання та відновлення інформаційних систем.

Висновки:

- **Необхідно створити єдиний механізм реагування:** забезпечити цілодобовий обмін інформацією між кіберпідрозділами, ПФР, банками, телеком- і фінтех-компаніями та постачальниками послуг у сфері віртуальних активів.
- **Кіберрозслідування мають бути стандартизовані:** необхідно забезпечити підрозділи інструментами цифрової криміналістики, аналізу шкідливого програмного забезпечення, відстеження криптоактивів і виявлення дипфейків.
- **Потрібно посилити захист даних і цифрової ідентичності:** необхідно запровадити обов'язкове повідомлення про інциденти, кібер-аудити критичної інфраструктури, резервне копіювання та контроль синтетичних ідентичностей.
- **Протидіяти всій злочинній екосистемі:** припиняти роботу серверів, шахрайських центрів і ботнетів, заморожувати доходи та оцінювати результат за повернутими активами й завершеними провадженнями.

У цілому звіт показує, що кіберзлочинність стала одним із ключових елементів сучасної транснаціональної організованої злочинності. Її розвиток підтримується доступністю генеративного штучного інтелекту, моделями «кіберзлочинність як послуга», викраденими персональними даними, слабкими системами цифрової ідентифікації та можливістю швидкого переміщення злочинних доходів через банки, мобільні платформи, підставні компанії й криптоактиви. Відповідь на ці загрози має поєднувати технічне припинення злочинної інфраструктури з фінансовими розслідуваннями, відстеженням і заморожуванням активів, установленням підставних отримувачів коштів та притягненням до відповідальності організаторів злочинних мереж. Кібербезпека в такій моделі є не лише функцією захисту інформаційних технологій, а невід'ємною складовою економічної безпеки, протидії відмиванню коштів, захисту критичної інфраструктури та збереження суспільної довіри до цифрової економіки.

Регулювання

Іспанія: попередній законопроєкт про комплексні заходи у сфері ПВК/ФТ/ФРЗМЗ і створення Національного органу фінансової доброчесності (ANIFI) [3]

28 липня 2026 року Рада міністрів Іспанії схвалила в першому читанні попередній законопроєкт (anteproyecto de ley) про комплексні заходи у сфері запобігання відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Окремим рішенням санкціоновано термінову адміністративну процедуру опрацювання документа, передбачену статтею 27.1.a) Закону 50/1997 про Уряд, що свідчить про намір скоротити строки проходження. Документ передається на публічні слухання та інформування громадськості перед подальшим розглядом. Уряд формулює подвійну мету реформи: зміцнення інституційної архітектури через створення спеціалізованого незалежного органу та

[3] https://www.lamoncloa.gob.es/consejodeministros/referencias/Paginas/2026/20260728-referencia-rueda-de-prensa-ministros.aspx

приведення іспанського законодавства у відповідність до європейського антилегалізаційного пакета 2024 року і стандартів FATF.

Центральною новелою є створення Національного органу фінансової доброчесності (Autoridad Nacional de Integridad Financiera, ANIFI) – незалежного адміністративного органу, що об'єднає компетенції, розподілені сьогодні між SEPBLAC і Секретаріатом Комісії із запобігання відмиванню коштів. ANIFI інтегрує функції підрозділу фінансової розвідки, нагляду та інспектування, санкційні повноваження та повноваження у сфері міжнародних фінансових санкцій. Додатково орган отримує компетенцію щодо фінансування розповсюдження зброї масового знищення, яка досі не була закріплена за жодним іспанським органом, – це усунення прямої інституційної прогалини, що зазвичай стає предметом зауважень під час взаємних оцінок. ANIFI також визначено єдиним контактом Іспанії у відносинах з AMLA.

Найбільш дискусійним з методологічного погляду є поєднання в одному органі функції підрозділу фінансової розвідки з наглядовою та санкційною функціями. Рекомендація 29 FATF не забороняє такої моделі, проте вимагає операційної незалежності підрозділу фінансової розвідки та захисту інформації, отриманої в межах повідомлень про підозрілі операції. Аргументом уряду є усунення фрагментації та підвищення видимості зобов'язань Іспанії; ризик полягає в потенційному напруженні між аналітичною логікою фінансової розвідки, що спирається на добровільну співпрацю підзвітних осіб і конфіденційність, та правозастосовною логікою нагляду, що передбачає перевірки й санкції щодо тих самих осіб. Практична відповідь на це напруження зазвичай полягає у внутрішньому функціональному відокремленні та обмеженні обміну даними між напрямами, і саме ці деталі мають з'ясуватися на етапі публічних консультацій.

Модель фінансування є автономною: ANIFI не залежатиме від державного бюджету і фінансуватиметься за рахунок збору із підзвітних осіб, що діють на підставі адміністративної ліцензії – насамперед фінансових установ і операторів грального бізнесу, – а також обмеженої частки накладених ним санкцій, спрямованої на фінансування діяльності із запобігання й переслідування та міжнародного співробітництва. Механізм спрямування частки штрафів на власну діяльність органу об'єктивно створює питання конфлікту інтересів, яке у порівняльній практиці знімається встановленням верхньої межі такої частки, її цільового призначення та зовнішнього аудиту використання коштів. Для прискорення запуску орган будуватиметься на структурі чинного Фонду впорядкованої банківської реструктуризації (FROB) з використанням його операційних служб і досвіду роботи у фінансовому секторі.

Перетворення FROB спричиняє паралельну реформу режиму банківського врегулювання. Виконавчі функції врегулювання передаються органам, що вже здійснюють превентивне врегулювання, – Банку Іспанії щодо кредитних установ і Національній комісії з ринку цінних паперів щодо інвестиційних фірм, – так що для кожного типу установ існуватиме єдиний орган врегулювання, що відповідає рекомендаціям Міжнародного валютного фонду. Передавання супроводжується вимогою функціонального відокремлення від наглядової діяльності в межах кожного органу задля запобігання конфлікту інтересів та збереженням участі Міністерства економіки в рішеннях із бюджетним впливом або впливом на фінансову стабільність.

Матеріальна частина реформи оновлює національне законодавство відповідно до європейських і міжнародних стандартів: розширюється перелік підзвітних осіб,

Висновки:

- Іспанія об'єднує підрозділ фінансової розвідки, нагляд і санкційні повноваження в одному незалежному органі.
- Компетенцію щодо протидії фінансування розповсюдження ЗМЗ уперше прямо закріплено за конкретним органом.
- Самофінансування через збір із підзвітних суб’єктів знімає залежність від бюджету, але потребує запобіжників.
- Орган будується на базі FROB – використання наявної інфраструктури замість створення структури з нуля.

посилюється прозорість кінцевої бенефіціарної власності з наданням Центральному реєстру нових інспекційних і санкційних повноважень, посилюються вимоги до ділової репутації, які унеможливлюють для осіб, засуджених за відмивання коштів, статус підзвітної особи або керівництво нею, а також посилюється контроль за рухом готівки. За повідомленнями, до кола підзвітних осіб уперше включаються постачальники послуг, пов'язаних з криптоактивами, платформи краудфандингу, а також професійні футбольні клуби та агенти – останнє відображає типології зловживань у професійному спорті, які раніше документувалися FATF і Радою Європи.

Для України іспанський досвід становить інтерес насамперед як матеріал для порівняльного аналізу інституційної моделі. Держфінмоніторинг поєднує функції підрозділу фінансової розвідки з окремими наглядовими повноваженнями, і питання про межі такого поєднання періодично актуалізується під час оцінювання відповідності стандартам FATF.

Іспанський законопроєкт дає предметний приклад того, як держава-член ЄС розв'язує три супутні завдання одночасно: консолідацію інституцій, закріплення компетенції щодо фінансування розповсюдження зброї масового знищення та побудову самофінансованої наглядової спроможності без навантаження на державний бюджет.

Санкції

Персональні санкції проти 23 юридичних і 20 фізичних осіб, залучених до постачання компонентів для російського ВПК [4]

3 серпня 2026 року Президент України підписав Указ № 704/2026, яким уведено в дію рішення Ради національної безпеки і оборони України від 2 липня 2026 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)». Рішення ухвалено відповідно до статті 5 Закону України «Про санкції» на підставі пропозицій, внесених Службою безпеки України; обмежувальні заходи застосовано до фізичних осіб згідно з додатком 1 та до юридичних осіб згідно з додатком 2. Указ набирає чинності з дня опублікування. Окремої уваги заслуговує місячний розрив між ухваленням рішення РНБО (2 липня) і введенням його в дію (3 серпня): для суб'єктів первинного фінансового моніторингу юридично значущим є саме момент набрання чинності указом, тоді як публічні згадки про рішення Ради можуть з'являтися раніше і не породжують обов'язку застосування заходів.

Обсяг заходів охоплює 23 компанії та 20 пов'язаних із ними фізичних осіб, які виробляють і постачають обладнання та компоненти для російського військово-промислового комплексу і силових структур в обхід чинних санкційних режимів. За повідомленнями, обмеження застосовано безстроково та на строк десять років і передбачають блокування активів, повне припинення торговельних операцій, анулювання ліцензій та заборону виведення капіталів за межі України. Такий набір заходів вимагає від суб'єктів первинного фінансового моніторингу не лише замороження активів, а й перегляду наявних договірних відносин та операцій, що перебувають у процесі виконання, включно з тими, де підсанкційна особа виступає непрямим вигодоодержувачем.

Профіль фігурантів дає уявлення про пріоритети санкційної політики. До переліку включено компанію «Кідма Тек», що виготовляє оптичні прилади, засоби протиповітряної оборони та реактивні системи залпового вогню й ремонтує авіаційні та протитанкові керовані ракети; завод імені Морозова у структурі підсанкційного «Ростєха», який виробляє вибухові речовини, ракетне паливо та матеріали для ракетних комплексів і, зокрема, постачає твердопаливні заряди для двигуна балістичної ракети «Іскандер-М»; підприємство «Спецелектронкомплект», залучене до виробництва керованих авіаційних ракет; підприємство «Аурум», що постачає системи радіоелектронної боротьби та безпілотні

[4] https://www.rnbo.gov.ua/ua/Ukazy/7713.html

апарати. Окремим блоком є російські підприємства у сфері інформаційних технологій, які розробляють цифрові рішення та програмні продукти інформаційної безпеки для державних і приватних замовників. Останнє відображає розширення санкційного фокусу з кінцевих виробників озброєння на постачальників технологічної інфраструктури, що забезпечує стійкість оборонного сектору.

Методологічно вартою уваги є присутність у переліку зареєстрованого на Львівщині спільного підприємства «Бориславська нафтова компанія». Застосування персональних спеціальних економічних заходів до резидента України порушує низку практичних питань: порядок блокування активів національної юридичної особи, обсяг і строки повідомлення Держфінмоніторингу, режим обслуговування рахунків контрагентів і пов'язаних осіб. Підстави включення офіційно не розкриваються, що об'єктивно обмежує можливості суб'єктів первинного фінансового моніторингу провести ризик-орієнтований аналіз кола афілійованих осіб і визначити, чи поширюються ризики на пов'язані структури, формально не внесені до переліку.

Пункт 4 рішення РНБО зобов'язує Міністерство закордонних справ поінформувати компетентні органи Європейського Союзу, Сполучених Штатів Америки та інших держав про застосування санкцій і порушити перед ними питання запровадження аналогічних обмежувальних заходів. Це відображає усталений підхід санкційної синхронізації, за якого українські позначення дедалі частіше слугують попереднім етапом для подальшого включення тих самих суб'єктів до переліків партнерів.

Звіти окремих інституцій та експертів

Системна протидія шахрайству з авторизованими платежами: підходи до державної політики та управління [5]

Документ є практичним методологічним посібником, присвяченим формуванню державної політики у сфері протидії шахрайству з авторизованими платежами, яке в міжнародній практиці часто позначається як APP fraud. Посібник орієнтований насамперед на держави, у яких національна система протидії такому виду шахрайства лише формується або залишається фрагментарною. Його цільовою аудиторією є розробники державної політики, центральні банки, регулятори фінансового сектору, правоохоронні органи, установи кримінальної юстиції, телекомунікаційні та цифрові регулятори, органи захисту прав споживачів і персональних даних, банки, платіжні установи, телекомунікаційні компанії, цифрові платформи, громадські організації та дослідники. Документ може використовуватися як цілісне керівництво або як довідковий інструмент для розв’язання конкретних практичних питань, зокрема оцінювання національного шахрайського середовища, визначення пріоритетів, залучення ключових учасників, створення механізмів обміну інформацією та вибору найбільш реалістичних заходів з урахуванням наявних ресурсів.

Під шахрайством з авторизованими платежами автори розуміють ситуації, у яких злочинці за допомогою обману, соціальної інженерії, психологічного тиску, маніпуляції або примусу спонукають потерпілу особу самостійно ініціювати чи підтвердити переказ коштів або передання інших цінностей. На відміну від неавторизованого платіжного шахрайства, коли злочинець використовує викрадені платіжні реквізити або скомпрометовану систему без відома власника рахунку, у випадку APP fraud платіж формально підтверджується самим клієнтом, але його рішення ґрунтується на неправдивій інформації або сформоване під впливом злочинця. Саме ця особливість суттєво ускладнює виявлення операцій і визначення відповідальності між потерпілим, банком, платіжною установою, телекомунікаційним оператором, цифровою платформою та іншими учасниками. Автори також звертають увагу на

[5] https://static.rusi.org/authorised-payment-fraud-approaches-policy-governance-jul-2026.pdf

проблематичність терміна «скам», оскільки його використання може применшувати тяжкість злочину та створювати враження, що йдеться лише про необережність потерпілої особи. Водночас цей термін зберігається в документі через його широке застосування в офіційних політичних і регуляторних інструментах різних держав.

Вихідною тезою дослідження є те, що шахрайство з авторизованими платежами не повинно розглядатися виключно як проблема захисту споживачів або внутрішнього банківського контролю. Його наслідки виходять далеко за межі індивідуальних фінансових втрат, оскільки систематичне поширення шахрайських схем підриває довіру населення до банків, платіжних сервісів, державних установ і цифрових технологій, створює додаткове навантаження на правоохоронні органи, послаблює фінансову інклюзію та може негативно впливати на економічну стабільність і цілісність фінансової системи. Особливо значними такі ризики є для держав із низьким або середнім рівнем доходу, де цифровізація фінансових послуг може відбуватися швидше, ніж формування належних механізмів захисту, нагляду та реагування. За таких умов зростання шахрайства здатне зруйнувати довіру до безготівкових платежів і нівелювати результати державної політики щодо розширення доступу населення до фінансових послуг.

Посібник ґрунтується на комплексному огляді міжнародної літератури та інтерв'ю з 36 представниками заінтересованих сторін із 13 країн. На підставі цього аналізу автори визначають спільні елементи різних національних систем протидії шахрайству та фактори, які сприяють їх ефективному практичному функціонуванню. Документ свідомо не встановлює універсального переліку обов'язкових заходів, оскільки національні системи відрізняються за структурою фінансового сектору, рівнем цифровізації, поширеними видами шахрайства, правовими повноваженнями органів влади, доступністю даних, інституційною спроможністю та ресурсами. Натомість державам пропонується визначити власну вихідну позицію, сформулювати цілі та обрати ті заходи, які є найбільш життєздатними, потенційно результативними та можуть бути послідовно впроваджені в конкретному національному контексті.

Автори зазначають, що протягом останніх років у відповідь на зростання масштабів платіжного шахрайства було розроблено значну кількість міжнародних рекомендацій і національних стратегій. Сінгапур, Велика Британія та Австралія запровадили загальнодержавні моделі, у межах яких відповідальність за протидію шахрайству поступово поширюється за межі банківського сектору. Сінгапур у 2019 році створив один із перших спеціалізованих центрів протидії шахрайству, а у 2024 році запровадив Рамкову модель спільної відповідальності за протидію шахрайству (Shared Responsibility Framework), яка установила обов'язки фінансових установ і телекомунікаційних операторів щодо протидії фішинговим схемам. Велика Британія у 2026 році оновила державну стратегію боротьби з шахрайством, закріпивши загальносистемний підхід і передбачивши створення центру протидії онлайн-злочинам із залученням державного та приватного секторів. Австралія у 2025 році ухвалила Рамкову система запобігання шахрайству (Scams Prevention Framework), який законодавчо закріпив колективну відповідальність банків, телекомунікаційних компаній і цифрових платформ. На міжнародному рівні відповідні підходи розвивають FATF, Організація Об'єднаних Націй, Інтерпол та інші організації, які наголошують на необхідності міжсекторальної співпраці та використання наявних механізмів ПВК/ФТ для виявлення, блокування і відстеження доходів від шахрайства.

Незважаючи на відмінності між національними моделями, міжнародні підходи збігаються в розумінні того, що сучасне шахрайство має багатосекторальний і часто транскордонний характер. Одна шахрайська операція може одночасно передбачати використання соціальної мережі для пошуку потерпілої особи, платної цифрової реклами для поширення неправдивої інвестиційної пропозиції, телекомунікаційного зв'язку для психологічного впливу, банківського або платіжного рахунку для одержання коштів і мережі підставних осіб для їх подальшого переказу та зняття. Фрагментарний нагляд призводить до ситуації, коли кожна установа бачить лише окремий елемент шахрайської схеми й не має достатньої інформації або

повноважень для її припинення. Тому ізольовані заходи, запроваджені виключно банками, поліцією, телекомунікаційними компаніями або цифровими платформами, не можуть забезпечити суттєвого зниження ризику. Ефективна модель повинна охоплювати державний і приватний сектори, установлювати належний розподіл юридичних обов'язків, створювати механізми міжсекторального співробітництва, визначати зрозумілі цілі та забезпечувати чітке лідерство і підзвітність.

Основою запропонованої методології є системний підхід до проєктування політики. Автори зауважують, що в багатьох країнах механізми протидії шахрайству виникали як реакція на окремі кризові ситуації та спочатку розвивалися в межах певного сектору або платіжного каналу. Такий підхід може давати локальні результати, але без загальної архітектури призводить до труднощів із вимірюванням ефективності, обмеженого обміну інформацією, недостатнього охоплення ринку та слабкої участі окремих суб'єктів. Тому навіть тоді, коли держава має можливість упровадити лише один або декілька первинних заходів, вони повинні бути пов'язані із ширшими стратегічними цілями та проєктуватися таким чином, щоб у майбутньому їх можна було масштабувати, інтегрувати з іншими інструментами або адаптувати відповідно до зміни шахрайських методів.

Для побудови національної системи документ пропонує п'ять взаємопов'язаних напрямів політичного проєктування. Першим є встановлення реальної картини шахрайства, тобто визначення поширених схем, масштабів і характеру збитків, використовуваних платіжних каналів, найбільш уразливих категорій населення та установ, які вже здійснюють запобіжні або реактивні заходи. Другим напрямом є визначення політичного власника проблеми – державного органу, посадової особи або координаційного механізму, які матимуть достатній мандат для встановлення пріоритетів, залучення різних секторів і контролю за виконанням стратегії. Третій напрям передбачає формування чітких цілей політики, які можуть включати скорочення кількості потерпілих, зменшення фінансових втрат, прискорення блокування шахрайських платежів, підвищення рівня повернення активів, посилення кримінального переслідування та захист фінансової інклюзії. Четвертим напрямом є визначення сфери політики, тобто встановлення видів шахрайства, секторів, платіжних інструментів і категорій учасників, які мають бути охоплені насамперед. П'ятим є визначення партнерів, без яких реалізація заходів буде неможливою, з урахуванням того, хто володіє необхідними даними, технічними можливостями, правовими повноваженнями та безпосереднім доступом до відповідного етапу шахрайської схеми.

Послідовність реалізації цих напрямів не є жорстко встановленою. У деяких державах першочерговим завданням може бути визначення відповідального політичного органу, без якого неможливо забезпечити міжвідомчу співпрацю. В інших країнах спочатку необхідно сформувати доказову базу та переконливо продемонструвати масштаби проблеми, щоб одержати політичну підтримку і фінансування. Саме тому документ пропонується використовувати як діагностичну рамку, за допомогою якої можна встановити, які елементи системи вже існують, які функціонують лише частково, а які потребують створення. Автори рекомендують пов'язувати цілі протидії шахрайству з ширшими національними пріоритетами, такими як цифровізація, громадська безпека, фінансова інклюзія, довіра до державних установ і розвиток безготівкової економіки. Це допомагає забезпечити політичну підтримку, міжвідомче співробітництво та необхідні ресурси.

Особливе значення приділяється оцінюванню національного шахрайського середовища. Політика повинна спиратися на інформацію про види шахрайства, частоту їх учинення, демографічні характеристики потерпілих, розмір фінансових і нефінансових втрат, способи встановлення контакту зі споживачами та механізми переміщення коштів. Відповідні дані можуть уже міститися в національній оцінці ризиків ВК/ФТ, статистиці правоохоронних органів, матеріалах кримінальних проваджень, повідомленнях банків і платіжних установ, зверненнях до органів захисту споживачів, даних телекомунікаційних регуляторів, інформації цифрових платформ і дослідженнях громадських організацій. Проте такі дані часто збираються за різними методиками, не є взаємопорівнюваними та не дають повної картини

через низький рівень повідомлення про шахрайство. Потерпілі можуть не звертатися до компетентних органів через сором, страх осуду, недовіру до правоохоронної системи, незначний розмір індивідуального збитку або переконання, що повернення коштів є неможливим.

Якщо адміністративних даних недостатньо, автори рекомендують використовувати цільові дослідницькі методи. Одним із найбільш доступних способів є включення питань про шахрайство до національних опитувань щодо віктимізації. Це дає змогу оцінити фактичну поширеність шахрайства, включно з випадками, які не були офіційно зареєстровані, а також установити демографічні групи, що зазнають найбільшого ризику. Додатково можуть проводитися спеціальні опитування споживачів, фокус-групи, експертні панелі, консультації з приватним сектором та міжвідомчі семінари. Залучення правоохоронних органів, установ захисту споживачів, фінансових установ, телекомунікаційних компаній і громадських організацій дозволяє швидко сформувати початкове уявлення про загрози, вразливості та вже наявні механізми реагування навіть за відсутності масштабної статистичної системи.

Для аналізу ролей різних учасників документ застосовує модель ланцюга шахрайства, яка охоплює підготовку та створення інфраструктури, ініціювання контакту, виконання шахрайської схеми і виведення отриманих активів. Підготовчий етап включає створення технічної та фізичної інфраструктури, зокрема шахрайських центрів, SIM-ферм, підроблених вебсайтів, фальшивих профілів, баз персональних даних, рахунків підставних осіб та інструментів масової комунікації. На етапі ініціювання злочинці знаходять потенційних потерпілих, установлюють із ними контакт і формують довіру або відчуття терміновості. Це може здійснюватися через інвестиційні, романтичні, кредитні чи благодійні схеми, а також шляхом видавання себе за працівників банків, державних органів, поліції, відомих компаній або родичів потерпілої особи. На етапі виконання злочинець спонукає жертву здійснити переказ, передати персональні чи платіжні дані, зображення, документи або інші цінності. На завершальному етапі кошти переміщуються через мережу рахунків, оскільки вони рідко надходять безпосередньо на особистий рахунок організатора шахрайства. Для приховування походження, маршруту та кінцевого одержувача активів можуть використовуватися підставні особи, швидкі транзитні перекази, готівка, криптоактиви та транскордонні платіжні канали.

Такий підхід дає змогу визначити, які суб’єкти мають найбільші можливості для втручання на кожному етапі. Телекомунікаційні компанії можуть виявляти та блокувати підроблені номери, масові шахрайські повідомлення і SIM-ферми. Цифрові платформи можуть обмежувати фальшиві акаунти, шахрайську рекламу та посилання на підроблені вебресурси. Банки та платіжні установи можуть здійснювати моніторинг операцій, виявляти нетипову поведінку клієнта, перевіряти інформацію про одержувача, застосовувати затримку або додаткове підтвердження ризикових платежів, блокувати рахунки підставних осіб і передавати інформацію компетентним органам. Правоохоронні органи повинні забезпечувати розслідування, збирання доказів, міжнародну співпрацю та переслідування організаторів. Органи захисту споживачів і громадські організації можуть здійснювати інформування населення, збирати скарги та підтримувати потерпілих. Регулятори персональних даних, у свою чергу, повинні гарантувати, щоб обмін інформацією не призводив до непропорційного втручання у приватність або неправомірного використання даних.

Документ наголошує, що формальне визначення цілей і ролей учасників саме по собі не гарантує ефективності політики. Для її практичної реалізації необхідні належні законодавчі повноваження, інституційна спроможність, професійні кадри, технологічна інфраструктура, стимули для участі приватного сектору та антикорупційні механізми. Учасники повинні мати правові підстави для збирання, аналізу та передавання інформації, блокування рахунків, номерів, доменів або рекламних оголошень, а також для оперативного замороження і повернення коштів. Водночас навіть достатні повноваження не матимуть практичного значення, якщо органам бракує аналітичних систем, підготовлених працівників, фінансування або чітких процедур реагування. Приватні компанії також можуть не мати достатньої мотивації інвестувати у протидію шахрайству, якщо законодавство не встановлює

відповідальності за слабкі механізми контролю або якщо фінансові втрати повністю перекладаються на потерпілих чи інші сектори.

Координована система вимагає створення правових і технічних механізмів обміну інформацією, спільної таксономії та постійних зворотних зв'язків. Єдині визначення та класифікації необхідні для того, щоб банки, правоохоронні органи, телекомунікаційні компанії та цифрові платформи однаково розуміли основні види шахрайства, його етапи, використовувані інструменти та результати реагування. Без спільної таксономії показники різних установ не можна належним чином порівнювати, а оцінка загальної результативності політики стає ненадійною. Зворотний зв'язок повинен діяти на кількох рівнях: між державною політикою та окремими заходами, між учасниками одного заходу, між різними заходами, а також між споживачами та державними органами. Політика встановлює цілі та критерії успішності, а виконавці повинні повідомляти про результати, проблеми й необхідність коригування. Інформація, отримана в межах одного механізму, має використовуватися для підсилення інших: наприклад, дані з бази шахрайських рахунків можуть застосовуватися для платіжного моніторингу, блокування інфраструктури та правоохоронного розслідування.

Значна частина посібника присвячена п'ятнадцяти типам практичних заходів. Перший передбачає адаптацію правоохоронної та кримінально-правової відповіді до складності сучасного шахрайства, включно зі спеціалізацією підрозділів, удосконаленням процедур розслідування, міжнародним співробітництвом і роботою з цифровими доказами. Другий полягає у створенні закритих баз даних про шахрайські події, злочинців, підставних осіб, рахунки, номери телефонів, домени та інші інструменти. Третій спрямований на «усунення шахрайства через проєктування», тобто зміну фінансових продуктів, цифрових сервісів і бізнес-процесів таким чином, щоб зменшити можливості злочинців. Четвертий охоплює руйнування злочинної інфраструктури, наприклад блокування шахрайських центрів, SIM-ферм, вебсайтів, доменів, телефонних номерів і рекламних акаунтів. П'ятий спрямований на стимулювання громадян і підприємств повідомляти про спроби та випадки шахрайства. Шостий передбачає гармонізацію підходів до фінансових втрат, включно з правилами відповідальності та відшкодування. Сьомий полягає у використанні заходів ПВК, які вже застосовуються регульованими установами, для виявлення рахунків підставних осіб, відстеження коштів і подання повідомлень про підозрілі операції. Восьмий передбачає міжустановний моніторинг платіжних ризиків. Дев'ятий спрямований на проактивне виявлення та обмеження шахрайських каналів. Десятий передбачає надання клієнтові інформації про одержувача до завершення платежу. Одинадцятий полягає в оприлюдненні інформації про реєстраційний статус або попередні порушення суб'єктів, які пропонують фінансові продукти. Дванадцятий охоплює інформаційні кампанії щодо методів, масштабів і наслідків шахрайства. Тринадцятий передбачає встановлення стандартів виявлення шахрайства та реагування на інциденти на рівні окремих установ. Чотирнадцятий стосується підтримки потерпілих, а п'ятнадцятий – відстеження злочинних доходів і комунікацій шляхом багатосторонньої співпраці.

Кожен із цих заходів оцінюється за етапом шахрайського ланцюга, на який він спрямований, за його превентивною або реактивною природою, правовими та операційними передумовами, наявністю міжнародних стандартів, потенційною вартістю, необхідними учасниками й можливими небажаними наслідками. Автори застерігають, що поділ на превентивні й реактивні заходи не є абсолютним. Реагування на вже вчинене шахрайство може створювати інформацію, необхідну для подальшого запобігання, а підтримка потерпілих здатна знижувати ризик повторної віктимізації. Аналогічно, встановлення нових механізмів контролю може змусити злочинців перейти до інших платіжних каналів або методів. Таке переміщення ризику не обов'язково означає неефективність заходу, оскільки воно може свідчити про успішне ускладнення попереднього злочинного методу. Однак держава повинна постійно відстежувати ці зміни та своєчасно адаптувати систему.

Документ також підкреслює необхідність оцінювання ненавмисних наслідків. Посилені механізми моніторингу, блокування та обміну інформацією можуть створювати ризики

неправомірного використання персональних даних, помилкового блокування законних операцій, фінансового виключення окремих категорій клієнтів або надмірного обмеження доступу до цифрових послуг. Особливо вразливими можуть бути особи з нестабільними доходами, мігранти, люди похилого віку, мешканці віддалених регіонів і користувачі, які не мають достатньої цифрової грамотності. Тому ефективна політика повинна поєднувати безпеку з принципами пропорційності, захисту персональних даних, справедливого ставлення до клієнтів і збереження доступу до фінансових послуг. Окремо наголошується на необхідності антикорупційних запобіжників, оскільки витік інформації, сприяння злочинним мережам або зловживання повноваженнями можуть істотно знизити ефективність навіть добре спроєктованої системи.

Автори не рекомендують державам одночасно впроваджувати всі п'ятнадцять заходів. Пріоритетність повинна визначатися на основі ризиків, наявних повноважень, інституційної готовності та операційної доцільності. Для юрисдикцій із менш розвиненою цифровою або регуляторною інфраструктурою доцільно починати з тих механізмів, які можуть спиратися на вже наявні державні структури та потребують порівняно обмежених законодавчих змін. До таких заходів документ відносить посилення правоохоронної відповіді, руйнування злочинної інфраструктури, використання чинних заходів ПВК, інформаційні кампанії та підтримку потерпілих. Для розвитку обміну інформацією ключовими є створення закритих баз даних, міжустановний моніторинг платіжних ризиків і багатостороннє відстеження коштів. Для залучення телекомунікаційних компаній і цифрових платформ найбільш важливими є блокування шахрайських каналів, проактивне обмеження шахрайських інструментів, надання інформації про контрагентів, підвищення обізнаності та встановлення стандартів виявлення інцидентів.

Висновки:

- **Необхідно сформувати цілісну національну картину платіжного шахрайства** шляхом об'єднання даних державних органів, фінансових установ, телекомунікаційних операторів і цифрових платформ.
- **Потрібно визначити єдиний координаційний центр** та чітко розподілити обов'язки між усіма учасниками системи протидії шахрайству.
- **Необхідно впроваджувати заходи поетапно,** починаючи з наявних механізмів ПВК, посилення повідомлення про шахрайство, блокування злочинної інфраструктури та підтримки потерпілих.
- **Потрібно оцінювати результативність не лише за сумою збитків,** а й за швидкістю реагування, часткою повернутих коштів, якістю обміну даними та зниженням повторної віктимізації.

Загальний висновок документа полягає в тому, що ефективна протидія шахрайству з авторизованими платежами потребує переходу від набору ізольованих банківських, телекомунікаційних, цифрових і правоохоронних заходів до цілісної національної системи. Вона повинна охоплювати весь ланцюг шахрайства – від створення злочинної інфраструктури та встановлення контакту з потерпілим до переказу, переміщення, замороження і повернення активів. Результативність такої системи залежить не лише від формального ухвалення законів або кількості запроваджених інструментів, а насамперед від чітких цілей, політичного лідерства, належного розподілу відповідальності, спільної термінології, оперативного обміну інформацією, зворотного зв'язку, підтримки потерпілих і здатності учасників постійно адаптуватися до зміни злочинних методів. Саме системний, міжсекторальний і ризик-орієнтований підхід автори розглядають як основну передумову довгострокового зниження масштабів платіжного шахрайства та збереження довіри до цифрової фінансової системи.

Механізм перегляду Конвенції UNTOC: аналіз викликів та перспективи реформування [6]

У жовтні 2026 року держави-учасниці Конвенції ООН проти транснаціональної організованої злочинності (UNTOC) зберуться у Відні на тринадцяту сесію Конференції сторін, і цей захід відбувається в момент, коли понад чверть століття минуло з моменту ухвалення самої Конвенції.

Механізм перегляду, який було започатковано шість років тому, мав би за ідеальних умов завершити свою роботу через п'ять років, однак реальна ситуація є вкрай тривожною – цей механізм фактично паралізований через брак як фінансових ресурсів, так і політичної волі, і наразі видається малоймовірним, що він зможе виконати своє мандатне завдання. Найбільше занепокоєння викликає те, що відсутність прогресу в механізмі перегляду становить пряму загрозу самим цілям Конвенції та свідчить про тривожну втрату інтересу й підтримки з боку держав-учасниць, що ставить під сумнів майбутнє цього ключового міжнародного інструменту боротьби з організованою злочинністю.

Тринадцята сесія Конференції відбувається на тлі екзистенційних фінансових, ресурсних та політичних криз, що охопили Організацію Об'єднаних Націй загалом, однак ситуація з механізмом перегляду Конвенції є особливо загрозливою, якщо порівнювати поставлені завдання та цільові графіки з тим, що було реально досягнуто.

Протягом кількох років спостерігається очевидна відсутність прогресу в роботі механізму перегляду, що безпосередньо впливає на спроможність держав і дослідників оцінювати імплементацію основної мети Конвенції. Держави-члени вже не можуть ігнорувати той факт, наскільки механізм відстає від графіка та наскільки він позбавлений реального впливу. Встановлений графік передбачає низку дедлайнів, усі з яких будуть пропущені, якщо спиратися на робочий план, ухвалений державами в рамках резолюції 9/1. Цей план передбачав, що всі три групи країн, кожна з яких налічує приблизно 60 держав, мають провести перегляд усіх чотирьох кластерів Конвенції із запланованою датою завершення у 2031 році, однак реальність виявилася невблаганною.

Напередодні дванадцятої сесії Конференції сторін у 2024 році Глобальна ініціатива проти транснаціональної організованої злочинності вже представляла оновлену інформацію щодо прогресу механізму перегляду, і хоча з того часу було досягнуто певних незначних зрушень, загалом процес залишається надзвичайно далеким від графіка.

Найбільш промовистим свідченням цього є той факт, що лише чотири держави – Естонія, Ізраїль, Італія та Канада – завершили свої перегляди в межах кластеру криміналізації та юрисдикції. Оскільки для переходу до наступного кластеру необхідно, щоб 70 відсотків будь-якої групи держав-учасниць завершили свої перегляди, жодна група навіть приблизно не наблизилася до цього показника, і тому всі групи застрягли в першому кластері без жодних перспектив просування вперед у найближчому майбутньому. За таких темпів кластер міжнародного співробітництва, який є серцевиною Конвенції, не буде переглянуто протягом десятиліть або навіть століть, а фінальний кластер, присвячений запобіганню – тому, що необхідно для стримування поширення транснаціональних злочинів, – іронічно, буде розглянуто ще пізніше.

На основі поточних траєкторій можна змоделювати приблизні терміни завершення фаз перегляду, і ці розрахунки виглядають справді приголомшливо. Найгірший сценарій, що базується на темпах завершення переглядів за перші п'ять років, які становлять лише 2 відсотки, свідчить про те, що процес перегляду може тривати сімсот років, щоб досягти лише 70-відсоткового рівня завершення. Інший сценарій, заснований на переглядах, які вже перебувають на фінальній стадії, що становить 9 відсотків, вказує на те, що процес займе трохи більше 150 років. Навіть найоптимістичніший сценарій, який ґрунтується на переглядах, що

[6] https://globalinitiative.net/analysis/untoc-cop-review-mechanism-united-nations-vienna-2026/

перебувають на передостанньому етапі завершення, тобто 44 відсотки, все одно означатиме, що для досягнення 70-відсоткового рівня завершення в усіх кластерах знадобиться понад 30 років. Хоча ці розрахунки є грубими і точні терміни не піддаються прогнозуванню, головний висновок полягає в тому, що не існує жодного сценарію, за якого механізм перегляду завершить свою роботу хоч скільки-небудь близько до запланованих термінів, і за нинішньої моделі це неодмінно займе кілька поколінь.

Незважаючи на брак аналітичних даних із боку механізму, держави мають доступ до Збірника справ Управління ООН з наркотиків і злочинності, який містить приклади застосування Конвенції у питаннях міжнародного співробітництва, однак сам Збірник визнає, що не існує чіткої картини того, наскільки часто країни покладаються на Конвенцію при здійсненні транскордонної взаємодії.

Доповідь, підготовлена секретаріатом до тринадцятої сесії Конференції сторін, підтверджує цю прогалину, зазначаючи, що перегляд положень Конвенції про міжнародне співробітництво, який спочатку планувалося розпочати в листопаді 2022 року, було відкладено через те, що занадто мало країн завершили свої національні перегляди. У цьому ж документі ідентифікується брак послідовних даних щодо ефективності імплементації цих положень, низький рівень звітності з боку деяких регіонів та нагальна потреба у більш надійному способі збору інформації про те, як Конвенція підтримує міжнародну співпрацю у протидії організованій злочинності.

Якби механізм перегляду виконувався у запланованому темпі, міжнародна спільнота вже мала б доступ до десятків національних звітів із висновками та аналізом, підготовленим секретаріатом на основі цих матеріалів. Натомість, маючи лише чотири набори переглянутих спостережень і лише 18 добровільно опублікованих попередніх запитальників, в наявності є надзвичайно мало даних, на основі яких можна було б робити будь-які узагальнення щодо імплементації Конвенції.

Наслідком цього стало те, що складова механізму перегляду, яка передбачає повноцінну участь громадянського суспільства, так звані Конструктивні діалоги, нині проводиться без жодної доказової бази, отриманої в результаті процесу перегляду. Ці зустрічі перетворилися на загальні дискусії на теми, обрані відповідно до робочих груп, що працюють виключно на рівні держав-членів, які також проводять свої засідання, не маючи практично жодних результатів механізму перегляду для обговорення. Понад те, через брак фінансування Конструктивні діалоги тепер проводяться в онлайн-форматі, що суттєво знижує їхню цінність як форуму для залучення та взаємного обміну, і цей перехід до віртуального формату призвів до зниження інтересу з боку держав-членів та меншої взаємодії, попри стійку зацікавленість з боку громадянського суспільства.

Однак проблеми механізму перегляду є набагато глибшими, ніж брак фінансування та повільний темп, і GI-TOC наголошує на тому, що він страждає від серйозних конструктивних недоліків, які вже неможливо ігнорувати. Найбільш тривожним у цьому сценарії є те, що він означає для політичної відданості Конвенції загалом, оскільки організована злочинність нині значно тісніше пов'язана з державними елементами, ніж це було на момент ухвалення Конвенції, а отже, більше держав, ніж будь-коли раніше, мають чіткий інтерес уникати будь-якого контролю за тим, як вони застосовують Конвенцію на практиці.

Поряд із цим існують держави, які, здається, цілком комфортно почуваються із застійним станом Конвенції, або ж просто втратили до неї інтерес, і те, що необхідно зараз, – це не просто додаткове вливання ресурсів, але й нове політичне зобов'язання з боку тих, хто підтримує цілі Конвенції.

Погоджені державами «принципи та характеристики» механізму породили процес, який надає пріоритет праву держав самостійно оцінювати власну роботу, усуває незручні докази та замовчує те відкрите й чесне обговорення проблем, яке насправді необхідне для ефективної роботи. Водночас цей процес створив бюрократичну та надзвичайно тривалу процедуру без

жодних стимулів – таких як додаткові ресурси чи візити на місця – які б спонукали держав брати на себе зобов'язання, і без жодних санкцій за порушення графіків.

Ефективність самої Конвенції проти транснаціональної організованої злочинності, звісно, може бути предметом дискусій, однак беззаперечним є те, що провал її механізму перегляду позбавив міжнародну спільноту того самого інструменту, який мав слугувати для вимірювання дотримання Конвенції державами та якості її імплементації. Коли держави зберуться у жовтні на чергову сесію, настав час повернутися до первинних цілей Конвенції та переосмислити, яким має бути дієвий механізм перегляду, адже інакше під загрозою опиниться сама довіра до Конвенції, а не лише до її механізму перегляду.

Висновки:

- **Механізм перегляду UNTOC фактично паралізований –** лише 4 зі 192 держав-учасниць завершили повний цикл оцінки, через що перегляд кластеру міжнародного співробітництва, який мав розпочатися ще у 2022 році, відкладено на невизначений термін.
- **За поточних темпів завершення процесу неможливе –** навіть за оптимістичним сценарієм досягнення 70% охоплення займе понад 30 років, а за песимістичним – процес розтягнеться на століття.
- **Системні конструктивні недоліки механізму унеможливлюють об'єктивну оцінку** – держави самостійно «оцінюють власну роботу», відсутні санкції за пропуск дедлайнів, а громадянське суспільство та експертні дані майже не залучені до змістовної частини перевірок.
- **Криза механізму перегляду підриває легітимність усієї Конвенції –** брак даних про реальну імплементацію UNTOC позбавляє міжнародну спільноту інструменту для вимірювання ефективності боротьби з транснаціональною злочинністю та свідчить про втрату політичної волі держав.

Для досягнення ефективних результатів на тринадцятій сесії Конференції сторін необхідно вжити низку ключових заходів, серед яких передусім варто відзначити потребу в тому, щоб новий виконавчий директор Управління ООН з наркотиків і злочинності та секретаріат розробили стратегію створення політичного імпульсу на найвищому рівні для пожвавлення Конвенції, яка є центральною платформою ООН та основним мандатом у сфері боротьби з організованою злочинністю.

Це має бути доповнено конкретними варіантами реформування механізму перегляду з визнанням того факту, що нинішній формат не працює, і ці ідеї мають включати способи більш стратегічного використання ресурсів, виділених на поточний щорічний календар засідань, для підвищення рівня політичного інтересу. Вкрай важливо також домогтися зобов'язань від широкого кола держав-членів щодо поновлення їхньої відданості справі та конкретних дій, наприклад, шляхом формування групи прискореного перегляду, в межах якої держави проводили б взаємну оцінку одна одної.

Нарешті, секретаріату слід розглянути питання про те, як найкраще використовувати зовнішню інформацію, докази та зацікавлені сторони для заповнення прогалин у даних, що існують у поточному процесі, та зробити оновлену Конвенцію, яка отримає політичну підтримку, більш релевантною та відповідною до тих викликів, які їй належить долати.

Біткоїн-нативні фінанси: народження нової крипто-парадигми[7]

Біткоїн, як найбільший та найвпливовіший актив у криптовалютному просторі, завжди був наріжним каменем індустрії, проте його величезний потенціал залишався значною мірою нереалізованим.

[7] https://surl.li/qpsxzp

З ринковою капіталізацією, що перевищує 1,3 трильйона доларів, він являє собою найбільший пул капіталу, однак парадоксальним чином 99% цього багатства залишається пасивним, не приносячи жодного прибутку своїм власникам.

Протягом багатьох років власники біткоїнів мали вибір, який, по суті, зводився до двох неприйнятних варіантів, і більшість з них, керуючись здоровим глуздом, відмовлялися від обох. Перший шлях передбачав передачу контролю над своїми монетами стороннім платформам в обмін на обіцянку прибутку, але історія пам'ятає безліч крахів таких сервісів разом із коштами клієнтів, що зробило цей ризик абсолютно невиправданим. Другий варіант вимагав використання версій біткоїна на інших блокчейнах, що часто призводило до концентрації ризиків у єдиному кастодіані або неперевірених мостах, створюючи непрозору для звичайного користувача систему довіри.

Таким чином, перша хвиля біткоїн-децентралізованих фінансів (DeFi) зазнала невдачі не через відсутність попиту, а через те, що не змогла відповідати стандартам безпеки та прозорості, яких вимагають самі власники біткоїна. Наслідком цього стало значне скорочення капіталу в таких рішеннях, що виразилося у падінні заблокованої вартості (TVL) на біткоїн-сайдчейнах та рішеннях другого рівня на 74% до першого кварталу 2026 року.

На тлі цього розчарування та відтоку капіталу з альткоїнів спостерігається зовсім інша, більш значуща тенденція – консолідація капіталу навколо самого біткоїна. Інституційні інвестори через біржові фонди (ETF) лише підсилюють цей рух, а більшість альткоїнів з першої п'ятірки демонструють гірші показники порівняно з біткоїном. Індикатором цього домінування є стабільне утримання показника BTC Dominance на рівні 55-60% протягом 2026 року. Навіть корпоративний сектор демонструє зростаючу довіру до головної криптовалюти: публічні компанії сукупно володіють понад 1,16 мільйона біткоїнів, що становить більше 5% від загальної емісії, причому лише за перший квартал 2026 року корпоративні казначейства збільшили свої запаси на 62 000 BTC.

Аналітики називають цю зміну парадигми «Біткоїн-казначейство 2.0», де компанії переходять від простого утримання активу до його активного використання як робочого капіталу, прагнучи генерувати прибуток, не відмовляючись від прямого володіння. Саме цей зазор між величезною, але пасивною капітальною базою та активним попитом на її продуктивне використання створює умови для народження нової категорії – біткоїн-нативних фінансів, які, за прогнозами, визначать обличчя наступного ринкового циклу.

Цей новий напрямок дедалі чіткіше окреслюється як окрема ідентичність, і компанії вже починають структурувати свій бізнес навколо біткоїна як базового активу. Публічні компанії, як-от Nakamoto Inc., заявляють про свою місію у розвитку екосистеми біткоїн-нативних підприємств. Амбітний проєкт Twenty One Capital, створений за участі Tether та SoftBank, вимірює свій успіх у біткоїнах на акцію, а не у фіатному прибутку на акцію, володіючи понад 43 000 BTC. Навіть у стартап-середовищі з'являються проєкти, які позиціонують себе як біткоїн-нативні необанки, що будують споживчу фінансову інфраструктуру виключно на принципах самозберігання. Першим інституційним стейкхолдером на новому поприщі стає UTXO Management, що є ще одним

Висновки:

- **Капітал консолідується навколо біткоїна, але залишається пасивним.** Майже 99% ринкової капіталізації BTC не використовується, що створює величезний попит на безпечні інструменти для отримання прибутку без втрати контролю над активом.
- **Перша хвиля Bitcoin DeFi провалилася через ризики, а не через відсутність попиту**. Крах платформ та непрозорість мостів (bridges) змусили капітал відступити, але на зміну їм приходить категорія "біткоїн-нативних" рішень із пріоритетом на самозберігання та безпеку.
- **Чотири стовпи біткоїн-нативності – це безпека, довіра, зручність та BTC-номінація.** Справжні проєкти забезпечують розрахунки на рівні біткоїна, зберігають ключі у власника та виплачують прибуток виключно у BTC.

підтвердженням серйозності цього тренду з боку традиційних фінансових гравців. Це дозволяє сформулювати чітке визначення: біткоїн-нативні фінанси – це фінансова діяльність, прив'язана до біткоїна, захищена ним та номінована в ньому, навіть якщо операції виконуються на вищому рівні, ніж базовий блокчейн.

Для того, щоб відрізнити справді нативні рішення від тих, що лише використовують біткоїн, необхідно оцінювати їх за чотирма ключовими змінними. По-перше, це безпека: активність має розраховуватися безпосередньо на біткоїні та успадковувати його хеш-потужність, а не покладатися на окремий набір валідаторів. Другим критерієм є мінімізація довіри, де самозберігання є стандартом, а забезпечення активів має бути верифікованим. Третім аспектом виступає користувацький досвід, що має відповідати швидкості та вартості сучасних блокчейнів, а рух біткоїна має відбуватися нативно. І, нарешті, ключовою умовою є біткоїн-номінація, коли всі позиції та прибуток вимірюються у біткоїнах.

Подальший розвиток біткоїн-нативних фінансів передбачається трьома фазами, кожна з яких зміцнюватиме чотири ключові ознаки цієї категорії.

Таким чином, біткоїн-нативні фінанси постають не просто як черговий тренд, а як логічний та довгоочікуваний етап еволюції біткоїна з пасивного сховища вартості на активний, продуктивний та незалежний фінансовий інструмент.

Інші новини

Штраф FinCEN у 125 млн дол. США проти UBS Financial Services: невиконання попереднього припису як самостійний чинник визначення розміру санкції [8]

3 серпня 2026 року Мережа боротьби з фінансовими злочинами Міністерства фінансів США (FinCEN) видала Наказ за згодою № 2026-02, яким наклала цивільний грошовий штраф у розмірі 125 000 000 дол. США на UBS Financial Services Inc. (UBSFS) за умисні порушення Закону про банківську таємницю (Bank Secrecy Act, BSA). Це найбільша санкція, коли-небудь застосована до брокера-дилера за порушення BSA. UBSFS визнала виклад фактичних обставин і кваліфікацію порушень: нездатність запровадити та підтримувати програму протидії відмиванню коштів, що відповідає мінімальним вимогам BSA (31 U.S.C. § 5318(h), 31 C.F.R. §§ 1023.210, 1026.210), і несвоєчасне та неточне повідомлення про підозрілі операції (§ 5318(g), 31 C.F.R. §§ 1023.320, 1026.320). Юридично суттєвим є застереження самого наказу: «умисність» у цивільному провадженні за § 5321(a)(1) не потребує доведення наміру чи обізнаності про протиправність - достатньо необачної байдужості або свідомого нехтування.

Ключовою обставиною, що визначила розмір санкції, є рецидивність. У грудні 2018 року UBSFS уклала з FinCEN Наказ за згодою зі штрафом 14,5 млн дол. США за порушення, вчинені у 2004-квітні 2017 років, серед яких – неналежний моніторинг переказів в іноземній валюті через товарні та роздрібні брокерські рахунки внаслідок вад автоматизованої системи. Установа запевнила FinCEN, що запровадить нову систему автоматизованого моніторингу до середини 2019 року; фактично її розгорнуто лише в березні 2021 року, причому вже через кілька тижнів після укладення наказу 2018 року керівництву UBSFS і головному офісу UBS було відомо про неможливість дотримання строку. Про ці затримки FinCEN не було поінформовано. Як наслідок, понад 61 500 переказів в іноземній валюті сукупною вартістю понад 10,5 млрд дол. США залишалися поза належним моніторингом упродовж більш ніж чотирьох років.

Аналіз проміжного «ручного» контролю, на який установа покладалася з 2012 до 2021 року, є одним із найбільш методологічно змістовних фрагментів наказу. FinCEN виокремлює три

[8] FinCEN Assesses Historic $125 Million Penalty Against UBS Financial Services Inc. for Recidivist BSA Violations | FinCEN.gov

вади, що робили контроль непридатним для мети: звіт будувався лише на трьох параметрах і не був пристосований до ризиків клієнтської бази; процес його формування був ненадійним (дванадцять кроків ручних запитів до чотирьох систем із подальшим копіюванням даних до файла Excel, причому в одному з прогонів майже половина записів не містила дійсного номера рахунку); періодичність – щоквартальна або й рідша, що унеможливлювало своєчасне виявлення підозрілої діяльності (у 2019 році весь масив операцій було охоплено фактично двома прогонами замість чотирьох). Окремо задокументовано дефект коду, через який упродовж близько двох років систематично занижувалася вартість валютних переказів для цілей порогового параметра (еквівалент 300 тис. дол. США на домогосподарство за місяць); персонал, який виявив проблему наприкінці 2020 року, не ескалював її та не з'ясував обсяг пропущених операцій. Внутрішній зворотний перегляд, розпочатий у грудні 2020 року, не завершився поданням жодного повідомлення про підозрілу операцію, попри наявність у масиві операцій венесуельської фінансової установи, клієнта, бенефіціарного власника якого перебував під розслідуванням щодо відмивання коштів, та клієнта з ознаками транзитної діяльності.

Не менш показовим є опис вад упровадження нової автоматизованої системи. Установа обрала неповний канал даних замість повного (end-of-day), унаслідок чого, за оцінкою на місячній вибірці, понад 5 % валютних переказів взагалі не потрапляли до системи моніторингу, а ще близько 12 % надходили без відомостей про контрагента. Логіка зіставлення даних про контрагента з операцією не мала унікального ідентифікатора і давала збої через елементарне округлення обмінного курсу. У сховищі даних не було передбачено черги винятків або механізму звітування про помилки, тобто система структурно не могла повідомити про те, що операція не була оброблена. Кореневою причиною FinCEN визнає неприкладення політик управління даними до процесу транзакційного моніторингу: цілісну систему управління даними впроваджено лише у квітні 2023 року, повне відображення й тестування походження даних не проводилося, а щомісячні звіти моніторингу продуктивності моделі не виявили жодної проблеми. Внутрішній аудит групи у звіті 2020 року помилково констатував наявність адекватних компенсаційних контролів.

Другий блок порушень стосується належної перевірки клієнтів. FinCEN наводить конкретні приклади, які ілюструють не поодинокі помилки, а системну ваду процесу. Клієнту, чий консалтинговий дохід був пов'язаний із проєктом підсанкційного російського олігарха, присвоєно низький рівень ризику, що виключило посилену перевірку; зв'язок виявлено лише напередодні висунення цій особі обвинувачення в порушенні санкційного законодавства. Інший клієнт у 2013 році змінив місце проживання на російську федерацію та обійняв керівну посаду в технічному університеті, пов'язаному з підсанкційною особою, однак понад вісім років його профіль не оновлювався попри численні індикатори – додавання російського телефонного номера, доступ до онлайн-сервісів з території рф, надходження понад 2 млн дол. США з рахунку в російській філії, – а два згенеровані алерти було закрито без розслідування. У випадку кіпрської персональної інвестиційної компанії установа встановила, що її бенефіціарний власник є братом російського олігарха, підозрюваного, за виявленими самою установою публікаціями, у відмиванні мільярдів доларів, а джерелом статків клієнта є заробіток у компанії, віднесеній внутрішніми політиками UBSFS до категорії «небажаних ділових відносин», і подарунок у 40 млн дол. США; зв'язки з мережею Troika Laundromat зафіксовано, але не враховано під час оцінки ризику, а внутрішній меморандум підсумував, що «формальних негативних новин немає».

Найбільш ілюстративним є випадок клієнтів, бенефіціарним власником яких є російський олігарх із широко описаними зв'язками з керівництвом рф. Скринінг негативних новин під час встановлення відносин дав тисячі збігів у понад 300 публікаціях, а періодичний перегляд – понад 150 статей, з яких було переглянуто лише перші двадцять п'ять. Критику щодо походження статків від програми «позики в обмін на акції» установа відхилила формулюванням про «лише припущення» за відсутності судових проваджень; повідомлення про причетність до схеми відмивання за участю професійного спортивного клубу та осіб зі

списку SDN відхилено на підставі оцінки самого фінансового радника, який рекомендував «взагалі не зважати» на ці публікації. Статус політично значущої особи не визнано попри власні знахідки про близькі відносини з політичним керівництвом. Запроваджені для цих рахунків обмеження щодо переказів на користь третіх осіб на практиці не виконувалися: близько трьох чвертей від понад 60 млн дол. США вихідних переказів були саме такими, зокрема на адресу підконтрольного тому самому власникові постачальника послуг, пов'язаних з віртуальними активами. Окремим сюжетом є синдикатна схема: через кілька відділень було відкрито понад 40 рахунків для десятків фіктивних компаній, що приховували фінансування третіх осіб задля максимізації часток у синдикованих розміщеннях і первинних публічних пропозиціях; схема діяла понад десять років і виявлена лише після регуляторного запиту.

Структура фінансової санкції заслуговує на окрему увагу як інструмент регуляторної політики. Із 125 млн дол. США FinCEN зараховує 48 млн дол. паралельних виплат – 20 млн дол. FINRA, 20 млн дол. Комісії з цінних паперів і бірж та 8 млн дол. Комісії з торгівлі товарними ф'ючерсами. До Міністерства фінансів США підлягає сплаті 62 млн дол.; решта 15 млн дол. – до 31 травня 2028 року, причому ця сума може бути списана в межах «кваліфікованих витрат», фактично понесених на незалежний огляд програми ПВК/ФТ і впровадження рекомендацій. До витрат, що зараховуються, прямо не належать видатки, які установа понесла б у звичайному режимі підтримання програми, включно з незалежним тестуванням. Зобов'язання за наказом охоплюють зворотний перегляд повідомлень про підозрілі операції силами незалежного консультанта (звіт – упродовж 180 днів, подання повідомлень – упродовж 90 днів після звіту з правом одного 60-денного продовження) та незалежний огляд програми ПВК/ФТ, сфокусований на пріоритетних ризиках незаконних фінансів: південно-західний кордон США й картелі, Іран, росія, Венесуела.

Для української системи ПВК/ФТ/ФР справа має щонайменше три прикладні виміри. По-перше, вона підтверджує, що якість і повнота даних, які надходять до систем автоматизованого моніторингу, є самостійним предметом наглядової оцінки: правильно налаштовані сценарії не мають значення, якщо частина операцій до системи не потрапляє, а механізму виявлення таких пропусків не передбачено. По-друге, наказ дає розгорнутий каталог неприйнятних практик належної перевірки – формальне закриття негативних новин без аналізу, покладання на висновок особи, зацікавленої в утриманні клієнта, невизнання статусу політично значущої особи попри власні знахідки, невиконання встановлених обмежень за рахунком, – які повністю відтворювані в українському контексті обслуговування клієнтів з високоризикових юрисдикцій.

Кібератака на Реєстр бенефіціарних власників Ліхтенштейну: скопійовано дані приблизно 31 000 правових утворень [9]

У ніч на 30 липня 2026 року невстановлені особи отримали протиправний цифровий доступ до Реєстру бенефіціарних власників (Verzeichnis wirtschaftlich berechtigter Personen, VwbP), який веде Управління юстиції Князівства Ліхтенштейн. Про інцидент повідомлено 2 серпня 2026 року на терміново скликаній пресконференції у Вадуці за участю глави уряду Бріґітте Гаас, урядового радника Емануеля Шедлера та керівника Управління юстиції Мартіна Альґе. Скопійовано дані приблизно 31 000 правових утворень – товариств, фондів і трастових компаній. За поясненням Управління юстиції, викрадений масив охоплює персональні дані бенефіціарних власників, їхнє громадянство та країну проживання, тобто відомості, які за законом мають залишатися конфіденційними в розпорядженні органів влади.

Хронологія реагування така: неправомірний доступ стався в ніч на 30 липня, упродовж того самого дня в Управлінні юстиції виявлено відхилення в роботі системи, після аналізу з боку Управління інформатики вжито заходів із забезпечення збереження даних, а уражену систему

[9] https://www.srf.ch/news/international/hackerangriff-cyberangriff-auf-wirtschaftsdaten-im-fuerstentum-liechtenstein

відключено від мережі. Кризовий штаб створено ввечері 1 серпня та формально затверджено 2 серпня. Станом на момент оприлюднення вимог викупу не надходило, масив не з'являвся в даркнеті й не пропонувався до продажу, ознак зміни чи видалення даних у самій системі не виявлено. Реєстр тимчасово недоступний в інтернеті; запроваджено централізований інформаційний пункт для потерпілих осіб, оскільки орган зобов'язаний повідомити їх про порушення захисту персональних даних.

Правовий контекст надає інциденту системного значення. VwbP ведеться на підставі спеціального закону (VwbPG), яким імплементовано вимоги директив ЄС у сфері запобігання відмиванню коштів, і саме через онлайн-портал цього реєстру правові утворення зобов'язані вносити відомості про своїх бенефіціарних власників. Отже, скомпрометовано не допоміжну базу даних, а центральний елемент інфраструктури прозорості, створений на виконання наднаціональних зобов'язань у сфері ПВК/ФТ. Одночасно з реєстром у профілактичних цілях було виведено в офлайн і низку інших централізованих фінансово-адміністративних систем, що ілюструє ступінь взаємопов'язаності державних реєстрів.

Ширший висновок стосується всіх юрисдикцій, що розбудовують або централізують реєстри бенефіціарної власності. Після рішення Суду ЄС у об'єднаних справах C-37/20 і C-601/20 (листопад 2022 року) публічний доступ до таких реєстрів було обмежено з мотивів пропорційності втручання у право на приватність, і центральним контраргументом прихильників відкритості залишалася теза про мінімальний практичний ризик для суб'єктів даних. Ліхтенштейнський інцидент показує, що ризик концентрації чутливих відомостей реалізується не через режим доступу, а через кіберстійкість самої інфраструктури. Для України, де відомості про кінцевих бенефіціарних власників зберігаються в Єдиному державному реєстрі юридичних осіб, фізичних осіб – підприємців та громадських формувань, це ставить питання захисту реєстрової інфраструктури в один ряд із питаннями повноти й достовірності самих даних.

Від Тегерана до Техасу: Як «золотий паспорт» перетворив засудженого шахрая на визнаного кінорежисера [10]

Історія Маз'яра Махана, людини, яка зуміла перетворити кримінальне минуле на голлівудську мрію, є яскравим прикладом вразливості глобальної імміграційної системи, особливо її «золотих» сегментів, призначених для заможних інвесторів.

Розслідування, проведене OCCRP, відкриває завісу над неймовірною трансформацією, яка видається малоймовірною для пересічного громадянина: від засудженого за шахрайство втікача з Ірану до визнаного режисера та викладача в Техаському університеті, чиї фільми отримують нагороди на міжнародних фестивалях.

В Ірані Махан відомий під своїм оригінальним прізвищем Махтавіфар. У 2009 році він залишив країну, залишивши по собі зруйновані долі сотень співгромадян, які інвестували свої заощадження у фінансову піраміду під назвою Palinure. Ця схема, замаскована під витончений інвестиційний фонд, що нібито працював з золотом та цінними паперами, обіцяла неймовірні прибутки – до 25 відсотків щомісяця, що на тлі економічних труднощів Ірану, обтяженого санкціями та інфляцією, звучало як справжній порятунок.

Шахраї вміло створили ілюзію легітимності: вони демонстрували потенційним інвесторам професійно розроблений вебсайт, на якому стверджувалося, що компанія зареєстрована в Сполучених Штатах, проводили пишні семінари в Дубаї та Таїланді, де виступали навіть запрошені американські мотиваційні спікери, такі як Ренді Гейдж, який отримав за свій виступ

[10] https://www.occrp.org/en/investigation/from-tehran-to-texas-how-a-convicted-iranian-pyramid-scheme-ringleader-built-a-new-life-in-the-us

близько 25-30 тисяч доларів. Усе це створювало враження надійності та глобального масштабу.

Жертвами стали переважно прості люди, які не мали спеціальних фінансових знань: фермери, державні службовці, домогосподарки, викладачі університетів, які несли свої заощадження в офіси компанії готівкою або через банківські перекази.

Згідно з остаточним вироком іранського суду, загальний дохід від шахрайської діяльності Palinure перевищив 25 мільйонів доларів США, причому «значна частина» цих коштів була виведена за кордон. У 2016 році суд заочно засудив Махана (тоді ще Махдавіфара) до трьох років ув'язнення, а також наклав на нього мільйонні штрафи на користь постраждалих та іранської держави. Ще один спільник Махана, а також подружжя, яке управляло активами компанії та придбало понад 1700 золотих монет на суму приблизно 2,5 мільйона доларів, були засуджені до смертної кари, яку згодом замінили на 20 років позбавлення волі.

За іронією долі, у 2009 році п'ятеро постраждалих самі опинилися на лаві підсудних за звинуваченням у викраденні Махана: вони зустрілися з ним, щоб запитати про свої гроші, і, за версією слідства, утримували його проти його волі. Цей епізод яскраво демонструє, наскільки розпачливим було становище жертв, які вже тоді, в 2009 році, намагалися повернути свої кошти будь-якими методами, але зрештою лише самі ледь не стали злочинцями через дії шахрая.

Незважаючи на очевидні докази та вирок іранського суду, юридичні представники Махана в Сполучених Штатах, фірма Brandy Austin, категорично заперечують будь-яку провину свого клієнта. Вони стверджують, що весь цей процес є частиною скоординованої кампанії іранського режиму з дискредитації політичних дисидентів, і що Махан «ніколи не засновував» компанію Palinure та не був причетним до «жодної шахрайської фінансової діяльності». Адвокати наголошують, що Махан, на їхнє переконання, «ніколи не отримував вироку від іранського суду» під час свого проживання в Ірані, і що він залишив країну майже два десятиліття тому.

Вони представляють його винятково як видатного вченого, режисера та автора, чия творчість активно виступає проти репресивного режиму в Тегерані, особливо проти придушення прав жінок. Однак розслідування OCCRP не знайшло жодних публічних записів чи доказів того, що Махан був відвертим критиком іранського уряду до свого від'їзду до Сполучених Штатів. Його політична активність, як видається, розпочалася вже після того, як він отримав притулок на Заході, що може свідчити про прагматичне використання політичного дискурсу для зміцнення свого статусу біженця та створення позитивного іміджу, необхідного для успішної інтеграції в американське академічне та культурне середовище.

Ключовим елементом феноменальної втечі Махана стало отримання ним паспорта громадянина Домініки в 2014 році. Цей документ, придбаний за програмою так званого «золотого паспорта» (Citizenship by Investment), коштував приблизно 100 000 доларів США, що на той час було стандартною ціною для індивідуального заявника. Разом із дружиною, яка також була фігуранткою справи (хоча згодом її виправдали), Махан став громадянином маленької карибської острівної держави.

Цей крок фактично перетворив іранського втікача, за яким полювала його власна країна, на людину з новою юридичною ідентичністю, що відкрило перед ним двері для безперешкодних подорожей та легалізації в інших країнах.

Озброєний новим паспортом, Махан зробив наступний і, мабуть, найважливіший крок до своєї американської мрії. Ще у 2010 році він здійснив значну інвестицію в розмірі 500 000 доларів США у будівництво комерційної нерухомості Home Plate Center у Сіетлі, штат Вашингтон. Цей проєкт, що розташовувався поруч із бейсбольним стадіоном T-Mobile Park, розвивала компанія American Life, яка спеціалізується на допомозі іноземцям у отриманні імміграційних віз через інвестиції. Внесок Махана ідеально вписувався в умови державної програми EB-5,

яка надає посвідку на постійне проживання (зелену карту) іноземцям, що вкладають значні кошти в економіку США та створюють робочі місця для американців.

Таким чином, Махан отримав легальну можливість жити в Каліфорнії, де він розпочав своє академічне та культурне сходження. У 2017 році він отримав ступінь молодшого спеціаліста з журналістики в коледжі Санта-Моніки, а згодом вступив до магістратури з кінознавства в престижному університеті Чепмена в Оранджі, який у 2019 році закінчив із магістерським дипломом. Згодом він вступив до докторантури Техаського університету в Далласі, де працював викладачем-асистентом, готуючи нове покоління американських кіномитців.

Кінематографічний дебют Махана, фільм «Exile Echoes», що вийшов у 2025 році, став його найуспішнішим проєктом, отримавши нагороди на багатьох міжнародних фестивалях. Стрічка розповідає історії іранських жінок, які рятуються від репресій поліції моралі. Адвокати Махана використовують його творчість як доказ його політичної позиції, стверджуючи, що звинувачення в шахрайстві є лише помстою іранського режиму за його мистецьку та правозахисну діяльність.

Однак жертви Palinure в Ірані бачать в цьому лише цинічну гру, яка дозволяє злочинцю не лише уникнути покарання, а й отримати славу та визнання за рахунок тем, які резонують із західною аудиторією. Вони зазначають, що до свого від'їзду з Ірану Махан ніколи не виявляв політичної активності, а його опозиційність стала зручним інструментом для отримання притулку та побудови нової кар'єри на Заході.

Реєстри власності підтверджують, що в червні 2021 року Махан та його дружина придбали одноповерховий будинок у передмісті Далласа за 336 000 доларів США, використовуючи іпотечний кредит. На праві власності вже фігурувало нове прізвище Махан, так само як і нове прізвище його дружини, що остаточно юридично закріпило їхню нову ідентичність. Вже у 2024 році подружжя було внесене до списків виборців Техасу, що є беззаперечним доказом отримання ними американського громадянства.

Однак залишається незрозумілим, як перевірки не виявили факту засудження Махана в Ірані, адже заявка на натуралізацію в США вимагає розкриття всіх попередніх судимостей, звинувачень та вироків. Можна припустити, що відсутність міжнародного ордера на арешт від Інтерполу (якщо він не був виданий через політичний характер справи) або недостатній обмін інформацією дозволили Махану уникнути уваги імміграційних служб.

Ця історія піднімає незручні та фундаментальні питання про те, наскільки легко люди зі злочинним минулим можуть скористатися прогалинами в системі глобальної імміграції та міжнародного правосуддя. Справа демонструє, як тонко можна балансувати між статусом політичного біженця та фінансового злочинця, використовуючи один ярлик для маскування іншого. Адвокати Махана наполягають на його невинуватості та політичному переслідуванні, і хоча іранська судова система справді має репутацію репресивної та несправедливої, особливо щодо політичних опонентів, факти, викладені в розслідуванні OCCRP, є надто численними та послідовними, щоб їх можна було просто відкинути. Вирок суду, свідчення десятків постраждалих, детальні описи роботи схеми, включно з виплатами та залученням нових учасників, а також сам ланцюжок переміщень вимальовують картину, яка суперечить образу невинного дисидента, що постраждав за свої переконання.

Як дієтичні препарати перетворилися на зброю злочинних синдикатів [11]

Останнім часом на тлі глобального попиту на препарати для схуднення, світ став свідком неочікуваного, але дуже показового феномену, який розгорнувся на стику кордонів Парагваю, Бразилії та Аргентини.

[11] https://www.occrp.org/en/feature/slim-shady-smugglers-eye-big-profits-running-weight-loss-drugs-into-brazil

Мова йде про стрімке перетворення ліків на основі тирзепатиду, відомих під брендом Mounjaro, на надприбутковий товар для транснаціональних злочинних синдикатів. Як свідчать дані, оприлюднені в розслідуванні OCCRP та бразильського видання Revista piaui, ця речовина, що початково розроблялася для лікування діабету другого типу, стала сучасним "чорним золотом", яке перекроює логістику й методи роботи організованої злочинності в регіоні Ла-Плати.

На перший погляд, ситуація виглядає як класичний арбітраж, породжений різницею в регуляторних політиках двох сусідніх країн. У Парагваї виробництво тирзепатиду є легальним, а вартість тижневої дози на внутрішньому ринку становить близько 40 доларів США. Це створює вигідне підґрунтя для виробництва та реалізації препарату, адже фармацевтична індустрія в країні активно нарощує оберти – кількість зареєстрованих аптек в департаменті Альто-Парана зросла з півтори тисячі у 2024 році до трьох тисяч у 2026-му.

Однак сусідня Бразилія, яка потерпає від епідемії ожиріння (згідно з даними Всесвітньої організації здоров'я, кожен четвертий дорослий бразилець має цей діагноз, і ця цифра продовжує зростати), запровадила жорсткі обмеження на обіг цього препарату. На території Бразилії дозволено продаж виключно оригінального Mounjaro американської компанії Eli Lilly, вартість якого майже в сім разів вища за парагвайський еквівалент і сягає 278 доларів за тижневу дозу. Всі інші форми ввезення заборонені законом, але саме ця заборона стала каталізатором для створення величезного чорного ринку.

За даними бразильської митної служби, вже за перше півріччя 2026 року обсяги вилучених флаконів тирзепатиду перевищили показники всього 2025 року більш ніж у десять разів, а аналітики банку Itaú BBA оцінюють річні доходи тіньового ринку на рівні 485 мільйонів доларів. Такі цифри не могли залишитися поза увагою кримінальних угруповань, які історично контролюють контрабанду цигарок, зброї та наркотиків у цьому прикордонному трикутнику.

Специфіка географії та недостатній контроль на кордонах створюють ідеальне середовище для розквіту цієї торгівлі. Щодня міст Дружби (Puente de Amistad), що сполучає парагвайське Сьюдад-дель-Есте з бразильським Фос-ду-Ігуасу, перетинають понад сто тисяч людей. Офіцери бразильської федеральної податкової служби зізнаються, що через надзвичайну завантаженість вони фізично спроможні перевірити лише 1-5% від загального потоку людей і транспорту. Це створює умови для функціонування так званих "мурашиних мереж" (ant networks), де оптові продавці наймають дрібних кур'єрів для переправлення забороненого вантажу.

Ампули та картриджі з діючою речовиною перевозять, прикріпивши до тіла, ховають в автомобілях, мотоциклах, косметиці чи навіть харчових продуктах. Потрапляючи до Бразилії, ці дороговартісні вантажі часто транспортуються з порушенням температурного режиму – в неохолоджуваних вантажівках, що не лише знижує ефективність, але й піддає ризику здоров'я кінцевих споживачів, які часто навіть не підозрюють про умови зберігання придбаного препарату.

Однак найбільш тривожним аспектом цього феномену є те, що торгівля тирзепатидом переросла з дрібної контрабанди в повномасштабну кримінальну індустрію з використанням важкого озброєння та спецоперацій, подібних до пограбувань інкасаторських машин чи банків. За словами представника Національної поліції Парагваю, протягом 2026 року на автомагістралях, що ведуть до бразильського кордону, фіксується в середньому майже одне велике пограбування вантажівок із тирзепатидом на тиждень, не рахуючи численних дрібних крадіжок з аптек. Ці напади відзначаються надзвичайною жорстокістю – зловмисники використовують автоматичну зброю та великокаліберні гвинтівки.

Правоохоронці Парагваю не виключають, що до організації цих пограбувань причетні найвпливовіші бразильські угруповання, зокрема "Перше столичне командування" (PCC) та "Червоне командування" (Comando Vermelho). Це вказує на те, що фармацевтичний ринок стає новим напрямком диверсифікації діяльності для злочинних синдикатів, які раніше

спеціалізувалися виключно на наркотрафіку та торгівлі зброєю. Парагвайський прокурор Італіко Рієнці назвав фармацевтичні препарати "новим чорним золотом" для угруповань, адже рівень доходів і простори для маневру тут не менш привабливі, ніж у традиційному наркобізнесі.

Варто відзначити, що проблему посилює ще й поява підроблених препаратів на цьому ж ринку. У липні 2026 року парагвайська поліція вилучила чотири тисячі флаконів, які нібито виготовляла місцева компанія Indufar. Однак при детальному дослідженні виявилося, що всередині пляшечок знаходився лише фізіологічний розчин. Такий фальсифікат не лише завдає фінансових збитків пацієнтам, але й становить смертельну небезпеку для тих, хто покладається на ці ліки для контролю рівня цукру в крові чи зниження ваги. Крім того, у поле зору поліції потрапляють і китайські аналоги препарату, за складом майже ідентичні до парагвайської продукції, що свідчить про глобалізацію цього підпільного ринку.

У відповідь на зростання загрози парагвайське Національне управління санітарного нагляду запровадило систему відстеження, яка передбачає присвоєння унікального коду кожній упаковці препарату для посилення контролю за обігом. Місцеві фармацевтичні асоціації закликають владу вжити більш рішучих заходів, адже власники аптек живуть у постійному страху через хвилю пограбувань. Утім, журналістське розслідування показало, що навіть у великих мережевих аптеках Сьюдад-дель-Есте співробітники відкрито пропонують послуги кур'єрів-контрабандистів, які доставляють замовлення до будь-якої точки Бразилії. Тобто системний характер цього явища вже не викликає жодних сумнівів.

Таким чином, історія з тирзепатидом є яскравим прикладом того, як регуляторні прогалини та жадоба до надприбутків можуть перетворити звичайні ліки на двигун злочинної економіки. Доки уряд Бразилії намагається обмежити ввезення препарату для захисту інтересів великих фармацевтичних корпорацій, а Парагвай не може ефективно контролювати власний виробничий ланцюг і точки продажу, організована злочинність перехоплює ініціативу.

Ситуація погіршується через щоденний величезний потік людей через кордон та обмежені ресурси правоохоронців, які можуть перевіряти мізерну частку трафіку. Як наслідок, насильство, пов'язане з перевезенням цих медикаментів, зростає, а якість препаратів, які потрапляють до кінцевих споживачів у Бразилії, залишається небезпечно непрогнозованою.

Можна стверджувати, що у цьому регіоні сформувалася нова модель злочинного бізнесу, де фармацевтичний сектор поступово витісняє традиційну контрабанду за рівнем прибутковості та впливу на криміногенну ситуацію, і для стримування цієї загрози потрібні вже не локальні поліцейські операції, а масштабна реформа прикордонного та митного контролю, а також гармонізація законодавств обох країн.

Імітація довіри: нова хвиля шахрайства загрожує інвесторам [12]

Канадська адміністрація цінних паперів (Canadian Securities Administrators, CSA) оприлюднила попередження, яке стосується зростаючої кількості шахрайських схем, що використовують ім'я та репутацію відомого швейцарського приватного банку Union Bancaire Privée (UBP).

Цей випадок є класичним прикладом того, як зловмисники експлуатують довіру до усталених фінансових інституцій, щоб виманювати кошти в осіб, які вже постраждали від попередніх інвестиційних афер, зокрема у сфері криптовалют. Ситуація набуває особливого резонансу, оскільки вона демонструє еволюцію шахрайських методів у бік більшої витонченості, психологічної глибини та використання багатошарових схем, які важко розпізнати навіть досвідченим учасникам ринку.

[12] https://www.securities-administrators.ca/news/investor-alert-fraudsters-impersonate-union-bancaire-privee-ubp-sa-to-target-canadian-investors/

Суть шахрайства полягає у витонченій багатоступеневій схемі, яка вражає своєю продуманістю. Як зазначається у звіті CSA, жертвами стають переважно ті інвестори, які раніше втратили свої заощадження через нелегальні крипто-платформи. Серед таких платформ, на які вже були випущені окремі попередження, Plusinvesting, Spotrade, CenexPro та Altercoin. Ці платформи, як правило, діяли без будь-якої реєстрації або ліцензування, заманюючи інвесторів обіцянками надприбутків на ринку цифрових активів, який і без того є високоризикованим. Коли жертви втрачали свої гроші через технічні збої, неможливість вивести кошти або відверте шахрайство з боку цих платформ, вони залишалися у стані розпачу та фінансової невизначеності. Саме у цей момент на сцену виходять нові зловмисники, які, володіючи, ймовірно, базами даних постраждалих, цілеспрямовано атакують їхню вразливість.

Шахраї, знаючи про вразливе становище цих людей та їхнє бажання повернути втрачене, вступають з ними в контакт, часто у позаплановий спосіб – електронною поштою, телефоном або навіть через месенджери. Вони повідомляють обнадійливу новину: їхні кошти не зникли безвісти, а тимчасово заблоковані на рахунках у престижному банку, такому як UBP. Ця версія звучить особливо правдоподібно через те, що швейцарські банки мають репутацію надійних сховищ капіталу, а сам факт "блокування" коштів нібито через юридичні або регуляторні процедури виглядає переконливо для недосвідченого інвестора. Більше того, зловмисники часто створюють цілу історію про те, що вони є спеціальними агентами або юристами, які ведуть цю справу, додаючи додатковий шар офіційності та терміновості.

Для надання своїм словам ваги та правдоподібності зловмисники вдаються до підробки офіційних документів. Інвесторам надсилаються виписки з рахунків, підтвердження переказів або платіжні повідомлення, які візуально майже не відрізняються від справжніх. Ці документи містять логотипи, бланки, печатки та інші фірмові елементи банку UBP, що створює ілюзію повної легітимності.

Цей підхід будується на довірі: людина, яка вже втратила гроші, хапається за будь-яку можливість, і авторитет всесвітньо відомого банку стає ідеальним інструментом для маніпуляції. Психологічний аспект цієї схеми не можна недооцінювати. Жертви, які пережили фінансову травму, часто перебувають у стані когнітивного дисонансу – вони не хочуть визнавати, що втратили все остаточно, тому будь-яка нитка, що веде до повернення грошей, сприймається як рятівне коло. Шахраї майстерно грають на цих емоціях, використовуючи професійну термінологію, створюючи відчуття ексклюзивної можливості та постійно підкріплюючи думку, що діяти треба негайно, інакше рахунки будуть "заморожені назавжди" або гроші передані державі.

Кульмінацією шахрайства є вимога сплатити так звані комісії за "звільнення" або "обробку" коштів. Жертві пояснюють, що для того, щоб отримати доступ до своїх нібито врятованих активів, необхідно внести невелику (відносно загальної суми) передоплату за юридичні чи адміністративні послуги. Суми можуть варіюватися від декількох сотень до тисяч доларів, залежно від передбачуваного розміру втрат. Вони можуть надсилати рахунки-фактури, договори про надання послуг та інші юридично оформлені документи, створюючи повну ілюзію законності операції. Однак, як підкреслює CSA, це пастка.

Після того, як гроші за "комісію" переказані, зв'язок із шахраями, як правило, припиняється, або ж вони вигадують нові приводи для подальших зборів, продовжуючи висмоктувати з жертви кошти, доки та не усвідомлює обману. У деяких випадках постраждалі повідомляли, що їм телефонували повторно, представляючись вже іншими особами – нібито керівниками вищого рівня або представниками регуляторних органів, – які вимагали додаткових платежів для "розблокування" або "страхування" транзакції. Таким чином, загальна сума втрат може значно перевищувати первісну комісію, і жертва опиняється у ситуації, коли вона втратила не лише свої первинні інвестиції, але й додаткові кошти, які намагалася витратити на їхнє повернення.

Цей випадок є яскравим нагадуванням про те, що фінансовий світ стає дедалі більш витонченим. Особливу тривогу викликає той факт, що шахраї використовують бренд не просто якоїсь випадкової компанії, а одного з найстаріших та найповажніших приватних банків Швейцарії, що свідчить про високий рівень їхньої підготовки та серйозний підхід до планування афер. Це також підкреслює, що регуляторні органи стикаються з викликами, які виходять за межі традиційного моніторингу ринку, оскільки шахрайські схеми дедалі частіше перебувають на перетині кіберзлочинності, фінансових маніпуляцій та соціальної інженерії.

CSA закликає бути вкрай обережними та звертати увагу на ключові тривожні сигнали: несподівані пропозиції допомоги у поверненні інвестицій, вимоги сплатити авансові внески, неможливість самостійно перевірити автентичність наданих документів, надмірний тиск із вимогою діяти негайно, а також використання неофіційних каналів зв'язку.

Головною порадою залишається перевірка реєстрації будь-якої фірми чи особи, яка пропонує фінансові послуги.

Особливо важливо підкреслити, що подібні схеми можуть бути адаптовані під будь-яку відому фінансову установу, тому пильність не повинна обмежуватися. Історично шахраї використовували імена таких гігантів, як JPMorgan Chase, Goldman Sachs, HSBC та інших, тому головним уроком має стати критичне ставлення до будь-яких несподіваних пропозицій, незалежно від того, наскільки авторитетним виглядає бренд. Канадські регулятори нагадують, що законна фінансова діяльність завжди передбачає прозорі умови, чіткі контракти та відсутність потреби у передоплаті для доступу до власних коштів.

Підсумовуючи, слід зазначити, що ця справа ілюструє, як зростання популярності криптовалют та онлайн-трейдингу створює нові можливості для зловмисників, які користуються інформаційною асиметрією та емоційною вразливістю інвесторів. Відповідь на цю загрозу потребує комплексного підходу, який включає як посилення регуляторного контролю, так і підвищення загального рівня фінансової освіти населення. У світі, де довіра є найдорожчим активом, її втрата може мати руйнівні наслідки не лише для окремих інвесторів, але й для репутації всієї фінансової інфраструктури, тому пильність та обережність мають стати невід'ємними рисами кожного учасника ринку.

Ваша думка важлива!

1. Наскільки може різниця в регуляторних підходах між Україною та країнами ЄС створювати цінові «арбітражні зони» та стимулювати контрабанду ліків через кордон?
2. Як на вашу думку в Україні працює система фінансової освіти та оповіщення населення про нові види шахрайства, враховуючи, що багато постраждалих не звертаються до правоохоронних органів через недовіру або сором?
3. Які вимоги до кіберстійкості доцільно закріпити для української реєстрової інфраструктури в частині відомостей про кінцевих бенефіціарних власників?
4. Як Україні забезпечити належний захист персональних даних громадян у державних реєстрах, якщо ці дані можуть використовуватися для створення синтетичних ідентичностей і обходу процедур перевірки клієнтів?
5. Як Україні забезпечити баланс між швидким упровадженням генеративного AI в державне управління та належним захистом службової інформації, персональних даних і національної безпеки?
6. Як інтегрувати протидію платіжному шахрайству в національну систему ПВК/ФТ, щоб ефективніше виявляти рахунки підставних осіб, відстежувати рух коштів і повертати активи потерпілим, не перевантажуючи фінансові установи надмірними вимогами?

Контактуйте щодо цього документу з Міністерством фінансів України:

- **Email:** aml_bulletin@minfin.gov.ua
- **Поштова адреса:** Міністерство фінансів України, Україна, 04071, м. Київ, вул. Межигірська, 11
- **Ідентифікація контакту:** стосовно Методологічного Бюлетеня № МінФін-AML-2026-32

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

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