Методологічний бюлетень

Серійний номер: МінФін-AML-2026-26

Червень 2026

“Той, хто пересуває гори, починає з того, що відносить маленькі камінці!”

давньокитайська мудрість

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

Підсумки Пленарного засідання FATF (17–19 червня 2026 року) [1]

Пленарне засідання Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF), що відбулося в Парижі з 17 по 19 червня 2026 року, стало знаковою подією, яка підвела підсумки діяльності під головуванням Мексики та окреслила стратегічні орієнтири на майбутнє під егідою Сполученого Королівства.

Це заключне засідання засвідчило консолідацію міжнародних зусиль у протидії відмиванню коштів, фінансуванню тероризму та розповсюдженню зброї масового знищення, продемонструвавши системний підхід до регулювання фінансових потоків у відповідь на стрімку цифровізацію та появу нових кримінальних схем. Представники понад 200 юрисдикцій та спостерігачів, що входять до глобальної мережі FATF, обговорили як поточні виклики, так і довгострокові ініціативи, спрямовані на зміцнення цілісності світової фінансової системи.

Одним із центральних питань порядку денного стало оновлення самих стандартів FATF, що є наріжним каменем усієї системи протидії фінансовим злочинам. Пленарне засідання ухвалило рішення про внесення змін до Рекомендації 6, що регулює цільові фінансові санкції, з метою забезпечення безперешкодного доступу до гуманітарної допомоги. Цей крок є надзвичайно

[1] https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2026.html

важливим у контексті балансування між жорсткими фінансовими обмеженнями та необхідністю підтримки базових потреб населення в зонах конфліктів чи гуманітарних криз. Інтеграція гуманітарних винятків, закріплених у резолюціях Ради Безпеки ООН 2664 та 2761, безпосередньо до Рекомендацій FATF, свідчить про адаптивність нормативної бази до реалій сучасного світу. Таким чином, FATF не лише посилює контроль, але й демонструє гнучкість, дозволяючи гуманітарним організаціям виконувати свою місію без надмірних бюрократичних перешкод, що є критичним для збереження життів у найбільш вразливих регіонах планети.

Значну частину роботи Пленуму було присвячено питанням комплаєнсу та моніторингу юрисдикцій, що традиційно є одним із найбільш резонансних напрямів діяльності FATF. У рамках оновлення «сірого» списку було ухвалено рішення про включення Боснії та Герцеговини й Іраку до переліку юрисдикцій, що перебувають під посиленим моніторингом. Зазначені країни взяли на себе зобов'язання реалізувати конкретні плани дій для усунення стратегічних недоліків у своїх системах протидії відмиванню коштів та фінансуванню тероризму у визначені терміни.

Водночас Пленум привітав Алжир та Намібію з успішним завершенням їхніх планів дій, що підтверджено результатами виїзних перевірок на місцях. Виключення цих країн з-під посиленого моніторингу є позитивним сигналом, який засвідчує ефективність механізму FATF та готовність держав докладати суттєвих зусиль для приведення національного законодавства та практик у відповідність до міжнародних стандартів. Варто зазначити, що Алжир продовжуватиме співпрацю зі своїм регіональним органом MENAFATF, а Намібія – з ESAAMLG, що підкреслює важливість регіональної координації та підтримки для сталості досягнутих результатів та подальшого вдосконалення систем протидії фінансовим злочинам.

Окрім моніторингових процедур, Пленум приділив значну увагу оцінці ефективності національних систем через механізм взаємних оцінок. Було обговорено та ухвалено звіти щодо Канади та Туреччини, які були підготовлені в рамках нового раунду взаємних оцінок. Ці звіти, що оцінюють як технічну відповідність рекомендаціям FATF, так і практичну ефективність заходів країн у боротьбі з фінансовими злочинами, будуть опубліковані у вересні-жовтні 2026 року після завершення процедури контролю якості та узгодженості в межах Глобальної мережі. Ключовим нововведенням цього раунду є надання країнам дорожніх карт із переліком ключових рекомендованих дій, які необхідно виконати протягом трьох років для посилення захисту від незаконних фінансових потоків. Цей підхід трансформує саму філософію оцінювання, перетворюючи його з простого аудиту на інструмент стратегічного планування та підтримки реформ, що сприяє більш глибокій та стійкій імплементації стандартів FATF на національному рівні.

Окремим блоком роботи стали стратегічні ініціативи, спрямовані на посилення глобальних оборонних механізмів проти фінансових загроз, що швидко еволюціонують. Усвідомлюючи, що ера цифровізації та фрагментації транзакцій вимагає нових підходів до співпраці, було схвалено новий глобальний огляд партнерства між державним та приватним секторами та механізмів захисту даних. Ця публікація, яка з'явиться наступного місяця, презентуватиме різноманітні моделі обміну інформацією з усього світу, що має на меті сприяти дієвому обміну розвідувальними даними для боротьби зі злочинністю з дотриманням вимог щодо захисту персональних даних. Такий крок є визнанням того, що без тісної взаємодії між фінансовими установами, регуляторами та правоохоронними органами неможливо своєчасно виявляти та припиняти складні схеми відмивання коштів, особливо в умовах, коли транзакції дедалі частіше виходять за межі національних кордонів і здійснюються з використанням новітніх технологій.

Посилення прозорості платежів стало ще одним пріоритетним напрямком, у межах якого було схвалено публічне консультування щодо нових рекомендацій із імплементації посиленого стандарту FATF щодо прозорості транскордонних платежів (Рекомендація 16). Це свідчить про те, що FATF продовжує уважно стежити за вразливостями, які виникають у зв'язку зі стрімким зростанням обсягів міжнародних переказів, особливо в контексті боротьби з

шахрайством, яке стає дедалі витонченішим. Розроблені рекомендації допоможуть як державам, так і фінансовим установам посилити контроль за платіжними потоками, що, своєю чергою, сприятиме виявленню та блокуванню операцій, пов'язаних із фінансуванням тероризму, відмиванням коштів та іншими тяжкими злочинами. Консультаційний процес, який розпочнеться вже наступного тижня, дозволить залучити широке коло зацікавлених сторін до вдосконалення цих механізмів, що гарантує врахування практичних потреб та реалій фінансового сектору.

Окрему увагу було приділено новим викликам, пов'язаним із використанням технологічних інновацій у злочинних цілях. Пленарне засідання схвалило нову публікацію, присвячену виявленню та припиненню діяльності з фінансування тероризму, що здійснюється через соціальні мережі, месенджери та стрімінгові платформи. Цей документ є логічним продовженням оновленого звіту FATF про ризики фінансування тероризму, опублікованого у 2025 році, і містить конкретні рекомендації щодо протидії зловживанням, включаючи акцент на проактивній взаємодії з представниками технологічного сектору. Також було схвалено новий звіт, присвячений аналізу ризиків використання підпільних банківських систем, таких як хавала, та інших подібних сервісів для незаконної фінансової діяльності, що особливо актуально у світлі стрімких технологічних змін, які спрощують переміщення коштів поза традиційною банківською системою. Крім того, розпочато роботу над оновленням розуміння ризиків у секторі казино та грального бізнесу загалом, зокрема через призму розширення онлайн-платформ. Розробка індикаторів ризику для цієї сфери допоможе правоохоронцям та фінансовим розвідкам ефективніше виявляти злочинні схеми в цьому динамічному секторі економіки.

Не менш важливим аспектом діяльності FATF є забезпечення відповідальних технологічних інновацій у фінансовому секторі, особливо у сфері віртуальних активів. Пленум схвалив сьоме цільове оновлення щодо імплементації стандартів FATF стосовно віртуальних активів та постачальників послуг віртуальних активів. Це свідчить про постійну увагу FATF до цього стрімко зростаючого ринку, де ризики відмивання коштів та фінансування тероризму залишаються надзвичайно високими через анонімність та швидкість транзакцій. З огляду на зростання платформ децентралізованого фінансування (DeFi) та їхнього потенційного впливу на фінансову систему, було ухвалено рішення про підготовку нового тематичного звіту, який розгляне відповідні регуляторні виклики. Обидва ці звіти будуть опубліковані вже наступного місяця, що дозволить країнам та бізнесу оперативно адаптувати свої підходи до регулювання цієї складної та мінливої сфери.

Ключовою подією Пленуму стало представлення цілей майбутнього головування Великої Британії на період з 1 липня 2026 року по 30 червня 2028 року. Новий президент FATF, Giles Thomson, окреслив пріоритети, які повністю відповідають стратегічним напрямкам, узгодженим на нещодавній міністерській зустрічі у Вашингтоні.

У центрі уваги британського головування будуть три ключові напрямки: посилення міжнародного реагування на епідемію шахрайства, що включає ризики відмивання коштів та фінансування тероризму, пов'язані з так званими «шахрайськими центрами» (scam compounds); зміцнення імплементації ризик-орієнтованого підходу та ризик-орієнтованого нагляду; та покращення обміну інформацією й розвиток державно-приватного партнерства.

Безпосередня увага до проблеми шахрайства є надзвичайно актуальною, адже цей вид злочинів не лише завдає колосальних економічних збитків, але й часто є джерелом фінансування більш серйозної злочинної діяльності, включно з торгівлею людьми та наркотиками. Напередодні передачі повноважень чинна президентка Elisa de Anda Madrazo провела спеціальну сесію за участю оперативних експертів та представників приватного сектору для обміну досвідом у боротьбі з цією глобальною загрозою, що забезпечило плавний перехід до нової тематики.

Нарешті, учасники засідання підтвердили прихильність FATF до інклюзивного та глобального підходу у боротьбі з фінансовими злочинами.

Було засвідчено продовження участі Ямайки та Нігерії як повноправних членів через ініціативу ESRB Guest Initiative, що розширює географію впливу та залучає нові голоси до процесу прийняття рішень.

Започаткування нової Глобальної стратегічної групи, яка провела свою першу зустріч 15 червня під головуванням президента FATF та об'єднала голів регіональних органів за типом FATF, є важливим кроком до посилення координації між усіма ланками Глобальної мережі. Цей дорадчий орган консультуватиме зі стратегічних питань, включаючи транскордонні ризики та можливості для партнерства.

Крім того, FATF поповнилася новим спостерігачем – Альянсом фінансової інклюзії (AFI), який представляє мережу центральних банків та фінансових регуляторів із 83 країн, що розвиваються. Це членство допоможе FATF підтримувати ефективну імплементацію стандартів із дотриманням ризик-орієнтованого підходу, що сприятиме фінансовій інклюзії – одному з ключових пріоритетів мексиканського головування.

Висновки:

- **Гуманізація санкційних стандартів.** FATF оновила Рекомендацію 6, офіційно закріпивши можливість звільнення гуманітарної допомоги від фінансових обмежень, що дозволяє уникати блокування критично важливих ресурсів для населення у кризових зонах.
- **Зміни у списках моніторингу.** До «сірого списку» додано Боснію та Герцеговину й Ірак, натомість Алжир та Намібія успішно виконали плани дій та виключені з-під посиленого нагляду.
- **Фокус на технологічні вразливості.** Схвалено нові звіти та ініціативи щодо протидії використанню соціальних мереж, месенджерів, децентралізованих фінансів (DeFi) та підпільних платіжних систем (хавала) для фінансування тероризму та відмивання коштів.
- **Стратегічний пріоритет нового головування.** Велика Британія, яка очолить FATF з липня 2026 року, визначила боротьбу з «епідемією шахрайства», посилення ризик-орієнтованого нагляду та розвиток публічно-приватного партнерства як ключові цілі на найближчі два роки.

Окремим пунктом стало обрання нового віце-президента FATF на період 2026-2027 років, яким став пан Vivek Aggarwal з Індії.

У підсумку, червневе Пленарне засідання FATF 2026 року заклало міцний фундамент для подальшого зміцнення глобальної архітектури протидії фінансовим злочинам, окресливши чіткі шляхи реагування на сучасні виклики та забезпечивши наступність у роботі організації на найближчі роки.

Оновлене керівництво з ризик-орієнтованого підходу Wolfsberg Group [2]

Оновлене керівництво Wolfsberg Group, є важливим етапом у розвитку підходів до протидії відмиванню коштів та фінансуванню тероризму. Цей документ не просто актуалізує попередні напрацювання, а й пропонує цілісне бачення того, як фінансові установи ма ють вибудовувати свої програми управління ризиками фінансових злочинів у сучасному динамічному середовищі.

В основі цього бачення лежить ризик-орієнтований підхід, який розглядається як критичний елемент ефективного функціонування будь-якої фінансової інституції, незалежно від її розміру, географічного охоплення чи бізнес-моделі. Wolfsberg Group наголошує, що ризик-орієнтований підхід є не просто вимогою регуляторів, а стратегічним інструментом, який

[2] https://db.wolfsberg-group.org/assets/6c32b34b-bc02-4e8b-9b3f-f36e9bd109c3/Wolfsberg%20Group%20-%20Risk%20Based%20Approach%20Guidance%20_June2026.pdf

дозволяє фінансовим установам зосередити свої зусилля на найбільш пріоритетних загрозах, одночасно переглядаючи або навіть припиняючи ті види діяльності, які не роблять вагомого внеску у боротьбу з фінансовими злочинами. Такий підхід є особливо актуальним в умовах безпрецедентного рівня інновацій та технологічного прогресу, які створюють як нові можливості, так і нові вразливості у фінансовій системі.

Ключовою ідеєю, яка проходить через увесь документ, є необхідність відходу від універсальних, шаблонних рішень. Wolfsberg Group чітко заявляє, що підхід, який передбачає однакові заходи для всіх, не може вважатися ризик-орієнтованим. Кожна фінансова установа є унікальною, і її програма управління ризиками має бути пропорційною рівню властивого ризику, що визначається її бізнес-стратегією та операційною моделлю.

Цей принцип пропорційності є одним із трьох стовпів, на яких ґрунтується оновлене керівництво, поряд з пріоритезацією та ефективністю. Пропорційність передбачає, що фінансова установа повинна враховувати свої розміри, масштаби діяльності, клієнтську базу та географічну присутність, а також власний апетит до ризику, який встановлюється вищим керівництвом. Цей апетит до ризику визначає межі, в яких установа готова приймати ризики для досягнення своїх цілей, а також ті ризики, які вона категорично не толерує. Важливим аспектом тут є також врахування очікувань щодо фінансової інклюзії, що свідчить про баланс між необхідністю жорсткого контролю та доступністю фінансових послуг для різних верств населення.

Другим ключовим елементом є пріоритезація, яка передбачає спрямування уваги та ресурсів на клієнтів та види діяльності з підвищеним ризиком. Цей принцип ґрунтується на розумінні того, що спроба охопити всі аспекти ризику одночасно призводить до розпорошення зусиль і, як наслідок, до неефективності. Для ідентифікації найбільш ризикових зон Wolfsberg Group пропонує аналізувати дві основні категорії змінних: хто є клієнтом та що він робить. У першій категорії розглядаються такі фактори, як тип клієнта, галузь, в якій він працює, структура власності, а також країна реєстрації або ведення бізнесу. Наприклад, компанії з номінальними акціонерами, акціями на пред'явника або ті, що ведуть діяльність у юрисдикціях з високим рівнем ризику, потребують підвищеної уваги. З іншого боку, публічні компанії, які підлягають жорстким вимогам розкриття інформації, можуть розглядатися як такі, що становлять менший ризик. У другій категорії аналізується поведінка клієнта, включаючи його транзакційну активність, використання продуктів та послуг, а також будь-які відхилення від очікуваного профілю. Нестандартна поведінка, спроби використання продуктів для збільшення анонімності або ускладнення відстежуваності операцій є важливими індикаторами ризику. Група також наголошує на важливості використання даних із систем моніторингу та скринінгу для отримання додаткових аналітичних інсайтів, які допомагають уточнювати ризик-профіль клієнта в динаміці.

Третім, і, можливо, найбільш важливим елементом є ефективність. Wolfsberg Group переходить від простого переліку вимог до оцінки практичних результатів діяльності фінансової установи у сфері протидії фінансовим злочинам.

Ефективність, згідно з документом, вимірюється трьома факторами: дотриманням законодавчих вимог, створенням розумної та ризик-орієнтованої системи контролю, а також наданням високоякісної інформації державним органам. Це означає, що установа має не просто формально виконувати приписи, а й робити реальний внесок у розкриття та запобігання злочинам.

Саме цей акцент на корисності інформації для правоохоронних органів виводить ризик-орієнтований підхід на новий рівень, перетворюючи фінансові установи з пасивних виконавців на активних учасників системи фінансової безпеки. Для демонстрації ефективності необхідні прозорі механізми управління, які забезпечують підзвітність у прийнятті рішень, що дозволяє зберігати довіру з боку наглядових органів та аудиторів. Водночас наголошується, що управлінські структури не повинні бути надмірно ускладненими, оскільки це може

перешкоджати оперативному прийняттю рішень та відволікати ресурси від основної діяльності з управління ризиками.

Окрему увагу в керівництві приділено питанням взаємодії з наглядовими органами та аудиторами. Wolfsberg Group закликає до відмови від так званого "галочного" підходу, коли основна увага приділяється формальній наявності документів, а не реальній ефективності заходів. Встановлення нереалістичних очікувань, таких як вимога абсолютної безпомилковості або подання повідомлень про всі без винятку підозрілі операції, розглядається як контрпродуктивність, оскільки це відволікає ресурси від справді важливих ризиків, збільшує витрати та створює зайві незручності для клієнтів. Натомість, нагляд та аудит мають бути адаптовані до бізнес-моделі та ризик-профілю кожної конкретної установи, оцінюючи практичний внесок у боротьбу з фінансовими злочинами. Ключову роль у цьому процесі відіграє постійний діалог між державним та приватним секторами, а також регулярна комунікація з аудиторами, що сприятиме взаєморозумінню та прийняттю ризик-орієнтованого підходу, який відповідає унікальним особливостям діяльності кожної установи.

Не менш важливим аспектом є підготовка кадрів та формування відповідної культури. Люди залишаються ключовим елементом системи управління ризиками, і тому їхня підготовка має бути цільовою та відповідати рівню ризику виконуваних функцій. Співробітники, які обіймають посади з підвищеним ризиком, повинні отримувати спеціалізоване навчання, що дозволяє їм ефективно виявляти, оцінювати та управляти ризиками. Важливо, щоб програми навчання розвивали навички критичного мислення та допитливості, заохочували співробітників до проактивної позиції та вміння приймати зважені рішення. Керівництво відіграє вирішальну роль у цьому процесі, задаючи "тон зверху" та демонструючи особисту прихильність принципам боротьби з фінансовими злочинами. Тільки за таких умов можна сформувати культуру, де управління ризиками є не тягарем, а невід'ємною частиною бізнес-процесів, що веде до досягнення практичних результатів.

Висновки:

- **Відмова від шаблонів на користь пропорційності.** Універсальний підхід до управління ризиками є неефективним; кожна фінансова установа має вибудовувати програму захисту виключно під власну бізнес-модель, масштаби та клієнтську базу.
- **Пріоритезація ресурсів за принципом "фокус на найвищих ризиках".** Зусилля та ресурси мають спрямовуватися на найризикованіших клієнтів та операції, тоді як заходи щодо низькоризикових сегментів можуть бути послаблені або переглянуті.
- **Зміна критеріїв ефективності: від "галочок" до корисних результатів.** Головним показником успіху є не кількість перевірених документів, а якість та корисність інформації, переданої правоохоронним органам для реального протистояння злочинам.
- **Відмова від "культури нульової толерантності до помилок".** Нагляд та аудит мають відійти від вимог абсолютної безпомилковості, натомість оцінюючи загальну ефективність системи управління ризиками, що дозволяє установам зосередитись на справді важливих загрозах.

У підсумку, оновлене керівництво Wolfsberg Group пропонує комплексне бачення ризик-орієнтованого підходу, яке виходить за межі простого дотримання нормативних вимог. Воно закликає фінансові установи до глибокого аналізу власної діяльності, свідомої пріоритезації ресурсів та орієнтації на реальну ефективність у боротьбі з фінансовими злочинами. Успішне впровадження цього підходу можливе лише за умов тісної співпраці з регуляторами, які мають підтримувати гнучкість інституцій та оцінювати результати їхньої роботи, а не формальні процедури.

Цей комплексний підхід, що поєднує пропорційність, пріоритезацію, ефективність, належне навчання та сильну корпоративну культуру, створює основу для посилення фінансової безпеки

як на рівні окремих установ, так і всієї глобальної фінансової системи, що є спільним пріоритетом як для приватного, так і для державного секторів.

Фінансова розвідка в дії: як британські SARs захищають суспільство [3]

Буклет, підготовлений Підрозділом фінансової розвідки Сполученого Королівства (UKFIU), представляє ґрунтовний аналіз ролі та ефективності системи повідомлень про підозрілі операції (SARs) у боротьбі з фінансовими злочинами та організованою злочинністю. Цей документ є не просто звітністю, а важливим інструментом зворотного зв'язку, який демонструє, як фінансова розвідувальна інформація, отримана від приватного сектору, трансформується в реальні слідчі дії та вагомі судові результати. Він висвітлює синергію між фінансовими установами, які виступають "очима та вухами" системи, та правоохоронними органами, які використовують цю інформацію для захисту суспільства від найсерйозніших загроз.

Документ одразу задає тон, підкреслюючи критичну важливість SARs як джерела розвідувальної інформації. У вступному слові Вінса О'Браєна, очільника UKFIU, наголошується, що ці повідомлення надають правоохоронцям ключові дані, такі як номери телефонів, адреси, реквізити компаній, інформацію про інвестиційну активність, банківські рахунки та інші активи. Цей набір даних є фундаментом для ініціювання нових розслідувань та збагачення вже існуючих справ. Особливо показовим є перелік злочинів, для розкриття яких використовуються SARs: від виявлення сексуальних злочинців та жертв шахрайства до пошуку підозрюваних у вбивствах, зниклих безвісти, торговців людьми, утікачів від правосуддя та осіб, причетних до фінансування тероризму. Це свідчить про те, що система SARs є універсальним інструментом, здатним охопити практично весь спектр кримінальних загроз, що дозволяє стверджувати про її фундаментальну роль у національній безпеці країни.

Аналіз наведених у буклеті кейсів дозволяє глибше зрозуміти механізми роботи системи та її практичну цінність. Найбільш показовим є приклад із виявленням великого стороннього кредиту на суму понад 60 000 фунтів стерлінгів на рахунку бізнесу, який не відповідав його профілю діяльності. Цей випадок ілюструє типовий сценарій відмивання грошей через етап "розшарування" (layering), коли кошти, отримані злочинним шляхом, переміщуються для приховування їхнього походження. Підзвітний суб'єкт не просто зафіксував аномалію, а провів додаткову перевірку, яка виявила зв'язки з іншим підозрілим бізнесом та примітивний веб-сайт компанії. Відмова UKFIU в наданні дозволу на операцію (DAML) та подальше поширення інформації дозволили правоохоронцям не лише ідентифікувати потенційного "грошового мула" (директора бізнесу), але й оперативно накласти арешт на кошти через Ордер на замороження рахунку (AFO). Цей ланцюжок дій – від повідомлення підзвітного суб'єкта до реального блокування активів – є ідеальним прикладом ефективної співпраці, яка перериває злочинний потік на самому його етапі.

Інший важливий аспект, який випливає з буклету, – це здатність системи SARs виявляти та руйнувати цілі злочинні мережі. Наприклад, у справі про організоване шахрайство проти транспортних операторів, множинні повідомлення від різних підзвітних суб'єктів дозволили правоохоронцям встановити зв'язки між різними суб'єктами, які зловживали системою повернення коштів за квитками. Це призвело не лише до арешту коштів на суму понад 15 000 фунтів, але й до засудження зловмисників та можливості використання конфіскованих коштів для компенсації збитків.

Ще більш масштабною є історія з використанням одного пристрою для доступу до кількох клієнтських рахунків, що вказувало на шахрайство. Завдяки SARs слідчі змогли не лише відстежити рух коштів до вербувальника "мулів", але й завдяки співпраці з репортером встановити фізичну адресу та пристрій, які використовувала мережа. Результатом стали арешт організатора та його спільника, судові заборони та попередження для понад 40 "грошових

[3] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/817-sars-reporter-booklet-june-2026/file

мулів", що демонструє системний підхід до боротьби з явищем, а не лише з його окремими проявами.

Окремо варто відзначити роль SARs у справах, які мають не лише фінансове, але й значне суспільне значення, таких як викрадення людей або торгівля людьми. У випадку з розслідуванням викрадення, своєчасне повідомлення дозволило ідентифікувати рахунок підозрюваного, на який надійшло понад 200 000 фунтів, і заблокувати ці кошти. Це не лише завадило легалізації коштів, але й позбавило злочинців фінансового ресурсу.

Схожим чином, у справі про можливу торговлю людьми, банківські SARs виявили готівкові депозити на десятки тисяч фунтів та транзакції на веб-сайти для дорослих. Відмова в DAML та скоординована робота підрозділів з боротьби з рабством привели до обшуків, вилучення 60 000 фунтів готівкою та арешту трьох підозрюваних за серйозними статтями, включаючи контроль проституції та злочини за Законом про сучасне рабство. Цей приклад яскраво ілюструє, як фінансова розвідка стає інструментом соціального захисту, допомагаючи виявляти та рятувати вразливих осіб, які постраждали від експлуатації.

Буклет також висвітлює інші важливі аспекти використання SARs, зокрема їхню роль у виявленні корупції, шахрайств із державними кредитами (Bounce Back Loan) та нелегальної підприємницької діяльності. Справа про співробітника правоохоронних органів, який працював за кордоном, показує, як повідомлення, що виявили невідповідність між доходами та надходженнями на рахунки, допомогли викрити розкрадання на суму понад 260 000 фунтів і повернути кошти роботодавцю. Приклад із підробленим бізнесом із продажу металобрухту, який отримав понад 400 000 фунтів без належної ліцензії, демонструє, як SARs дозволяють боротися з тіньовим сектором економіки, що живиться за рахунок доходів від злочинів. Нарешті, історія про зловживання довіреністю для контролю над коштами вразливих осіб підкреслює важливість SARs у захисті найменш захищених верств населення, де завдяки повідомленням вдалося виявити переміщення близько 1 мільйона фунтів, захистити жертв та забезпечити конфіскацію понад 250 000 фунтів.

Таким чином, інформаційний буклет за червень 2026 року є переконливим доказом того, що система повідомлень про підозрілі операції у Великій Британії є не просто бюрократичною процедурою, а потужним, динамічним і багатофункціональним механізмом боротьби з фінансовою злочинністю.

Наведені приклади демонструють, як інформація, надана фінансовими

Висновки:

- **SARs є критичним інструментом ініціації та підтримки розслідувань:** повідомлення про підозрілі операції надають правоохоронцям конкретні дані, які дозволяють розпочинати нові справи та посилювати вже існуючі розслідування у сферах від шахрайства до тероризму.
- **Відмова в DAML та подальше замороження активів є ключовим механізмом переривання злочинних потоків:** у більшості наведених кейсів UKFIU відмовляє в дозволі на операцію, що дозволяє правоохоронцям накладати арешти на рахунки (AFO) та блокувати кошти, які інакше були б втрачені.
- **Система SARs ефективно виявляє та руйнує цілі організовані злочинні мережі:** множинні повідомлення від різних репортерів дозволяють встановлювати зв'язки між суб'єктами, відстежувати рух коштів до організаторів, ідентифікувати "грошових мулів" та проводити масштабні операції із затриманнями й конфіскаціями.
- **Фінансова розвідка виконує не лише економічну, але й соціально-захисну функцію:** SARs допомагають виявляти випадки торгівлі людьми, сексуальної експлуатації та шахрайств із державними коштами, забезпечуючи захист найменш захищених верств населення.

установами, перетворюється на конкретні дії: від замороження рахунків і конфіскації активів до руйнування злочинних мереж, притягнення винних до відповідальності та захисту жертв злочинів. Документ не лише інформує про успіхи, але й виконує освітню та мотиваційну функцію, заохочуючи підзвітних суб'єктів до пильності та підкреслюючи їхню незамінну роль у загальній системі національної безпеки, що робить його цінним ресурсом для всіх учасників режиму фінансового моніторингу.

Кіберзлочинність без кордонів: основні загрози цифровій безпеці Азії та Тихоокеанського регіону [4]

Звіт Інтерполу є комплексним дослідженням сучасного стану кіберзлочинності в Азійсько-Тихоокеанському регіоні та містить оцінку основних загроз, тенденцій і викликів, які визначали розвиток кіберкримінального середовища у 2024–2025 роках. Документ демонструє, що кіберзлочинність у регіоні продовжує стрімко зростати як за масштабами, так і за рівнем організованості, перетворюючись на один із найбільш значущих факторів ризику для економічної стабільності, державної безпеки та довіри до цифрових технологій.

На тлі швидкої цифровізації, розвитку електронної комерції, мобільного банкінгу, хмарних сервісів, дистанційної роботи та широкого впровадження штучного інтелекту злочинні угруповання отримують дедалі більше можливостей для проведення складних транскордонних операцій. Автори наголошують, що нерівномірний рівень кіберстійкості між окремими державами регіону створює сприятливе середовище для діяльності організованих злочинних мереж, які використовують юрисдикції зі слабшими можливостями реагування як бази для проведення міжнародних атак.

Особливу увагу звіт приділяє трансформації кіберзлочинності у високоприбуткову індустрію. У країнах Південно-Східної Азії спостерігається активний розвиток масштабних шахрайських центрів, створених транснаціональними організованими злочинними групами. Такі центри функціонують як повноцінні кримінальні підприємства із власною інфраструктурою, кадровими структурами та системами управління. Вони спеціалізуються на романтичних шахрайствах, інвестиційних аферах, криптовалютних схемах, незаконних азартних іграх та інших видах цифрового шахрайства. При цьому значна частина таких операцій пов’язана з використанням примусової праці та торгівлі людьми, що підкреслює тісний взаємозв’язок між кіберзлочинністю та традиційною організованою злочинністю. За оцінками, сукупний дохід таких схем сягає десятків мільярдів доларів США щороку, що робить їх одним із найприбутковіших напрямів діяльності злочинних мереж у регіоні.

У документі підкреслюється, що кіберзлочинність уже стала домінуючою категорією правопорушень для багатьох держав регіону. Більше половини країн, які взяли участь в опитуванні Інтерполу, повідомили, що частка кіберзлочинів перевищує 30% усіх зареєстрованих кримінальних правопорушень. Найбільш поширеними видами злочинів залишаються онлайн-шахрайство та фішинг, банківські трояни й програми для викрадення інформації, атаки програм-вимагачів, компрометація ділового листування та злочини, пов’язані з використанням технологій штучного інтелекту й дезінформації. Особливо небезпечним явищем є те, що кіберзлочинність дедалі частіше поєднує технічні засоби компрометації із психологічними методами впливу на жертв, використовуючи соціальну інженерію як ключовий інструмент досягнення злочинних цілей.

Найбільш масовою загрозою залишаються онлайн-шахрайство та фішингові кампанії. Автори зазначають, що сучасний фішинг уже давно вийшов за межі традиційних електронних листів і трансформувався у високоточні атаки, спрямовані на конкретних осіб або організації. Зловмисники активно використовують SMS-повідомлення, месенджери, соціальні мережі та

[4] https://www.interpol.int/News-and-Events/News/2026/New-INTERPOL-report-highlights-escalating-cyber-threats-across-Asia-and-South-Pacific

сервіси миттєвого обміну повідомленнями. Водночас стрімкий розвиток генеративного штучного інтелекту дозволив кіберзлочинцям створювати надзвичайно переконливі повідомлення та підроблені цифрові профілі, які практично неможливо відрізнити від справжніх без спеціалізованих інструментів перевірки. Саме тому людський фактор залишається найбільш експлуатованою вразливістю сучасних інформаційних систем.

Однією з центральних тем звіту є поширення програм-вимагачів. Упродовж 2024 року в регіоні було зафіксовано понад 135 тисяч таких атак, які вразили підприємства, державні установи та об'єкти критичної інфраструктури. Автори звертають увагу на поступовий перехід від класичного шифрування даних до моделей подвійного вимагання, коли злочинці спочатку викрадають конфіденційну інформацію, а потім погрожують її оприлюдненням у разі несплати викупу. Значний резонанс отримала атака на Національний центр даних Індонезії, яка призвела до порушення роботи понад 280 державних сервісів. Такі випадки демонструють, що сучасні кіберінциденти можуть мати прямі наслідки для функціонування державного управління, транспортної інфраструктури та надання критично важливих послуг населенню.

Окремий блок дослідження присвячений поширенню шкідливого програмного забезпечення. Найбільшу частку серед усіх виявлених видів шкідливого програмного забезпечення становлять троянські програми, потенційно небажане програмне забезпечення (grayware), шпигунські програми типу «бекдор», призначені для несанкціонованого віддаленого доступу до інформаційних систем. Особливу увагу автори приділяють стрімкому зростанню ролі програм для викрадення інформації, які стали одним із ключових інструментів сучасної кіберзлочинності. Таке шкідливе програмне забезпечення використовується для збору облікових даних, банківської та платіжної інформації, відомостей про криптоактиви, а також інших конфіденційних даних, що надалі можуть використовуватися для фінансового шахрайства, захоплення облікових записів, програм-вимагачів та інших злочинних операцій. Отримані дані надалі продаються на даркнет-майданчиках і використовуються для здійснення фінансового шахрайства, викрадення особистої інформації, компрометації корпоративних систем та запуску подальших атак. Таким чином, програми для викрадення інормації фактично стали одним із базових елементів сучасної кіберзлочинної екосистеми, забезпечуючи злочинців ресурсами для здійснення широкого спектра інших кримінальних дій.

За результатами міжнародної операції Operation Secure Інтерпол ідентифікував п'ять найбільш поширених у регіоні родин шкідливого програмного забезпечення для викрадення інформації – RedLine Stealer, LummaC2, LokiBot, Negasteal та ZBot. Основною функцією цих програм є несанкціонований збір облікових даних користувачів, інформації веббраузерів, відомостей про криптовалютні гаманці, корпоративних даних та іншої конфіденційної інформації, яка в подальшому використовується для фінансового шахрайства, компрометації облікових записів та здійснення інших кіберзлочинів.

Водночас звіт демонструє подальшу комерціалізацію кіберзлочинності та її трансформацію у високорозвинену сервісну екосистему. На нелегальних онлайн-майданчиках окремими «послугами» пропонуються шкідливе програмне забезпечення, інфраструктура для проведення атак, викрадені дані, а також інструменти для приховування злочинної діяльності та легалізації одержаних доходів. Такі моделі, відомі як шкідливе програмне забезпечення як послуга (MaaS), кіберзлочинні інструменти як послуга (CaaS) та програми-вимагачі як послуга (RaaS), значно спрощують доступ до кіберзлочинної діяльності для нових учасників, знижують технічні бар'єри входу та сприяють подальшому масштабуванню транснаціональної кіберзлочинності.

Важливим напрямом аналізу є вплив штучного інтелекту на еволюцію кіберзагроз. Автори констатують різке зростання використання діпфейк-технологій, які дозволяють створювати високореалістичні підроблені відео, аудіозаписи та цифрові образи. Такі технології використовуються для імітації керівників компаній, обходу процедур перевірки особи, поширення дезінформації та проведення фінансових шахрайств. Звіт підкреслює, що

кіберзлочинність дедалі більше зміщується від технічного зламу систем до маніпулювання поведінкою людей, використовуючи психологічний вплив та штучний інтелект як основні інструменти досягнення злочинного результату.

Поряд із цим документ фіксує суттєве зростання кількості DDoS-атак та випадків витоку даних. У 2024 році кількість DDoS-інцидентів збільшилася майже вдвічі порівняно з попереднім роком, причому головними цілями стали державні органи та фінансові установи. Водночас близько 80% усіх зафіксованих витоків даних були пов'язані із системними проникненнями, а більшість інцидентів супроводжувалася використанням шкідливого програмного забезпечення або програм-вимагачів. Це свідчить про те, що компрометація даних продовжує залишатися одним із ключових інструментів отримання прибутку кіберзлочинцями.

Загалом звіт доходить висновку, що кіберзлочинність у країнах Азії та Південного Тихоокеанського регіону переходить на новий рівень організованості, технологічної складності та міжнародної координації. Подальше зростання використання штучного інтелекту, поширення сервісних моделей кіберзлочинності, розвиток даркнет-екосистем та інтеграція фінансових і технологічних злочинних сервісів створюють передумови для подальшого ускладнення загроз. У цих умовах ключовими чинниками ефективної протидії визначаються міжнародний обмін інформацією, спільні правоохоронні операції, розвиток технічних спроможностей держав, підвищення рівня кіберобізнаності населення та формування комплексної системи цифрової стійкості на національному і регіональному рівнях.

Висновки:

- **Онлайн-шахрайство, фішинг та кампанії із використанням програм для викрадення інформації стали основними драйверами кіберзлочинності в регіоні,** а викрадення облікових даних дедалі частіше виступає початковим етапом складніших атак.
- **Штучний інтелект і deepfake-технології суттєво підвищують ефективність кіберзлочинців,** дозволяючи автоматизувати соціальну інженерію, створювати переконливі підробки та обходити процедури перевірки особи.
- **Кіберзлочинність дедалі більше функціонує як організований транснаціональний бізнес,** використовуючи моделі RaaS та MaaS, даркнет-маркетплейси та міжнародну інфраструктуру для масштабування атак.
- **Найбільшим викликом для держав регіону залишається нерівномірний рівень кіберспроможностей,** зокрема нестача цифрової криміналістики, спеціалізованого навчання та технічних ресурсів.

Від повідомлень про підозрілі операції до викриття корупції: роль підрозділів фінансової розвідки у сучасних системах ПВК/ФТ [5]

Документ Transparency International присвячений комплексному дослідженню ролі підрозділів фінансової розвідки (ПФР) у виявленні корупції, відстеженні незаконних фінансових потоків та протидії легалізації доходів, одержаних злочинним шляхом. У центрі дослідження перебуває питання того, наскільки ефективно сучасні ПФР здатні трансформувати великі масиви фінансової інформації у практично придатну розвідувальну інформацію для правоохоронних органів та антикорупційних інституцій. Для цього автори провели порівняльний аналіз двадцяти країн із різними правовими системами, рівнем економічного

[5] https://files.transparencycdn.org/images/Report_Connecting-The-Dots-English_2026.pdf

розвитку та моделями організації фінансової розвідки, охопивши держави Європи, Північної та Південної Америки, Африки, Азії та Близького Сходу.

Документ виходить із того, що практично будь-яка корупційна діяльність зрештою залишає фінансовий слід. Незалежно від того, чи йдеться про хабарництво, розкрадання бюджетних коштів, зловживання службовим становищем, незаконне збагачення або інші корупційні злочини, отримані кошти потребують приховування, переміщення, інвестування чи інтеграції в легальну економіку. Саме тому фінансова система стає одним із найбільш вразливих елементів корупційних схем, а підрозділи фінансової розвідки – органами, які мають унікальні можливості для їх виявлення. На відміну від інших державних органів, ПФР отримують інформацію безпосередньо від фінансових установ та визначених нефінансових установ і професій, аналізують повідомлення про підозрілі операції, поєднують їх з іншими джерелами даних та здійснюють подальше поширення фінансової розвідувальної інформації серед компетентних органів.

Особливу увагу автори приділяють тому, чому саме ПФР здатні виявляти корупцію там, де інші органи не бачать повної картини. По-перше, вони функціонують як центральний вузол отримання повідомлень про підозрілі операції від банків, страхових компаній, платіжних установ, нотаріусів, адвокатів, бухгалтерів та інших суб'єктів фінансового моніторингу. Це дозволяє отримувати сигнали про ризикову діяльність ще до початку офіційного кримінального розслідування. По-друге, ПФР мають можливість інтегрувати інформацію з різних джерел, включаючи банківські дані, інформацію про кінцевих бенефіціарних власників, податкові відомості, дані правоохоронних органів, корпоративні реєстри та інші адміністративні бази даних. По-третє, ПФР виступають важливими координаторами інформаційного обміну між державними органами як усередині країни, так і на міжнародному рівні, що особливо важливо для розслідування складних транскордонних корупційних схем.

Дослідження демонструє реальні приклади того, як фінансова розвідка допомагає викривати корупційні злочини. У Чилі аналіз невідповідності між офіційними доходами та фактичними витратами працівника поліції дозволив виявити значно ширшу систему корупції всередині правоохоронного органу, що призвело до численних кримінальних переслідувань і понад ста обвинувальних вироків. У Франції ПФР зміг встановити приховані механізми виплати хабарів місцевому посадовцю через фінансування спортивних організацій, тоді як окремі транзакції самі по собі виглядали цілком законними. У Нігерії фінансова розвідка відіграла ключову роль у викритті масштабної міжнародної корупційної схеми за участю політично значущих осіб та офшорних компаній, що дозволило відстежити рух коштів через кілька юрисдикцій та повернути близько 50 мільйонів доларів незаконно виведених активів. Ці приклади використовуються авторами для демонстрації того, що ефективна фінансова розвідка є дієвим інструментом як у внутрішньодержавних, так і у транскордонних корупційних справах.

Водночас документ наголошує, що потенціал ПФР значною мірою залежить від умов, у яких вони функціонують. Для оцінки цих умов Transparency International розробила систему з дев'яти взаємопов'язаних компонентів, які охоплюють правовий мандат, повноваження, доступ до інформації, механізми отримання повідомлень про підозрілі операції, аналітичну діяльність, співпрацю з правоохоронними органами, міжнародне співробітництво, ресурсне забезпечення, операційну незалежність та прозорість діяльності. Автори підкреслюють, що навіть високопрофесійний ПФР не може бути ефективним без належного законодавчого середовища, достатніх ресурсів та підтримки інших державних інституцій.

Однією з центральних тем дослідження є питання правового статусу та повноважень ПФР. У документі детально аналізуються різні моделі організації ПФР – адміністративна, правоохоронна, судова та змішана. Переважна більшість досліджених країн використовує адміністративну модель, коли ПФР функціонує як самостійний орган або структурний підрозділ фінансового відомства чи центрального банку. Значна увага приділяється додатковим повноваженням ПФР, зокрема праву тимчасово зупиняти підозрілі фінансові операції або заморожувати рахунки. Автори зазначають, що такі інструменти мають особливе

значення для боротьби з корупцією, оскільки дозволяють оперативно запобігати виведенню коштів до того, як правоохоронні органи отримають можливість втрутитися. Водночас надмірне або необґрунтоване використання таких повноважень може створювати ризики розкриття факту розслідування та завчасного попередження підозрюваних.

Окремий розділ присвячений аналізу повідомлень про підозрілі операції як основного джерела фінансової розвідувальної інформації. Автори наголошують, що ефективність ПФР безпосередньо залежить не лише від кількості отриманих повідомлень, а насамперед від їх якості, своєчасності та інформативності. Документ детально аналізує проблему надмірно формального звітування, коли суб'єкти фінансового моніторингу подають повідомлення про підозрілі операції не стільки через наявність обґрунтованих підозр, скільки з метою дотримання регуляторних вимог та уникнення потенційної відповідальності, що негативно впливає на якість фінансової розвідки. Такі повідомлення створюють надмірне навантаження на ПФР, відволікають ресурси від аналізу справді ризикових операцій та знижують загальну ефективність системи ПВК/ФТ.

Одним із найбільш показових висновків дослідження є встановлення суттєвої різниці між проактивним та реактивним використанням фінансової розвідки. Аналіз показав, що інформація, яку ПФР готує у відповідь на конкретні запити правоохоронних органів у межах уже відкритих розслідувань, значно частіше використовується на практиці та має більший вплив на результати кримінальних проваджень. Натомість фінансова розвідка, яку ПФР самостійно формує та направляє компетентним органам без попереднього запиту, використовується значно рідше. Це свідчить про те, що в багатьох країнах фінансова розвідка залишається переважно інструментом підтримки вже існуючих розслідувань, а не механізмом раннього виявлення корупційних ризиків. Автори вважають таку ситуацію серйозною системною проблемою та закликають держави розвивати механізми інтеграції фінансової розвідки у процеси виявлення злочинів на початкових стадіях.

Значна частина документа присвячена аналізу системних недоліків у роботі ПФР. Найбільш поширеною проблемою визначено обмежений доступ до критично важливої інформації. Лише частина досліджених ПФР має прямий доступ до реєстрів кінцевих бенефіціарних власників, податкових баз даних та інформаційних ресурсів правоохоронних органів. У багатьох країнах доступ до такої інформації забезпечується через міжвідомчі угоди або інші неформальні механізми, що створює ризики затримок, обмежень та політичного впливу. Автори також звертають увагу на відсутність повноцінних реєстрів бенефіціарних власників у низці країн, що істотно ускладнює розслідування складних корупційних схем із використанням компаній-посередників та номінальних власників.

Суттєвим викликом визнається також неповне охоплення режимом ПВК/ФТ окремих секторів підвищеного ризику. Особливо критичною є ситуація у сферах юридичних послуг, операцій з нерухомістю та корпоративного сервісу, які традиційно використовуються для приховування корупційних доходів та легалізації активів. Документ наголошує, що відсутність належного охоплення цих секторів обмежує можливості ПФР отримувати інформацію про фінансові потоки, які проходять поза банківською системою.

Важливе місце в дослідженні займає питання операційної незалежності ПФР. Автори підкреслюють, що ПФР дедалі частіше стикаються з політичним тиском саме через успішне виявлення фінансових операцій, пов'язаних із політично значущими особами, високопосадовцями або впливовими бізнес-групами. Аналіз законодавства показав, що в багатьох країнах існують ризики політичного впливу через механізми призначення та звільнення керівників ПФР, залежність від інших органів влади або нечіткість правових гарантій незалежності. Документ наголошує, що ефективна фінансова розвідка можлива лише за умови існування реальних інституційних гарантій незалежності, які дозволяють приймати аналітичні рішення без зовнішнього втручання.

Окремо розглядаються питання міжнародного співробітництва між ПФР. У зв'язку з тим, що значна частина корупційних коштів переміщується через декілька юрисдикцій, ефективний

обмін інформацією між ПФР є критично важливим. Водночас дослідження показує, що навіть за наявності міжнародних механізмів співробітництва їх практична ефективність часто знижується через різні правові режими, вимоги до конфіденційності, відмінності в аналітичних підходах та процедурні бар'єри щодо використання отриманої інформації в кримінальному судочинстві.

Завершується документ масштабним блоком рекомендацій для урядів, ПФР та міжнародних організацій.

Transparency International закликає забезпечити підрозділам фінансової розвідки прямий та захищений доступ до інформації про бенефіціарних власників, податкових даних та інформаційних ресурсів правоохоронних органів, розширити їхні превентивні повноваження щодо тимчасового блокування підозрілих активів, усунути прогалини у звітуванні секторів підвищеного ризику, інвестувати у сучасні аналітичні технології та професійний розвиток персоналу, посилити механізми зворотного зв'язку між ПФР та правоохоронними органами, підвищити прозорість діяльності ПФР та забезпечити їх реальну операційну незалежність.

Висновки:

- **Прямий доступ ПФР до інформації про кінцевих бенефіціарних власників, податкових та правоохоронних баз даних** є критичною умовою ефективного виявлення корупції та схем ВК/ФТ; залежність від неформальних механізмів доступу суттєво знижує результативність фінансової розвідки.
- **Найбільший практичний ефект фінансова розвідувальна інформація демонструє тоді, коли вона інтегрована в розслідування на ранній стадії** та активно використовується правоохоронними органами, а не лише реагує на вже відкриті кримінальні провадження.
- **Для підвищення якості фінансової розвідки необхідно розширити охоплення вимогами ПВК/ФТ секторів підвищеного ризику,** зокрема юридичних, корпоративних та рієлторських послуг, а також покращити якість повідомлень про підозрілі операції та механізми зворотного зв'язку із суб'єктами фінансового моніторингу.
- **Операційна незалежність ПФР повинна бути законодавчо захищена** через прозорі процедури призначення керівництва, гарантії автономності аналітичної діяльності та захист від політичного втручання, особливо у справах щодо політично значущих осіб та масштабної корупції.

Загальний висновок дослідження полягає в тому, що підрозділи фінансової розвідки залишаються одним із найпотужніших інструментів викриття корупції та відстеження незаконних фінансових потоків, однак їхній потенціал далеко не повністю реалізований і потребує подальшого інституційного та законодавчого посилення.

Європейська система захисту викривачів: прогалини імплементації та виклики практичного застосування [6]

Документ Transparency International є комплексним дослідженням стану захисту викривачів у державах-членах Європейського Союзу після запровадження Директиви ЄС 2019/1937 про захист осіб, які повідомляють про порушення права Союзу. Звіт аналізує не лише формальне виконання вимог Директиви на законодавчому рівні, але й фактичну ефективність створених механізмів захисту, здатність держав забезпечувати безпечні канали повідомлення про правопорушення, захищати викривачів від репресій та гарантувати належне реагування на отриману інформацію.

[6] https://files.transparencycdn.org/images/How-effective-is-whistleblower-protection-in-the-EU_Report.pdf

Автори виходять із того, що викривачі є одним із найважливіших елементів сучасної системи доброчесності, оскільки саме завдяки їхнім повідомленням суспільство отримує інформацію про корупцію, фінансові зловживання, шахрайство, порушення прав людини, екологічні злочини, нецільове використання бюджетних коштів та інші форми неправомірної діяльності, які часто залишаються поза увагою традиційних механізмів державного контролю.

У документі наголошується, що попри стратегічне значення викривачів для забезпечення верховенства права, демократичного врядування та підзвітності державних інституцій, рішення повідомити про правопорушення продовжує супроводжуватися значними особистими ризиками. Викривачі нерідко стикаються зі звільненням, пониженням у посаді, втратою доходів, дисциплінарними стягненнями, судовими позовами, репутаційними втратами, психологічним тиском та соціальною ізоляцією. Автори окремо звертають увагу на гендерний аспект проблеми, зазначаючи, що жінки можуть стикатися з додатковими перешкодами під час повідомлення про порушення через нерівність у доступі до керівних посад, ризик дискредитації, професійних обмежень або недовіри до їхніх повідомлень. Також підкреслюється, що представники інших вразливих груп населення можуть зазнавати непрямих форм репресій, які складніше виявити та довести.

Значна частина дослідження присвячена аналізу процесу транспозиції Директиви ЄС 2019/1937 до національного законодавства держав-членів. Звіт демонструє, що процес гармонізації законодавства відбувався повільно та нерівномірно. Більшість країн не змогли виконати вимоги Директиви у встановлені строки, а деякі держави ухвалили відповідне законодавство із затримкою в декілька років. Водночас навіть після прийняття національних законів численні країни були змушені переглядати свої нормативні акти через виявлені прогалини, зауваження Європейської Комісії або проблеми практичного застосування. Автори доходять висновку, що основні труднощі пов’язані не стільки з відсутністю законодавства, скільки з його неповною або неправильною імплементацією, а також зі слабким механізмом реалізації на практиці.

Документ детально аналізує інституційну архітектуру захисту викривачів у країнах ЄС. Встановлено, що держави використовують різні моделі організації системи приймання та розгляду повідомлень. Частина країн створила спеціалізовані органи із захисту викривачів, тоді як інші розподілили відповідні повноваження між антикорупційними органами, омбудсменами, органами захисту персональних даних, правоохоронними структурами або регуляторами окремих секторів. Така різноманітність моделей призвела до суттєвих відмінностей у спроможності держав забезпечувати ефективний захист. У багатьох країнах спостерігається фрагментація повноважень, дублювання функцій між різними органами, недостатня координація та складність для потенційних викривачів у визначенні належного каналу повідомлення. Додатковими проблемами залишаються обмежені фінансові та кадрові ресурси, нестача спеціалізованої підготовки працівників та недостатні повноваження щодо застосування заходів захисту або санкцій до осіб, які здійснюють переслідування викривачів.

Особливу увагу приділено питанню компенсації та відшкодування шкоди, завданої викривачам унаслідок репресій. Звіт розглядає принцип повного відновлення становища особи, який закладений у Директиві та передбачає повернення викривача до стану, в якому він перебував би за відсутності негативних наслідків повідомлення про порушення. Йдеться не лише про виплату компенсації, але й про поновлення на роботі, скасування незаконних дисциплінарних заходів, відновлення кар’єрних можливостей, компенсацію моральної шкоди та відшкодування витрат на юридичний захист. Однак аналіз показує, що в більшості держав ці механізми залишаються неповними або малоефективними. Реальні приклади успішного поновлення викривачів на роботі є поодинокими, а судові процедури часто є тривалими та фінансово обтяжливими.

Окремий розділ присвячений принципу доведення, який розглядається як одна з ключових гарантій ефективного захисту викривачів. Відповідно до цього принципу, якщо після повідомлення про порушення особа зазнає негативних наслідків, саме роботодавець або інша

сторона повинна довести відсутність зв'язку між вжитими заходами та фактом викриття. Документ демонструє, що багато країн або неповністю перенесли цей механізм у національне законодавство, або застосовують його занадто вузько через судову практику. У результаті викривачі часто змушені самостійно доводити причинно-наслідковий зв'язок між повідомленням і репресіями, що істотно знижує рівень їхнього захисту.

Значний обсяг дослідження присвячений питанням санкцій за порушення законодавства про захист викривачів. Автори констатують, що між державами-членами існують суттєві відмінності щодо видів, розмірів та порядку застосування санкцій. У багатьох випадках штрафи є надто низькими для виконання стримувальної функції або взагалі майже не застосовуються. Крім того, компетентні органи часто не мають достатніх повноважень для оперативного реагування на випадки переслідування викривачів, що негативно впливає на довіру до системи захисту.

Висновки:

- **Державам-членам необхідно забезпечити повну імплементацію принципу доведення та механізмів повного відшкодування шкоди,** включаючи поновлення на роботі, компенсацію матеріальних і нематеріальних збитків та застосування тимчасових заходів захисту до завершення судового розгляду.
- **Ефективність систем захисту викривачів безпосередньо залежить від наявності незалежних, належно профінансованих і наділених реальними повноваженнями органів,** здатних приймати повідомлення, розглядати скарги на репресії та застосовувати санкції до порушників.
- **Організації громадянського суспільства фактично стали ключовим елементом підтримки викривачів у багатьох країнах ЄС,** тому їхня роль повинна бути офіційно інтегрована до національних систем захисту із забезпеченням належного фінансування та інституційної підтримки.
- **Для належного моніторингу ефективності системи захисту викривачів доцільно забезпечити** регулярний збір і публікацію інформації про результати розгляду повідомлень, випадки застосування заходів впливу до викривачів, притягнення винних осіб до відповідальності та практику застосування механізмів захисту.

Документ також розглядає функціонування внутрішніх каналів повідомлення про порушення у державному та приватному секторах. Попри те, що Директива покладає обов'язок створення внутрішніх механізмів повідомлення на широкий спектр організацій, фактичний рівень виконання цих вимог залишається нерівномірним. У багатьох випадках створені канали мають формальний характер, не забезпечують належної конфіденційності або не гарантують своєчасного реагування на отримані повідомлення. Також виявлено недостатній рівень контролю за виконанням вимог законодавства щодо організації внутрішніх систем викривання.

Важливе місце у звіті займає аналіз механізмів консультаційної, юридичної, фінансової та психологічної підтримки викривачів. Автори наголошують, що більшість країн ЄС не створили повноцінних систем незалежної допомоги особам, які повідомляють про порушення. Унаслідок цього значну частину функцій підтримки взяли на себе організації громадянського суспільства, які надають юридичні консультації, допомагають із підготовкою повідомлень, забезпечують представництво інтересів викривачів та здійснюють моніторинг реалізації законодавства. Документ підкреслює, що роль таких організацій залишається критично важливою для функціонування систем захисту викривачів, однак у більшості країн вона не закріплена належним чином на інституційному рівні та не забезпечена стабільним фінансуванням.

Завершальна частина дослідження присвячена питанням моніторингу, збору статистичних даних та оцінки ефективності систем захисту викривачів. Автори наголошують, що значна

частина держав-членів не здійснює системного збору інформації про кількість повідомлень, результати їх розгляду, випадки застосування санкцій або заходів захисту. Особливо критичною проблемою є відсутність гендерної статистики та даних щодо різних соціальних груп, що унеможливлює оцінку рівня доступності та ефективності захисту для різних категорій населення.

Загалом звіт доходить висновку, що Європейський Союз створив одну з найбільш прогресивних нормативних основ захисту викривачів у світі, однак реальна ефективність цих механізмів залишається обмеженою через неповну імплементацію законодавства, слабкість інституційних механізмів, недостатній рівень ресурсного забезпечення та відсутність системного контролю за практичним виконанням встановлених гарантій захисту.

Грошові перекази та фінансова безпека: практичні механізми виявлення підозрілих операцій [7]

Практичний методичний посібник, підготовлений Координаційним органом Швеції з питань протидії відмиванню коштів та фінансуванню тероризму для постачальників послуг з переказу коштів, спрямований на підвищення рівня обізнаності суб'єктів ринку щодо ризиків використання сервісів грошових переказів для легалізації злочинних доходів та фінансування тероризму, а також роз'яснення практичних обов'язків, які випливають із законодавства у сфері ПВК/ФТ. Документ поєднує нормативні вимоги, практичні рекомендації, опис типових схем зловживань та перелік індикаторів ризику, які можуть свідчити про використання платіжної інфраструктури в незаконних цілях.

У документі наголошується, що сектор грошових переказів посідає особливе місце серед фінансових послуг через низку специфічних характеристик, які роблять його привабливим для злочинців. На відміну від традиційних банківських послуг, переказ коштів часто може здійснюватися без відкриття платіжного рахунку як для відправника, так і для отримувача. Така модель дозволяє значно ускладнити встановлення зв'язку між особою та коштами, що створює додаткові можливості для приховування злочинного походження активів. Окремо підкреслюється, що у Швеції внаслідок поступового скорочення використання готівки банківським сектором злочинні угруповання дедалі активніше використовують альтернативні канали для переміщення та маскування готівкових коштів, серед яких сервіси міжнародних грошових переказів відіграють важливу роль. Поєднання готівкових операцій, транскордонного характеру переказів та розгалужених агентських мереж формує підвищений рівень ризику використання цих сервісів для відмивання коштів і фінансування тероризму.

Значна частина документа присвячена поясненню нормативної бази та регуляторних вимог. Автори наголошують, що діяльність провайдерів переказу коштів підлягає регулюванню відповідно до Закону Швеції про запобігання відмиванню коштів та фінансуванню тероризму, нормативних актів Шведської служби фінансового нагляду та європейського законодавства щодо супроводження переказів інформацією про платників та отримувачів. Документ підкреслює, що надання послуг з переказу коштів є ліцензованою діяльністю, а суб'єкти ринку повинні відповідати встановленим вимогам фінансового нагляду. Особливу увагу приділено неформальним системам переказу коштів, зокрема системі «hawala», яка може функціонувати на законних підставах лише за умови отримання відповідного дозволу та дотримання вимог законодавства у сфері ПВК/ФТ. Водночас підкреслюється, що саме такі альтернативні системи можуть створювати додаткові ризики через складність відстеження руху коштів та можливість здійснення розрахунків без фактичного переміщення грошей між юрисдикціями.

Ключовою концепцією документа є ризик-орієнтований підхід, який розглядається як основа всієї системи внутрішнього контролю. Провайдери грошових переказів зобов'язані

[7] https://polisen.se/siteassets/dokument/om-polisen/penningtvatt/penningoverforaren_a5_2025_uk_ta.pdf/download/?v=cb6c43540263d028e17f51dc680e8a13

здійснювати комплексну загальну оцінку ризиків, що охоплює продукти та послуги, клієнтську базу, канали надання послуг, географічні фактори та діяльність агентів. Підкреслюється, що оцінка ризиків не повинна бути формальним документом, а має постійно оновлюватися відповідно до змін у бізнес-моделі, ризиковому середовищі та нових загрозах, які ідентифікують правоохоронні та наглядові органи. Саме результати такої оцінки повинні визначати структуру внутрішніх політик, процедур контролю, механізмів моніторингу та заходів з управління ризиками. Особливо важливою є вимога враховувати ризики, пов'язані з діяльністю агентів, включаючи їхнє розташування, характер операцій та особливості клієнтської бази.

Документ детально розкриває питання оцінки ризику клієнтів та належної перевірки. Провайдери повинні формувати індивідуальний ризиковий профіль кожного клієнта на основі доступної інформації та результатів загальної оцінки ризиків. Перед встановленням ділових відносин необхідно здійснювати ідентифікацію та верифікацію особи клієнта, перевіряти наявність статусу політично значущої особи, з'ясовувати мету та очікуваний характер використання послуг. Важливою особливістю є встановлення порогового значення у 1000 євро для проведення заходів належної перевірки під час разових операцій, причому документ окремо наголошує на необхідності враховувати пов'язані між собою транзакції, які можуть бути штучно розділені для обходу контролю. Якщо суб'єкт не може отримати достатньо інформації для розуміння діяльності клієнта та належного управління ризиками, встановлення або продовження ділових відносин є неприпустимим.

Окремий блок присвячений постійному моніторингу клієнтів та операцій. Автори підкреслюють, що фінансовий моніторинг не завершується після проведення первинної перевірки, а повинен тривати протягом усього періоду взаємодії з клієнтом. Провайдери повинні аналізувати відповідність операцій відомому профілю клієнта, виявляти незвичні транзакції, зміни у фінансовій поведінці та операції, які можуть свідчити про відмивання коштів або фінансування тероризму. Рівень моніторингу має залежати від ризик профілю клієнта: клієнти з підвищеним ризиком потребують значно інтенсивнішого контролю та частішого перегляду інформації. Документ підкреслює, що обов'язок повідомлення про підозрілу діяльність виникає не після встановлення факту злочину, а вже за наявності обґрунтованої підозри. Такий підхід відповідає міжнародним стандартам FATF та спрямований на своєчасне виявлення потенційно незаконної діяльності.

Важливе місце займає роз'яснення вимог щодо подання повідомлень до Підрозділу фінансової розвідки. Документ наголошує, що провайдери не мають права проводити операції, якщо існує підозра щодо їх зв'язку з відмиванням коштів або фінансуванням тероризму, за винятком випадків, коли відмова від проведення операції може завадити розслідуванню. При цьому повідомлення підлягають поданню навіть у разі відмови від здійснення операції або припинення ділових відносин. Особливу увагу приділено забороні інформування клієнта про проведення заходів фінансового моніторингу або факт подання повідомлення про підозрілу діяльність до підрозділу фінансової розвідки, що відповідає міжнародному принципу заборони розголошення інформації про здійснення відповідних перевірок. Документ також містить практичні інструкції щодо використання системи goAML для подання повідомлень про підозрілу діяльність.

Окремий напрям документа стосується внутрішнього контролю та кадрової політики. Провайдери повинні впроваджувати процедури оцінки доброчесності працівників, які залучені до виконання функцій ПВК/ФТ, а також забезпечувати регулярне навчання персоналу. Підготовка працівників має включати знання законодавства, внутрішніх процедур, результатів оцінки ризиків та практичних методів виявлення підозрілої діяльності. Таким чином, система ПВК/ФТ розглядається не лише як набір процедур, а як комплексна система управління ризиками, яка значною мірою залежить від професійної підготовки персоналу та корпоративної культури контролю.

Суттєва частина документа присвячена практичним прикладам ризиків та типологій. Автори детально описують використання готівки як одного з головних інструментів легалізації злочинних доходів, оскільки значна частина злочинної діяльності, включаючи наркоторгівлю, торгівлю зброєю, торгівлю людьми та різноманітні шахрайські схеми, генерує великі обсяги готівкових коштів. Розглядаються випадки використання підставних осіб та номінальних відправників чи отримувачів коштів, застосування підроблених документів, проведення операцій від імені третіх осіб та інші механізми приховування справжніх учасників фінансових операцій. Значна увага приділяється схемам дроблення платежів для обходу порогових значень фінансового моніторингу, коли кілька осіб надсилають кошти одному отримувачу або одна особа використовує різні платіжні системи для переказу коштів тому самому адресату. Документ також наголошує на ризиках використання інших платіжних послуг, таких як внесення готівки на рахунки, здійснення платежів через платіжні системи чи зняття готівки, які можуть використовуватися для інтеграції злочинних доходів у легальну економіку.

Особливий інтерес становить розділ, присвячений фінансуванню тероризму. Документ наголошує, що послуги грошових переказів можуть використовуватися для переміщення коштів до зон конфліктів, осередків діяльності терористичних організацій та країн із високим рівнем ризику. Автори звертають увагу на те, що фінансування тероризму часто не пов’язане зі значними сумами коштів і може здійснюватися за рахунок цілком законних джерел доходів. Визначальним фактором є не походження коштів, а їхнє кінцеве призначення. Підкреслюється, що навіть невеликі перекази можуть використовуватися для підтримки терористичних організацій, вербування, навчання або підготовки терористів. Окремо зазначається, що неформальні системи переказів типу «hawala» створюють додаткові ризики через можливість забезпечення анонімності учасників операцій, переказу коштів до юрисдикцій під санкціями та роботи в регіонах із недостатньо розвиненою фінансовою інфраструктурою.

Висновки:

- **Провайдери грошових переказів повинні розглядатися як сектор підвищеного ризику ВК/ФТ.** Поєднання готівкових операцій, транскордонних переказів, агентських мереж та можливості здійснювати операції без відкриття рахунків створює суттєві ризики відмивання коштів і фінансування тероризму.
- **Ефективна система ПВК/ФТ має базуватися на ризик-орієнтованому підході та безперервному моніторингу.** Загальна оцінка ризиків, індивідуальні ризик профілі клієнтів, належна перевірка та постійний контроль операцій є ключовими елементами управління ризиками.
- **Порогові значення не повинні бути єдиним критерієм контролю.** Злочинці активно використовують дроблення операцій, підставних осіб та множинні канали переказів для обходу вимог ідентифікації, тому моніторинг має орієнтуватися насамперед на поведінкові індикатори.
- **Для протидії фінансуванню тероризму критично важливим є контроль навіть невеликих транзакцій.** На відміну від відмивання коштів, джерело походження коштів може бути законним, а визначальним фактором є кінцева мета використання коштів, зокрема їх спрямування на підтримку терористичних організацій чи діяльності у зонах конфліктів.

Завершальна частина документа містить систематизований перелік індикаторів ризику, які повинні привертати увагу працівників. До них належать підозріла поведінка клієнтів, неможливість підтвердження особи, використання сумнівних документів, проживання в країнах високого ризику, регулярні перекази без зрозумілої економічної мети, різкі зміни у фінансовій поведінці, відправлення коштів особам, з якими клієнт не має очевидного зв’язку, небажання пояснювати

походження коштів або мету переказу, а також спроби уникнути перевірок шляхом поділу операцій на менші суми.

Документ наголошує, що жоден індикатор сам по собі не є доказом злочину, проте їх наявність повинна слугувати підставою для поглибленого аналізу та, за необхідності, подання повідомлення про підозрілу діяльність. Загалом документ формує комплексне бачення ризиків, характерних для сектору грошових переказів, та демонструє практичний підхід до впровадження ризик-орієнтованої системи ПВК/ФТ, спрямованої на своєчасне виявлення і запобігання використанню платіжної інфраструктури у злочинних цілях.

Від формальної відповідності до практичної ефективності: новий етап моніторингу міжнародної податкової прозорості [8]

Документ, підготовлений Глобальним форумом ОЕСР з питань прозорості та обміну інформацією для податкових цілей, присвячений оцінці рівня виконання міжнародного стандарту прозорості та обміну інформацією на запит (EOIR) і відображає результати першого раунду нового механізму посиленого моніторингу, який замінив традиційну систему щорічного нагляду за виконанням рекомендацій.

Звіт демонструє еволюцію міжнародної системи податкової прозорості від етапу створення законодавчих механізмів до етапу оцінювання їхньої фактичної ефективності та практичного застосування. Основною метою документа є визначення того, наскільки юрисдикції не лише формально імплементували міжнародні вимоги щодо прозорості та обміну інформацією, а й забезпечують реальне функціонування відповідних механізмів у щоденній діяльності компетентних органів.

У документі наголошується, що стандарт EOIR залишається одним із ключових інструментів міжнародної боротьби з ухиленням від оподаткування, приховуванням активів за кордоном та використанням непрозорих корпоративних структур. Стандарт базується на положеннях Модельної угоди ОЕСР про обмін інформацією з податкових питань, статті 26 Модельної податкової конвенції ОЕСР та відповідних положеннях Конвенції ООН. Його основою є принцип надання компетентним органам інших держав інформації, яка є передбачувано релевантною для адміністрування та забезпечення виконання податкового законодавства. Для цього кожна юрисдикція повинна забезпечити доступність інформації про власників компаній, кінцевих бенефіціарних власників, бухгалтерську документацію та банківські дані, а також створити механізми оперативного доступу до такої інформації і її передачі іноземним партнерам у відповідь на обґрунтовані запити.

Значна частина звіту присвячена поясненню нової моделі посиленого моніторингу, яка була запроваджена після завершення двох раундів комплексних взаємних оцінок юрисдикцій. Глобальний форум дійшов висновку, що більшість його учасників уже створили базові законодавчі механізми для реалізації стандарту EOIR, тому подальше проведення повномасштабних циклів перевірок для всіх країн є менш доцільним. Натомість було впроваджено систему безперервного моніторингу, яка дозволяє регулярно оцінювати прогрес у виконанні раніше наданих рекомендацій, аналізувати нові законодавчі зміни, враховувати інформацію від партнерських юрисдикцій та оперативно реагувати на випадки погіршення ситуації або виникнення нових ризиків. При цьому повноцінні поглиблені перевірки зберігаються як інструмент для окремих випадків, коли моніторинг виявляє суттєві проблеми або відсутність прогресу протягом тривалого часу.

Документ підкреслює практичну значущість міжнародного обміну інформацією на запит. За даними Глобального форуму, у 2024 році 139 юрисдикцій активно використовували механізм

[8] https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/enhanced-monitoring-report-on-the-implementation-of-the-standard-on-transparency-and-exchange-of-information-on-request-2026-update-june_959f4b86/9ef50941-en.pdf

EOIR та направили запити щодо щонайменше 32 тисяч платників податків. Від моменту створення сучасної системи податкової прозорості у 2009 році держави повідомили про виявлення понад 19 млрд євро додаткових податкових надходжень завдяки використанню міжнародного обміну інформацією. Таким чином, EOIR розглядається не лише як інструмент міжнародного співробітництва, а й як важливий механізм мобілізації внутрішніх доходів держав та протидії агресивному податковому плануванню, приховуванню доходів і транскордонним схемам ухилення від оподаткування.

У межах першого раунду посиленого моніторингу було проаналізовано 39 юрисдикцій, для яких завершено другий раунд взаємних оцінок. Загалом розглянуто 217 рекомендацій, із яких 76 стосувалися законодавчих і нормативних недоліків, а 141 – практичної реалізації встановлених вимог. Звіт демонструє позитивну динаміку виконання рекомендацій. Близько третини рекомендацій уже визнані виконаними, понад половина перебувають у процесі реалізації, а лише незначна частина залишилася без суттєвого прогресу. Такий результат свідчить про поступове підвищення рівня відповідності міжнародним стандартам та ефективність нового підходу до моніторингу, який забезпечує постійний тиск на юрисдикції щодо усунення виявлених недоліків.

Одним із центральних напрямів аналізу є забезпечення доступності інформації про кінцевих бенефіціарних власників. У документі зазначається, що саме прозорість структури бенефіціарної власності залишається одним із ключових викликів для міжнародної податкової системи. Багато юрисдикцій за останні роки створили централізовані реєстри бенефіціарної власності або модернізували вже існуючі системи. Водночас Глобальний форум наголошує, що сам факт створення реєстру не є достатнім. Критичне значення мають повнота охоплення юридичних осіб, актуальність даних, достовірність інформації та наявність ефективних механізмів перевірки. У багатьох випадках державам рекомендовано перейти до багатоканального підходу, коли інформація про бенефіціарних власників підтверджується через декілька незалежних джерел, що підвищує її надійність та знижує ризики використання підставних осіб і складних корпоративних структур для приховування справжніх власників активів.

Суттєву увагу приділено питанням доступності бухгалтерської інформації. Аналіз показує, що низка юрисдикцій продовжує стикатися з проблемами щодо забезпечення належного ведення бухгалтерського обліку, зберігання первинної документації та своєчасного доступу до неї з боку компетентних органів. Особливі труднощі виникають у випадках ліквідації компаній або припинення їх діяльності, коли документи можуть втрачатися або ставати недоступними для перевірки. Глобальний форум підкреслює, що наявність чітких вимог щодо збереження бухгалтерських записів та ефективний нагляд за їх виконанням є критично важливими для забезпечення можливості подальшого міжнародного обміну інформацією та проведення податкових розслідувань.

Важливим елементом звіту є оцінка фактичної ефективності міжнародного обміну інформацією. Для цього аналізуються статистичні показники щодо обробки запитів, строки надання відповідей, якість комунікації між компетентними органами та відгуки партнерських юрисдикцій. За результатами моніторингу встановлено, що 39 юрисдикцій отримали майже 18,5 тисяч запитів у 2023–2024 роках. У середньому 70% таких запитів були виконані протягом 90 днів, а ще 14% – протягом 180 днів.

Більшість держав покращили організаційні процедури, кадрове забезпечення та механізми внутрішньої координації, що позитивно вплинуло на швидкість та якість міжнародного співробітництва. Разом із тим окремі країни продовжують демонструвати проблеми із дотриманням строків, своєчасним інформуванням партнерів про хід виконання запитів та наданням необхідних уточнень щодо отриманої інформації.

Особливу роль у новій системі моніторингу відіграє механізм отримання інформації від партнерських юрисдикцій. У межах першого циклу було отримано понад 800 повідомлень від 53 членів Глобального форуму щодо практичного досвіду обміну інформацією з

Висновки:

- **Більшість юрисдикцій демонструють прогрес у виконанні стандарту EOIR:** із 217 проаналізованих рекомендацій 32% уже визнані виконаними, а ще 51% перебувають у процесі реалізації, що свідчить про загальне підвищення рівня міжнародної податкової прозорості.
- **Найважливішим напрямом реформ залишається забезпечення доступності та достовірності інформації про кінцевих бенефіціарних власників,** включаючи створення та вдосконалення централізованих реєстрів КБВ.
- **Основними невирішеними проблемами залишаються контроль за веденням і збереженням бухгалтерської документації,** особливо щодо неактивних або ліквідованих юридичних осіб, а також ефективність наглядових механізмів у цій сфері.
- **Подальше підвищення ефективності міжнародного обміну інформацією потребує** покращення оперативності відповідей на запити, системної комунікації між компетентними органами та своєчасного інформування партнерів про хід опрацювання запитів.

юрисдикціями, щодо яких здійснюється посилений моніторинг виконання стандарту EOIR. Більшість таких відгуків містили позитивну оцінку якості співробітництва, однак частина з них дозволила виявити окремі системні проблеми, які не були очевидними під час аналізу законодавства або самооцінок держав. Саме на основі таких сигналів Глобальний форум у деяких випадках формулював нові рекомендації або переводив юрисдикції до режиму більш інтенсивного нагляду. Документ підкреслює, що ефективність стандарту EOIR значною мірою залежить не лише від формальних норм права, а й від рівня довіри та якості взаємодії між податковими адміністраціями різних країн.

Загалом звіт відображає формування нового етапу розвитку глобальної системи податкової прозорості, у межах якого акцент поступово зміщується від оцінки формальної відповідності законодавства до аналізу фактичної ефективності механізмів доступу до інформації, прозорості структури власності, достовірності даних про кінцевих бенефіціарних власників, належного ведення бухгалтерського обліку та результативності міжнародного обміну податковою інформацією. Документ підтверджує тенденцію до посилення уваги міжнародної спільноти не лише до наявності нормативно-правових механізмів, а й до їх практичного застосування та здатності забезпечувати своєчасне отримання, перевірку й передачу інформації, необхідної для протидії транскордонному ухиленню від оподаткування, приховуванню активів і використанню непрозорих корпоративних структур.

Звіти окремих інституцій та експертів

Тіньова економіка та кримінальні мережі в Центральноафриканській Республіці [9]

Дослідження, проведене Глобальною ініціативою проти транснаціональної організованої злочинності (GI-TOC), детально розкриває механізми функціонування кримінальної екосистеми в Центральноафриканській Республіці.

Ця країна, яка вже тривалий час перебуває в стані перманентної кризи та часто характеризується як неспроможна держава, перетворилася на ключовий вузол

[9] https://globalinitiative.net/wp-content/uploads/2026/06/Nathalia-Dukhan-and-Ruben-De-Koning-Malicious-markets-Mapping-the-violent-ecosystem-in-the-Central-African-Republic-GI-TOC-June-2026-1.pdf

транснаціональної злочинності, де політична влада, військові структури та кримінальні мережі злилися в єдиний механізм хижацького контролю над ресурсами та населенням.

Дослідження констатує, що за останні п'ять років відбулася фундаментальна трансформація: від фрагментованого контролю численних озброєних угруповань, які колись домінували на понад вісімдесяти відсотках території, до більш централізованої та ієрархічної системи, що вибудовується навколо президента Фостена-Аршанжа Туадера та його ключового союзника – російської «Групи Вагнера». Цей альянс, попри міжнародні санкції та ребрендинг в «Африканський корпус», продовжує визначати силовий та економічний ландшафт країни, інтегруючи колишніх повстанців до державних структур та використовуючи насильство як основний інструмент ринкового контролю.

Центральноафриканська Республіка стала ареною жорсткого геополітичного протистояння, де традиційні партнери, такі як Франція та Європейський Союз, поступово витісняються новими гравцями – росією, Руандою, Об'єднаними Арабськими Еміратами та дедалі більше Туреччиною. Цей зсув балансу сил призвів до того, що забезпечення безпеки було де-факто приватизоване та передане транснаціональним кримінальним структурам, які інтегрувалися в державний апарат, зайнявши ключові позиції в міністерствах, силових відомствах, митній службі та стратегічних ресурсних секторах. Автори звіту наголошують, що доступ до природних багатств, зокрема золота, алмазів, лісу та худоби, тепер жорстко прив'язаний до політичної лояльності та готовності співпрацювати з режимом.

Ключовим інструментом підтримки режиму є контроль над потоками озброєнь, які надходять до країни в обхід міжнародних санкцій. Незважаючи на діюче з 2013 року ембарго ООН на постачання зброї до Центральноафриканської Республіки, ці обмеження систематично порушуються, особливо після початку масштабного контрнаступу за участі Групи Вагнера у 2021 році. Звіт фіксує безпрецедентне збільшення кількості та складності озброєнь, що використовуються у конфлікті, включно з важкими кулеметами, переносними зенітними комплексами, протитанковими ракетами та навіть реактивними системами залпового вогню, встановленими на гелікоптери. Це призводить до зростання кількості жертв серед цивільного населення, адже удари часто завдаються по густонаселених районах, ринках та таборах для переміщених осіб. Особливе занепокоєння викликає використання групою Вагнера бойової авіації, зокрема гелікоптерів Мі-8, оснащених ракетними блоками Б-8В20А, для повітряних бомбардувань повстанських баз, шахт та сіл, що свідчить про свідому ескалацію насильства та перетворення військових операцій на інструмент економічного тиску.

Поряд зі зброєю, критичними елементами, що живлять конфлікт та забезпечують мобільність військ, стали паливо та синтетичні наркотики, зокрема трамадол.

Внутрішній ринок пального, який мав би бути джерелом стабільних бюджетних надходжень, був повністю захоплений державно-злочинним картелем, що діє під прикриттям монополії. Надання ексклюзивного права на імпорт камерунській компанії Neptune Oil, яке порушило чинне законодавство про лібералізацію ринку, дозволило штучно завищувати ціни на пальне за допомогою маніпуляцій з міжнародними котируваннями та незаконних податкових пільг. За оцінками незалежного аудиту, проведеного на вимогу Міжнародного валютного фонду, ці зловживання принесли компанії та пов'язаним з нею посадовцям від 31 до 40 мільйонів доларів США незаконного прибутку лише у 2024 році. Ці надприбутки використовуються для фінансування силових структур та збагачення наближених до влади осіб, включно з дружиною начальника штабу армії, якій передано у власність конфісковані заправки. Паралельно Група Вагнера створила власний незалежний ланцюг постачання пального через компанію Petrolex, зареєстровану в країні, що фактично дозволяє їй вести автономну військову та економічну діяльність, не залежачи від державної монополії та отримуючи паливо з пільговим режимом оподаткування.

Ще одним смертоносним "інструментом війни" став трамадол, неконтрольоване споживання якого набуло масштабів епідемії. Як зазначається у звіті, контроль над цим високоприбутковим ринком останніми роками перейшов від озброєних угруповань до вищих

військових чиновників, які організували постачання через річку Убангі з Демократичної Республіки Конго, що вказує на глибоку системну криміналізацію державного апарату та використання наркотрафіку як джерела додаткового фінансування та політичного контролю.

Фінансовим двигуном цієї кримінальної системи є вивезення природних ресурсів, насамперед золота, яке стало найбільш динамічним та прибутковим товаром у країні. Якщо раніше золото видобувалося кустарним способом у зонах, контрольованих повстанцями, і вивозилося контрабандою через сусідні країни, то після 2021 року відбулася його кардинальна централізація. Група Вагнера через свої компанії, такі як Midas Ressources, захопила найбагатші копальні, включаючи родовище Ндассіма поблизу Бамбарі з оцінюваними запасами в 2,8 мільярда доларів США, вигнавши звідти як повстанців, так і кустарних старателів із застосуванням насильства та погроз. Ці концесії стали фактично приватними анклавами, повністю недоступними для державного контролю, де видобуток ведеться з грубими порушеннями прав людини та екологічних норм, а будь-які спроби чиновників провести перевірку жорстко припиняються, іноді з погрозами фізичної розправи.

Офіційного експорту з цих копалень майже не декларується, а весь видобутий метал вивозиться контрабандно двома основними каналами: через місцеві компанії-експортери, пов'язані з Групою Вагнера, такі як Sigma Gold, або безпосередньо військово-транспортними, які використовуються для перевезення персоналу та вантажів. Оціночний обсяг виробництва лише на копальні Ндассіма становить близько 5 тонн золота на рік вартістю понад 250 мільйонів доларів США, що майже дорівнює всьому легальному видобутку країни. Попри це, компанія Midas Ressources сплатила до державного бюджету лише близько 42 тисяч доларів податків, тоді як мала б виплатити роялті на суму понад 7,5 мільйонів доларів, що свідчить про колосальні втрати для держави. Золото з Центральноафриканської Республіки, як і з сусідніх країн, таких як Камерун та Чад, осідає в Об'єднаних Арабських Еміратах, які стали ключовим хабом для його відмивання та інтеграції у світові ринки, причому ці потоки часто супроводжуються грубим заниженням вартості експорту.

Висновки:

- **Держава перетворилася на кримінальний синдикат.** У Центральноафриканській Республіці органи влади, збройні сили та кримінальні мережі злилися в єдину систему, де доступ до ресурсів, посад і прибутків жорстко прив'язаний до політичної лояльності.
- **Група Вагнера є стрижнем економічного та військового контролю.** Російські найманці не лише забезпечують безпеку режиму, але й захопили ключові видобувні активи, зокрема золоті родовища.
- **Ресурсні ринки монополізовані через насильство та корупцію.** Паливний картель, очолюваний камерунською компанією Neptune Oil, приносить до 40 млн доларів незаконних надприбутків на рік завдяки штучному завищенню цін і податковим пільгам.
- **Криптовалютні авантюри створюють нові канали для відмивання коштів.** Президент Туадера ініціював випуск Sango Coin та SCAR, пропонуючи за них громадянство, землю та права на видобуток копалин без належних регуляторних механізмів. Це не лише підриває суверенітет і фінансову стабільність країни, але й відкриває широкі можливості для транснаціональних кримінальних мереж легалізувати доходи через непрозорі криптотранзакції.

Дослідження також проливає світло на механізми політичної інкорпорації, які використовуються урядом для консолідації контролю та послаблення збройної опозиції. Колишні польові командири озброєних угруповань, таких як UPC та 3R, що раніше кидали виклик владі в Бангі, тепер інтегровані до урядових структур, отримуючи міністерські портфелі та інші високі посади в обмін на лояльність та допомогу в територіальній реконкісті.

Додатковим викликом, що підриває суверенітет країни та створює нові ризики, є ризикована та непрозора фінансова політика уряду, зокрема захоплення криптовалютними авантюрами, ініційованими особисто президентом Туадера. У відповідь на міжнародну ізоляцію, скорочення бюджетної допомоги та нестачу ліквідності, президент ініціював низку проектів, включаючи створення власної криптовалюти Sango Coin та її послідовників, таких як мем-коїн SCAR. Як зазначають автори, ці ініціативи, реалізовані без належних регуляторних механізмів та з залученням осіб із сумнівною репутацією, створюють нові, ще більш непрозорі канали для відмивання грошей, незаконного збагачення та виснаження національних ресурсів. Пропозиції продавати громадянство, електронне резидентство, земельні ділянки та навіть права на видобуток корисних копалин за криптовалюту, яка не має реального забезпечення та відома своєю екстремальною волатильністю, фактично означає відчуження суверенних активів на користь неперевірених іноземних гравців. Це посилює залежність країни, підриває її фінансову стабільність та робить її надзвичайно вразливою до кримінального впливу та шахрайства, що викликало серйозну критику з Міжнародного валютного фонду та Конференції ООН з торгівлі та розвитку, які попередили про катастрофічні наслідки для економіки, що й так перебуває у кризовому стані.

На завершення, звіт малює похмуру картину країни, що потрапила в пастку, де транснаціональна організована злочинність та політичне насильство стали невід'ємними елементами системи управління. Фактичне функціонування держави ґрунтується на зловживаннях, корупції та використанні насильства для контролю над ресурсами, де державний апарат дедалі більше виконує функції кримінального синдикату, а не легітимної інституції.

Документ підкреслює, що для будь-якої міжнародної допомоги та спроб стабілізації необхідно визнати цю жорстоку реальність і розробляти комплексні стратегії, спрямовані не на формальну підтримку інституцій, а на системну боротьбу з організованою злочинністю, яка пустила коріння в самому серці держави, включаючи посилення контролю за фінансовими потоками, відновлення прозорості у видобувних галузях, реформу сектору безпеки з акцентом на боротьбу з контрабандою та рекетом, а також притягнення до відповідальності ключових фігур, причетних до військових злочинів та системного пограбування країни.

Тіньова конвергенція: як Китайський державний апарат інструменталізує «геокримінальність» [10]

Сучасна епоха глобалізації та загострення геополітичної конкуренції докорінно змінили характер транснаціональної організованої злочинності, перетворивши її з суто кримінального феномену на інструмент державної стратегії.

Свіжі аналітичні дані свідчать про виникнення явища, яке отримало визначення «геокримінальність» – довготривала форма взаємодії, за якої держава толерує і навіть приховано підтримує злочинні мережі за кордоном, доки їхня діяльність приносить стратегічну вигоду.

Найбільш виразно ця модель проявляється у діях Китайської Народної Республіки (КНР) та керівної Комуністичної партії Китаю (КПК) у регіоні Південно-Східної Азії. На відміну від епізодичних, директивних кримінальних операцій, які частіше асоціюються з іншими геополітичними гравцями, на кшталт росії, китайська модель не передбачає прямого мікроменеджменту з Пекіна. Замість цього функціонує гнучка система, де кримінальні актори, прагнучи капіталізувати свій статус або уникнути переслідувань, добровільно та інтуїтивно діють у межах негласних ліній, що збігаються з довгостроковими геостратегічними цілями КНР.

[10] https://globalinitiative.net/wp-content/uploads/2026/06/Beyond-boundaries-The-Chinese-party-state-and-geocriminality-in-South-East-Asia-GI-TOC-June-2026.pdf

Головним інтерфейсом та провідником цього впливу на периферії виступає розгалужена система Єдиного фронту (United Front System) – мережа під керівництвом КПК, що мобілізує сили поза межами самої партії, включаючи бізнес-асоціації, культурні організації, діаспору та, як демонструють факти, елементи кримінального світу для просування інтересів Китаю за кордоном. Генеза цієї взаємодії має глибоке коріння в історії КПК, яка ще з часів Мао Цзедуна та пізніших етапів реформ залучала тріади та таємні товариства для стабілізації контролю чи розв'язання делікатних завдань. Проте за правління Сі Цзіньпіна фінансування та статус Департаменту роботи Єдиного фронту (UFWD) були безпрецедентно посилені, перетворивши його на потужну зброю зовнішнього впливу, яка абсорбувала тисячі нових кадрів і отримала міністерський статус найвищого рівня.

Технологічний прогрес та транснаціональні фінансові потоки глобалізації дозволили вивести ці практики на новий рівень. Пекін формує permissive environment – дозвільну екосистему, де кримінальні ділки отримують легітимність, маскуючись під офіційні економічні ініціативи типу «Один пояс, один шлях» (BRI) або Регіонального всеосяжного економічного партнерства (RCEP).

Критичний аналіз чотирьох ключових країн регіону – Таїланду, Філіппін, Малайзії та Індонезії – наочно демонструє, як локальні умови, слабкість інституцій та рівень корумпованості місцевих еліт визначають архітектуру та глибину проникнення цього геокримінального впливу.

У Таїланді яскравим прикладом такого переплетення інтересів стала діяльність Таїландсько-Азійської економічної обмінної асоціації, створеної у 2019 році як платформа для китайських бізнесменів. Ця структура від початку демонструвала ідеологічне вирівнювання з Пекіном, активно використовуючи партійні гасла, як-от заклик «добре розповідати історію Китаю», що є офіційною доктриною Сі Цзіньпіна щодо зовнішньої пропаганди. Керівництво асоціації підтримувало тісні контакти з департаментами Єдиного фронту провінційного рівня в КНР, а її очільники займали високі неофіційні посади в пов'язаних з державою структурах, наприклад, у Раді сприяння мирному возз'єднанню Китаю.

Проте за фасадом легітимної економічної дипломатії та благодійності ховалися глибокі зв'язки з кримінальним підпіллям. Офіси асоціації ділилися з нелегальним Центром культурного обміну Оверсіз Хунмен, який використовувався як ширма для китайської організованої злочинності. Ба більше, віцепрезидент цієї асоціації Ван Їчен виявився пов'язаним із сумнозвісним скам-комплексом KK Park на тайсько-м'янманському кордоні, через чиї криптовалютні рахунки пройшли десятки мільйонів доларів, отриманих від кібершахрайства та відмивання грошей. Кримінальні мережі Хунмен тривалий час виступали посередниками для блокчейн-проєктів іншого кримінального авторитета Ше Чжицзяна, інтегруючи нелегальні капітали в концепції «розумних міст» на кордоні. Водночас кримінальне розслідування щодо самого президента асоціації Лі Шенцзяо у справі про масштабну контрабанду м'яса на мільярди батів підкреслило гібридний характер цієї структури. Паралельно асоціація вибудовувала системні зв'язки з тайськими військовими та високопосадовцями кіберполіції, фінансуючи ремонти залів засідань та виступаючи радниками, що дозволяло кримінальним елементам купувати лояльність та убезпечувати себе від переслідувань.

Найбільш глибоке проникнення іноземного кримінального елемента в державні інституції було зафіксовано на Філіппінах, де геокримінальні інтереси Пекіна увійшли у пряме протиріччя між собою. Головною стратегічною метою Китаю в Манілі було нівелювання рішення Постійної палати третейського суду в Гаазі 2016 року щодо Південно-Китайського моря, яке визнало безпідставними територіальні претензії КНР. Для цього Пекін зробив ставку на зміщення фокусу відносин у площину масштабних інвестицій та торгівлі, чому посприяло обрання президентом Родріго Дутерте.

Ключовою фігурою у цьому процесі став китайський підприємець Майкл Янг, який з кінця 1990-х років вибудував тісні особисті відносини з Дутерте та зрештою отримав офіційний

статус радника президента з економічних питань. Янг координував діяльність понад 50 компаній, інтегруючи китайські державні залізничні гіганти, такі як CREC та CRCC, у філіппінську інфраструктуру.

Водночас, згідно з матеріалами, переданими до Міжнародного кримінального суду, Янг стояв у центрі транснаціонального синдикату, що займався виробництвом метамфетаміну в Мінданао, торгівлею людьми, фінансовими махінаціями та організацією нелегального грального бізнесу (POGO). Попри серйозні розслідування антинаркотичних служб, політичний дах блокував будь-яке переслідування Янга. Його партнер Аллан Лім, зафіксований спецслужбами як небезпечний наркоділок, паралельно брав участь у самітах «Один пояс, один шлях» у Гонконзі як офіційний представник торгової палати, де дипломатичні представники КНР обіцяли повне сприяння. Застосування корпоративного нашарування та підставних філіппінських громадян дозволило кримінальному синдикату Янга та Ліма проникнути у сферу державних закупівель медикаментів під час пандемії через компанію Pharmally, а також пов'язати свої інтереси з гучною справою ексмера Еліс Го (Го Хуапін), чий скам-хаб у Bamban став притулком для тисяч жертв торгівлі людьми. Це демонструє пастку системної геокримінальності: наділивши кримінальних авторитетів автономією для лобіювання геополітичного розвороту Філіппін від США, Пекін отримав неконтрольований сплеск онлайн-казино та відтоку капіталу з самого Китаю, що змусило китайську владу згодом розпочати вибіркове жорстке полювання на закордонні кримінальні осередки, коли репутаційні та фінансові втрати перевищили вигоду.

Малайзійський сценарій продемонстрував іншу модель геокримінальності – опортуністичне використання державою вже наявних корупційних та компрометуючих обставин усередині транснаціональних еліт. Етнічний китаєць малайзійського походження Джо Лоу став архітектором одного з найбільших фінансових пограбувань століття, привласнивши 4,5 мільярда доларів із суверенного фонду 1MDB, який безпосередньо контролював тодішній прем'єр-міністр Наджиб Разак. Коли у 2015-2016 роках корупційна схема була викрита міжнародними розслідувачами, уряд Наджиба опинився у критичній ізоляції. Пекін свідомо скористався відчаєм малайзійської верхівки. Через Джо Лоу китайська сторона уклала низку інфраструктурних угод на загальну суму 34 мільярди доларів, при цьому вартість проєктів була штучно завищена на 120-140%, щоб абсорбувати та покрити борги фонду 1MDB в обмін на геополітичну лояльність Куала-Лумпура та доступ до стратегічних морських шляхів. Після електорального краху Наджиба у 2018 році Китай надав Джо Лоу офіційний притулок та захист, розглядаючи його як унікального носія інформації про корупцію західних та глобальних еліт.

Інший малайзійський кейс Нікі Ляо, лідера фінансових схем та криптошахрайства, пов'язаного з мережею колишнього ватажка тріади 14K Вана Куок-коя («Зламаний Зуб»), продемонстрував, що навіть дрібні кримінальні елементи без глибокого політичного впливу легко вербуються структурами Єдиного фронту (наприклад, через UFWD провінції Хунань) завдяки фіктивній благодійності та купівлі титулів. Проте, на відміну від Філіппін, китайському криміналітету не вдалося закріпитися у вищих ешелонах малайзійського грального бізнесу через потужний опір місцевих етнічних малайзійсько кланів, які монополізували зв'язки з владою.

В Індонезії, яка традиційно дотримується політики неприєднання та балансування між світовими центрами сили, китайський геокримінальний вплив набув специфічного нормативно-регуляторного забарвлення. Замість класичних фігур організованої злочинності, на перший план вийшли великі китайські комерційні структури, що діють у капіталомісткому та слабко регульованому секторі видобутку металів та мінералів.

Гігант металургійної промисловості Tsingshan Holdings Group, що контролює Індустріальний парк Моровалі, користується всебічною підтримкою китайських державних банків та вищих дипломатів КНР, будучи флагманом концепції спільного майбутнього. Розслідування виявили на території парку катастрофічні порушення: від масштабного екологічного забруднення та

приховування мільйонів тонн відходів до використання нелегальної праці й навіть функціонування прихованого приватного аеропорту, який діяв шість років без митного та прикордонного контролю індонезійської влади. Для інтеграції у місцеве середовище Tsingshan залучив бізнес-мережі, пов'язані з впливовим відставним генералом Лухутом Бінсаром Панджайтаном, ключовим довіреною особою екпрезидента Відодо та архітектором економічної політики країни. Спільні інтереси призвели до ухвалення резонансного закону 2020 року, який суттєво послабив екологічні норми та права робітників, фактично декриміналізувавши та легалізувавши ті практики видобутку, які раніше вважалися протиправними. Ця колізія демонструє вищий ступінь геокримінальності, коли синергія іноземного державного капіталу та місцевої військово-політичної еліти трансформує саме законодавче поле країни, знімаючи кримінальну відповідальність заради гарантування безперебійного доступу Пекіна до стратегічної сировини.

Підсумовуючи, результати комплексного дослідження підтверджують, що системна геокримінальність Китаю функціонує як гнучка, адаптивна латентна мережа. Не вдаючись до централізованого мікроменеджменту кримінальних синдикатів, китайська партійно-державна машина створює умови, за яких транснаціональні злочинці змушені демонструвати свою корисність державним інтересам КНР для збереження власного бізнесу та безпеки. Головними каталізаторами вразливості країн Південно-Східної Азії залишаються хронічний брак ресурсів у правоохоронних органах, інституційна корупція та готовність національних еліт до змови.

Висновки:

- **Феномен системної геокримінальності:** КНР під керівництвом КПК використовує модель, за якої держава без прямого мікроменеджменту толерує та підтримує закордонні кримінальні мережі, доки їхня діяльність приносить стратегічну або економічну вигоду для Пекіна.
- **Єдиний фронт як інтерфейс впливу:** Розгалужена мережа інституцій Єдиного фронту (включаючи бізнес-асоціації, культурні групи та діаспори) слугує головним каналом взаємодії між китайським партійно-державним апаратом та закордонним криміналом.
- **Роль компрометації місцевих еліт:** Успіх та глибина проникнення китайського геокримінального впливу критично залежать від вразливості, корумпованості чи прямої залученості місцевих політичних та військових еліт.
- **Вибіркове правозастосування як важіль:** Пекін демонструє гнучкість, жорстко переслідуючи закордонні кримінальні елементи лише тоді, коли їхні дії починають завдавати КНР значних репутаційних збитків або провокують неконтрольований відтік капіталу.

Водночас єдиними ефективними інструментами протидії та стримування цього прихованого втручання виявляються незалежна журналістика, активне громадянське суспільство та механізми багатопартійної політичної конкуренції, які здатні витягти на світло тіньові альянси між державою та криміналом. Подальша безпекова динаміка в регіоні цілковито залежатиме від здатності міжнародної спільноти та локальних урядів вчасно розпізнавати кримінальний вимір у діяльності легальних на перший погляд інститутів та асоціацій Єдиного фронту.

Тіньові платіжні посередники в епоху санкційної війни [11]

Повномасштабне вторгнення росії в Україну в лютому 2022 року спричинило безпрецедентну санкційну хвилю з боку країн Заходу, що суттєво ускладнило міжнародну торгівлю для російського бізнесу.

Сполучені Штати, Європейський Союз та Сполучене Королівство запровадили обмеження на широкий спектр товарів, від ноутбуків та розкішних годинників до нафти, зрідженого природного газу та озброєння. Від понад сімдесяти російських банків було відключено доступ до системи SWIFT, що фактично паралізувало звичні канали міжнародних фінансових розрахунків. Утім, як свідчить розслідування, проведене журналістами SourceMaterial та Delfi у співпраці з OCCRP, ці обмеження породили нову тіньову індустрію, яка пропонує російським підприємцям шляхи обходу санкцій за допомогою багатошарових фінансових структур та посередників, що активно діють у месенджері Telegram.

Індустрія платіжних агентів, які спеціалізуються на обході санкцій, значною мірою розквітла саме завдяки зростанню кількості обмежувальних заходів проти росії. Як зазначає Еліз Томас із британського дослідницького центру Centre for Information Resilience, виникла справжня "кустарна індустрія сумнівних міжнародних платіжних провайдерів", які створюють кілька рівнів посередників між законними фінансовими установами та своїми справжніми клієнтами. Використовуючи фінансові структури, розосереджені по різних країнах, ці оператори ускладнюють правоохоронним органам можливість боротьби з такою діяльністю.

У ході розслідування журналісти провели серію дій під прикриттям, видаючи себе за російських бізнесменів, які шукали допомоги з міжнародними платежами. Вони обмінялися повідомленнями з вісьмома потенційними платіжними провайдерами, які рекламували свої послуги в Telegram – найпопулярнішій російській соціальній мережі та месенджері, що дозволяє користувачам спілкуватися анонімно. Переважна більшість цих організацій діяла під торговельними назвами, яких не вдалося знайти в російських чи інших корпоративних реєстрах, а деякі взагалі існували виключно у віртуальному просторі Telegram, не маючи жодних офіційних реєстраційних даних. Незважаючи на те, що журналісти не проводили фактичних платежів, у п'яти випадках агенти погодилися допомогти в операціях, які мали забезпечити доставку коштів до європейських компаній, приховуючи російське походження грошей. У цих розмовах репортери прямо зазначали, що санкції є перешкодою – або через те, що товари, які компанія нібито купувала в Європі, потрапили під чорні списки, або через те, що сама російська компанія перебувала під санкціями.

Один із таких агентів, який представився Дімою та діяв від імені CW Group, запевняв журналістів, що "не буде жодних слідів російської компанії, а платіж буде успішним". CW Group рекламувала широкий спектр розпливчастих фінансових послуг у Telegram, проте не мала жодного веб-сайту, і журналістам не вдалося знайти корпоративних документів, які б підтверджували, що це зареєстрований бізнес. Діма відверто визнав текучу природу своєї роботи: "Одна структура може існувати сьогодні, а інша – завтра", – пояснював він, додаючи, що банки та юрисдикції регулярно змінюють вимоги, тому важливо працювати з актуальними "чистими" компаніями, які обробляють транзакції без затримок. Його кінцева мета полягала в тому, щоб знайти "сучасні рішення, які працюють бездоганно і дозволяють завершити транзакцію без жодних зайвих питань від банків". Інший агент, Fin Platform, який наразі вже припинив своє існування, пропонував на своєму веб-сайті статтю про те, "як отримати оплату за товари, якщо клієнт не хоче мати справу з росією", а в Telegram-каналі розміщував рекламні оголошення, які обіцяли "реальні рішення", коли "санкції тасують карти".

Особливу тривогу викликають зв'язки, виявлені між цими платіжними посередниками та мережею TGR, яку Сполучене Королівство та Сполучені Штати звинувачують у створенні системи відмивання грошей, що допомагала російським елітам обходити санкційні

[11] https://www.occrp.org/en/investigation/there-will-be-no-trace-russias-sanctions-busting-middlemen-tout-services-on-telegram

обмеження. У грудні 2024 року американські органи влади запровадили санкції проти українця Джорджа Россі та росіянки Олени Чирикян, яких вважають лідерами TGR, за використання компаній мережі для надання "широкого спектру послуг з розміщення, структурування та інтеграції незаконних фінансових схем у глобальну фінансову систему". Санкційне повідомлення описувало TGR як "масштабну мережу ухилення від санкцій та відмивання грошей", яка підтримувала "контактні точки по всьому світу" для "маскування незаконної діяльності своїх клієнтів".

Корпоративні записи Литви та Канади виявили, що ключові фігури як у канадській компанії Grata Payments Ltd, яку Діма запропонував використовувати для отримання платежу через рахунок у литовській електронній грошовій установі TeslaPay, так і в самій TeslaPay були пов'язані з керівництвом TGR. Директором Grata Payments виявився естонський юрист Олексій Ратніков, який також значився директором One Remit – британської компанії, що здійснювала міжнародні грошові перекази для нині підсанкційної TGR Partners, згідно з архівною версією веб-сайту останньої. На час призначення Ратнікова директором One Remit, Олена Чирикян, яку вважають другою особою в ієрархії TGR, була власницею холдингової компанії фірми, зареєстрованої на Кіпрі. Сам Ратніков заперечував будь-яку обізнаність про CW Group або діяльність у Telegram, стверджуючи, що банківські реквізити від Діми не належать Grata, і що він став жертвою шахрайства, оскільки його призначили директором One Remit без його згоди. Однак офіційні записи компаній Сполученого Королівства свідчать, що він обіймав посаду директора протягом трьох років – з червня 2021 року до ліквідації компанії в травні 2024 року.

Не менш показовою є роль литовської компанії TeslaPay, заснованої в 2017 році. Російський бізнесмен Філіп Ларін значився в корпоративному документі як голова наглядової ради протягом чотирьох місяців 2018 року, а в онлайн-профілі описувався як співзасновник TeslaPay. Однак на цьому зв'язки не закінчуються: Ларін також є акціонером, головою ради директорів та одним із бенефіціарів іншого агентства з грошових переказів, зареєстрованого в Латвії Eastern European Payment System SIA, яке вказувало TGR Partners як свого клієнта на своєму веб-сайті. Згідно з даними розслідування, після санкцій проти TGR Partners, Eastern European Payment System виступала як частина фінансової інфраструктури мережі, управляючи платіжною картковою системою для групи. Ні Ларін, ні TeslaPay не відповіли на запити журналістів.

Окрему увагу в розслідуванні приділено використанню криптовалют, які стають все більш важливим інструментом для міжнародних транзакцій росії. Найбільш значущою подією стало створення рублевого стейблкоїну A7A5, запущеного на початку 2025 року компанією молдавсько-російського олігарха Ілана Шора, яка перебуває під санкціями Великої Британії та ЄС, разом із російським державним банком "Промсвязьбанк", що, за даними Національного агентства з боротьби зі злочинністю Великої Британії, "підтримував компанії, залучені до російського військово-промислового комплексу". Попри те, що цій криптовалюті ще немає й двох років, її веб-сайт стверджує, що вона використовується майже в 20% міжнародних транзакцій росії. До середини травня 2026 року A7A5 випустила понад 44 мільярди токенів вартістю понад 600 мільйонів доларів за поточним курсом. Хоча це лише частка від приблизно 185 мільярдів доларів, що зберігаються у провідному світовому стейблкоїні Tether, вплив A7A5 є непропорційно великим. За даними платформи аналітики блокчейну Chainalysis, ця віртуальна валюта слугує спеціалізованою фінансовою артерією для російської торгівлі та була використана в транзакціях на суму 93,3 мільярда доларів протягом десяти місяців, що еквівалентно приблизно половині річних військових витрат росії, за оцінками Міністерства закордонних справ Великої Британії.

Реакція Заходу не забарилася: Європейський Союз уже почав цілеспрямовано блокувати платформи, що торгують A7A5, і в квітні 2026 року запровадив санкції проти киргизької фірми, яка оперує платформою з великими обсягами торгівлі цією криптовалютою, а також заборонив транзакції з усіма російськими платформами, що торгують криптовалютою. Міністр закордонних справ Великої Британії Іветт Купер у травні 2026 року заявила: "Якщо

кремль вважає, що зможе обійти наші санкції, ховаючись за криптомережами та тіньовими фінансовими системами, він глибоко помиляється. Ми атакуємо інфраструктуру, яка підтримує його військову економіку, одночасно з тим, як Україна посилює тиск на росію на полі бою". Компанія A7 не відповіла на запити про коментар.

У контексті цього розслідування особливо показовою є розмова з Дімою щодо транзакції за участю китайського покупця, який, за задумом журналістів, мав придбати обладнання у фірми з банківськими рахунками в Європі, не підозрюючи, що насправді угода укладається з російською компанією. Хоча Китай не запроваджував санкцій проти росії, великі китайські банки все частіше обмежують операції з росією через побоювання вторинних санкцій з боку Заходу. Діма порадив своєму потенційному клієнту не сплачувати понад 200 тисяч доларів на день, "щоб не привертати зайвої уваги". Він запропонував використовувати кілька компаній-посередників, щоб забезпечити "відсутність видимого зв'язку з росією", і надав банківські реквізити для тестового платежу до канадської компанії Grata Payments Ltd, яка мала рахунок у литовській TeslaPay.

Висновки:

- **Цілісна тіньова індустрія обходу санкцій:** на базі Telegram діє розгалужена мережа платіжних агентів, які публічно рекламують послуги з приховування російського походження міжнародних транзакцій через багаторівневих посередників у різних юрисдикціях.
- **Прямі зв'язки з кримінальною інфраструктурою TGR:** запропоновані посередники (зокрема Grata Payments та TeslaPay) пов'язані з керівниками мережі TGR, яка перебуває під санкціями США та Великої Британії за відмивання грошей для російських еліт.
- **Криптовалюта A7A5 як системний інструмент:** створений за підтримки державного "Промсвязьбанку" рублевий стейблкоїн забезпечує майже 20% міжнародних розрахунків рф.
- **Динамічна еволюція схеми:** способи обходу санкцій змінюються щодня, випереджаючи адаптацію західних регуляторів, використовуючи комбінацію криптоактивів, підставних компаній у третіх країнах та традиційних переказів.

Як зазначає Еліз Томас, мережі на кшталт TGR є еволюційним кроком у світі незаконних фінансів. Вони поєднують новітні витончені методи відмивання грошей, зокрема використання криптовалют, із "класичними методами", такими як засновані на довірі схеми – неформальні системи переказу коштів, які залишаються популярними в багатьох куточках світу. Ці високодиверсифіковані операціїмстановлять значний виклик для правоохоронних органів та слідчих.

Розслідування демонструє, що, попри потужний санкційний тиск, російський бізнес продовжує знаходити способи підтримувати міжнародну торгівлю, використовуючи складні багатошарові структури, підставні компанії та новітні фінансові технології, що створює серйозні виклики для глобальної системи фінансового моніторингу та потребує постійного вдосконалення методів протидії з боку міжнародної спільноти.

Роль нотаріусів, адвокатів та бухгалтерів у легалізації злочинних доходів: досвід країн Західних Балкан [12]

Документ присвячений комплексному аналізу ролі професійних посередників у функціонуванні систем відмивання коштів у країнах Західних Балкан. Дослідження розглядає професійне відмивання коштів не як окремі випадки недбалості чи порушення законодавства, а як структурний елемент сучасної архітектури незаконних фінансових потоків, у якій ключову роль відіграють представники юридичних та фінансових професій.

У центрі уваги перебувають нотаріуси, адвокати, бухгалтери та аудитори, які завдяки своїм професійним повноваженням, доступу до фінансової та корпоративної інфраструктури, а також суспільній довірі можуть як запобігати легалізації злочинних доходів, так і сприяти їй. Автори наголошують, що саме ці професії знаходяться на критичному перетині між законною економічною діяльністю та кримінальними фінансовими потоками, а тому їхня поведінка значною мірою визначає ефективність національних систем ПВК/ФТ.

У документі зазначається, що країни Західних Балкан протягом останніх років суттєво наблизили своє законодавство до стандартів Європейського Союзу, FATF та MONEYVAL, однак реальна ефективність систем ПВК/ФТ залишається обмеженою через низку інституційних та практичних проблем. Дослідження демонструє, що основні ризики походять не від відсутності нормативної бази, а від слабкої реалізації існуючих вимог, недостатнього контролю за діяльністю визначених нефінансових установ та професій (ВНУП), фрагментованого нагляду, обмеженого обміну інформацією між державними органами та низького рівня виявлення підозрілих операцій. Важливим фактором ризику є також поширена практика надмірного трактування професійної таємниці, яка часто використовується як аргумент для уникнення виконання обов'язків щодо повідомлення про підозрілі операції. Автори підкреслюють, що в багатьох випадках професійна таємниця перетворюється на інструмент захисту сумнівних фінансових операцій та створює суттєві прогалини у системі фінансового моніторингу.

Значна увага приділяється концепції осіб, які професійно надають послуги з відмивання коштів, яку FATF визначає як осіб, групи або мережі, що спеціалізуються на наданні третім сторонам послуг з легалізації злочинних доходів за винагороду. На відміну від традиційного підходу до відмивання коштів, де злочинці самостійно намагаються приховати походження активів, особи, які професійно надають послуги з відмивання коштів виступають окремими сервісними провайдерами, які забезпечують повний спектр послуг з розміщення, розшарування та інтеграції незаконних коштів. Вони використовують складні корпоративні структури, офшорні компанії, номінальних власників, трасти, фіктивні контракти, транскордонні фінансові операції та інші механізми для створення багаторівневої системи приховування походження активів. Особливу небезпеку становить той факт, що такі посередники можуть одночасно обслуговувати різні злочинні мережі та працювати незалежно від конкретного предикатного злочину, перетворюючи відмивання коштів на окремий високоприбутковий вид діяльності.

Документ детально аналізує структуру професійних мереж відмивання коштів та функціональний розподіл ролей між їх учасниками. Відповідно до підходів FATF, у таких мережах можуть діяти організатори, які здійснюють стратегічне управління операціями, посередники, що залучають клієнтів, провайдери корпоративної інфраструктури, які створюють компанії та відкривають рахунки, менеджери, відповідальні за підготовку контрактів та іншої документації, номінальні особи, координатори логістичних операцій, інвестори в активи та особи, що здійснюють переміщення коштів між юрисдикціями. Такий

[12] https://globalinitiative.net/wp-content/uploads/2026/06/Anesa-Agovic%CC%81-Dozo-and-Dardan-Koc%CC%A7ani-Licence-to-launder-Professional-enablers-and-the-architecture-of-illicit-finance-in-the-western-Balkans-GI-TOC-June-2026.pdf

розподіл функцій дозволяє значно підвищити рівень захисту учасників схеми та ускладнює роботу правоохоронних органів щодо встановлення повного ланцюга легалізації коштів. Автори підкреслюють, що саме залучення професійних посередників забезпечує злочинним організаціям можливість використовувати законну фінансову та корпоративну інфраструктуру для приховування незаконного походження активів.

Найбільш детально дослідження зосереджується на ролі нотаріусів як однієї з найбільш ризикових категорій ВНУП. Нотаріуси займають особливе місце у фінансовій системі регіону, оскільки саме через них проходить значна частина операцій із нерухомістю, корпоративними правами та іншими активами, що підлягають офіційному посвідченню. У більшості країн Західних Балкан нотаріуси виступають обов'язковою ланкою при оформленні угод з нерухомістю, що фактично робить їх ключовими «гейткіперами» формальної економіки. Водночас дослідження демонструє, що реальна ефективність виконання нотаріусами функцій у сфері ПВК/ФТ залишається недостатньою. Незважаючи на законодавчі вимоги щодо проведення належної перевірки клієнтів, встановлення бенефіціарної власності та подання повідомлень про підозрілі операції, рівень повідомлень у багатьох країнах залишається непропорційно низьким порівняно з масштабами операцій, які проходять через нотаріальні процедури. Це особливо помітно у сфері нерухомості, яка визначається як один із головних каналів інтеграції злочинних доходів у легальну економіку.

У документі описано широкий спектр типологій відмивання коштів, у яких використовуються нотаріальні послуги. Серед найбільш поширених схем виділяються операції із завищенням або заниженням вартості нерухомості, використання фіктивних договорів позики, багаторазовий перепродаж майна між пов'язаними особами, оформлення активів на номінальних власників, використання офшорних компаній для фінансування придбання майна та легалізація незаконно збудованих об'єктів нерухомості. Значну увагу приділено також використанню нотаріально посвідчених документів для створення формально правдоподібного пояснення походження коштів. У таких випадках договори позики, корпоративні документи, інвестиційні угоди або інші юридичні інструменти використовуються для створення штучної легальної історії походження активів, яка ускладнює подальше розслідування та доведення злочинного характеру коштів.

Окремий розділ присвячений адвокатам, бухгалтерам та аудиторам. Автори зазначають, що адвокати часто залучаються до створення корпоративних структур, супроводження угод та підготовки правових механізмів, які дозволяють приховувати справжніх власників активів або створювати додаткові рівні юридичного дистанціювання між злочинцем та його майном. Бухгалтери, своєю чергою, відіграють ключову роль у формуванні фінансової документації, підготовці бухгалтерських записів та створенні фінансових пояснень походження коштів. Аудитори можуть використовуватися для надання додаткової легітимності корпоративним структурам та фінансовій звітності, навіть якщо реальна економічна діяльність компаній має ознаки фіктивності. Дослідження демонструє, що найбільш небезпечними є випадки, коли всі зазначені професійні категорії діють у координації, створюючи комплексну систему прикриття незаконних фінансових потоків.

Важливим висновком документа є те, що професійні посередники дедалі активніше використовують сучасні фінансові інструменти та транскордонні механізми для приховування активів. Автори відзначають зростання використання криптоактивів, офшорних структур, трастів, міжнародних корпоративних мереж та складних схем бенефіціарної власності. Попри законодавчі вимоги щодо ідентифікації кінцевих бенефіціарних власників, практичний доступ до достовірної інформації про структури власності часто залишається обмеженим. Це створює можливості для приховування контролю над активами та суттєво ускладнює роботу фінансових розвідок і правоохоронних органів. Додатковими факторами ризику залишаються високий рівень використання готівки, значні обсяги транскордонних операцій, фрагментованість державних реєстрів та недостатня інтеграція інформаційних систем між різними державними органами.

Загалом дослідження формує цілісну картину функціонування професійних посередників як одного з ключових елементів сучасної інфраструктури відмивання коштів у Західних Балканах. Автори доходять висновку, що ефективність систем ПВК/ФТ у регіоні обмежується не стільки законодавчими прогалинами, скільки недостатньою якістю нагляду, слабкою міжвідомчою координацією, низьким рівнем виявлення підозрілої діяльності та фактичною безкарністю окремих категорій професійних посередників. У результаті нотаріуси, адвокати, бухгалтери та аудитори, які повинні виступати важливими захисними бар'єрами проти легалізації злочинних доходів, у низці випадків перетворюються на ключових учасників або каталізаторів складних схем відмивання коштів.

Документ наголошує на необхідності переходу від формального виконання вимог ПВК/ФТ до реального ризик-орієнтованого нагляду, посилення відповідальності професійних посередників, покращення доступу до інформації про бенефіціарну власність та зміцнення спроможності фінансових розвідок і правоохоронних органів щодо виявлення та переслідування осіб, які професійно надають послуги з відмивання коштів.

Висновки:

- **Нотаріуси, адвокати, бухгалтери та аудитори є критично важливими вузлами у схемах відмивання коштів,** оскільки саме через них здійснюється юридичне оформлення, документування та легітимізація складних фінансових операцій.
- **Основною вразливістю регіону є не законодавство, а його практичне виконання:** нагляд на основі ризик-орієнтованого підходу за ВНУП залишається слабким, а дисциплінарні та правоохоронні заходи щодо професійних посередників застосовуються вкрай рідко.
- **Сектор нерухомості залишається головним каналом легалізації злочинних доходів,** зокрема через маніпулювання вартістю об'єктів, використання номінальних власників, фіктивних позик та багаторазових перепродажів активів.
- **Для підвищення ефективності систем ПВК/ФТ необхідно** посилити контроль за ВНУП, забезпечити якісний зворотний зв'язок між фінансовими розвідками та професійними спільнотами, удосконалити доступ до даних про бенефіціарну власність та розширити практику притягнення професійних посередників до відповідальності.

Протидія незаконній онлайн-торгівлі об'єктами дикої природи: новий міжнародний підхід до цифрового моніторингу [13]

Документ є практичним методичним посібником, спрямованим на формування єдиного підходу до виявлення, моніторингу та документування незаконної торгівлі об'єктами дикої природи в цифровому середовищі. Документ виходить із того, що незаконна торгівля дикими тваринами, рослинами та похідною продукцією дедалі активніше переміщується в онлайн-простір, використовуючи соціальні мережі, електронні торговельні майданчики, платформи оголошень, месенджери, спеціалізовані форуми та інші цифрові канали комунікації. Автори підкреслюють, що така діяльність становить не лише серйозну загрозу для біорізноманіття та збереження рідкісних видів, але й є складовою ширших транснаціональних злочинних ринків, які можуть бути пов'язані з організованою злочинністю, корупцією, незаконними фінансовими потоками та іншими формами екологічної злочинності.

Центральною ідеєю є необхідність переходу від фрагментарного та несистемного пошуку інформації в інтернеті до структурованого, стандартизованого та відтворюваного моніторингу

[13] https://globalinitiative.net/wp-content/uploads/2026/06/Combating-the-illegal-wildlife-trade-online-A-guide-for-cyber-units-NGOs-and-researchers-GI-TOC-June-2026.pdf

онлайн-торгівлі об’єктами дикої природи. Для цього пропонується універсальна рамкова модель, яка охоплює весь життєвий цикл аналітичної діяльності: від постановки цілей і визначення сфери моніторингу до збору, перевірки, аналізу, передачі та використання отриманих даних. Автори наголошують, що будь-яка діяльність із моніторингу повинна розпочинатися з чіткого визначення кінцевої мети. Такою метою може бути формування оперативних матеріалів для правоохоронних органів, картування злочинних ринків, виявлення нових тенденцій, оцінка впливу правоохоронних заходів на поведінку торговців, підтримка природоохоронної політики або документування зловживань цифровими платформами. Саме поставлена мета повинна визначати географічне охоплення дослідження, перелік платформ для спостереження, категорії видів чи продукції, які потребують особливої уваги, а також набір даних, що підлягають збору та аналізу.

Документ детально розглядає процес визначення пріоритетних видів та продуктів для моніторингу. Оскільки ресурси більшості організацій є обмеженими, автори рекомендують використовувати ризик-орієнтований підхід до пріоритетизації. Для цього запропоновано багатофакторну систему оцінювання, яка враховує рівень міжнародного та національного правового захисту виду, його природоохоронний статус, включення до додатків Конвенції про міжнародну торгівлю видами дикої фауни і флори, що перебувають під загрозою зникнення (CITES), ступінь загрози з боку незаконної торгівлі, правоохоронну значущість, наявність зв’язків із організованою злочинністю, а також можливість достовірної ідентифікації об’єкта за інформацією, що міститься в онлайн-оголошеннях. Окремо наголошується, що не всі види можуть бути однаково ефективно виявлені в цифровому середовищі, тому під час планування моніторингу необхідно враховувати рівень складності їхньої ідентифікації, наявність видів-двійників та особливості реалізації продукції у переробленому вигляді.

Важливу увагу приділено вибору цифрових платформ для спостереження. Автори рекомендують формувати первинний перелік платформ на основі аналізу наукових досліджень, звітів, інформації про вилучення незаконної продукції та попередніх правоохоронних розслідувань. До сфери моніторингу можуть входити популярні соціальні мережі, електронні торговельні майданчики, сайти оголошень, форуми колекціонерів, бізнес-платформи, месенджери, а за наявності законних підстав – також окремі закриті ресурси та сегменти даркнету. Водночас документ наголошує, що ефективна система моніторингу повинна залишатися гнучкою, оскільки торговці постійно змінюють використовувані платформи, канали комунікації та методи приховування своєї діяльності. Саме тому після початкового етапу рекомендується проводити регулярний аналіз нових платформ, каналів та моделей поведінки учасників незаконного ринку.

Одним із ключових елементів посібника є впровадження стандартизованої моделі даних Global Data Model, яка покликана забезпечити сумісність та порівнюваність інформації між різними проєктами, організаціями та країнами. Документ пропонує єдині підходи до фіксації інформації про види, типи продукції, кількість товару, ціни, географічне походження, маршрути переміщення, продавців, покупців, контактні дані, правовий статус продукції та рівень ризику. Для забезпечення якості та подальшої аналітичної обробки рекомендується використовувати стандартизовані назви видів, міжнародні формати дати і часу, уніфіковані географічні коди, а також єдині правила присвоєння ідентифікаторів записам. Автори підкреслюють, що саме стандартизація даних створює передумови для побудови міжнародних систем обміну інформацією та інтеграції результатів різних проєктів у єдині аналітичні платформи.

Окремий великий розділ присвячений організації збору даних та побудові систем управління інформацією. Документ рекомендує використовувати структуровані бази даних або електронні таблиці з контрольованими полями введення, що мінімізують кількість помилок та забезпечують можливість автоматизованого аналізу. Значна увага приділяється веденню журналів аудиту, фіксації джерел інформації, способів її отримання, часу збору та осіб, відповідальних за внесення і перевірку даних. Автори наголошують на необхідності забезпечення належного рівня кібербезпеки, контролю доступу до інформації, резервного

копіювання та захисту чутливих даних. Такий підхід розглядається як необхідна умова для подальшого використання результатів моніторингу в аналітичній роботі або правоохоронній діяльності.

Документ детально описує методики ручного моніторингу, які розглядаються як базовий елемент усієї системи. Рекомендується використовувати структуровані процедури пошуку, працювати з локальними мовами та діалектами, систематично оновлювати словники ключових слів, жаргонних виразів, евфемізмів та кодових позначень, які використовують торговці. Значна увага приділяється роботі з різними типами платформ, оскільки поведінка користувачів та механізми приховування діяльності суттєво відрізняються між соціальними мережами, маркетплейсами, форумами та месенджерами. Особливо важливим визнається забезпечення однакових стандартів документування інформації шляхом збереження скриншотів, посилань, текстів оголошень та інших метаданих, що дозволяють підтвердити походження та зміст виявленої інформації.

Для підвищення ефективності моніторингу автори рекомендують поступово впроваджувати автоматизовані інструменти, включаючи системи сповіщень, автоматизований збір даних з вебресурсів, API платформ, засоби машинного навчання та алгоритми штучного інтелекту. Документ містить ґрунтовний аналіз можливостей і обмежень таких технологій. Зокрема, штучний інтелект може використовуватися для попереднього відбору підозрілих оголошень, автоматичного аналізу текстів і зображень, класифікації видів або формування ризик профілів. Водночас наголошується, що жоден алгоритм не здатний повністю замінити людський аналіз, оскільки оцінка законності торгівлі, достовірності інформації та контексту завжди потребує експертного судження. Документ також звертає увагу на ризики помилкових спрацювань, зміну поведінки злочинців, деградацію моделей штучного інтелекту та технічні обмеження платформ, які можуть впливати на якість автоматизованого моніторингу.

Значне місце в посібнику займає використання методів розвідки з відкритих джерел (OSINT). Автори розглядають OSINT як системний процес збору та аналізу інформації з відкритих джерел, який передбачає використання пошукових операторів, аналіз цифрових слідів, дослідження зв’язків між акаунтами, зворотний пошук зображень, роботу з електронними адресами, телефонами та іншими цифровими

Висновки:

- **Ефективна протидія незаконній онлайн-торгівлі дикою природою потребує переходу від епізодичного пошуку інформації до системного моніторингу,** заснованого на ризик-орієнтованому підході та визначенні пріоритетів найбільш загрозливих видів.
- **Визначення пріоритетних видів та продуктів має здійснюватися на основі ризик-орієнтованого підходу з урахуванням їхнього статусу** відповідно до CITES та Червоного списку Міжнародного союзу охорони природи (IUCN), правоохоронних пріоритетів, можливих зв’язків з організованою злочинністю, а також можливості достовірної ідентифікації відповідних об’єктів в онлайн-середовищі.
- **Автоматизація, штучний інтелект та OSINT повинні використовуватися як інструменти підсилення аналітичних можливостей, але не можуть замінити експертну оцінку аналітиків,** особливо при визначенні законності операцій та формуванні матеріалів для правоохоронних органів.
- **Найбільшу практичну цінність мають системи моніторингу, інтегровані з правоохоронними, митними та аналітичними структурами,** які забезпечують перетворення онлайн-спостережень у розслідування, вилучення незаконної продукції та виявлення злочинних мереж.

ідентифікаторами. При цьому підкреслюється необхідність дотримання вимог законодавства, етичних принципів та правил цифрової безпеки. Документ наголошує, що відкрита розвідка повинна бути документованою, методологічно обґрунтованою та здійснюватися виключно в межах правового поля.

Окремий акцент зроблено на перетворенні результатів моніторингу на практичні правоохоронні та регуляторні заходи. Автори зазначають, що онлайн-моніторинг не має самостійної цінності, якщо його результати не використовуються для розслідувань, вилучення незаконної продукції, притягнення винних до відповідальності або вдосконалення політики. Для цього рекомендується розвивати партнерські відносини між природоохоронними органами, кіберпідрозділами, митними службами, правоохоронними органами, неурядовими організаціями та цифровими платформами. Особливе значення надається формуванню якісних аналітичних продуктів, які містять структуровані висновки, оцінку ризиків та практичні рекомендації замість передачі великих масивів необроблених даних.

У завершальній частині документа розглядаються питання законності обробки даних, захисту приватності та майбутніх тенденцій розвитку незаконної торгівлі дикою природою. Автори наголошують на необхідності дотримання принципів мінімізації даних, обмеження мети їх використання, захисту персональної інформації та впровадження механізмів анонімізації й псевдонімізації. Водночас прогнозується подальше ускладнення цифрового середовища через розвиток штучного інтелекту, появу нових платформ, поширення зашифрованих каналів зв'язку та дедалі тісніше переплетення незаконної торгівлі дикою природою з іншими формами транснаціональної організованої злочинності, включаючи відмивання коштів, корупцію та незаконні фінансові потоки. У зв'язку з цим автори доходять висновку, що майбутні системи моніторингу повинні бути модульними, технологічно гнучкими та здатними інтегрувати інформацію з різних сфер кримінальної діяльності для формування комплексної картини ризиків.

Інші новини

Санкційний транзит: як європейське обладнання живить російський ВПК [14]

На основі розслідування OCCRP, можна зробити детальний аналіз ситуації, що свідчить про серйозні прогалини в системі міжнародних санкцій та їхнього правозастосування.

Центральна тема розслідування – діяльність турецької компанії Redwing Metal Uluslararasi Ticaret Anonim Sirketi, яка, попри публічні заперечення свого європейського співвласника, постачала до росії критично важливе обладнання європейського виробництва, що підпадає під санкційні обмеження. Це обладнання, вартістю понад 5 мільйонів доларів, було передане двом російським металургійним підприємствам, які безпосередньо пов'язані з оборонно-промисловим комплексом країни-агресора.

Згідно з митними та торговельними даними, отриманими журналістами Kyiv Independent та IrpiMedia, кінцевими отримувачами забороненого в ЄС устаткування стали компанії Aluminum Metallurg Rus (AMR) та Stupino Metallurgical Company (SMK). Ці підприємства спеціалізуються на виробництві спеціалізованих металевих сплавів, які використовуються для створення бойових літаків та крилатих ракет. Таким чином, постачання обладнання до цих заводів є прямим сприянням військовому потенціалу росії, що використовується проти України.

Ключовою фігурою в цій історії виступає Олександр Теттерсолл, громадянин Нідерландів, який проживає у Швейцарії та володіє 40-відсотковою часткою в турецькій компанії Redwing Metal. Решта акцій належить турецькому юристу Вейселю Дженгізу Сойлемезоглу. У своїй

[14] https://www.occrp.org/en/scoop/eu-citizens-company-funneled-sanctioned-equipment-to-russian-defense-firms

письмовій відповіді на запитання журналістів Теттерсолл намагався дистанціюватися від діяльності компанії, заявивши, що він є лише позаштатним консультантом і має обмежені знання про її операції. Він категорично заперечив будь-яку причетність Redwing Metal до схем постачання санкційних товарів до росії. Однак ці твердження суперечать фактичним даним, адже Теттерсолл є не лише співвласником, але й єдиною контактною особою, зазначеною на вебсайті компанії, що свідчить про його безпосередню залученість до управління бізнесом. Прикметно, що він також обіймає посади генерального директора у трьох компаніях AMR у Швейцарії, США та Німеччині, які займаються експортом алюмінієвих сплавів з росії до Європи та Америки. Хоча ця діяльність сама по собі не є порушенням санкцій, вона демонструє глибокий зв'язок Теттерсолла з російською металургійною промисловістю, що викликає додаткові запитання щодо його ролі в організації незаконних поставок.

Розслідування виявляє типову схему обходу санкцій, яка активно використовується для поставок критичних технологій. Оскільки прямі закупівлі в ЄС для росії заборонені, компанії-посередники в країнах, які не приєдналися до санкційного режиму, наприклад, у Туреччині, Киргизстані, Узбекистані чи Гонконзі, безперешкодно купують європейське обладнання, а потім реекспортують його до росії. У випадку з Redwing Metal мова йде про високотехнологічне італійське обладнання, зокрема, верстати з числовим програмним керуванням (CNC), виробництва компанії M.C.M. MADAR COSTRUZIONI MECCANICHE S.P.A. (MCM). Ці верстати, призначені для обробки металу, були доставлені на завод SMK наприкінці 2023 року. Сама італійська компанія MCM підтвердила факт продажу своєї продукції Redwing Metal, але зазначила, що в угоді був пункт, який прямо забороняв реекспорт до країн або суб'єктів, що перебувають під санкціями. Водночас представники MCM заявили, що не знали про подальше перенаправлення обладнання до росії, що, на жаль, є типовою ситуацією, коли європейські виробники стають мимовільними учасниками схем обходу санкцій через недобросовісних посередників.

Окрім верстатів з ЧПК, до переліку поставленого обладнання входили промислова піч для термічної обробки металу, гідравлічний прес та інші компоненти, що разом формують сучасну виробничу лінію в металургії. Експерти, залучені до аналізу, наголошують, що це не випадковий набір звичайних промислових товарів, а цілеспрямований набір критичних потужностей, необхідних для підтримки оборонно-промислової бази росії. Деякі з цих товарів були заборонені до експорту ще в першій половині 2022 року, що свідчить про те, що їхню важливість для російської військової машини було визначено на самому початку повномасштабного вторгнення. Експерти наголошують, що така діяльність несе серйозні юридичні ризики для громадянина ЄС Теттерсолла. Якщо буде доведено, що він свідомо сприяв обходу експортних обмежень через посередника в третій країні, йому можуть загрожувати як значні фінансові штрафи, так і кримінальна відповідальність за законодавством країни його громадянства, тобто Нідерландів. Хоча наголошується, що такі справи досі рідко доходять до суду, юридичний ризик для нього є беззаперечним.

Окремим і важливим аспектом є діяльність отримувачів обладнання – компаній AMR та SMK. Вони належать Миколі Тімохіну, який є зятем Ігоря Зав'ялова, заступника голови російського державного оборонного конгломерату «Ростех». Цей факт безпосередньо пов'язує заводи з вищим керівництвом російської оборонної промисловості, яке саме перебуває під міжнародними санкціями. Аналіз даних показує, що між 2022 та 2025 роками AMR та SMK продавали металеві компоненти понад 40 російським оборонним компаніям, включаючи виробників танків, артилерії, винищувачів, крилатих та балістичних ракет. Це робить їх ключовими елементами в ланцюгу постачання для російського ВПК. Крім того, AMR мала ліцензію від ФСБ росії на проведення робіт з використанням державної таємниці, що свідчить про особливий статус підприємства та його допуск до надсекретної інформації в інтересах оборони країни.

Цікавим доповненням до основної схеми є інші поставки, здійснені Redwing Metal. Згідно з даними, компанія також відправила товарів на суму 1,3 мільйона доларів для компанії SMK-Снаб (яка згодом змінила назву на «Системи металургійного постачання»). Це було

суднобудівне обладнання європейського виробництва: якорі, швартові лебідки, вентилятори системи вентиляції, системи очищення стічних вод та інші компоненти. Це обладнання призначалося для встановлення на двох суднах, які будувалися в межах програм російського військово-морського флоту. Одне з цих суден, «Михайло Калашников», було завершене в середині 2025 року, менше ніж через рік після останніх поставок. Це розширює масштаби порушень, показуючи, що компанія не лише постачала обладнання для сухопутної військової техніки, а й сприяла розвитку військово-морських сил росії. Німецька компанія Wolter GmbH, яка виготовила вентилятори, у своїй відповіді зазначила, що їм важко визначити, хто саме міг продати ці товари турецькій компанії, оскільки вони могли бути придбані через різноманітні канали, зокрема через трейдерів.

Таким чином, це розслідування є яскравим прикладом того, як навіть найжорсткіші санкції можуть бути неефективними через існування посередників у «дружніх» або нейтральних країнах. Воно демонструє складність відстеження кінцевого призначення високотехнологічних товарів і відповідальність, яку несуть європейські виробники та громадяни, навіть якщо вони формально не порушують закон, але створюють можливості для його обходу. Історія з Redwing Metal та AMR/SMK показує глибоке проникнення російських оборонних інтересів у міжнародні бізнес-ланцюги та потребу в посиленні контролю за реекспортом, щоб запобігти використанню таких прогалин на шкоду безпеці України та всієї Європи.

Для загального розвитку

Азія як новий центр глобального капіталу: тенденції, ризики та регуляторні пріоритети [15]

Звіт OECP є масштабним аналітичним дослідженням розвитку ринків капіталу Азії та їхньої ролі у фінансуванні економічного зростання, інновацій та структурної трансформації регіону в умовах посилення глобальної невизначеності. Документ демонструє, що азійські ринки капіталу набули стратегічного значення не лише для регіональної економіки, а й для світової фінансової системи загалом. На країни Азії припадає близько третини світового ВВП, понад половина усіх публічних компаній світу та значна частка глобальної венчурної активності. Водночас розвиток окремих сегментів фінансових ринків залишається нерівномірним, а регіон продовжує стикатися з низкою структурних викликів, які стримують його подальшу фінансову інтеграцію та конкурентоспроможність.

Однією з ключових тем звіту є вплив торговельної політики та геополітичної напруженості на функціонування ринків капіталу. OECP зазначає, що протягом 2025 року та першої половини 2026 року фінансові ринки Азії перебували під впливом двох взаємопов'язаних факторів – загострення тарифної невизначеності у світовій торгівлі та ескалації конфлікту на Близькому Сході. Через високу інтегрованість азійських економік у міжнародні виробничі ланцюги, їхню залежність від глобальної торгівлі та критичну роль енергетичних поставок із Близького Сходу будь-які зміни у міжнародному середовищі безпосередньо впливають на інвестиційну активність, вартість капіталу та фінансову стабільність регіону. Особливої уваги приділено залежності азійських економік від ринку США, який залишається одним із ключових напрямів експорту для більшості країн регіону. Водночас вплив торговельних ризиків є нерівномірним: окремі держави Південно-Східної Азії демонструють значно вищу залежність від американського ринку порівняно з великими та більш диверсифікованими економіками, такими як Китай або Індонезія.

У звіті детально аналізується реакція фінансових ринків на зростання невизначеності. Після оголошення нових тарифних заходів та загострення геополітичної ситуації спостерігалося

[15] https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/asia-capital-markets-report-2026_c2b3e716/08f87bed-en.pdf

різке зростання волатильності фондових ринків, розширення кредитних спредів, підвищення нестабільності на ринках державного боргу та зміна напрямків міжнародних потоків капіталу. Інвестори дедалі частіше переорієнтовувалися з акцій на боргові інструменти, що забезпечували більш прогнозовану дохідність у нестабільному середовищі. Незважаючи на складні умови, азійські ринки капіталу зберегли здатність забезпечувати фінансування економіки. У 2025 році через публічні ринки регіону було залучено близько 3,3 трлн доларів США, що становило майже 40% світового обсягу залученого капіталу. Разом із тим темпи зростання фінансування виявилися нижчими, ніж у багатьох інших регіонах світу, а структура залучення коштів зазнала суттєвих змін. Активність первинних публічних розміщень акцій залишалася пригніченою, тоді як компанії дедалі частіше використовували додаткові випуски акцій та корпоративні облігації для залучення фінансування.

Окремий блок дослідження присвячено борговим ринкам. OECP підкреслює, що ринки державного боргу Азії продемонстрували високий рівень стійкості завдяки переважному використанню фінансування у національній валюті, значній частці облігацій із фіксованою ставкою та відносно довгим строкам погашення. Сукупний обсяг випуску державних облігацій досяг рекордних значень, а загальний обсяг непогашеного державного боргу продовжив зростати. Водночас підвищення геополітичних ризиків та інфляційного тиску створює потенційні ризики для майбутнього рефінансування як державного, так і корпоративного боргу. Особливе занепокоєння викликає той факт, що значна частина корпоративних облігацій підлягає погашенню протягом найближчих кількох років, що робить компанії вразливими до можливого зростання відсоткових ставок або погіршення умов доступу до капіталу.

Важливе місце у звіті займає аналіз проблеми систематично низької ринкової оцінки азійських компаній. Попри високі темпи економічного зростання та появу численних глобально конкурентоспроможних корпорацій, значна частина компаній регіону продовжує торгуватися нижче своєї балансової вартості. Автори пояснюють це поєднанням структурних чинників, серед яких домінування концентрованих моделей власності, недостатній рівень захисту міноритарних акціонерів, обмежена роль інституційних інвесторів, консервативна політика розподілу прибутку та недосконалі механізми корпоративного управління.

У відповідь на поширене явище недооцінки публічних компаній низка азійських юрисдикцій реалізує програми підвищення корпоративної вартості («value-up» initiatives), метою яких є посилення ефективності розподілу капіталу, зростання акціонерної вартості, удосконалення механізмів корпоративного управління та підвищення довіри інвесторів через покращення прозорості та якості розкриття інформації. OECP зазначає, що перші результати таких програм є неоднозначними: в окремих юрисдикціях вони сприяли підвищенню ринкової активності та інтересу інвесторів, однак не завжди призводили до довгострокового зростання оцінки компаній.

Значна увага приділяється інституційним інвесторам та їхній ролі у розвитку ринків капіталу. У порівнянні з розвиненими фінансовими центрами світу роль інституційних інвесторів в Азії залишається відносно обмеженою. Частка інституційної власності на фондових ринках регіону майже вдвічі нижча за середньосвітовий рівень. При цьому суттєву роль відіграють саме іноземні інституційні інвестори, тоді як внутрішні пенсійні фонди, страхові компанії та інвестиційні фонди в багатьох країнах ще не досягли необхідного масштабу розвитку.

Водночас спостерігається швидке зростання пасивного інвестування та впливу глобальних індексів на розподіл інвестиційних потоків. Документ приділяє значну увагу розвитку практик відповідального здійснення прав акціонерів, механізмів корпоративного діалогу між інвесторами та компаніями, використанню інструментів акціонерного контролю через голосування, а також інтеграції екологічних, соціальних та управлінських чинників (ESG) у процеси оцінки ризиків і прийняття інвестиційних рішень.

Окремий розділ присвячений людському капіталу як новому фактору формування корпоративної вартості. OECP наголошує, що сучасні інвестори дедалі частіше оцінюють не лише фінансові показники компаній, а й якість управління персоналом, рівень професійної

підготовки працівників, умови праці, гендерну різноманітність, показники плинності кадрів та безпеки праці. Аналіз показує, що компанії з більш ефективними практиками управління людським капіталом часто демонструють кращі фінансові результати та вищу рентабельність. Водночас відсутність єдиних міжнародних стандартів розкриття інформації про людський капітал ускладнює порівняння компаній між собою та обмежує можливості інвесторів для об'єктивної оцінки ризиків. Особливої актуальності ця тема набуває в умовах поширення штучного інтелекту та автоматизації, які можуть суттєво змінити структуру ринку праці та вимоги до навичок працівників.

Завершальна частина звіту присвячена розвитку ринку криптоактивів. ОЕСР відзначає, що Азія стала одним із світових центрів криптовалютної активності та демонструє найвищі темпи зростання обсягів транзакцій із використанням блокчейн-технологій. Паралельно зростає участь як роздрібних, так і інституційних інвесторів у цьому сегменті фінансового ринку. Водночас розвиток криптоекономіки супроводжується посиленням ризиків для фінансової стабільності, захисту споживачів та ринкової доброчесності. Особливу увагу приділено проблемам шахрайства, кіберзлочинності, втратам від хакерських атак, використанню криптоактивів для незаконного фінансування, відмивання коштів та інших форм фінансових злочинів. У документі наголошується на необхідності формування узгоджених міжнародних підходів до регулювання криптоактивів, розвитку наглядових механізмів, посилення контролю за постачальниками послуг у сфері криптоактивів та розширення міжнародної співпраці між регуляторами.

Загалом звіт демонструє, що азійські ринки капіталу вступають у новий етап розвитку, де ключового значення набувають не лише обсяги залучення фінансування, а й якість корпоративного управління, ефективність використання капіталу, роль інституційних інвесторів, стійкість до геополітичних ризиків, розвиток людського капіталу та здатність фінансової системи адаптуватися до цифрової трансформації.

Документ підкреслює, що подальше зміцнення фінансової стійкості регіону потребуватиме поглиблення ринків капіталу, диверсифікації джерел фінансування, розширення внутрішньої бази інвесторів, вдосконалення корпоративного управління та формування ефективного регуляторного середовища для нових фінансових технологій.

Ваша думка важлива!

1. Як Україна може адаптувати оновлену Рекомендацію 6 FATF до власних реалій, щоб забезпечити безперебійне надходження гуманітарної допомоги та критичних товарів, водночас не створюючи прогалин у фінансовому моніторингу?
2. Які законодавчі, інституційні та наглядові зміни необхідно впровадити в Україні для забезпечення ефективного застосування ризик-орієнтованого підходу щодо ВНУП і запобігання використанню нотаріальних, юридичних та бухгалтерських послуг у схемах легалізації злочинних доходів?
3. Які інструменти можуть бути запроваджені в Україні для виявлення номінальних власників та прихованого контролю над компаніями, якщо формально інформація про КБВ уже внесена до реєстру?
4. Як Україна може вплинути на країни-посередники (Туреччину, Киргизстан, Узбекистан тощо), щоб вони приєдналися до санкційної політики ЄС або посилили контроль за реекспортом, враховуючи, що ці поставки безпосередньо призводять до загибелі мирних громадян?

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-2026-26

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].